

Aruba Instant 6.5.1.0-4.3.1.0 Command-Line Interface



Reference Guide

Copyright Information

© Copyright 2016 Hewlett Packard Enterprise Development LP.

Open Source Code

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

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

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

The following informational icons are used throughout this guide:



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

Table 2: *Support Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	licensing.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

What is New in This Release

This section lists the new and modified commands in Instant 6.5.1.0-4.3.1.0.

New Commands

The following commands are introduced in this release:

Table 3: *New Commands*

Command	Description
<code>clarity</code>	This command enables inline monitoring statistics for important IAP events such as Authentication, DHCP, DNS, and STA.
<code>cluster-security</code>	This command enables cluster security in dtls mode and provides secure communication for control plane messages exchanged between the IAPs in the cluster.
<code>cluster-security logging</code>	This command allows you to set per module logging levels and retrieve the debugging logs on a one-time basis.
<code>show ap client-match-ssid-table</code>	This command displays the SSID table list over the radios of the current IAP and all other neighboring IAPs.
<code>show log papi-handler</code>	This command displays the cluster security debugging logs.
<code>show cluster-security</code>	This command displays cluster security configuration details for all the IAPs in the cluster.
<code>show clarity config</code>	This command displays the status of the clarity configuration parameters on the IAP.
<code>show clarity history</code>	This command displays the history of the clarity configuration parameters.

Modified Commands

The following command is modified in this release:

Table 4: *Modified Commands*

Command	Description
<code>wlan auth-server</code>	A new parameter called RFC5997 is added to determine the availability of the Accounting or Authentication server.

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

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

```
(Instant AP) #
```

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

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

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

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

The 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 (VC) 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, Aruba recommends that you configure fewer changes at a time and apply the changes at regular intervals.

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

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

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

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

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

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

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

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

Example:

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

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

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

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

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

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


Using Sequence Sensitive Commands

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

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

Table 5: *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command
<code>opendns <username <password></code>	<code>no opendns</code>
<code>rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit deny src-nat dst-nat {<IP-address> <port> <port>}} [<option1...option9>]</code>	<code>no rule <dest> <:mask> <match> <protocol> <start-port> <end-port> {permit deny src-nat dst-nat {<IP-address> <port> <port>}} [<option1...option9>]</code>
<code>mgmt-auth-server <auth-profile-name></code>	<code>no mgmt-auth-server <auth-profile-name></code>
<code>set-role <attribute>{{equals not-equals starts-with ends-with contains} <operator> <role> value-of}</code>	<code>no set-role <attribute>{{equals not-equals starts-with ends-with contains} <operator> value-of}</code> <code>no set-role</code>
<code>set-vlan <attribute>{{equals not-equals starts-with ends-with contains} <operator> <VLAN-ID> value-of}</code>	<code>no set-vlan <attribute>{{equals not-equals starts-with ends-with contains} <operator> value-of}</code> <code>no set-vlan</code>
<code>auth-server <name></code>	<code>no auth-server <name></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 AP) # show running-config
```

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

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

Commands that Reset the 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 6: *Line Editing Keys*

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

Specifying Addresses and Identifiers in Commands

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

Table 7: *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).
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 IAP. A unique BSSID applies to each frequency— 802.11a and 802.11g—used from the AP. Use the same format as for a MAC address.
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.

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 IAP regulatory domain.
<tx-power>	Configures the specified transmission power values.	0-127 dBm 127dBm is the maximum possible power that you can set for a radio. Although the IAP allows you to set the transmission power to the 127dBm, power is allocated based on the limits set by the radio hardware and country code in which the IAP operates. The country code and the IAP hardware may support significantly lower transmission power values than 127dBm and in such cases, the transmission power limit set by the country code and the IAP hardware takes precedence.

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 AP)# 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: • Dipole/Omni • Panel • Sector	Dipole/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 IAP device supports external antenna connectors, see the *Install Guide* that is shipped along with the IAP device.

EIRP and Antenna Gain

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

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

The following table describes this formula:

Table 8: 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.

Example

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

(Instant AP) # 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

aaa test-server

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

Description

This command tests a configured authentication server.

Syntax

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

Usage Guidelines

This command verifies the status of RADIUS authentication between the IAP and RADIUS/AAA 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

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 AP) (config)# aeroscout-rtls 192.0.2.2 3030 include-unassoc-sta  
(Instant AP) (config)# end  
(Instant AP)# 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 [dlna-only| mdns-only]
  enable-guest-multicast
  multi-swarm
  no...
no aigroup
```

Description

This command configures the AirGroup settings on an IAP.

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® or DLNA 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 [dlna-only mdns-only]	Enables the mDNS or DLNA or both. When dlna-only command is executed with enable , the DLNA support is enabled for AirGroup enabled devices. When mdns-only command is executed with enable , the Bonjour support is enabled for AirGroup enabled devices.	—	—
enable-guest-multicast	Allows the users to use the Bonjour or DLNA services enabled in a guest	—	—

Parameter	Description	Range	Default
	VLAN. When enabled, the Bonjour or DLNA devices will be visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN.		
multi-swarm	Enables inter cluster mobility. When enabled, the IAP shares the mDNS database information with the other clusters. The AirGroup records in the VC can be shared with all the VCs specified for L3 Mobility.	—	Disabled
no...	Removes the configuration settings for parameters under the airgroup command.	—	—
no airtgroup	Removes the AirGroup configuration.	—	—

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

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 configuration sub-mode.

airgroupservice

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

Description

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

Syntax

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

Parameter	Description	Default
	You can allow all services or add custom services. Up to 10 services can be configured on an IAP.	
description <description>	Adds a description to the AirGroup service profile.	—
disable	Disables AirGroup services for the profile.	—
disallow-role <role>	Restricts the user roles specified for role from accessing the AirGroup service.	Disabled
disallow-vlan <VLAN-ID>	Restricts the AirGroup servers connected on the specified VLANs from being discovered.	Disabled
enable	Enables the AirGroup service for the profile.	—
id <airgroupserviceid>	Allows you to specify the AirGroup service ID corresponding to the service that you are trying to configure. NOTE: The service IDs cannot be added for the pre-configured services.	—
no...	Removes the AirGroup service configuration.	—

Usage Guidelines

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

Example

The following example configures AirGroup services:

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

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is modified.
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 AP) (config) # airwave-rtls ams-ip 192.0.2.3 3030 pass@1234 5 include-unassoc-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 VC 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 AP) (config) # ale-report-interval 60
```

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

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
<code>ale-server <server></code>	Allows you to specify the Fully Qualified Domain Name (FQDN) or IP address of the ALE server.
<code>no...</code>	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 AP) (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
  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
vocera-disable	Disables the VOCERA protocol.	Enabled
no...	Removes the specified configuration parameter.	—

Usage Guidelines

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

Example

The following example configures the ALG protocols:

```
(Instant AP) (config) # alg
(Instant AP) (ALG) # sccp-disable
(Instant AP) (ALG) # no sip-disable
(Instant AP) (ALG) # no vocera-disable
(Instant AP) (ALG) # end
(Instant AP) # 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. When this command is enabled, only the licensed slave IAPs can join the cluster.

Example

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

```
(Instant AP) (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 IAP 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 AP) (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

a-max-clients

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

Description

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

Syntax

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

Usage Guidelines

Use this command to set the maximum number of clients allowed to connect to 5 GHz radio channels for a specific SSID profile.

Example

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

```
(Instant AP)# a-max-clients ssid4 35
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	The ssid_profile parameter is added.
Aruba Instant 6.4.4.4-4.2.3.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All Platforms	Privileged EXEC mode

ams-backup-ip

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

Description

This command adds the IP address or domain name of the backup 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 VC switches to the backup server automatically.

Example

The following command configures an AirWave backup server.

```
(Instant AP) (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 Groups 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 AP) (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 AirWave Management Server.

```
(Instant AP) (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 VC 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 IAP in the IAP network.

Example

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

```
(Instant AP) (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

ap1x

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

Description

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

Syntax

Parameter	Description
peap	Configures PEAP based 802.1X authentication type.
tls	Configures TLS based 802.1X authentication type.
tpm	Configures a factory-installed TPM (Trusted Platform Module) certificate for IAP authentication.
validate-server	Validates the authentication server credentials against the CA certificate in the IAP database.
no...	Removes the configuration.

Usage Guidelines

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

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

ap-frequent-scan

ap-frequent-scan <band>

Description

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

Syntax

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

Usage Guidelines

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

The following checks must be performed before scanning:

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

Example

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

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

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

ap-installation

ap-installation default|indoor|outdoor

Description

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

Syntax

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

Usage Guidelines

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

Example

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

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

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

ap1x-peap-user

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

Description

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

Syntax

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

Usage Guidelines

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

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

apply

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

Description

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

Syntax

Parameter	Description
<code>cplogo-install</code>	Installs the captive portal logo on the IAP.
<code>cplogo-uninstall</code>	Uninstalls the captive portal logo on the IAP.
<code>debug-command</code>	Applies the configuration settings from the debug command .
<code>delta-config</code>	Applies the configuration settings from the delta-config command.

Usage Guidelines

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

Example

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

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

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

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

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC 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 [bad-snr <snr> | [calc-interval <interval>| calc-threshold <thresh>| client-
thresh <thresh> | debug <level>| good-snr <snr> | holdtime <second> | max-adoption
<adopt>| max-request <req>| nb-matching <percentage> |report-interval <interval>|
restriction-timeout slb-mode <mode>|snr-thresh <snr>| vbr-entry-age <age>]
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 IAPs with 5GHz radios, which support a very high throughput. NOTE: Only the IAPs that support 802.11ac can be configured with 80 MHz channels.	—	—
a-channels <a-channel>	Configures 5 GHz channels.	—	—
air-time-fairness-mode {<default-access> <fair-access> <preferred-access>}	Allows equal access to all clients on the wireless medium, regardless of client type, capability, or operating system and prevents the clients from monopolizing resources. You can configure any of the following modes: • default-access—To provide access based on client requests. When this mode is configured, the per user and per SSID bandwidth limits are not enforced. • fair-access—To allocate Airtime evenly across all the clients. • preferred-access—To set a preference where 11n clients are assigned more airtime than 11a/11g. The 11a/11g clients get more airtime	default-access,fair-access, preferred-access	default-access

Command/Parameter	Description	Range	Default
	than 11b. The ratio is 16:4:1.		
band-steering-mode {<balance-bands> <prefer-5ghz> <force-5ghz> <disable>}	Assigns the dual-band capable clients to the 5 GHz band on dual-band. It reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than on the 2.4 GHz band. You can configure any of the following band-steering modes: • prefer-5ghz—To allow the 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. • 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. • 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. • disable—To allow the clients to select the bands.	balance-bands, prefer-5ghz, force-5ghz, disable	balance-bands
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 IAPs. When the client match feature is enabled on an IAP, the IAP measures the RF health of its associated clients. If the client's Received Signal Strength Indication (RSSI) is less than 18dB but has a good RSSI with another IAP having an RSSI of more than 30db or atleast 10db more than its current RSSI, the client will be moved to the IAP with the higher RSSI for better performance and client experience. In the current release, the		

Command/Parameter	Description	Range	Default
	client match feature is supported only within the IAPs within the swarm.		
bad-snr <snr>	The clients with an SNR value below the threshold value will be moved to a potential target IAP.	0-100	18
calc-interval<seconds>	Configures an interval at which client match is calculated.	1-600 in seconds	3
calc-threshold <threshold>	Configures a threshold that takes acceptance client count difference among all the channels of Client match into account. When the client load on an IAP reaches or exceeds the threshold in comparison, client match is enabled on that IAP.	1-255	5
client-thresh <thresh>	When the number of clients on a radio exceeds the value, SLB algorithm will be triggered.	0-255	30
debug <level>	Displays information required for debugging client match issues.	0-4 0—none, 1— error, 2— information, 3—debug, 4—dump	1— error
good-snr <snr>	The IAPs with a RSSI higher than the specified good-snr value will be considered as a potential target IAP.	0-100	30
holdtime <number>	Configures the hold time for the next client match action on the same client.	1—1800	300
max-adoption <count>	Configure a maximum number for adopting clients.	0-100	10
max-request <count>	Configures the maximum number of requests for client match.	0-100	10
nb-matching <percentage>	Configures a percentage value to be considered in the same virtual RF neighborhood of Client match.	20-100%	75%

Command/Parameter	Description	Range	Default
report-interval <interval>	Configures the report interval of VBR on each IAP.	0-3600	30
restriction-timeout	Configures the timeout interval during which non-target IAP will not respond to a specific client.	1—255	10
slb-mode <mode>	Configures a balancing strategy for client match. The applicable values are: 1—Channel-based 2—Radio-based 3—Channel and Radio based	1—3	1
snr-thresh <snr>	The snr value of the Client RSSI must be higher than the current IAP for a potential target IAP.	0-100	10
vbr-entry-age <age>	Denotes the aging time for stable VBR entries	1-3600	300
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 IAP is not supported by the IAP 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 IAP. If the maximum transmission EIRP configured on an IAP is not supported by the IAP model, the value is reduced to the highest supported power setting. NOTE: Higher power level settings may be constrained by local regulatory requirements and IAP 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 IAP 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 802.11 ac, a, b, g, and n client types to inter-operate at the highest performance levels.

Example

The following example configures an ARM profile:

```
(Instant AP) (config) # arm
(Instant AP) (ARM) # 80mhz-support
(Instant AP) (ARM) # a-channels 44
(Instant AP) (ARM) # min-tx-power 18
(Instant AP) (ARM) # max-tx-power 127
(Instant AP) (ARM) # band-steering-mode prefer-5ghz
(Instant AP) (ARM) # air-time-fairness-mode fair-access
(Instant AP) (ARM) # scanning
(Instant AP) (ARM) # client-aware
(Instant AP) (ARM) # client-match
(Instant AP) (ARM) # wide-bands 5
(Instant AP) (ARM) # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.4.3.2-4.2.1	The restriction-timeout parameter was added to the client-match command.
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 IAPs.
no...	Removes the specified configuration parameter.

Usage Guidelines

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

Example

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

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

Command History

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 AP) (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 AP) (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

banner

```
banner motd <motd_text>  
no...
```

Description

This command defines a text banner to be displayed at the login prompt when a user is on a Telnet or SSH session of an IAP.

Syntax

Parameter	Description
<motd_text>	Indicates the text message that you define.
no...	Removes the banner configuration.

Usage Guidelines

The banner you define is displayed at the login prompt of the IAP. The banner is specific to the IAP on which you configure it. The configured banner is displayed at the CLI login prompt of the IAP. Instant supports up to 16 lines text, and each line accepts a maximum of 255 characters including spaces.

Example

The following example configures a banner:

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

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	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 <MAC-address></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 AP) (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 AP) (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

ble

ble

```
config <token> <url>
mode <opmode>
```

Description

This command enables Bluetooth Low Energy (BLE) beacon management by Beacon Management Console (BMC) and configures the BLE operation mode.

Syntax

Parameter	Description	Range	Default
config	Allows you to enable BLE beacon management by BMC.	—	—
<token>	Configures a text string of text string of 1-255 characters as the Bluetooth Low Energy (BLE) endpoint authorization token. The authorization token is used by the BLE devices in the HTTPS header when communicating with the BMC.	—	—
<url>	Configures the URL of the server to which the BLE monitoring data is sent.	—	—
mode <opmode>	Configures the operation modes for the built-in Bluetooth Low Energy (BLE) chip in the IAP. IAPs support the following BLE operation modes: ● Beaconing: The built-in BLE chip of the IAP functions as an iBeacon combined with the beacon management functionality. ● Disabled: The built-in BLE chip of the IAP is turned off. BLE operation mode is set the Disabled by default. ● DynamicConsole: The built-in BLE chip of the IAP functions in the beaconing mode and dynamically enables access to IAP console over BLE when the link to the Local Management Switch (LMS) is lost. ● PersistentConsole: TThe built-in BLE chip of the IAP provides access to the IAP console over BLE and also operates in the Beaconing mode.	beaconing disabled dynamic-console persistent-console	Disabled

Usage Guidelines

The BLE beacon management feature allows you to configure parameters for managing the BLE beacons from the Aruba BLE devices connected to an IAP and establishing secure communication with the Beacon Management Console (BMC). You can also configure the BLE operation modes that determine the functions of the built-in BLE chip in the IAP.



The BLE beacon management and BLE operation mode feature is supported only on IAP-334/335, IAP-314/315, IAP-324/325, IAP-214/215, and IAP-224/225 devices.

Example

The following example enables BLE beacon management:

```
(host)(config)# ble config
MmZjYzkyNTZlYzExODY2MjU3OTBlNTkyZjA0MjdmNjU6OWVhNjdlMjk3MDAxYzFjZjA2ZTQ3Y2UxYWExMmMwYTE=
https://edit.meridianapps.com/api/beacons/manage
(host)(config)# end
```

```
(host) (config)# commit apply
```

The following example enables the beaconing BLE operation mode:

```
(host) (config)# ble mode beaconing
(host) (config)# end
(host) (config)# commit apply
```

Command History

Release	Modification
Aruba Instant 6.5.0.0-4.3.0.0	The IAP-314/315 and IAP-334/335 platforms are added.
Aruba Instant 6.4.4.4-4.2.3	This command was introduced.

Command Information

Platforms	Command Mode
IAP-334/335 IAP-314/315 IAP-324/325 IAP-214/215 IAP-224/225 IAP-205H	Configuration mode

calea

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

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 calea 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 an IAP.	—	—
ip mtu <size>	Configures the Maximum Transmission Unit size to use.	68—1500	1500
gre-type	Specifies GRE type.	—	25944
no...	Disables the parameters configured under the calea command.	—	—
no calea	Removes the CALEA configuration	—	—

Usage Guidelines

Use this command to configure an 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 AP) (config)# calea
(Instant AP) (calea)# ip 192.0.8.29
(Instant AP) (calea)# ip mtu 1500
(Instant AP) (calea)# encapsulation-type gre
```

```
(Instant AP) (calea) # gre-type 25944
(Instant AP) (calea) # end
(Instant AP) # commit apply
```

Command History

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

Description

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

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-country <modem-country>	Specifies the country for the deployment.	—	—
modem-isp <modem_isp>	Specifies the name of the ISP to connect.	—	—
usb-auth-type <usb_authentication_type>	Specifies the authentication type for USB.	PAP, CHAP	PAP
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
<code>usb-modeswitch <usb-modeswitch></code>	Specifies the parameter used to switch modem from storage mode to modem mode.	—	—
<code>usb-type <usb-type></code>	Configures the driver type for the 3G modem.	acm, airprime, hso, option, pantech-3g, sierra-evdo, sierra-gsm,none	—
<code>usb-tty <usb-tty></code>	Specifies the modem tty port.	—	—
<code>usb-user <usb-user></code>	Specifies the username of subscriber of the selected ISP.	—	—
<code>no...</code>	Removes the configuration settings of parameters under the cellular-uplink-profile command.	—	—
<code>no cellular-uplink-profile</code>	Removes the cellular uplink configuration profile.	—	—

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 IAPs to automatically choose the available network in a specific region.



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



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

Example 1

The following example configures a cellular uplink profile:

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


Example 2

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

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

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is modified.
Aruba Instant 6.4.3.4-4.2.1.0	The pin-enable , pin-puk , and pin-renew parameters were removed. These parameters are now available as commands in the privileged Exec mode.
Aruba Instant 6.4.3.1-4.2	The pin-enable , pin-puk , and pin-renew parameters were added.
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

clarity

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

Description

This command enables inline monitoring statistics for the IAP. The information is collected and forwarded to AirWave to debug client connectivity issues.

Syntax

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

Usage Guidelines

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

Example

The following example configures a clarity profile:

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

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	This command is introduced.

Command Information

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

clear airgroup state statistics

clear airgroup state statistics

Description

This command removes the AirGroup statistics.

Usage Guidelines

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

Example

The following command clears AirGroup statistics:

```
(Instant AP) (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

```
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 AP)# 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-cert

```
clear-cert {ap1x| ap1xca| ca|cp|radsec|radsecca|server}
```

Description

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

Syntax

Parameter	Description
ap1x	Clears the user certificate used for TLS based 802.1x authentication of the IAP.
ap1xca	Clears CA certificate used for 802.1x authentication of the IAP against its uplink wired ports.
ca	Clears the CA certificates.
cp	Clears the captive portal server certificate.
radsec	Clears the RadSec server certificate.
radsecca	Clears the RadSec CA certificate.
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 AP)# clear-cert server
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	The ap1x and ap1xca parameters were introduced.
Aruba Instant 6.4.3.1-4.2	The radsec and radsecca parameters were introduced.
Aruba Instant 6.3.1.0-4.0	The cp parameter was introduced.
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 AP) # 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

cluster-security

cluster-security
dtls
no...

Description

This command enables cluster security in DTLS mode.

Syntax

Command/Parameter	Description	Range	Default
dtls	Enables cluster security on the IAP using DTLS and secures the control plane messages between IAPs in the cluster.	—	Disabled
no...	Removes the configuration and returns the values to its default setting	—	—

Usage Guidelines

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

Example

The following example configures a cluster-security profile:

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

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	This command is introduced.

Command Information

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

cluster-security logging

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

Description

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

Syntax

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

Usage Guidelines

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

Example

The following example creates a log for the peer module:

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

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	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>  
<eweeek> <eday> <emonth> <ehour>  
no...
```

Description

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

Syntax

Parameter	Description	Range
<code>clock summer-time <timezone></code>	Configures Daylight Saving time.	Timezones that support daylight saving configuration
<code>recurring</code>	Indicates the recurrences.	—
<code><start-week></code>	Indicates the week from which the daylight saving configuration is effective.	—
<code><start-day></code>	Indicates the day from which the daylight saving configuration applies.	—
<code><start-month></code>	Indicates the month from which the daylight saving configuration applies.	—
<code><start-hour></code>	Indicates the hour from which the daylight saving configuration applies.	1-24
<code><eweeek></code>	Indicates the week in which the daylight saving configuration ends.	—
<code><eday></code>	Indicates the day on which daylight saving configuration ends.	—
<code><emonth></code>	Indicates the month in which daylight saving configuration ends.	—
<code><ehour></code>	Indicates the hour at which daylight saving configuration ends.	1-24
<code>no...</code>	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 AP) (config)# clock summer-time PST recurring 7 10 March 9PM 38 10 October 9PM  
(Instant AP) (config)# end
```

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

Command History

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 AP) (config)# clock timezone PST -8 0
(Instant AP) (config)# end
(Instant AP) # 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 write memory or commit apply command.
revert	Reverts the changes committed to the current configuration of an IAP.

Usage Guidelines

Each command processed by the VC 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 AP) # 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 AP) (config)#
```

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

Example

The following command allows you to enter configuration commands:

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

Command History

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.

console

```
console
  enable
  disable
no console
```

Description

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

Syntax

Command/Parameter	Description
console	Allows you to enter the console configuration mode.
enable	Enables console access to the IAP.
disable	Disables console access to the IAP.
no...	Removes the console access settings.

Usage Guidelines

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

Example

The following example disables console access to the IAP:

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

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Console configuration sub mode

content-filtering

content-filtering
no...

Description

This command enables content filtering feature. When content filtering is enabled on an SSID, all DNS requests to non-corporate domains on this wireless network are sent to 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 AP) # content-filtering
(Instant AP) # end
(Instant AP) # 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.

Syntax

Parameter	Description	Range
<mode>	Provisions the IAP as remote AP or campus AP in a controller-based network.	RAP, CAP.
<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.

For more information, see the *Converting an IAP to a Remote AP and Campus AP* topic in *Aruba Instant User Guide*.

Example

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

```
(Instant AP)# 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> {ap1x {ca|cert} <password> format pem}| cpserver cert
<password> format {p12|pem}| portal logo| radsec {ca|cert <password>} format pem| 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.
ap1x {ca cert}	Copies user or CA certificate required for 802.1X authentication of the IAP.
cpserver cert <password>	Copies internal captive portal server certificate.
portal logo	Copies customized logo for the internal captive portal server.
radsec {ca cert <password>	Copies RadSec server or CA certificates.
system	Copies the file to the system partition.
1xca	Copies the CA certificate used for 802.1X authentication from the TFTP server.
der pem	Indicates the system partition file extensions.

Parameter	Description
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 AP)# copy config tftp 10.0.0.1 filename.cfg
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	The ap1x parameter is introduced.
Aruba Instant 6.4.3.1-4.2	The radsec parameter is introduced.
Aruba Instant 6.3.1.1-4.0	The cpserver parameter is introduced.
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 AP) (config) # deny-inter-user-bridging
(Instant AP) (config) # end
(Instant AP) # 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 AP) (config) # deny-local-routing  
(Instant AP) (config) # end  
(Instant AP) # 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 IAP 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 AP) (config)# device-ID Device1
(Instant AP) (config)# end
(Instant AP)# 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

disable-prov-ssid

disable-prov-ssid
no...

Description

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

Usage Guidelines

The default provisioning SSID is used during the initial configuration of the IAP if the automatic provisioning of the IAP fails and if AirWave or Central are not reachable.

Example

The following example disables the default provisioning SSID:

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

disconnect-user

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

Description

This command disconnects the clients from an IAP.

Syntax

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

Example

The following example disconnects all clients associated with an IAP:

```
(Instant AP) # 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

dot11a-radio-disable

dot-11a-radio-disable
no...

Description

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

Syntax

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

Usage Guidelines

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

Example

The following example disables the 5 GHz radio profile:

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

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	This command was introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

dot11g-radio-disable

dot-11g-radio-disable
no...

Description

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

Syntax

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

Usage Guidelines

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

Example

The following example disables the 2.4 GHz radio profile:

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

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	This command was introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

download-cert

download-cert

```
aplx <url> format pem [psk <psk>]
aplxca <url> format pem
ca <url> format {der|pem}
cp <url> format pem [psk <psk>]
radsec <url> format pem [psk <psk>]
radsecca <url> format pem [psk <psk>]
server <url> format pem [psk <psk>]
```

Description

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

Syntax

Parameter	Description
aplx	Downloads user certificate for TLS based 802.1X authentication of the IAP.
aplxca	Downloads Certificate Authority (CA) certificates.
ca	Downloads CA certificates for validating the identity of the client.
cp	Downloads captive portal server certificates for validating the identity of the internal captive portal server identity to the client.
radsec	Downloads RadSec certificates for mutual authentication between the IAP and the client.
radsecca	Downloads RadSec CA certificates for authentication between the IAP and the client.
server	Downloads authentication server certificates for validating the identity of the server to the client.
<url>	Allows you to specify the FTP, TFTP, or HTTP URL.
format	Allows you to specify the certificate format. The following types of certificate formats are supported: • CA certificate—PEM or DER format • Authentication server—PEM format with PSK • Captive portal certificate—PEM format with PSK • RadSec—PEM format with PSK
psk <psk>	Allows you to specify the passphrase for server, captive portal, and RadSec certificates.

Usage Guidelines

Use this command to download certificates.

Example

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

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

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	The ap1x and ap1xca parameters were introduced.
Aruba Instant 6.4.3.1-4.2.0	The radsec and radsecca parameters were introduced.
Aruba Instant 6.3.1.1-4.0	The cp parameter was introduced.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

dpi

dpi
no...

Description

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

Syntax

Parameter	Description
dpi	Enables AppRF feature.
no...	Removes the configuration.

Usage Guidelines

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

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

For more information access rule configuration and web-filtering options, see *Aruba Instant 6.5.1.0-4.3.1.0 User Guide* and the [wlan access-rule](#) command page.

Example

The following command configures DPI support:

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

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is modified.
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

dpi-error-page-url

dpi-error-page-url <idx> <url>
no...

Description

This command allows you to create a custom list of URLs to which users can be redirected when they access a blocked website.

Syntax

Parameter	Description
<idx>	Index number of the URL.
<url>	URL of the website.
no...	Removes the configuration.

Usage Guidelines

Use this command to create a custom list of URLs. The URLs configured by this command are used for defining an access rule (using the **wlan access-rule <rule> dpi-error-page-url** command) to redirect users to a specific URL when they access a blocked website.

Example

The following example shows how to add a URL:

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

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration 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 auto option is the default and recommended setting.
disable	Disables CPU management on all IAPs, typically for small networks. This setting protects the user experience.
enable	Enables the CPU management feature. When configured, the client and network management functions are protected. This setting helps in large networks with a high client density.

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

Command History

Version	Description
Aruba Instant 6.2.1.0-3.4.0.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

dynamic-dns

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

Description

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

Syntax

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

Usage Guidelines

Use this command to perform a one time dynamic update of the DNS records.

Example

The following example manually adds the SOA record:

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

The following example manually deletes the SOA record.

```
(Instant AP)# dynamic-dns delete 10.17.132.7 test.ddns host-anand 10.17.132.85 key hmac-sha1:arubaddns:16YuLPdH21rQ6PuK9udsVltJw3Y=
(Instant AP)# commit apply
```



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

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

dynamic-dns-ap

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

Description

This command enables the IAP and clients to dynamically update the DNS server.

Syntax

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

Usage Guidelines

Dynamic DNS configuration is allowed only on Master IAPs.

Example

The following example enables the dynamic dns feature:

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



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

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

dynamic-dns-interval

dynamic-dns-interval <ddns_interval>

Description

This command configures a time interval at which the DNS updates are synced to the server.

Syntax

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

Usage Guidelines

Use this command to set a time interval during which the DNS are periodically updated on the server.

Example

The following example configures a DDNS time interval:

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

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	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 VC for communication with external RADIUS servers.

Syntax

Command/Parameter	Description
dynamic-radius-proxy	Enables dynamic RADIUS proxy feature to allow the VC network to use the IP address of the VC when communicating with the external RADIUS servers.
no...	Removes the configuration.

Usage Guidelines

Ensure that you set the VC 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 AP) (config) # dynamic-radius-proxy
(Instant AP) (config) # end
(Instant AP) # 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

dynamic-tacacs-proxy

dynamic-tacacs-proxy
no...

Description

This command enables the VC network to use the IP Address of the VC for communication with external TACACS servers.

Syntax

Command/Parameter	Description
dynamic-tacacs-proxy	Allows the VC network to use the IP address of the VC when communicating with the external TACACS servers. NOTE: When dynamic-tacacs-proxy is enabled on the IAP, the TACACS server cannot identify the slave IAP that generates the TACACS traffic as the source IP address is changed.
no...	Removes the configuration.

Usage Guidelines

Use this command to enable the VC to channel all TACACS related traffic from the slave IAPs to the external TACACS server.

Example

The following example enables the dynamic TACACS proxy feature:

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

Command History

Version	Description
Aruba Instant 6.4.3.4-4.2.1.0	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	Default
enet-vlan <vlan-ID>	Configures VLAN for the upstream switch to which the IAP is connected.	0-4093	1
no...	Removes the configuration.	—	—

Usage Guidelines

Use this command to configure VLAN settings for upstream switch to which the IAP is connected. By default, the value is set to 1. The VLAN setting configured by this command is used for restricting the IAP from sending out tagged frames to clients connected on the SSID that has the same VLAN as the native VLAN of the upstream switch, to which the IAP is connected.

Example

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

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

Command History

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 IAPs 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 AP) # 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 AP) (config)# enet0-port-profile <name>
(Instant AP) (config)# end
(Instant AP)# 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 AP) (config)# enet1-port-profile <name>
(Instant AP) (config)# end
(Instant AP)# 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 AP) (config)# enet2-port-profile <name>
(Instant AP) (config)# end
(Instant AP)# 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 AP) (config)# enet3-port-profile <name>
(Instant AP) (config)# end
(Instant AP)# 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 AP) (config)# enet4-port-profile <name>
(Instant AP) (config)# end
(Instant AP)# 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. Extended SSID is enabled by default in the factory default settings of Instant APs. Disabling the extended ssid option in the factory default mode will not take effect.

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.

Example

The following example enables the configuration of extended SSIDs:

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

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	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

facebook

facebook <id> <secret>

Description

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

Syntax

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

Usage Guidelines

Use this command to verify the ID and secret text generated after the successful integration of an IAP with Facebook.

Command History

Version	Description
Aruba Instant 6.4.2.x-4.1.1.x	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 AP) (config)# factory-ssid-enable
(Instant AP) (config)# end
(Instant AP)# 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

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

Description

This command allows control over the Access Control Entries (ACEs) that are automatically programmed due to expansion of the Access Control Lists (ACLs).

Syntax

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

Usage Guidelines

Use this command to remove the default auto topology rules created for predefined ACLs and WLAN Access Rules. When **disable-auto-topology-rules** is configured on the IAP and the Inbound Firewall rule is set using the Instant UI, the user rules take precedence over the guest VLAN ACL expansion and overrides the auto-expanded rules. However, the corporate and local VLAN expansions will continue to take precedence over the user rules.

Example

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

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

Command History

Version	Description
Aruba Instant 6.4.4.6-4.2.4.0	This command is introduced.

Command Information

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

firewall-external-enforcement

```
firewall-external-enforcement pan
  disable
  enable
  domain-name <name>
  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.	—	—
domain-name <name>	Configures a static domain name to be prefixed with the client user id sent to the PAN firewall.	—	—
no...	Removes the specified configuration parameter.	—	—

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

Command History

Version	Description
Aruba Instant 6.4.4.3-4.2.2.0	This command is modified.
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 IAP regulatory domain.
<tx-power>	Configures the specified transmission power values.	0-127 dBm 127dBm is the maximum possible power that you can set for a radio. Although the IAP allows you to set the transmission power to the 127dBm, power is allocated based on the limits set by the radio hardware and country code in which the IAP operates. The country code and the IAP hardware may support significantly lower transmission power values than 127dBm and in such cases, the transmission power limit set by the country code and the IAP hardware takes precedence.

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 AP) # 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: • Dipole/Omni • Panel • Sector	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 IAP device supports external antenna connectors, see the *Install Guide* that is shipped along with the IAP device.

EIRP and Antenna Gain

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

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

The following table describes this formula:

Table 9: 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.

Example

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

(Instant AP) # 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.

g-max-clients

g-max-clients <ssid_profile> <max-clients>

Description

This command configures the maximum number of clients allowed for an SSID profile on a 2.4 GHz radio channel.

Syntax

Parameter	Description	Range
<ssid_profile>	Denotes the SSID profile for which the maximum clients limit is to be configured.	—
<max-clients>	Denotes the maximum number of clients that can be configured on the 2.4 GHz radio channel of the IAP.	1 to 255.

Usage Guidelines

Use this command to set the maximum number of clients allowed to connect to 2.4 GHz radio channels for a specific SSID profile.

Example

The following example configures the maximum number of clients for a 2.4 GHz radio channel:

```
(Instant AP)# g-max-clients ssid3 77
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0.	The ssid_profile parameter is added.
Aruba Instant 6.4.4.4-4.2.3.0	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 VC.

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 VC.

Example

The following example creates a GRE tunnel for the IAP:

```
(Instant AP) (config)# gre per-ap-tunnel
(Instant AP) (config)# end
(Instant AP) # 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
<code>gre primary <name></code>	Specifies the fully qualified domain name (FQDN) of the primary host.
<code>no...</code>	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 AP) (config)# gre primary <name>  
(Instant AP) (config)# end  
(Instant AP)# 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 AP) (config)# gre type 0
(Instant AP) (config)# end
(Instant AP)# 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

hash-mgmt-password

hash-mgmt-password

Description

This command enables hashing of the management user password.

Usage Guidelines

Use this command to enable hashing of a management user password. When this command is configured, the **mgmt-user** command will not longer be available to add, modify, or remove management users. You will be redirected to the **hash-mgmt-user** command to add, modify, or remove management users.

Example

The following example enables password hashing for management users:

```
(Instant AP) (config) # hash-mgmt-password
(Instant AP) (config) # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

hash-mgmt-user

```
hash-mgmt-user <username> password {{cleartext <cleartext_password>} | {hash <hash_password>
}} [usertype <type>]
no...
```

Description

This command is used to configure management users by using clear text or hash as the password input.

Syntax

Parameter	Description
<username>	Indicates the username of the management user.
password	Indicates the management user password.
cleartext	Indicates if a user will enable clear text as the password input format.
<cleartext_password>	Indicates the password in plain text format.
hash	Indicates that the input password is in hash format.
<hash_password>	Indicates the password in hash format.
usertype	Indicates the type of management user.
<type>	Indicates the type of management user. For example, users with guest-management, local, or read-only privilege.
no	Removes the management user configuration.

Usage Guidelines

Use this command to configure management user credentials to access and configure the IAP. After you configure the **hash-mgmt-password** command, the **mgmt-user** command will no longer be valid. You will be directed to this command for management user configuration.

Example

The following example adds a management user with read-only privilege:

```
(Instant AP) (config) # hash-mgmt-user john password cleartext password01 usertype read-only
(Instant AP) (config) # end
(Instant AP) # commit apply
```

The following examples removes a management user with read-only privilege:

```
(Instant AP) (config) # no hash-mgmt-user read-only
(Instant AP) (config) # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	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 VC.

Syntax

Parameter	Description
<name>	Configures a hostname for the VC.

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

Command History

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

Command History

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 IAP using this profile to advertise a public IPv4 network.

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

Command History

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 nai-realm-auth-id-1 command to send the one of the following authentication methods for the primary NAI realm ID. Use the nai-realm-auth-id-2 command to send the one of the following authentication methods for the secondary NAI realm ID.	—
<auth-id>	Configures any of the following types of authentication ID: ● credential— Uses credential authentication. ● eap-inner-auth—Uses EAP inner authentication type. ● exp-inner-eap— Uses the expanded inner EAP authentication method. ● expanded-eap—Uses the expanded EAP authentication method. ● non-eap-inner-auth—Uses non-EAP inner authentication type. ● reserved—Uses the reserved authentication method.	credential eap-inner-auth exp-inner-auth expanded-eap non-eap-inner-auth reserved

Parameter	Description	Range
nai-realm-auth-value-1 nai-realm-auth-value-2	Configures a value for NAI realm authentication. Use the nai-realm-auth-value-1 command to select an authentication value for the authentication method specified by nai-realm-auth-id-1 . Use the nai-realm-auth-value-2 command to select the authentication value for the authentication method specified by nai-realm-auth-id-2 .	—
<auth-value>	Configures any of following types of authentication values for the specified <auth-id>: - For credential <auth-ID>, specify the following values: - sim - usim - nfc-secure - hw-token - softoken - certificate - uname-password - none - reserved - vendor-specific - For eap-inner-auth <auth-ID>, specify the following values: - reserved - pap - chap - mschap - mschapv2 - For exp-inner-eap <auth-ID>, specify exp-inner-eap as the authentication value. - For expanded-eap <auth-ID>, specify expanded-eap as the authentication value - For non-eap-inner-auth <auth-ID> specify any of the following values: - reserved - pap - chap - mschap - mschapv2	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.	

Parameter	Description	Range
<eap-method>	Configures any of the following EAP methods: • crypto-card—Crypto card authentication • eap-aka—EAP for UMTS Authentication and Key Agreement • eap-sim—EAP for GSM Subscriber Identity Modules • eap-tls—EAP-Transport Layer Security • eap-ttls—EAP-Tunneled Transport Layer Security • generic-token-card—EAP Generic Token Card (EAP-GTC) • identity—EAP Identity type • notification—The hotspot realm uses EAP Notification messages for authentication. • one-time-password—Authentication with a single-use password • peap—Protected Extensible Authentication Protocol • peapmschapv2—Protected Extensible Authentication Protocol with Microsoft Challenge Handshake Authentication Protocol version 2	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
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 AP) (config)# hotspot anqp-nai-realm-profile home
(Instant AP) (nai-realm "home")# nai-realm-name home-hotspot.com
(Instant AP) (nai-realm "home")# nai-realm-encoding utf8
(Instant AP) (nai-realm "home")# nai-realm-eap-method eap-sim
(Instant AP) (nai-realm "home")# nai-realm-auth-id-1 non-eap-inner-auth
(Instant AP) (nai-realm "home")# nai-realm-auth-value-1 mschapv2
(Instant AP) (nai-realm "home")# nai-home-realm
(Instant AP) (nai-realm "home")# enable
(Instant AP) (nai-realm "home")# end
(Instant AP)# commit apply
```

Command History

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: • accept-term-and-cond—When configured, the network requires the user to accept terms and conditions. NOTE: This option requires you to specify a redirection URL string as an IP address, FQDN or URL. • online-enrollment—When configured, the network supports the online enrollment. • http-redirect—When configured, additional information on the network is provided through HTTP/HTTPS redirection. • dns-redirect—When configured, additional information on the network is provided through DNS redirection. NOTE: This option requires you to specify a redirection URL string as an IP address, FQDN or URL.	accept-term-and-cond, online-enrollment, http-redirect, dns-redirect
url	Configures URL, IP address, or FQDN used by the hotspot network for the accept-term-and-cond or dns-redirect network authentication types.	—
no...	Removes any existing configuration.	—

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 AP) (config)# hotspot anqp-nwk-auth-profile default
(Instant AP) (network-auth "default")# nwk-auth-type dns-redirection
(Instant AP) (network-auth "default")# url http://www.example.com
(Instant AP) (network-auth "default")# enable
(Instant AP) (network-auth "default")# end
(Instant AP)# commit apply
```

Command History

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 roam-cons-oi-len parameter must equal upon the number of octets of the roam-cons-oi field. • 0: 0 Octets in the OI (Null) • 3: OI length is 24-bit (3 Octets) • 5: OI length is 36-bit (5 Octets)	—
no...	Removes any existing configuration.	—

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

Command History

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 IAPs associated with this hotspot profile. • assembly • business • educational • factory-and-industrial • institutional • mercantile • outdoor • residential • storage • utility-and-misc • vehicular NOTE: This parameter only defines the venue group advertised in the IEs from hotspot IAPs. To define the venue group to be included in ANQP responses, use anqp-venue-name-profile	assembly, business, educational, factory-and-industrial, institutional, mercantile, outdoor, residential, storage, unspecified, utility-and-misc, vehicular	unspecified

Parameter	Description	Range	Default
	<profile-name> command.		
venue-lang-code <language>	Configures an ISO 639 language code that identifies the language used in the Venue Name field.	—	—
venue-name <name>	Configures the venue name to be advertised in the ANQP IEs. If the venue name includes spaces, the name must be enclosed in quotation marks, e.g. "Midtown Shopping Center".	—	—
venue-type <type>	Specifies the venue type to be advertised in the IEs.	The complete list of supported venue types is described in hotspot anqp-venue-name-profile on page 136.	unspecified
no...	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
assembly	• arena • stadium • passenger-terminal • amphitheater • amusement-park • place-of-worship • convention-center • library • museum

Venue Group	Associated Venue Type Value
	• restaurant • theater • bar • coffee-shop • zoo-or-aquarium • emergency-cord-center • unspecified
business	• doctor • bank • fire-station • police-station • post-office • professional-office • research-and-dev-facility • attorney-office • unspecified
educational	• school-primary • school-secondary • univ-or-college • unspecified
factory-and-industrial	• factory • unspecified
institutional	• hospital • long-term-care • alc-drug-rehab • group-home • prison-or-jail • unspecified
mercantile	• retail-store • grocery-market • auto-service-station • shopping-mall • gas-station • unspecified
outdoor	• muni-mesh-network • city-park

Venue Group	Associated Venue Type Value
	- rest-area - traffic-control - bus-stop - kisok - unspecified
residential	- private-residence - hotel - dormitory - boarding-house - unspecified
storage	unspecified
utility-and-misc	unspecified
vehicular	- unspecified - automobile-or-truck - airplane - bus - ferry - ship - train - motor-bike

Example

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

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

Command History

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

Command History

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

Command History

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

Command History

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.	—	—

Parameter	Description	Range	Default
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)
uplink-speed <speed>	Use the uplink <speed> parameter to indicate the current WAN backhaul uplink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the uplink speed is unknown or unspecified.	0 - 2,147,483,647 kbps	0 (unspecified)
wan-metrics-link-status	Define the status of the WAN Link by configuring one of the following values.	—	—
<status>	Configures any of the following states: • link-up— Indicates if WAN link is up. • link-down— Indicates if WAN link is down • link-under-test—Indicates if WAN link is currently in a test state.	link-down, link-under-test, link-up	unspecified

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

Command History

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-
  nw-auth|anqp-roam-cons|anqp-venue-name|h2qp-conn-cap|h2qp-oper-class|h2qp-oper-name|h2qp-
  wan-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
access-network-type <type>	Configures any of the following access network (802.11u network type) type: • private—This network is accessible for authorized users only. For example, home networks or enterprise networks that require user authentication. The corresponding integer value for this network type is 0. • private-with-guest—This network is accessible to guest users based on guest authentication methods. For example, enterprise networks that allow guest users with captive portal authentication.	private, private-with-guest,chargeable-public, free-public, personal-device, emergency-services, test, wildcard	chargeable-public

Parameter	Description	Range	Default
	The corresponding integer value for this network type is 1. • chargeable-public— This network provides access to the Internet based on payment. For example, a subscription-based Internet access in a coffee shop or a hotel offering chargeable in-room Internet access service. The corresponding integer value for this network type is 2. • free-public—This network is accessible to all without any charges applied. For example, a hotspot in airport or other public places that provide Internet access with no additional cost. The corresponding integer value for this network type is 3. • personal-device—This network is accessible for personal devices. For example, a laptop or camera configured with a printer for the purpose of printing. The corresponding integer value for this network type is 4. • emergency-services—This network is limited to accessing emergency services only. The corresponding integer value for this network type is 5. • test—This network is used for test purposes only. The corresponding integer value for this network type is 14. • wildcard—This network indicates a wildcard network. The corresponding integer value for this network type is 15.		

Parameter	Description	Range	Default
addtl-roam-cons-ois <addtl-roam-cons-ois>	Configures the number of additional roaming consortium Organization Identifiers (OIs) advertised by the IAP. This feature supports up to three additional OIs, which are defined using the roam-cons-oi-1, roam-cons-oi-2 and roam-cons-oi-3 parameters.	—	—
advertisement-profile {anqp-3gpp 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 h2qp-wan-metrics}	Associates an advertisement profile with the hotspot profile. You can associate any of the following advertisement profiles: • 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 • h2qp-wan-metrics	—	—
<profile-name>	Allows you to associate a specific advertisement profile to the hotspot profile.	—	—
advertisement-protocol <protocol>	Configures the anqp : Access Network Query Protocol (ANQP) advertisement protocol.	anqp	—
asra	Indicates if any additional steps are required for network access.	—	—

Parameter	Description	Range	Default
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.	—	—
no	Removes any existing configuration.	—	—
p2p-cross-connect	Advertises support for P2P Cross Connections.	—	Disabled

Parameter	Description	Range	Default
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 IAP to indicate whether the IAP 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 roam-cons-len-1 parameter is based upon the number of octets of the roam-cons-oi-1 field.	0: Zero Octets in the OI (Null), 3: OI length is 24-bit (3 Octets), 5: OI length is 36-bit (5 Octets)	—
roam-cons-len-2	Length of the OI. The value of the roam-cons-len-2 parameter is based upon the number of octets of the roam-cons-oi-2 field.	0: Zero Octets in the OI (Null), 3: OI length is 24-bit (3 Octets), 5: OI length is 36-bit (5 Octets)	—

Parameter	Description	Range	Default
roam-cons-len-3	Length of the OI. The value of the roam-cons-len-3 parameter is based upon the number of octets of the roam-cons-oi-3 field.	0 : Zero Octets in the OI (Null), 3 : OI length is 24-bit (3 Octets), 5 : OI length is 36-bit (5 Octets)	—
roam-cons-oi-1 roam-cons-oi-2 roam-cons-oi-3	Configures the roaming consortium OI to assign to one of the service provider's top three roaming partners. This additional OI will only be sent to a client if the addtl-roam-cons-<oisaddtl-roam-cons-ois> parameter is set to 1 or higher. NOTE: The service provider's own roaming consortium OI is configured using the hotspot anqp-roam-cons-profile command.	—	—
venue-group <venue-group>	Configures one of the following venue groups to be advertised in the IEs from IAPs associated with this hotspot profile. • assembly • business • educational • factory-and-industrial • institutional • mercantile • outdoor • residential • storage • unspecified • utility-and-misc • vehicular NOTE: This parameter only defines the venue group advertised in the IEs from hotspot IAPs. To define the venue group to be included in ANQP responses, use anqp-venue-name-profile <profile-name> command.	assembly, business, educational, factory-and-industrial, institutional, mercantile, outdoor, residential, storage, unspecified, utility-and-misc, vehicular	business

Parameter	Description	Range	Default
<code>venue-type <venue-type></code>	Specifies the venue type to be advertised in the IEs from IAPs associated with this hotspot profile. The complete list of supported venue types is described in Venue Types on page 156 NOTE: This parameter only defines the venue type advertised in the IEs from hotspot IAPs. To define the venue type to be included in ANQP responses, use the hotspot anqp-venue-name-profile <profile-name> 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 IAP 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 IAP to the client to identify the network and service provider of the IAP. If a client requests this information through a GAS query, the hotspot IAP then sends the ANQP Capability list in the GAS Initial Response frame indicating support for the following IEs:

- **Venue Name** - Defined using the **hotspot anqp-venue-name-profile** command.
- **Domain Name**: Defined using the **hotspot anqp-domain-name-profile** command.
- **Network Authentication Type**: Define using the **hotspot anqp-nwk-auth-profile** command.
- **Roaming Consortium List**: Defined using the **hotspot anqp-roam-cons-profile** command.
- **NAI Realm**: Defined using the **hotspot anqp-nai-realm-profile** command.
- **Cellular Network Data**: Defined using the **hotspot anqp-3gpp-nwk-profile** command.
- **Connection Capability**: Defined using the **hotspot h2qp-conn-capability-profile** command.
- **Operator Class**: Defined using the **hotspot h2qp-op-cl-profile** command.
- **Operator Friendly Name**: Defined using the **hotspot h2qp-operator-friendly-name-profile** command.
- **WAN Metrics**: Defined using the **hotspot h2qp-wan-metrics-profile** command.

Roaming Consortium OIs

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 **addtl-roam-cons-ois <1-3>** parameter, then define those elements using the following parameters:

- **roam-cons-oi-1** and **roam-cons-len 1**
- **roam-cons-oi-2** and **roam-cons-len 2**
- **roam-cons-oi-3** and **roam-cons-len 3**

The configurable values for each additional OI include the Organization Identifier itself, the OI length, and the venue group and venue type associated with those OIs.

Venue Types

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

Table 10: Venue Types

Venue Group	Associated Venue Type Value
unspecified The associated numeric value is 0 .	—
assembly The associated numeric value is 1 .	- unspecified—The associated numeric value is 0. - arena—The associated numeric value is 1. - stadium—The associated numeric value is 2. - passenger-terminal—The associated numeric value is 3. - amphitheater—The associated numeric value is 4. - amusement-park—The associated numeric value is 5. - place-of-worship—The associated numeric value is 6. - convention-center—The associated numeric value is 7. - library—The associated numeric value is 8. - museum—The associated numeric value is 9. - restaurant—The associated numeric value is 10. - theater—The associated numeric value is 11. - bar—The associated numeric value is 12. - coffee-shop—The associated numeric value is 13. - zoo-or-aquarium—The associated numeric value is 14. - emergency-cord-center—The associated numeric value is 15.
business The associated numeric value is 2 .	- unspecified—The associated numeric value is 0. - doctor—The associated numeric value is 1 - bank—The associated numeric value is 2 - fire-station—The associated numeric value is 3 - police-station—The associated numeric value is 4 - post-office—The associated numeric value is 6 - professional-office—The associated numeric value is 7 - research-and-dev-facility—The associated numeric value is 8 - attorney-office—The associated numeric value is 9
educational The associated numeric value is 3 .	- unspecified—The associated numeric value is 0. - school-primary—The associated numeric value is 1. - school-secondary—The associated numeric value is 2. - univ-or-college—The associated numeric value is 3.
factory-and-industrial The associated numeric value is 4 .	- unspecified—The associated numeric value is 0. - factory—The associated numeric value is 1.
institutional The associated numeric value is 5 .	- unspecified—The associated numeric value is 0. - hospital—The associated numeric value is 1.

Venue Group	Associated Venue Type Value
	- long-term-care—The associated numeric value is 2. - alc-drug-rehab—The associated numeric value is 3. - group-home—The associated numeric value is 4. - prison-or-jail—The associated numeric value is 5.
mercantile The associated numeric value is 6 .	- unspecified—The associated numeric value is 0. - retail-store—The associated numeric value is 1. - grocery-market—The associated numeric value is 2. - auto-service-station—The associated numeric value is 3. - shopping-mall—The associated numeric value is 4. - gas-station—The associated numeric value is 5.
residential The associated numeric value is 7 .	- unspecified—The associated numeric value is 0. - private-residence—The associated numeric value is 1. - hotel—The associated numeric value is 3. - dormitory—The associated numeric value is 4. - boarding-house—The associated numeric value is 5.
storage The associated numeric value is 8 .	unspecified—The associated numeric value is 0 .
utility-misc The associated numeric value is 9 .	unspecified—The associated numeric value is 0 .
vehicular The associated numeric value is 10 .	- unspecified—The associated numeric value is 0. - automobile-or-truck—The associated numeric value is 1. - airplane—The associated numeric value is 2. - bus—The associated numeric value is 3. - ferry—The associated numeric value is 4. - ship—The associated numeric value is 5. - train—The associated numeric value is 6. - motor-bike—The associated numeric value is 7.
outdoor The associated numeric value is 11 .	- unspecified—The associated numeric value is 0. - muni-mesh-network—The associated numeric value is 1. - city-park—The associated numeric value is 2. - rest-area—The associated numeric value is 3. - traffic-control—The associated numeric value is 4. - bus-stop—The associated numeric value is 5. - kiosk—The associated numeric value is 6.

Example

The following commands configure a hotspot profile:

```

(Instant AP) (config)# hotspot hs-profile hs1
(Instant AP) (Hotspot2.0 "hs1")# enable
(Instant AP) (Hotspot2.0 "hs1")# comeback-mode
(Instant AP) (Hotspot2.0 "hs1")# gas-comeback-delay 10
(Instant AP) (Hotspot2.0 "hs1")# no asra
(Instant AP) (Hotspot2.0 "hs1")# no internet
(Instant AP) (Hotspot2.0 "hs1")# query-response-length-limit 127
(Instant AP) (Hotspot2.0 "hs1")# access-network-type chargeable-public
(Instant AP) (Hotspot2.0 "hs1")# roam-cons-len-1 3
(Instant AP) (Hotspot2.0 "hs1")# roam-cons-oi-1 123456
(Instant AP) (Hotspot2.0 "hs1")# roam-cons-len-2 3
(Instant AP) (Hotspot2.0 "hs1")# roam-cons-oi-2 223355
(Instant AP) (Hotspot2.0 "hs1")# addtl-roam-cons-ois 0
(Instant AP) (Hotspot2.0 "hs1")# venue-group business
(Instant AP) (Hotspot2.0 "hs1")# venue-type research-and-dev-facility
(Instant AP) (Hotspot2.0 "hs1")# pame-bi
(Instant AP) (Hotspot2.0 "hs1")# group-frame-block
(Instant AP) (Hotspot2.0 "hs1")# p2p-dev-mgmt
(Instant AP) (Hotspot2.0 "hs1")# p2p-cross-connect
(Instant AP) (Hotspot2.0 "hs1")# end
(Instant AP)# commit apply

```

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

```

(Instant AP) (config)# hotspot hs-profile hs1
(Instant AP) (Hotspot2.0 "hs1")# advertisement-protocol anqp
(Instant AP) (Hotspot2.0 "hs1")# advertisement-profile anqp-3gpp 3gpp1
(Instant AP) (Hotspot2.0 "hs1")# end
(Instant AP)# 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 AP) # 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-asleap
signature-deassociation-broadcast
signature-deauth-broadcast
wired-containment
wired-containment-ap-adj-mac
wired-containment-susp-l3-rogue
wireless-containment <type>
no...
```

no ids

Description

This command configures an IDS policy for an IAP.

Syntax

Parameter	Description	Range	Default
ids	Creates an IDS policy	—	—
client-detection-level <type>	Sets the client detection level.	off, low, medium, high	off
client-protection-level <type>	Sets the client protection level.	off, low, medium, high	off
detect-adhoc-network	Enables detection of adhoc networks.	—	—
detect-ap-flood	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.	—	—
detect-ap-impersonation	Enables detection of IAP impersonation. In AP impersonation attacks, the attacker sets up an IAP that assumes the BSSID and ESSID of a valid IAP. IAP impersonation attacks can be done for man-in-the-middle attacks, a rogue IAP attempting to bypass detection, or a honeypot attack.	—	—
detect-ap-spoofing	Enables IAP Spoofing detection.	—	—
detect-bad-wep	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.	—	—
detect-beacon-wrong-channel	Enables detection of beacons advertising the incorrect channel.	—	—
detect-block-ack-attack	Enables detection of attempts to reset traffic receive windows using the forged Block ACK Add messages.	—	—
detect-chopchop-attack	Enables detection of ChopChop attack.	—	—
detect-client-flood	Enables detection of client flood attack.	—	—
detect-cts-rate-anomaly	Enables detection of CTS rate anomaly.	—	—

Parameter	Description	Range	Default
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 IAP. 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 IAPs 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.	—	—
detect-malformed-large-duration	Enables detection of unusually large	—	—

Parameter	Description	Range	Default
	durations in frames.		
detect-omerta-attack	Enables detection of Omerta attack.	—	—
detect-overflow-eapol-key	Enables detection of overflow EAPOL key requests.	—	—
detect-overflow-ie	Enables detection of overflow Information Elements (IE).	—	—
detect-power-save-dos-attack	Enables detection of Power Save DoS attack.	—	—
detect-rate-anomalies	Enables detection of rate anomalies.	—	—
detect-rts-rate-anomaly	Enables detection of RTS rate anomaly.	—	—
detect-tkip-replay-attack	Enables detection of TKIP replay attack.	—	—
detect-unencrypted-valid	Enables detection of unencrypted valid clients.	—	—
detect-valid-clientmisassociation	Enables detection of misassociation between a valid client and an unsafe IAP. This setting can detect the following misassociation types: • MisassociationToRogueAP • MisassociationToExternalAPI • MisassociationToHoneypotAP • MisassociationToAdhocAP • MisassociationToHostedAP	—	—
detect-valid-ssid-misuse	Enables detection of interfering or Neighbor APs using valid or protected SSIDs.	—	—
detect-windows-bridge	Enables detection of Windows station bridging.	—	—
detect-wireless-bridge	Enables detection of wireless bridging.	—	—
infrastructure-detection-level <type>	Sets the infrastructure detection level.	off, low, medium, high	off
infrastructure-protection-level <type>	Sets the infrastructure protection level.	off, low, medium, high	off

Parameter	Description	Range	Default
protect-adhoc-network	Enables protection from adhoc networks. When adhoc networks are detected, they are disabled using a denial of service attack	—	—
protect-ap-impersonation	Enables protection from IAP impersonation attacks. When IAP impersonation is detected, both the legitimate and impersonating IAP 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 IAP.	—	—
protect-windows-bridge	Enables protection of a windows station bridging	—	—
rogue-containment	Controls Rogue IAPs. When rogue IAPs are detected, they are not automatically disabled. This option automatically shuts down rogue IAPs. When this option is enabled, clients attempting to associate to an IAP classified as a rogue are disconnected through a denial of service attack.	—	—
signature-airjack	Enables signature matching for the AirJack frame type.	—	—
signature-asleap	Enables signature matching for the ASLEAP frame type.	—	—
signature-deassociation-broadcast	Configures signature matching for the deassociation broadcast frame type.	—	—
signature-deauth-broadcast	Configures signature matching for the deauth broadcast frame type.	—	—
wired-containment	Controls Wired attacks.	—	—
wired-containment-ap-adj-mac	Enables a wired containment to Rogue IAPs whose wired interface MAC address is offset by one from its BSSID.	—	—
wired-containment-susp-13-rogue	Enables the user to identify and contain an IAP with a preset wired MAC address that is different from the BSSID of the IAP if the MAC address that the IAP provides to wireless	—	—

Parameter	Description	Range	Default
	clients as the Gateway MAC is offset by one character from its wired MAC address. NOTE: Enable this feature only when the specific containment is needed, to avoid a false alarm.		
wireless-containment <type>	Enable wireless containment including Tarpit Shielding. Tarpit shielding works by steering a client to a tarpit so that the client associates with it instead of the IAP that is being contained. - deauth-only— Enables Containment using deauthentication only . - none— Disables wireless containment. - tarpit-all-sta—Enables wireless containment by tarpit of all stations. - tarpit-non-valid-sta— Enables wireless containment by tarpit of non-valid clients	deauth-only, none, tarpit-all-sta, tarpit-non-valid-sta	deauth-only
no...	Removes configuration settings for parameters under the ids command.	—	—
no ids	Removes IDS configuration.	—	—

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 IAPs, interfering IAPs, 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 AP) (config) # ids
(Instant AP) (IDS) # infrastructure-detection-level low
(Instant AP) (IDS) # client-detection-level low
(Instant AP) (IDS) # infrastructure-protection-level low
(Instant AP) (IDS) # client-protection-level low
(Instant AP) (IDS) # wireless-containment deauth-only
(Instant AP) (IDS) # wired-containment
(Instant AP) (IDS) # detect-ap-spoofing
(Instant AP) (IDS) # detect-windows-bridge
(Instant AP) (IDS) # signature-deauth-broadcast
(Instant AP) (IDS) # signature-deassociation-broadcast
(Instant AP) (IDS) # detect-adhoc-using-valid-ssid
(Instant AP) (IDS) # detect-malformed-large-duration
(Instant AP) (IDS) # detect-ap-impersonation
(Instant AP) (IDS) # detect-adhoc-network
(Instant AP) (IDS) # detect-valid-ssid-misuse
(Instant AP) (IDS) # detect-wireless-bridge
(Instant AP) (IDS) # detect-ht-40mhz-intolerance
(Instant AP) (IDS) # detect-ht-greenfield
(Instant AP) (IDS) # detect-ap-flood
(Instant AP) (IDS) # detect-client-flood
(Instant AP) (IDS) # detect-bad-wep
(Instant AP) (IDS) # detect-cts-rate-anomaly
(Instant AP) (IDS) # detect-rts-rate-anomaly
(Instant AP) (IDS) # detect-invalid-addresscombination
(Instant AP) (IDS) # detect-malformed-htie
(Instant AP) (IDS) # detect-malformed-assoc-req
(Instant AP) (IDS) # detect-malformed-frame-auth
(Instant AP) (IDS) # detect-overflow-ie
(Instant AP) (IDS) # detect-overflow-eapol-key
(Instant AP) (IDS) # detect-beacon-wrong-channel
(Instant AP) (IDS) # detect-invalid-mac-oui
(Instant AP) (IDS) # detect-valid-clientmisassociation
(Instant AP) (IDS) # detect-disconnect-sta
(Instant AP) (IDS) # detect-omerta-attack
(Instant AP) (IDS) # detect-fatajack
(Instant AP) (IDS) # detect-block-ack-attack
(Instant AP) (IDS) # detect-hotspotter-attack
(Instant AP) (IDS) # detect-unencrypted-valid
(Instant AP) (IDS) # detect-power-save-dos-attack
(Instant AP) (IDS) # detect-eap-rate-anomaly
(Instant AP) (IDS) # detect-rate-anomalies
(Instant AP) (IDS) # detect-chopchop-attack
(Instant AP) (IDS) # detect-tkip-replay-attack
(Instant AP) (IDS) # signature-airjack
(Instant AP) (IDS) # signature-asleap
(Instant AP) (IDS) # protect-ssid
(Instant AP) (IDS) # rogue-containment
(Instant AP) (IDS) # protect-adhoc-network
(Instant AP) (IDS) # protect-ap-impersonation
(Instant AP) (IDS) # protect-valid-sta
(Instant AP) (IDS) # protect-windows-bridge
(Instant AP) (IDS) # end
(Instant AP) # 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.

ignore-image-check

ignore-image-check

Description

This command ignores the automatic image check feature. The automatic image check feature automatically checks for a new version of Instant on the image server, once after the IAP boots up and every week thereafter.

Usage Guidelines

Use this command to disable the automatic image check feature:

Example

The following example disables the image check feature:

```
(Instant AP) # ignore-image-check
```

Command History

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

inactivity-ap-timeout

inactivity-ap-timeout <seconds>
no...

Description

This command configures the timeout interval for inactive user sessions.

Syntax

Parameter	Description	Range	Default
inactivity-ap-timeout <seconds>	Configures the inactivity timeout interval in seconds.	1-1000	1000
no...	Removes any existing configuration.	—	—

Usage Guidelines

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

Example

The following example configures the inactivity timeout interval:

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

Command History

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

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

inbound-firewall

inbound-firewall

```
rule <subnet> <smask> <dest> <mask> <match/invert> <protocol> <sport> <eport>
{permit|deny|src-nat|dst-nat ip <IP-address> <port>} [<option1...option9>]
no...
```

Description

This command configures inbound firewall rules based on the source subnet.

Syntax

Command/Parameter	Description	Range	Default
inbound-firewall	Opens the inbound firewall configuration mode.	—	—
rule	Creates an access rule. You can create up to 128 access rules. However, it is recommended to delete any existing configuration and apply changes at regular intervals.	—	—
<subnet>	Allows you to specify the source subnet IP address	—	—
<smask>	Specifies the subnet mask of the source IP address.	—	—
<dest>	Allows you to specify the destination IP address.	—	—
<mask>	Specifies the subnet mask for the destination IP address.	—	—
<match/invert>	• match—Indicates if the rule specific to the destination IP address and subnet mask matches the value specified for protocol. • invert— Indicates if the rule allows or denies traffic with an exception to the specified destination IP address and subnet mask.	match invert	—
<protocol>	Configures any of the following: • Protocol number between 0-255 • any: any protocol • tcp: Transmission Control Protocol • udp: User Datagram Protocol	1-255	—
<sport>	Specifies the starting port number from	1-65534	—

Command/Parameter	Description	Range	Default
	which the rule applies.		
<eport>	Specifies the ending port number until which the rule applies	1-65534	—
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).	—	—
ip <IP-addr>	Specifies the destination NAT IP address for the specified packets when dst-nat action is configured.	—	—
<port>	Specifies the destination NAT port for the specified packets when dst-nat action is configured.	—	—
deny	Creates a rule to reject the specified packets	—	—
<option1...option9>	Allows you to specify any of the following options: - Log—Creates a log entry when this rule is triggered. - Blacklist—Blacklists the client when this rule is triggered. - Classify-media—Performs a packet inspection on all non-NAT traffic and marks the critical traffic. - Disable-scanning—Disables ARM scanning when this rule is triggered. - DSCP tag—Specifies a DSCP value to prioritize traffic when this rule is triggered. 802.1p priority—Sets an 802.1p priority.	—	—
no...	Removes the configuration	—	—

Usage Guidelines

Use this command to configure inbound firewall rules for the inbound traffic coming through the uplink ports of an IAP. The rules defined for the inbound traffic are applied if the destination is not a user connected to the

IAP. If the destination already has a user role assigned, the user role overrides the actions or options specified in inbound firewall configuration. However, if a deny rule is defined for the inbound traffic, it is applied irrespective of the destination and user role. Unlike the ACL rules in a WLAN SSID or wired profile, the inbound firewall rules can be configured based on the source subnet.

For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default.



Management access to the IAP is allowed irrespective of the inbound firewall rule. For more information on configuring restricted management access, see [restricted-mgmt-access](#).

The inbound firewall is not applied to traffic coming through GRE tunnel.

Example

The following example configures inbound firewall rules:

```
(Instant AP) (config) # inbound-firewall
(Instant AP) (inbound-firewall) # rule 192.0.2.1 255.255.255.255 any any match 6 631 631 permit
(Instant AP) (inbound-firewall) # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and inbound firewall configuration sub-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
<code>internal-domains</code>	Enables the internal-domain configuration sub-mode	—	—
<code>domain-name <domain-name></code>	Defines the valid domain names	—	—
<code>no...</code>	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 AP) (config) # internal-domains
(Instant AP) (domain) # domain-name www.example.com
(Instant AP) (domain) # end
(Instant AP) # 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 AP) # 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 <bid>
  client-count <idx>
  default-router <default_router>
  dhcp-relay
  dhcp-server <dhcp_server>
  disable-split-tunnel
  dns-server <dns_server>
  domain-name <domain-name>
  dynamic-dns [key <algo-name:keyname:keystring>]
  exclude-address <exclude_address>
  host <mac>
  ip-range <start_IP> <end_IP>
  lease-time <lease_time>
  option <option_type> <option_value>
  option82 alu
  reserve {first <count>| last <count>}
  server-type <server_type>
  server-vlan <idx>
  subnet <subnet>
  subnet-mask <Subnet-Mask>
  vlan-ip <VLAN_IP> mask <VLAN mask>
  no...
```

Description

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

Syntax

Parameter	Description	Range	Default
ip dhcp <profile>	Creates a DHCP profile with a unique name.	—	—
bid <bid>	Defines the branch ID. NOTE: You can allocate multiple 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	—	—

Parameter	Description	Range	Default
	with BID 0, which is mapped directly to the configured static subnet.		
<code>client-count <idx></code>	Defines the number of clients allowed per DHCP branch. NOTE: The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The 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.	—	—
<code>default-router <default_router></code>	Defines the IP address of the default router for the Distributed, L2 DHCP scope.	—	—

Parameter	Description	Range	Default
<code>dhcp-relay</code>	Enables the IAPs to intercept the broadcast packets and relay DHCP requests directly to corporate network. 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.	—	—
<code>dhcp-server <dhcp_server></code>	Defines the IP address of the corporate DHCP server for DHCP request relay.	—	—
<code>dynamic-dns</code>	Enables dynamic dns updates for this pool.	—	Disabled
<code>dynamic-dns [key <algo-name:keyname:keystring>]</code>	You can optionally choose to configure a TSIG shared secret key to secure the dynamic updates.	—	<code>hmac-sha1:arubaddns:16YuLPdH21rQ6PuK9udsVLtJw3Y=</code>

Parameter	Description	Range	Default
	The following algorithm names are supported: • hmac-md5 (used by default if algo-name is not specified) • hmac-sha1 • hmac-sha256 NOTE: When a key is configured, the update is successful only if IAP and DNS server clocks are in sync.		
<code>disable-split-tunnel</code>	Disables split tunnel functionality for Centralized, L2 subnets. Split tunneling allows a VPN user to access a public network and a local LAN or WAN network at the same time through the same physical network connection. When split-tunnel is disabled, all the traffic including the corporate and Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped.	—	—
<code>dns-server <IP-address></code>	Defines the DNS server IP address.	—	—

Parameter	Description	Range	Default
domain-name <domain-name>	Defines the domain name.	—	—
host <mac>	Allows you to specify the host MAC address.	—	—
exclude-address <exclude_address>	Defines the IP address to exclude for the Local, L3 DHCP scope. The value entered in the field determines the exclusion range of the subnet. Based on the size of the subnet, the IP addresses that come before or after the IP address value specified in this field are excluded.	—	—
ip-range <start_IP> <end_IP>	Defines a range of IP addresses to use in the Distributed, L2 and Distributed, L3 DHCP scopes. You can configure a range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically. You can configure up to four different ranges of IP addresses For Distributed, L2 mode, ensure that all IP ranges are in the same	—	—

Parameter	Description	Range	Default
	subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. For Distributed, L3 mode, you can configure any discontinuous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count.		
<code>lease-time <lease_time></code>	Defines a lease time for the client in seconds.	120–86400 seconds	43200 seconds (720 minutes)
<code>option <option_type> <option_value></code>	Defines the type and a value for the DHCP option to use. You can configure up to eight DHCP options supported by the DHCP server and enter the option value in "" not exceeding 255 characters.	—	—

Parameter	Description	Range	Default
option82 alu	Enables the DHCP Option 82 for the Centralized, L2 DHCP scope to allow clients to send DHCP packets with the Option 82 string.	—	—
reserve {first <count> last <count>}	Reserves the first few and last few IP addresses in the subnet.	—	—
server-type <server_type>	Defines any of the following DHCP assignment modes: • Distributed, L2 • Distributed, L3 • Local • Local, L2 • Local, L3 • Centralized, L2 • Centralized, L3	Distributed, L2; Distributed, L3; Local; Local, L2; Local, L3; Centralized, L2; Centralized, L3	Local
server-vlan <idx>	Configures a VLAN ID for the DHCP scope. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.	1-4093	—
subnet <subnet>	Defines the network IP address	—	—
subnet-mask <subnet_mask>	Defines the subnet mask for Local; Local, L3; and Distributed, L3 DHCP scopes. The subnet mask and the network determine the size of subnet.	—	—
vlan-id <VLAN_IP> mask	Defines the IP	—	—

Parameter	Description	Range	Default
<VLAN mask>	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 VC 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 VC 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 VC 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 VC is configured with a unique subnet and a corresponding scope.
- **Local**—In this mode, the VC 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 VC assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPsec tunnel or through the uplink. This DHCP assignment mode is used for the NAT forwarding mode.
- **Local, L2**—In this mode, the VC acts as a DHCP server with data center as the gateway. When Local, L2 DHCP scope is selected, the network address translation for client IPs is not carried out at the source.
- **Local, L3**— In this mode, the VC 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, L2**—When a Centralized, L2 DHCP scope is configured, the VC bridges the DHCP traffic to the controller over the VPN/GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN/GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the controller.
- **Centralized, L3**—For Centralized, L3 clients, the VC acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located either in the corporate or local network. The Centralized, L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

Example

The following example configures a Distributed, L2 DHCP scope:

```
(Instant AP) (config)# ip dhcp corpNetwork1
(Instant AP) (DHCP Profile"corpNetwork1")# ip dhcp server-type distributed,l2
(Instant AP) (DHCP Profile"corpNetwork1")# server-vlan 1
(Instant AP) (DHCP Profile"corpNetwork1")# subnet 192.0.1.0
(Instant AP) (DHCP Profile"corpNetwork1")# subnet-mask 255.255.255.0
(Instant AP) (DHCP Profile"corpNetwork1")# default-router 192.0.1.1
(Instant AP) (DHCP Profile"corpNetwork1")# client-count 0
```

```
(Instant AP) (DHCP Profile "corpNetwork1") # dns-server 192.0.1.2
(Instant AP) (DHCP Profile "corpNetwork1") # domain-name www.example.com
(Instant AP) (DHCP Profile "corpNetwork1") # lease-time 1200
(Instant AP) (DHCP Profile "corpNetwork1") # ip-range 192.0.1.0 192.0.1.17
(Instant AP) (DHCP Profile "corpNetwork1") # reserve first 2
(Instant AP) (DHCP Profile "corpNetwork1") # option 176
"MCIPADD=10.72.80.34,MCPOR=1719,TFTPSRVR=10.80.0.5,L2Q=1,L2QVLAN=2,L2QAUD=5,L2QSIG=3"
(Instant AP) (DHCP Profile "corpNetwork1") # end
(Instant AP) # commit apply
```

The following example configures a Distributed, L3 DHCP scope:

```
(Instant AP) (DHCP Profile <profile-name>) # ip dhcp server-type <Distributed,L3>
(Instant AP) (DHCP Profile <profile-name>) # server-vlan <vlan-ID>
(Instant AP) (DHCP Profile <profile-name>) # client-count <number>
(Instant AP) (DHCP Profile <profile-name>) # dns-server <name>
(Instant AP) (DHCP Profile <profile-name>) # dynamic-dns key <algo-name:keyname:keystring>
(Instant AP) (DHCP Profile <profile-name>) # domain-name <domain-name>
(Instant AP) (DHCP Profile <profile-name>) # lease-time <seconds>
(Instant AP) (DHCP Profile <profile-name>) # ip-range <start-IP> <end-IP>
(Instant AP) (DHCP Profile <profile-name>) # reserve {first | last} <count>
(Instant AP) (DHCP Profile <profile-name>) # option <type> <value>
(Instant AP) (DHCP Profile <profile-name>) # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3-4.2.3	This command is modified.
Aruba Instant 6.4.0.2-4.1	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 VC.

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.	2-43200 minutes	720 minutes
subnet <IP- address-subnet>	Defines IP address of the subnet.	—	—
subnet-mask <Subnet_Mask>	Defines the subnet mask of the IP address,	—	—
no...	Removes any existing configuration	—	—

Usage Guidelines

Use this command to configure a DHCP pool. The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the VC. 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 AP) (config)# ip dhcp pool
(Instant AP) (DHCP)# domain-name example.com
(Instant AP) (DHCP)# dns-server 192.0.2.1
(Instant AP) (DHCP)# lease-time 20
(Instant AP) (DHCP)# subnet 192.0.2.0
(Instant AP) (DHCP)# subnet-mask 255.255.255.0
(Instant AP) (DHCP)# end
(Instant AP)# commit apply
```

Command History

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.

ip-mode

```
ip-mode {v4-only|v4-prefer}  
no...
```

Description

This command configures the IP mode to enable the processing of IPv4 packets globally.

Syntax

Parameter	Description
ip-mode	Configures the IP mode to process IPv6 or IPv4 packets.
v4-only	Enables global processing of IPv4 packets.
v4-prefer	TBU
no...	Removes the configuration.

Usage Guidelines

Use this command to configure IP modes to enable global processing of IPv4 packets.

Example

The following example configures the IPv4 mode:

```
(Instant AP) (config) # ip-mode v4-only  
(Instant AP) (config) # end  
(Instant AP ) # commit apply
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is introduced.

Command Information

Platform	Command Mode
IAP-214/215, IAP-224/225, IAP-274/275, IAP-314/315, IAP-324/325, IAP-334/335	Privileged EXEC mode

I2tpv3 session

```
l2tpv3 session <l2tpv3_session_profile>
    cookie len <len_of_cookie> value <cookie_val>
default-l2-specific-sublayer
    l2tpv3 tunnel <l2tpv3_tunnel_prof_to_associate>
    tunnel-ip <local_ip_addr_tunnel> mask <tunnel_mask> vlan <tunnel_mgmt_vlan>
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 <len_of_cookie> value <cookie_val>	Configures the length and alphanumeric value for the cookie.	Length: 4/8 If cookie length is 4, the cookie value should have exactly 8 hexadecimal characters. If cookie length is 8, the cookie value should have exactly 16 hexadecimal characters	Not set.
default-l2-specific-sublayer	Enables the default l2 specific sublayer in the L2TPV3 session.		
l2tpv3 tunnel <l2tpv3_tunnel_prof_to_associate>	Selects the tunnel profile name where the session will be associated.	—	—
tunnel <local_ip_addr_tunnel> mask <tunnel_mask> vlan <tunnel_mgmt_vlan>	Configures the local IP address, network mask, and VLAN ID of the tunnel.	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 AP) (config) # l2tpv3 session test_session
```

```

(Instant AP) (L2TPv3 Session Profile "test_session")# cookie len 4 value 12345678
(Instant AP) (L2TPv3 Session Profile "test_session")# l2tpv3 tunnel test_tunnel
(Instant AP) (L2TPv3 Session Profile "test_session")# tunnel-ip 1.1.1.1 mask 255.255.255.0 vlan
2
(Instant AP) (L2TPv3 Session Profile "test_session")# end
(Instant AP)# commit apply

```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is modified.
Aruba Instant 6.4.0.2-4.1	This command is modified.
Aruba Instant 6.2.1.0-3.4	This command is introduced.

Command Information

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

l2tpv3 tunnel

```
l2tpv3 tunnel <l2tpv3_tunnel_profile>
  backup peer-address <peer_IP_address_backup_tunnel>
  checksum
  failover-mode <mode>
  failover-retry-count <retry_count>
  failover-retry-interval <interval_in_sec>
  hello-timeout <interval_in_sec>
  local-port <local_udp_port>
  message-digest-type <digest_algo>
  mtu <tunnel_MTU>
  peer-port <peer_udp_port>
  primary peer-address <peer_IP_address_primary_tunnel>
  secret-key <key>
  no...
no l2tpv3 tunnel <l2tpv3_tunnel_profile>
```

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.	—	—
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_sec>	Configures the interval (in seconds) at which hello packets are routed in the tunnel.	5-300	60

Parameter	Description	Range	Default
local-port <local_udp_port>	Assigns the local UDP port number of the client.	1—65535	1701
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 AP) (config)# l2tpv3 tunnel test_tunnel
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# primary peer-address 10.0.0.65
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# backup peer-address 10.0.0.63
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# failover-mode non-preemptive
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# failover-retry-count 5
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# failover-retry-interval 80
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# hello-timeout 150
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# mtu 1570
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# peer-port 3000
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# secret-key test123
(Instant AP) (L2TPv3 Tunnel Profile "test_tunnel")# end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant6.5.0.0-4.3.0.0	This command is modified.
Aruba Instant 6.2.1.0-3.4	This command is introduced.

Command Information

IAP Platform	Command Mode
RAP-108 RAP-109	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 VC assigns the home IAP for roamed clients by using a round robin policy. With this policy, the load for the IAPs 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 VC to the mobility domain. In a typical deployment scenario, all the IAPs are configured in one subnet and all the clients in another subnet. You can also deploy IAPs across different subnets, in which case the IAPs in each subnet will form a cluster with its own VC IP address. To allow clients to roam seamlessly among all the IAPs, the VC 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 VC 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 AP) (config)# l3-mobility
(Instant AP) (L3-mobility)# home-agent-load-balancing
(Instant AP) (L3-mobility)# virtual-controller 192.0.2.1
(Instant AP) (L3-mobility)# subnet 192.0.2.2 255.255.255.0 1 192.0.2.1
(Instant AP) (L3-mobility)# end
(Instant AP)# commit apply
```

Command History

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.

lACP-mode

```
lACP-mode {enable|disable}  
no..
```

Description

This command is introduced to support the static LACP configuration.

Syntax

Parameter	Description
enable	This parameter enables the static LACP configuration. The IAP will work on LACP mode irrespective of whether or not the peer switch works on the LACP mode.
disable	This parameter disables the static LACP configuration. The IAP will not work on LACP mode even it detects any LACP PDUs from the peer switch.
no	Removes the static LACP configuration

Usage Guidelines

Use this command to enable, disable, and remove the static LACP configuration. When an IAP boots up, it forms the LACP according to the static configuration.

Example

The following example configures the static LACP for the IAP.

```
(Instant AP)# lACP-mode enable  
(Instant AP)# lACP-mode disable
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3.0	This command is introduced.

Command Information

IAP Platform	Command Mode
IAP- 225, IAP-325, IAP-275	Privileged EXEC 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 AP) (config) # 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

loginsession

loginsession timeout <val>

Description

This command configures the management session (Telnet or SSH) to remain active without any user activity.

Syntax

Parameter	Description	Range	Default
timeout	Number of seconds or minutes that a management session remains active without any user activity.	5-60 minutes or 1-3600 seconds, 0 to disable	5 minutes

Usage Guidelines

The management user must re-login to the IAP after a Telnet or SSH session times out. If you set the timeout value to 0, sessions do not time out.

Example

The following example configures management sessions on the IAP to not time out:

```
(Instant AP) (config) # loginsession timeout 0
(Instant AP) (config) # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	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 AP) (config)# mas-integration
(Instant AP) (config)# end
(Instant AP)# 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

managed-mode-profile

```
managed-mode-profile
  automatic
  config-filename <filename>
  debug-managed-mode
  download-method <method>
  retry-poll-period <time-in-sync>
  server <server name>
  sync-time day <dd> | hour <hh> | min <mm> | window <window>
  username <username>
  password <password>
  no...
```

Description

This command is used to enable auto configuration of the IAPs in the management mode.

Syntax

Parameter	Description
managed-mode-profile	Configures the managed-mode-profile for automatic configuration.
automatic	Enabled the automatic mode to automatically generate the user credentials based on IAP MAC address.
config-filename <file_name>	Filename—Indicates filename within the alphanumeric format. Ensure that configuration file name does not exceed 40 characters.
download-method <method>	Denotes the method used for downloading configuration files (FTP or FTPS).
server <server_name>	Denotes the name of the server or the IP address of the server from which the configuration file must be downloaded.
sync-time day <dd> hour <hh> min <mm> window <window>	Configures the day and time at which the IAPs can poll the configuration files from the server. - day <dd>— Indicates day, for example to configure Sunday as the day, specify 01. To configure the synchronization period as everyday, enter 00. - hour <hh>—Indicates hour within the range of 0-23. - min <mm>—Indicates minutes within the range of 0-59. - window <hh>—Defines a window for synchronization of the configuration file. The default value is 3 hours.
retry-poll-period <time-in-sync>	Configures the time interval in minutes between two retries, after which IAPs can retry downloading the configuration file
username <username> password <password>	Denotes the user credentials set by the user to enable automatic configuration.
no...	Removes the configuration.

Usage Guidelines

Use this command to enable automatic configuration of the IAPs in the management mode.

The following checks must be performed before the configuration:

- Ensure that the IAPs running Aruba Instant 6.5.1.0-4.3.1.0 or later release version.
- When the IAPs are in the management mode, ensure that the IAPs are not managed by AirWave.

Example

The following example configures an IAP for automatic configuration:

```
(Instant AP) (config)# managed-mode-profile
(Instant AP) (managed-mode-profile)# username <username>
(Instant AP) (managed-mode-profile)# password <password>
(Instant AP) (managed-mode-profile)# config-filename instant.cfg
(Instant AP) (managed-mode-profile)# download-method ftps
(Instant AP) (managed-mode-profile)# sync-time day 00 hour 03 min 30 window 02
(Instant AP) (managed-mode-profile)# retry-poll-period 10
(Instant AP) (managed-mode-profile)# end
(Instant AP)# commit apply
```

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

managed-mode-sync-server

managed-mode-sync-server

Description

This command is used to retrieve a new set of configuration from the server ahead of the next scheduled sync-time.

Syntax

Parameter	Description
managed-mode-sync-server	Initiates the fetching of a new set of configuration from the server for the IAPs in the management mode.

Usage Guidelines

Use this command for a real-time retrieve and apply of the configuration from the server, even before its actual set sync-time.

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	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 VC. A Mesh portal (MPP) uses its uplink connection to reach the VC, 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 AP) (config) # mesh
(Instant AP) (config) # end
(Instant AP) # 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-accounting

mgmt-accounting command all
no...

Description

This command is used to enable accounting privileges on TACACS+ servers for management users.

Syntax

Parameter	Description
mgmt-accounting command all	Configures TACACS+ servers to enable accounting for management users.
no...	Removes the configuration.

Usage Guidelines

Use this command to record the user name of the management users and the respective IP address sending the request to account for the usage of the authorized network services.

Example

The following example configures a TACACS+ server for management accounting

```
(Instant Access Point) (config) # mgmt-accounting command all tacacs1  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 VC.

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 VC.

Example

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

```
(Instant AP) (config) # mgmt-auth-server server1  
(Instant AP) (config) # end  
(Instant AP) # 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 AP) (config) # mgmt-auth-server-load-balancing
(Instant AP) (config) # end
(Instant AP) # 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 VC management interface.

Example

The following example configures a backup internal authentication server:

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

Command History

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>]  
no..
```

Description

This command configures user credentials for access to the VC 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.
no..	Removes the configuration.

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 AP) (config)# mgmt-user User1 Password123 guest-mgmt  
(Instant AP) (config)# end  
(Instant AP)# 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

mtu

mtu <size>
no...

Description

This command configures the maximum transmission unit (MTU) size for the uplink interfaces.

Syntax

Parameter	Description
mtu <size>	Configures MTU size.
no...	Removes the configuration.

Usage Guidelines

Use this command to configure the MTU size for tunnel and br0 interfaces, and uplink interfaces such as 3G/4G. The configured MTU size is applied when the uplink changes.

Example

The following example sets the MTU size to 1200 bytes:

```
(Instant AP) (config) # mtu <1200>
(Instant AP) (config) # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	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 VC.

Usage Guidelines

Use this command to configure a name for the IAP:

Example

The following example configures a name for the IAP:

```
(Instant AP) # 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 AP) (config)# ntp-server <name>  
(Instant AP) (config)# end  
(Instant AP)# 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 AP) (config) # opendns <username> <password>  
(Instant AP) (config) # end  
(Instant AP) # 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: • AMP Role— "Org Admin" (initially disabled) • AMP User— "Org Admin" (assigned to the role "Org Admin") • Folder— "Org" (under the Top folder in AMP) • Configuration Group— "Org" You can also assign additional strings to create a hierarchy of sub folders under the folder named "Org": For example: • subfolder1 for a folder under the "Org" folder • subfolder2 for a folder under subfolder1
no...	Removes the configuration settings.	—

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 AP) (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

out-of-service-hold-on-time

out-of-service-hold-on-time <time>
no...

Description

This command configures a hold on time in seconds, after which out-of-service operation is triggered. For example, if the VPN is down, the effect of this out-of-service state impacts the SSID availability after the configured hold on time.

Syntax

Command/Parameter	Description	Range	Default
<time>	Configures the hold on time of out-of-service operations.	30–300 seconds	30 seconds
no...	Removes the configuration	—	—

Usage Guidelines

Use this command to configure a hold time after which the out-of-service operation is triggered.

Example

The following example sets the out of service hold on interval to 45 seconds:

```
(Instant AP) (config) # out-of-service-hold-on-time 45
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

per-ap-ssid

per-ap-ssid <ssid>
no...

Description

This command is used to set the environment variable, per_ap_ssid.

Syntax

Parameter	Description
<ssid>	Denotes the environment variable configured in apboot.
no...	Removes the environment variable.

Usage Guidelines

If the environment variable is defined in the apboot, then configure the ssid in the ssid profile by using the value of the variable. The ssid-profile ssid field is enhanced to accept \$per-ap-ssid.

Example

The following example sets the environment variable:

```
(Instant AP) # per-ap-ssid <ssid>
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged Exec mode

per-ap-vlan

per-ap-vlan <vlan>
no...

Description

This command is used to set the environment variable, per_ap_vlan.

Syntax

Parameter	Description
<vlan>	Denotes the environment variable configured in apboot.
no...	Removes the environment variable.

Usage Guidelines

If the environment variable is defined in the apboot, then configure the vlan in the ssid profile by using the value of the variable. The wired-port-profile native vlan must be enhanced to accept the \$per-ap-vlan.

Example

The following example sets the environment variable:

```
(Instant AP)# per-ap-vlan <vlan>
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	This command was introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged Exec mode

pin-enable

```
pin-enable <pin_current_used>  
no...
```

Description

This command enables locking of the SIM PIN for the 3G/4G modems.

Syntax

Parameter	Description
pin-enable <pin_current_used>	Enables locking of the SIM. To enable SIM PIN lock, the PIN code should be same as the PIN code that is currently used.
no...	Disables SIM PIN locking.

Usage Guidelines

Use this command to enable locking of SIM PIN of the cellular modem connected to an IAP.

Example

The following example enables SIM PIN locking:

```
(host)# pin-enable 12345678
```

The following example disables SIM PIN locking:

```
(host)# pin-enable 12345678
```

Command History

Version	Description
Aruba Instant 6.4.3.4-4.2.1.0	This command was introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged Exec mode

pin-puk

pin-puk <pin_puk>

Description

This command unlocks the cellular modems using the PUK code. The SIM PIN of a modem is locked if a user enters incorrect PIN code for three consecutive attempts.

Syntax

Parameter	Description
pin-puk <pin_puk> <pin_new>	Unlocks the SIM PIN using the PUK code provided by the ISP and by entering a new PIN code.

Usage Guidelines

Use this command to unlock a cellular modem using the PUK code provided by your ISP.

Command History

Version	Description
Aruba Instant 6.4.3.4-4.2.1.0	This command was introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged Exec mode

pin-renew

pin-renew <pin_current> <pin_new>

Description

This command renews PIN for the SIM card of the 3G/4G modem.

Syntax

Parameter	Description
pin-renew	Renews the SIM PIN of the modem.
<pin-current>	Allows you to enter the current PIN of the modem SIM.
<pin_new>	Allows you to specify a new SIM PIN for the modem.

Usage Guidelines

Use this command to renew the SIM PIN of the cellular modem.

Command History

Version	Description
Aruba Instant 6.4.3.4-4.2.1.0	This command was introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged Exec 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 AP) (config) # pppoe-uplink-profile
(Instant AP) (pppoe-uplink-profile) # pppoe-username User1
(Instant AP) (pppoe-uplink-profile) # pppoe-passwd Password123
(Instant AP) (pppoe-uplink-profile) # pppoe-svcname internet03
(Instant AP) (pppoe-uplink-profile) # pppoe-chapsecret 8e87644deda9364100719e017f88ebce
(Instant AP) (pppoe-uplink-profile) # pppoe-unnumbered-local-l3-dhcp-profile dhcpProfile1
(Instant AP) (pppoe-uplink-profile) # end
(Instant AP) # commit apply
```


Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	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 AP) (config)# proxy exception 192.0.2.2
(Instant AP) (config)# proxy server 192.0.2.1 8080
(Instant AP) (config)# end
(Instant AP)# 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 VC.

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 through a local console connected to the serial port, or through an SSH, Telnet, or UI 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 AP) (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 AP) (config) # restrict-corp-access
(Instant AP) (config) # end
(Instant AP) # 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 AP) (config) # restricted-mgmt-access 192.0.2.13 255.255.255.255  
(Instant AP) (config) # end  
(Instant AP) # 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>
  cell-size-reduction <reduction>
  csa-count <count>
  csd-override
  dot11h
  interference-immunity <level>
  legacy-mode
  max-tx-power <power>
  min-tx-power <power>
  max-distance <count>
  spectrum-band <type>
  spectrum-monitor
  very-high-throughput-disable
  no...
```

Description

This command configures a 5 GHz or 802.11a radio profile for an IAP.

Syntax

Parameter	Description	Range	Default
rf dot11a-radio-profile	Enables the 5 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
cell-size-reduction <reduction>	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an IAPs receive coverage area. It helps to minimize co-channel interference and optimizes channel reuse. The possible range of values for this feature are 0-55 dB. NOTE: This value should be changed if the network is experiencing performance issues. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.	1-55	0

Parameter	Description	Range	Default
	Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's transmission (Tx) power to match its new received (Rx) power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.		
<code>csa-count <count></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>csd-override</code>	Most transmissions to high throughput (HT) stations are sent through multiple antennas using cyclic shift diversity (CSD). When you enable the CSD Override parameter, CSD is disabled and only one antenna transmits data, even if they are being sent to high-throughput stations. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n CDD data. This option is disabled by default, and should only be enabled under the supervision of Aruba technical support. Use this feature to turn off antenna diversity when the AP must support legacy clients such as Cisco 7921g VoIP phones, or older 802.11g clients (e.g. Intel Centrino clients). NOTE: Enabling this feature can reduce overall throughput rates.	—	—
<code>dot11h</code>	Allows the IAP to advertise its 802.11d (country information) and 802.11h (transmit power control) capabilities.	—	Disabled
<code>interference-immunity <level></code>	Configures the immunity level to improve performance in high-interference environments. You can specify any of the following immunity levels: • Level 0— no ANI adaptation.	0-5	2

Parameter	Description	Range	Default
	- Level 1— Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. - Level 2— Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. - Level 3— Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. - Level 4— Level 3 settings, and FIR immunity. At this level, the IAP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. - Level 5— The IAP completely disables PHY error reporting, improving performance by eliminating the time the IAP would spend on PHY processing. NOTE: Increasing the immunity level makes the IAP to lose a small amount of range.		
legacy-mode	Enables the IAPs to run the radio in non-802.11n mode.	—	Disabled
max-tx-power <power>	Configures the maximum transmit power value for the 5 GHz radio profile.	3-max	3 dBm
min-tx-power <power>	Configures the minimum transmit power value for the 5 GHz radio profile.	3-max	3 dBm
max-distance <count>	Configures the maximum distance between a client and an IAP or between a mesh point and a mesh portal in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies the default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km.	600-1000	0

Parameter	Description	Range	Default
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 IAPs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.	—	—
very-high-throughput-disable	Disables very high throughput (VHT) for clients connecting on the 5 GHz band.	—	—
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 AP) (config)# rf dot11a-radio-profile
(Instant AP) (RF dot11a Radio Profile)# beacon-interval 100
(Instant AP) (RF dot11a Radio Profile)# legacy-mode
(Instant AP) (RF dot11a Radio Profile)# dot11h
(Instant AP) (RF dot11a Radio Profile)# interference-immunity 3
(Instant AP) (RF dot11a Radio Profile)# max-tx-power 33
(Instant AP) (RF dot11a Radio Profile)# min-tx-power 10
(Instant AP) (RF dot11a Radio Profile)# max-distance 600
(Instant AP) (RF dot11a Radio Profile)# csa-count 2
(Instant AP) (RF dot11a Radio Profile)# spectrum-monitor
(Instant AP) (RF dot11a Radio Profile)# end
```

Command History

Version	Description
Aruba Instant 6.4.3.4-4.2.1.0	The very-high-throughput-disable keyword was added. The cell-size-reduction parameter has been added.
Aruba Instant 6.4.3.1-4.2	The max-tx-power and min-tx-power parameters were added.
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>
  cell-size-reduction <reduction>
  csa-count <count>
  csd-override
  dot11h
  interference-immunity <level>
  legacy-mode
  max-distance <count>
  max-tx-power <power>
  min-tx-power <power>
  spectrum-monitor
  no...
```

Description

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

Syntax

Parameter	Description	Range	Default
rf dot11g-radio-profile	Enables the 2.4 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
cell-size-reduction <reduction>	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an IAPs receive coverage area. It helps to minimize co-channel interference and optimizes channel reuse. The possible range of values for this feature are 0-55 dB. NOTE: This value should be changed if the network is experiencing performance issues. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.	1-55	0

Parameter	Description	Range	Default
	Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's transmission (Tx) power to match its new received (Rx) power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.		
<code>csa-count <count></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>csd-override</code>	Most transmissions to high throughput (HT) stations are sent through multiple antennas using cyclic shift diversity (CSD). When you enable the CSD Override parameter, CSD is disabled and only one antenna transmits data, even if they are being sent to high-throughput stations. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n CDD data. This option is disabled by default, and should only be enabled under the supervision of Aruba technical support. Use this feature to turn off antenna diversity when the AP must support legacy clients such as Cisco 7921g VoIP phones, or older 802.11g clients (e.g. Intel Centrino clients). NOTE: Enabling this feature can reduce overall throughput rates.	—	—
<code>dot11h</code>	Allows the IAP to advertise its 802.11d (country information) and 802.11h (transmit power control) capabilities.	—	Disabled
<code>interference-immunity <level></code>	Configures the immunity level to improve performance in high-interference environments. You can specify any of the following immunity levels: • Level 0— no ANI adaptation.	0-5	2

Parameter	Description	Range	Default
	- Level 1— Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. - Level 2— Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. Level 3— Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. - Level 4— Level 3 settings, and FIR immunity. At this level, the IAP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. - Level 5— The IAP completely disables PHY error reporting, improving performance by eliminating the time the IAP would spend on PHY processing. NOTE: Increasing the immunity level makes the IAP to lose a small amount of range.		
legacy-mode	Enables the IAPs to run the radio in non-802.11n mode.	—	Disabled
max-tx-power <power>	Configures the maximum transmit power value for the 2.4 GHz radio profile.	3-max	3 dBm
min-tx-power <power>	Configures the minimum transmit power value for the 2.4 GHz radio profile.	3-max	3 dBm
max-distance <count>	Configures the maximum distance between a client and anIAP or between a mesh point and a mesh portal in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies the default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km.	600-1000	0

Parameter	Description	Range	Default
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 IAPs 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 2.4 GHz radio profile:

```
(Instant AP) (config)# rf dot11g-radio-profile
(Instant AP) (RF dot11g Radio Profile)# beacon-interval 200
(Instant AP) (RF dot11g Radio Profile)# no legacy-mode
(Instant AP) (RF dot11g Radio Profile)# dot11h
(Instant AP) (RF dot11g Radio Profile)# interference-immunity 3
(Instant AP) (RF dot11g Radio Profile)# max-tx-power 33
(Instant AP) (RF dot11g Radio Profile)# min-tx-power 10
(Instant AP) (RF dot11g Radio Profile)# max-distance 600
(Instant AP) (RF dot11g Radio Profile)# csa-count 2
(Instant AP) (RF dot11g Radio Profile)# spectrum-monitor
(Instant AP) (RF dot11g Radio Profile)# end
```

Command History

Version	Description
Aruba Instant 6.4.3.4-4.2.1.0	The cell-size-reduction parameter has been added.
Aruba Instant 6.4.3.1-4.2	The max-tx-power and min-tx-power parameters were added.
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| 5.0| 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: 2.4—For 2.4 GHz band or 802.11g configuration 5—For 5 GHz and 802.11a configuration - all - For a mixed configuration of 2.4.GHz and 5 GHz. If you do not specify any value, by default both 5 GHz and 2.4 GHz bands are selected.	2.4, 5.0, all	all

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 AP) (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

rft

rft test profile

```
antenna-connectivity ip-addr <IP-addr> dest-mac <MAC-addr> phy {a|g}
ht-link-quality ip-addr <IP-addr> dest-mac <MAC-addr> phy {a|g} mcs <mcs>
link-quality ip-addr <IP-addr> dest-mac <MAC-addr> phy {a|g}
raw ip-addr <IP-addr> dest-mac <MAC-addr> phy {a|g}
```

Description

This command is used for RF troubleshooting.

Syntax

Parameter	Description
rft test profile	Allows you to run RF troubleshooting commands
antenna-connectivity	Allows you to test the antenna connectivity
ht-link-quality	Allows you to test the HT link quality.
link-quality	Allows you to test the quality of the link.
raw	Performs a raw test.
ip-addr <IP-addr>	Indicates the IP address of the IAP that performs the test.
dest-mac <MAC-addr>	Specifies MAC address of the client to be tested.
phy	Indicates the 802.11 type, either a or g.
mcs <mcs>	Indicates the type of Modulation Coding Scheme (MCS).

Usage Guidelines

This command can run predefined test profiles for antenna connectivity, link quality, or raw testing. Run these commands only under the supervision of an Aruba support representative.



In this release, this command is not available on IAP-224/225 and IAP-274/275 platforms.

Example

The following example shows the RF test command that can be run for testing the antenna connectivity:

```
(Instant AP)# rft test profile 192.0.2.1 dest-mac 00:1A:1E:00:00:00 phy a
```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms except IAP-224/225, and IAP-274/275	Privileged EXEC mode

routing-profile

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

Description

This command configures a routing profile for a specific destination address or destination subnet.

Syntax

Parameter	Description
routing-profile <profile>	Creates a routing profile for routing traffic into a specific destination address or destination subnet.
route	Configures route parameters.
<destination>	Configures the destination network that is reachable through the VPN tunnel.
<mask>	Specify the subnet mask of network that is reachable through the VPN tunnel.
<gateway>	Specify the gateway to which traffic must be routed. This IP address must be the controller IP address on which the VPN connection is terminated.
<metric>	This is an optional field and is configures a metric for the datapath route from source to destination. The default metric value is 15.
no...	Removes configuration settings for parameters under the routing-profile command.
no routing-profile	Removes the routing profile configuration.

Usage Guidelines

Use this command to configure a routing profile for a specific destination address or destination subnet.

Example

The following example configures a routing profile:

```
(Instant AP) (config)# routing-profile
(Instant AP) (Routing-profile)# route 192.0.1.0 255.255.255.0 192.0.2.0 15
(Instant AP) (Routing-profile)# end
(Instant AP)# commit apply
```

Command History

Version	Description
Aruba Instant 6.4.4.6-4.2.4.0	The optional metric parameter is added.
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.arubanetworks.com, OU=GT28470348, OU=See www.geotrust.com/resources/cps (c)11, OU=Domain Control Validated - QuickSSL(R) Premium, CN=securelogin.arubanetworks.com

Issued On :2011-05-11 01:22:10

Expires On :2017-08-11 04:40:59

Signed Using :SHA1

RSA Key size :2048 bits

The output of this command describes details such as the version, serial number, subject, issue date, expiry date, type of encryption, and RSA key information for the 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           :225
Build Time     :2015-12-18 23:46:04 PST
Version        :6.4.4.3-4.2.2.0_53034
Website        :http://www.arubanetworks.com
Legal          :Copyright (c) 2002-2015, Aruba Networks, an HP company.
```

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 associated with an IAP.

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 example shows the output displayed for the **show access-rule** command:

```
Access Rule Profiles
-----
Name
----
ethersphere-instant-wpa2
default_wired_port_profile
wired-instant
ethersphere-instant-cp
ethersphere-instant
ether-wired
11-android
```

On specifying a name of the SSID or the port profile along with the **show access-rule <name>** command, the list of access rules configured for the specified profile is displayed. The following example shows the output of this command:

```
Access Rules
-----
Dest IP  Dest Mask  Dest Match  Protocol (id:sport:eport)  Application  Action  Log  TOS
802.1P  Blacklist  App Throttle  (Up:Down)  Mirror  DisScan  ClassifyMedia
-----
--  -----
any          any          match        any          permit 192.0.2.7
255.255.255.255  match        h323-tcp          permit
any          any          match        any          permit 192.0.2.7
255.255.255.255  match        h323-udp          permit
any          any          match        dhcp          permit
any          any          match        app bebo
any          any          match        deny
any          any          match        app babylon
any          any          match        deny
```



```

any          any          match          games          deny          app baidu-hi-
any          any          match          games          deny          app bluejayfilms
deny
any          any          match          games          deny          appcategory gaming
deny
any          any          match          games          deny          webcategory shopping
deny
any          any          match          games          deny          webcategory abused-drugs
deny
any          any          match          games          deny          webcategory dead-sites
deny
any          any          match          games          deny          webreputation
any          any          match          games          deny          high-risk-sites deny

Blacklist App Throttle (Up:Down) Mirror DisScan ClassifyMedia
-----
Vlan Id      :0
ACL Captive Portal:disable
ACL ECP Profile :default
CALEA        :disable
Bandwidth Limit :upstream disable

```

The output of this command displays information about the access rule parameters configured for a specific wired or wireless profile. It indicates whether a particular type of traffic is allowed to a particular destination, and the service and protocol in use and if options such as logging and prioritizing traffic are enabled when the rule is triggered. If the DPI access rules are configured, it displays the list of rules configured to allow or deny access to certain applications, application categories, web categories, and websites based on their reputation score.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 access-rule-all

show access-rule-all

Description

This command displays the details of the access rules configured for all wired and wireless profiles on the IAP.

Usage Guidelines

Use this command to view information access rules configured for all wired and wireless profiles on the IAP.

Example

The following example shows the partial output of the **show access-rule-all** command:

```
Access Rule Name :default_wired_port_profile
In Use :Yes
Access Rules
-----
Dest IP   Dest Mask  Dest Match  Protocol (id:sport:eport)  Application  Action  Log  TOS
802.1P   Blacklist  App Throttle (Up:Down)  Mirror  DisScan  ClassifyMedia
-----
--
any any match any permit
masterip 0.0.0.0 match http permit
masterip 0.0.0.0 match 6:4343:4343 permit
any any match dhcp permit

Vlan Id      :0
ACL Captive Portal:disable
ACL ECP Profile :default
CALEA        :disable
Bandwidth Limit :downstream disable upstream disable
Access Rule Name :NewRole17
In Use       :No
Access Rules
-----
Access Rules
-----
Dest IP   Dest Mask  Dest Match  Protocol (id:sport:eport)  Application  Action  Log  TOS
802.1P   Blacklist  App Throttle (Up:Down)  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
ACL ECP Profile :default
CALEA        :disable
Bandwidth Limit :downstream disable upstream disable
Access Rule Name :NewRole18
In Use       :No
```

The output of this command includes the following parameters:

Parameter	Description
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 acl

```
show acl {domains}
```

Description

This command displays the Access Control List (ACL) configuration details.

Syntax

Parameter	Description
domains	Displays the domains configured with an access control list.

Usage Guidelines

Use this command to view the ACL configuration details.

Example

The following example shows the output of the **show acl** command:

```
(Instant AP) # show acl
role-domain
-----
role-domain inused
-----
d8:c7:c8:c4:42:98#
```

The output of this command displays information about the role-domain.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show activate status

show activate status

Description

This command displays the status of the Aruba Activate cloud-based services.

Usage Guidelines

Use this command to view the provisioning status of Aruba Activate cloud-based services.

Example

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

```
Activate Server      :device.arubanetworks.com
Activate Status     :fail-prov-no-rule
IAP MAC Address     :18:64:72:c8:1e:30
IAP Serial Number   :CT0026395
Cloud Activation Key :II6JSV1X
```

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 airgroup

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

Description

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

Syntax

Parameter	Description
blocked-queries [dlna mdns]	Displays blocked queries if any.
blocked-service-id [dlna mdns]	Displays blocked services and service IDs if any.
cache <MAC-address> cache entries [dlna mdns]	Displays AirGroup cache details for a specific 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 [dlna mdns verbose]	Displays AirGroup server details.
status	Indicates the AirGroup feature activation status.
swarm-info	Displays information about the AirGroup cluster.
users [dlna mdns verbose]	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
----
-----
_airplay._tcp.local                     PTR       IN     4500  10.16.94.236 3696.00
Tue May 13 19:32:11 2014
_raop._tcp.local                        PTR       IN     4500  10.16.94.236 3794.31
Tue May 13 19:32:11 2014
BLR-DPARASAR-T4._airplay._tcp.local    SRV/NBSTAT IN     120   10.16.94.236 311.38
Tue May 13 19:32:11 2014
2577037A8680@BLR-DPARASAR-T4._raop._tcp.local SRV/NBSTAT IN     120   10.16.94.236 134.14
Tue May 13 19:32:11 2014
BLR-DPARASAR-T430S.local                A         IN     120   10.16.94.236 255.07
Tue May 13 19:32:11 2014
BLR-DPARASAR-T430S.local                AAAA      IN     120   10.16.94.236 393.69
Tue May 13 19:32:11 2014
BLR-DPARASAR-T4._airplay._tcp.local    TXT       IN     4500  10.16.94.236 3784.51
Tue May 13 19:32:11 2014
2577037A8680@BLR-DPARASAR-T4._raop._tcp.local TXT       IN     4500  10.16.94.236 3840.38
Tue May 13 19:32:11 2014
urn:schemas-upnp-org:device:MediaRenderer:1 N/A       N/A    1800  10.16.94.236 N/A
Tue May 13 19:33:51 2014
```

The output of this command includes the following information:

Column	Description
Name	Indicates the name of AirGroup server.
Type	Indicates the AirGroup model.
Class	Indicates the class of the mDNS record.
TTL	Indicates the duration after which the cache entries expire.

Column	Description
Origin	Indicates the origin IP address of the cache entries.
Expiry	Indicates the expiration details.
Last Update	Indicates when the entries were last updated.

show airgroup cppm auth server non-coa-only

The following output is displayed for the **show airgroup cppm auth server non-coa-only** command:

```
All Airgroup Non-CoA-only Servers known to MDNS
-----
Server IP-Address Port timeout rfc3576 rfc3576-only rfc3576-port
-----
test 192.0.2.0 1812 5 Disabled Disabled 5999
test123 192.0.2.1 1812 5 Disabled Disabled 5999
```

show airgroup cppm auth server coa-capable

The following output is displayed for the **show airgroup cppm auth server coa-capable** command:

```
All Airgroup CoA-capable Servers known to MDNS
-----
Server IP-Address Port timeout rfc3576 rfc3576-only rfc3576-port
-----
server1 192.0.1.1 1812 5 Enabled Enabled 5999
```

show airgroup cppm server

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

```
CPPM Servers
-----
Server IP-Address Port timeout rfc3576 rfc3576-only rfc3576-port
-----
test 192.0.2.0 1812 5 Disabled Disabled 5999
test123 192.0.2.1 1812 5 Disabled Disabled 5999
```

The output of these commands provide the following information:

Column	Description
Server	Indicates the name of the 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.
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 IAP name.
shared location-id AP-FQLN	Indicates the shared location ID associated with the fully qualified domain name of the IAP.
shared location-id AP-group	Indicates the shared location ID associated with the IAP group.
shared user-list	Indicates the list of shared users.
shared role-list	Indicates the list of shared user roles.
Num CPPM Entries	Indicates the number of 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 :0x7f
My ip address :192.168.10.251
My VC address :192.168.10.2
Peer VC address :192.168.10.2
Peer VC address :192.168.20.2
Peer VC address :192.168.30.2
Peer VC address :192.168.40.2
Peer VC address :0.0.0.0
Peer VC address :0.0.0.0
Peer VC address :0.0.0.0
Peer VC address :0.0.0.0
AirGroup Debug Statistics
-----
Key Value
---
network cache init counter 2(2)
mdns apdb init counter 7(7)
mdns apdb destroy counter 1(1)
user timed out 1(1)
airgroup restore count 1(1)
mdns mac move counter 4(4)
mdns master to vc hello rx 2060(2060)
mdns slave to slave hello rx 8240(8240)
mdns ap to ap mac sync resp rx 57(57)
mdns master to vc mac req rx 1580(1580)
swarm update counter rx 1(1)
mdns recieved valid swarm packet 11978(11978)
mdns recieved dlina pkt from device 177704(177704)
mdns partial hello tx 2059(2059)
mdns ap update tx 80(80)
mdns master to vc mac sync resp tx 232(232)
mdns ap to ap mac sync resp tx 1348(1348)
dropped init not done tx 6(6)
master to vc hello tx 2059(2059)
master to my swarm hello tx 2354(2354)
mdns ap to swarm hello tx 4118(4118)
mdns slave to slave mac sync req tx 57(57)
mdns total pkt sent to asap tx 112563(112563)
hello ap verification fail count 1(1)

```

The output of this command provides the following information:

Column	Description
Airgroup slave status	Indicates the AirGroup configuration status on the slave 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.
Key and Value	Displays details of AirGroup counters.

show airgroup internal-state statistics

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

```

Time: Fri May 16 09:30:22 2014
RADIUS Client Messages
-----

```

Type	Sent Since Last Read	Sent Total	Recv Since Last Read	Recv Total
Auth Req/Resp	0	0	0	0
RFC3576	N/A	N/A	0	0
CPPM Device-Entry Added	N/A	N/A	0	0
CPPM Device-Entry Deleted	N/A	N/A	0	0
Internal MDNS Statistics				
Functionality	Hit Count Since Last Read	Hit Count Total	Average Time in	
microsec (since last read)	Average Time in microsec (alltime)			
Response - Cache Update	0	0	0	0
Response	0	0	0	0
Query - prepare records + Policy	0	0	0	0
Query - Policy	0	0	0	0
Query - resp pkt gen & send	0	0	0	0
Query - Response packet send	0	0	0	0
Query	0	0	0	0
Internal DLNA Statistics				
Functionality	Hit Count Since Last Read	Hit Count Total	Average Time in	
microsec (since last read)	Average Time in microsec (alltime)			
Response - Cache Update	0	0	0	0
Response	0	0	0	0
Query - prepare records + Policy	0	0	0	0
Query - Policy	0	0	0	0
Query - resp pkt gen & send	0	0	0	0
Query - Response packet send	0	0	0	0
Query	0	0	0	0

The output of this command displays information about queries and responses, and RADIUS client messages.

show airgroup servers

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

```
AirGroup Servers
-----
MAC IP Type Host Name Service VLAN Wired/Wireless Role Group Username AP-Name
--- --
Num Servers: 0, Max Servers: 80.
```

The output of this command provides the following information:

Column	Description
MAC	Indicates the MAC address of the AirGroup servers.
IP	Indicates the IP address of the AirGroup servers.
Type	Indicates the type of server.
Hostname	Indicates the hostname of the AirGroup servers.
Service	Indicates if AirGroup services such as AirPlay or AirPrint are configured.
VLAN	Displays VLAN details of the AirGroup servers.
Wired/Wireless	Displays if the AirGroup server is connected to a wired or wireless interface.
Role	Displays the user role details.
Group	Displays the server group.
Username	Displays the username details.
AP-name	Displays the name of the IAP.
Num servers	Displays the total number of servers.
Max Servers	Displays the maximum number of servers that are supported.

show airgroup status

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

```
AirGroup Feature
-----
Status
-----
Disabled
AirGroup- MDNS Feature
-----
Status
-----
Disabled
AirGroup- DLNA Feature
-----
Status
-----
Disabled
AirGroup Multi Swarm
-----
Status
-----
Disabled
AirGroup Guest Multicast
-----
Status
-----
Disabled
CPPM Parameters
```

```

-----
Parameter Value
-----
CPPM Enforce Registration Disabled
CPPM Server query interval 10 Hours
CPPM Server dead time 100 Seconds
AirGroup Service Information
-----
Service Status
-----
airplay Disabled
airprint Disabled
itunes Disabled
remotemgmt Disabled
sharing Disabled
chat Disabled
Chromecast Disabled
DLNA Media Disabled
DLNA Print Disabled
allowall Disabled

```

The output of this command provides the following information:

Column	Description
Airgroup feature status	Indicates if the AirGroup feature such as DLNA or MDNS support is enabled.
AirGroup Multi Swarm status	Indicates if the inter cluster mobility is enabled.
AirGroup Guest Multicast	Indicates if a guest VLAN is used for Bonjour services.
CPPM Parameters	Displays 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.
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 6.4.0.2-4.1	This command was modified.
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 airgroupservice

```
show airgroupservice [disallow {role| vlan}]
```

Description

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

Syntax

Parameter	Description
<code>show airgroupservice</code>	Displays a summary of the configuration details for AirGroup services.
<code>disallow {role vlan}</code>	Displays the user roles or VLANs that are restricted from accessing AirGroup services. When the access to AirGroup services is restricted, the clients that are assigned with a specific role or VLAN will not be able to use the AirGroup service.

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 status Disallowed-Role Disallowed-VLAN ID
-----
airplay AirPlay Disabled _airp lay._tcp
_appl etv-v2._tcp
airprint AirPrint Disabled _ipp._tcp
_pdl- datastream._tcp
_prin ter._tcp
_scan ner._tcp
_univ ersal._sub._ipp._tcp
_univ ersal._sub._ipps._tcp
_prin ter._sub._http._tcp
_http ._tcp
_http -alt._tcp
_ipp- tls._tcp
_fax- ipp._tcp
_riou sbprint._tcp
_cups ._sub._ipp._tcp
_cups ._sub._fax-ipp._tcp
_ica- networking._tcp
_ptp._tcp
_cano n-bjnp1._tcp
_ipps ._tcp
_ica- networking2._tcp
itunes iTunes Disabled _home -sharing._tcp
_appl e-mobdev._tcp
_daap ._tcp
_dacp ._tcp
remotemgmt Remote management Disabled _ssh._tcp
_sftp -ssh._tcp
_ftp._tcp
```

```

_teln et._tcp
_rfb._tcp
_net- assistant._tcp
AirGroupService Details
-----
Service Description status Disallowed-Role Disallowed-VLAN ID
-----
sharing Sharing Disabled _odi sk._tcp
_afp overtcp._tcp
_xgr id._tcp
chat Chat Disabled _pre sence._tcp
Chromecast Chromecast Disabled urn: dial-multiscreen-org:service:dial:1
urn: dial-multiscreen-org:device:dial:1
DLNA Media Media Disabled urn: schemas-upnp-org:device:MediaServer:1
urn: schemas-upnp-org:device:MediaServer:2
urn: schemas-upnp-org:device:MediaServer:3
urn: schemas-upnp-org:device:MediaServer:4
urn: schemas-upnp-org:device:MediaRenderer:1
urn: schemas-upnp-org:device:MediaRenderer:2
urn: schemas-upnp-org:device:MediaRenderer:3
urn: schemas-upnp-org:device:MediaPlayer:1
DLNA Print Print Disabled urn: schemas-upnp-org:device:Printer:1
urn: schemas-upnp-org:service:PrintBasic:1
urn: schemas-upnp-org:service:PrintEnhanced:1
allowall Remaining-Services Disabled
Num Services:10
Num Service-ID:49

```

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

```

airplay
-----
default_wired_port_profile
port
airprint
-----
default_wired_port_profile
port

```

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

```

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

```


Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 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 AP)# show airgroupservice-ids airplay
airplay
-----
Service ids
-----
 _airplay._tcp
 _raop._tcp
 _appletv-v2._tcp
```

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

Command History

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 AP)# show ale config
ALE Config
-----
Type                Value
----                -
ale-server          AleServer1
ale-report-interval 60
```

The output of this command displays the ALE server details and the reporting interval at which the VC sends data to the ALE server.

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

```
(Instant AP)# show ale status
ALE Status
-----
Type                Value
----                -
ale login status    False
ale login status code
ale fail times      0
ale request state    Idle
```

The output of this command displays information about the ALE server status and data request status.

Command History

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 stats

show ale stats

Description

This command displays the number of times a specific message type such as AppRF statistics, and uplink bandwidth report was sent to the ALE server.

Usage Guidelines

Use this command to view the ALE statistics.

Example

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

```
(Instant AP)# show ale stats
ALE Stats
-----
Type                Value
----                -
VC package          0
RSSI package        0
APPRF package       0
URLv package        0
STATE package       0
STAT package        0
UPLINK BW package   0
Total               0
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2.0.0	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.

```
Client Alerts
-----
Timestamp Type MAC Address Description Access Point
-----
10:45:42 5 80:86:f2:85:51:6f 11 rno04-api-2
10:54:15 5 bc:3b:af:3d:32:bf 11 rno04-api-4
```

The output of this command provides the following information:

Parameter	Description
Timestamp	Displays the time at which the client alert was recorded.
Type	Displays the numeric value to indicate the type of event that triggered the alert. For more information, see .
MAC Address	Displays the MAC address of the client that caused the alert.
Description	Displays the description code for the alert. For example, Type 5 and Description 11 indicates that the DHCP request has timed out and the client did not receive a response to its DHCP request in time. For more information, see .
Access Point	Displays the IP address of the IAP to which the client is connected.

Table 11: *Client Alert —Type and Description Codes*

Type code	Description Code	Detailed Description
1	1	Internal error The IAP has encountered an internal error for this client.
	2	Unknown SSID in association request. The IAP cannot allow this client to associate because the association request received contains an unknown SSID.
	3	Mismatched authentication/encryption setting The IAP cannot allow this client to associate because its authentication or encryption settings do not match the configuration of the IAP.
	4	Unsupported 802.11 rate The IAP cannot allow this client to associate because it does not support the 802.11 rate requested by this client.
	5	Maximum capacity reached on IAP The IAP has reached maximum capacity and cannot accommodate any more clients.
2	6	Invalid MAC Address The IAP cannot authenticate this client because its MAC address is not valid.
3	7	Client blocked due to repeated authentication failures The IAP is temporarily blocking the 802.1x authentication request from this client because the credentials provided have been rejected by the RADIUS server too many times.
	8	Authentication server timeout The IAP cannot authenticate this client using 802.1x because the RADIUS server did not respond to the authentication request. If the IAP is using the internal RADIUS server, recommend checking the related configuration as well as the installed certificate and passphrase
	9	RADIUS server authentication failure The IAP cannot authenticate this client using 802.1x because the RADIUS server rejected the authentication credentials (password, etc) provided by the client.

Table 11: *Client Alert —Type and Description Codes*

Type code	Description Code	Detailed Description
4	10	Integrity check failure in encrypted message The IAP cannot receive data from this client because the integrity check of the received message (MIC) has failed. Recommend checking the encryption setting on the client and on the IAP.
5	11	DHCP request timed out This client did not receive a response to its DHCP request in time. Recommend checking the status of the DHCP server in the network.
10	12	Wrong Client VLAN VLAN mismatch between the IAP and upstream device. Upstream device can be upstream switch or radius 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 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
vocera Enabled
```

The output of this command displays if the ALG protocols such as Skinny Call Control Protocol (SCCP), Session Initiation Protocol (SIP), 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 a-max-clients

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

Description

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

Syntax

Parameter	Description	Range
<ssid_profile>	Denotes the SSID profile for which the maximum clients limit is to be configured.	—

Usage Guidelines

Use this command to view the maximum number of clients allowed for a 5 GHz radio channel SSID profile.

Example

The following example shows the output of the **show a-max-clients** command:

```
(Instant AP)# show a-max-clients ssid4  
a-max-clients: 35
```

The output of this command displays the maximum number of clients allowed to connect to the SSID profile.

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All Platforms	Privileged EXEC mode

show all monitor

show all monitor active-laser-beams

Description

This command shows information for Aruba Instant Air Monitors.

Usage Guidelines

Use this command to view the information on Aruba Instant Air Monitors.

Syntax

Parameter	Description
active-laser-beams	Show active laser beam generators. The output of this command shows a list of all IAPs that are actively performing policy enforcement containment such as rogue containment. This command can tell us which IAP is sending out deauthorization frames, although it does not specify which IAP is being contained.

Example

The following example shows the output of **show all monitor** command.

```
Swarm Active Laser Beam Sources
-----
bssid channel rssi ap name lms ip master ip inactive time reported by
-----
```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show amp-audit

show amp-audit

Description

This command displays the set of configurations on the AirWave Management Platform.

Usage Guidelines

Use this command to view the AMP related configurations.

Example

The following example shows the output of the **show amp-audit** command:

```
rule any any match any any any deny
wlan access-rule ssid1
    index 3
    rule any any match any any any deny
hotspot anqp-nai-realm-profile "name1"
    enable
    nai-realm-name ""
    nai-realm-eap-method eap-ttls
    nai-realm-auth-id-1 non-eap-inner-auth
    nai-realm-auth-value-1 mschapv2
    nai-realm-auth-id-2 credential
    nai-realm-auth-value-2 uname-password
    nai-realm-encoding utf8
    no nai-home-realm
hotspot anqp-nai-realm-profile "nr1"
    enable
    nai-realm-name "name1"
    nai-realm-eap-method eap-sim
    nai-realm-auth-id-1 non-eap-inner-auth
    nai-realm-auth-value-1 mschapv2
    nai-realm-auth-id-2 credential
    nai-realm-auth-value-2 uname-password
    nai-realm-encoding utf8
    nai-home-realm
hotspot anqp-venue-name-profile "Vn1"
    enable
    venue-group business
    venue-type research-and-dev-facility
    venue-lang-code en
    venue-name ""
hotspot anqp-venue-name-profile "vn1"
    enable
    venue-group business
    venue-type research-and-dev-facility
    venue-lang-code eng
    venue-name "vn1"
hotspot anqp-nwk-auth-profile "na1"
    enable
    nwk-auth-type accept-term-and-cond
    url "www.nwkauth.com"
hotspot anqp-roam-cons-profile "rc1"
    enable
    roam-cons-oi-len 3
    roam-cons-oi "888888"
hotspot anqp-3gpp-profile "3g"
    enable
```

```

3gpp-plmn1 "40486"
3gpp-plmn2 ""
3gpp-plmn3 ""
3gpp-plmn4 ""
3gpp-plmn5 ""
3gpp-plmn6 ""
hotspot anqp-ip-addr-avail-profile "ip1"
    enable
    ipv4-addr-avail
    no ipv6-addr-avail
    hotspot anqp-domain-name-profile "dn1"
    enable
    domain-name "DomainName"
hotspot h2qp-oper-name-profile "on1"
    enable
    op-lang-code eng
    op-fr-name "FriendlyName"
hotspot hs-profile "hs1"
    enable
    comeback-mode
    no asra
    no internet
    pame-bi
    group-frame-block
    p2p-dev-mgmt
    no p2p-cross-connect
    addtl-roam-cons-ois 0
    gas-comeback-delay 10
    query-response-length-limit 20
    access-network-type chargeable-public
    venue-group business
    venue-type research-and-dev-facility
    roam-cons-len-1 3
    roam-cons-oi-1 "123456"
    roam-cons-len-2 3
    roam-cons-oi-2 "223355"
    roam-cons-len-3 0
    roam-cons-oi-3 ""
    advertisement-profile anqp-nai-realm "nr1"
wlan ssid-profile test
    enable
    index 0
    type employee
    essid instant
    opmode opensystem
    max-authentication-failures 0
    rf-band all
    captive-portal disable
    dtim-period 1
    inactivity-timeout 1000
    broadcast-filter none
    dmo-channel-utilization-threshold 90
    local-probe-req-thresh 0
    max-clients-threshold 64
    dot11k
    dot11v
wlan ssid-profile ssid1
    enable
    index 1
    type employee
    essid hsProf
    opmode wpa2-aes

```

```

max-authentication-failures 0
vlan 200
rf-band all
captive-portal disable
mac-authentication
l2-auth-failthrough
dtim-period 1
inactivity-timeout 1000
broadcast-filter none
radius-accounting
blacklist
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64
hotspot-profile "hs1"
auth-survivability cache-time-out 24
wlan external-captive-portal
    server localhost
    port 80
    url "/"
    auth-text "Authenticated"
    auto-whitelist-disable
    https
blacklist-time 3600
auth-failure-blacklist-time 3600
ids
    wireless-containment none
wired-port-profile wired-instant
switchport-mode access
allowed-vlan all
native-vlan guest
no shutdown
access-rule-name wired-instant
speed auto
duplex auto
no poe
type guest
captive-portal disable
no dot1x
wired-port-profile default_wired_port_profile
    switchport-mode trunk
    allowed-vlan all
    native-vlan 1
    shutdown
    access-rule-name default_wired_port_profile
    speed auto
    duplex full
    no poe
    type employee
    captive-portal disable
    no dot1x
enet0-port-profile default_wired_port_profile
uplink
    preemption
    enforce none
    failover-internet-pkt-lost-cnt 10
    failover-internet-pkt-send-freq 30
    failover-vpn-timeout 180
airgroup
    disable
airgroupservice airplay
    disable

```

```

description AirPlay
airgroupservice airprint
disable
description AirPrint
per-ap-settings d8:c7:c8:c4:42:98
hostname d8:c7:c8:c4:42:98
ip-address 10.17.161.254 255.255.255.0 10.17.161.1 10.13.6.110 ""
swarm-mode cluster
wifi0-mode access
wifi1-mode access
g-channel 0 0
a-channel 0 0
uplink-vlan 0
g-external-antenna 0
a-external-antenna 0

```

The output of this command provides the following information:

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap-alert

show ap-alert <count>

Description

This command displays all the alerts received for the specified IAPs.

Usage Guidelines

Use this command to check all the alerts received for all the IAPs specified.

Example

The following example shows the output of **show ap-alert** command.

```
AP Alerts
-----
Timestamp Type MAC Address IP Address Description
-----
```

The output of this command includes the following information:

Column	Description
Timestamp	Indicates the time at which the alert was received.
Type	Indicates the type of alert received for the IAP.
MAC Address	Indicates the MAC address of the IAP clients.
IP Address	Indicates the IP address associated with the IAP.
Description	Displays a brief description of the alert received.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 IAP parameters such as the type of antenna used by an IAP. 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
lACP_mode:enable
ipaddr:10.17.161.254
netmask:255.255.255.0
gatewayip:10.17.161.1
dnsip:10.13.6.110
wifi0_mode:spectrum
wifi1_mode:spectrum
uplink_vlan: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 6.4.4.4-4.2.3	The output of this command was modified to display the static LACP configuration.
Aruba Instant 6.4.3.1-4.2	The output of this command was modified to include fields such as IP address, netmask, gateway IP address, DNS IP address, IAP radio modes, and uplink VLAN configuration.
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 ap1x

```
show ap1x {config|debug-logs|status}  
no...
```

Description

This command shows the status and the details of 802.1X supplicant configuration on an IAP.

Syntax

Parameter	Description
config	Shows the 802.1X supplicant configuration details.
debug-logs	Displays debug logs pertaining to the 802.1X supplicant configuration.
status	Shows the status of the 802.1X supplicant configuration.

Usage Guidelines

Use this command to view the 802.1X supplicant configuration details on an IAP.

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap1xcert

show ap1xcert

Description

This command displays the details of certificates used for 802.1X authentication with wired ports.

Usage Guidelines

Use this command to view information server and CA certificates used for validating the authentication server to which IAP authenticates as a 802.1X supplicant.

Example

The following example shows the output of the **show ap1xcert** command:

Current ap1x CA Certificate:

```
Version      :3
Serial Number :AB:C1:1E:06:77:69:20:4F
Issuer       :/C=CN/ST=Beijing/O=Aruba Networks/O=an HP company/OU=Aruba Instant/CN=Feng Ding
Subject      :/C=CN/ST=Beijing/O=Aruba Networks/O=an HP company/OU=Aruba Instant/CN=Feng Ding
Issued On    :Jan 26 08:48:16 2016 GMT
Expires On   :Jan 23 08:48:16 2026 GMT
Signed Using :SHA1-RSA
RSA Key size :2048 bits
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3.0	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.

Column	Description
Type	Displays the IAP model.
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	Displays the counters that indicate the number of scanning rejects due to voice traffic.

Column	Description
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	

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

Description

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

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 for the IAP-215 device:

```
Allowed Channels for AP Type 215 Country Code US
-----
PHY Type                Allowed Channels
-----
802.11g (indoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)         36 40 44 48 149 153 157 161 165
802.11g (outdoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)        149 153 157 161 165
802.11g 40MHz (indoor)   1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)   36-40 44-48 149-153 157-161
802.11g 40MHz (outdoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)  149-153 157-161
802.11a 80MHz (indoor)   36-48 149-161
802.11a 80MHz (outdoor)  149-161
802.11a (DFS)
```

The output of this command includes the following information:

Parameter	Description
PHY Type	Indicates the PHY type.
Allowed Channels	Displays the list of allowed channels for a specific regulatory domain.

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	The <country-code> parameter was removed.
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

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.

Usage Guidelines

Use this command to view the maximum EIRP settings for an 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** 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 52 56 60 64 100 104 108 112 116 120 124
128 132 136 140 149 153 157 161 165
-----
b 20 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 24 24 24 24 22 22 22 22 * * * 22 22
22 23 23 23 23 23
HT 20 22 22 22 22 22 22 22 22 22 22 22 22 * * * 21 21 21 21 24 24 24 24 22 22 22 22 22 * * * 22
22 22 22 23 24 24 24
HT 40 19 19 20 21 22 23 22 22 22 21 21 * * * 20 20 20 20 23 23 23 23 22 22 22 22 * * * * 22 22
22 22 22 22 20 17
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	The <country> parameter was removed.
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.

Column	Description
Shaping table	Displays information on the ARM configuration details for the clients associated with the IAP.
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 threshold exceeded, INV: Invalid Channel, G: Rogue AP Containment, M: Empty Channel, P+: Increase Power, P-: Decrease Power, 40INT: 40MHZ intol detected on 2.4G, NO40INT: 40MHz intol cleared on 2.4G, OFF: Turn off Radio, ON: Turn on Radio

The output of this command includes the following information:

Column	Description
Time of change	Indicates the timestamp of the channel changes for each interface.
Old Channel	Displays the channel number used by the IAP before the ARM change.

Column	Description
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.
essid	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	97	1/0/0/0/99	0/0 (0)	25/28//0/0 (53)
40	0	0	0	97	1/0/0/0/99	0/0 (0)	52/0//0/0 (52)
44	0	0	0	97	1/0/0/0/99	0/0 (0)	19/41//0/0 (60)
48	0	0	0	97	1/0/0/0/99	0/0 (0)	40/0//0/0 (40)
52	0	0	0	97	1/0/0/0/99	0/0 (0)	0/13//0/0 (13)
56	0	0	0	97	1/0/0/0/99	0/0 (0)	0/0//0/0 (0)
60	0	0	0	97	1/0/0/0/99	0/0 (0)	0/0//0/0 (0)
64	0	0	0	97	1/0/0/0/99	0/0 (0)	0/0//0/0 (0)
100	0	0	0	97	1/0/0/0/99	0/0 (0)	0/0//0/0 (0)
104	0	0	0	97	1/0/0/0/99	0/0 (0)	0/0//0/0 (0)
108	0	0	0	97	1/0/0/0/99	0/0 (0)	0/0//0/0 (0)
112	0	0	0	97	1/0/0/0/99	0/0 (0)	0/18//0/0 (18)
116	0	0	0	97	1/0/0/0/99	10/0 (10)	103/0//0/0 (103)
120	0	0	0	97	1/0/0/0/99	0/0 (0)	27/18//0/0 (45)
124	0	0	0	97	1/0/0/0/99	0/0 (0)	0/0//0/0 (0)
128	0	0	0	97	1/0/0/0/99	0/0 (0)	0/0//0/0 (0)
1	0	0	0	97	6/4/2/0/100	12/0 (12)	133/0//0/0 (133)

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

HT Channel Summary

channel_pair Pairwise_intf_index

116-120 148
100-104 0
124-128 0
108-112 18

Interface Name :wifi0
Current ARM Assignment :100+/6
Covered channels a/g :2/0
Free channels a/g :6/0
Last check channel/pwr :3m:17s/5m:4s
Last change channel/pwr :1h:18m:38s/1h:18m:38s
Next Check channel/pwr :4m:21s/1m:6s
Assignment Mode :Single Band
Interface Name :wifi1
Current ARM Assignment :1/3
Covered channels a/g :0/1
Free channels a/g :0/0
ARM Edge State :disable
Last check channel/pwr :3m:12s/5m:13s
Last change channel/pwr :3h:16m:53s/1h:32m:33s
Next Check channel/pwr :3m:17s/10s
Assignment Mode :Single Band

Channel quality history:wifi0

36 :Q: 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 100 100 100 100
100 100
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0
:N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97
97 97
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0

```

:U: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0
0 0
40 :Q: 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99
99 99
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0
:N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97
97 97
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0
:U: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1
44 :Q: 99 99 99 99 99 99 99 100 100 100 100 99 99 99 100 99 99 99
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
:N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
:U: 1 1 1 1 1 1 1 0 0 0 0 1 1 1 0 1 1 1
48 :Q: 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99
99 99
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0
:N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97
97 97
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0
:U: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1
52 :Q: 99 99 99 99 100 100 100 100 100 100 99 100 100 0 0 0
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
:N: 97 97 97 97 97 97 97 97 97 97 97 97 97 0 * 0 * 0
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 100 100 100
:U: 1 1 1 1 0 0 0 0 0 0 1 0 0 0 0 0
56 :Q: 99 99 99 99 99 99 100 100 100 99 99 99 99
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0
:N: 97 97 97 97 97 97 97 97 97 97 97 97 97
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0
:U: 1 1 1 1 1 1 0 0 0 1 1 1 1
60 :Q: 99 99 99 99 99 100 100 100 99 100 100 99 99 100
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
:N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0
:U: 1 1 1 1 1 0 0 0 1 0 0 1 1 0
64 :Q: 99 99 99 99 99 100 100 100 100 100 100 100 100
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
:N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0
:U: 1 1 1 1 1 0 0 0 0 0 0 0 0
100:Q: 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99
99 99
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0
:N: 97 97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97
*97 *97
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0
:U: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1
:R: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0
104:Q: 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 100 100 100 100
100 100
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0

```

```

:N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97
    97 97
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    0 0
:U: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0
    0 0
108:Q: 99 99 99 99 99 99 99 99 99 99 100 100 99 100
     :c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97
     :s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :U: 1 1 1 1 1 1 1 1 1 1 0 0 1 0
112:Q: 99 99 99 99 99 99 99 99 99 99 100 99 99 100
     :c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97
     :s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :U: 1 1 1 1 1 1 1 1 1 1 0 1 1 0
116:Q: 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99
     :c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97
     :s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :U: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
120:Q: 99 99 99 99 99 99 99 99 99 99 99 100 100 100 100 100 99 100 100 100 99 100
     :c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97 97
     :s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :U: 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 1 0 0 0 1 0
124:Q: 99 99 99 99 99 99 99 99 99 99 100 100 100 100 0
     :c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :N: 97 97 97 97 97 97 97 97 97 97 97 97 97 0
     :s: 0 0 0 0 0 0 0 0 0 0 0 0 0 100
     :U: 1 1 1 1 1 1 1 1 1 0 0 0 0 0
128:Q: 99 99 99 100 100 100 100 99 99 99 99 99 99 100
     :c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :N: 97 97 97 97 97 97 97 97 97 97 97 97 97 97
     :s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     :U: 1 1 1 0 0 0 0 1 1 1 1 1 1 0

```

Channel quality history:wifi1

```

1:Q: 99 98 100 100 100 100 99 100 99 99 99 100 99 100 100 100 99 98 100 100 99 99
    100 99
:c: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    0 0
:N: *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97
    *97 *97
:s: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    0 0
:U: 1 2 0 0 0 0 1 0 1 1 1 0 1 0 0 0 1 2 0 0 1 1
    0 1
:R: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    0 0

```

The output of this command includes the following information:

Column	Description
channel	Displays the list of channels enabled on 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 IAPs on a specified 802.11 channel, and "y" is the weighted calculation of the IAPs SNR detected by the neighboring IAPs 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: • Metric value "a" is the channel interference the IAP sees on its selected channel. • Metric value "b" is the interference the IAP sees on the adjacent channel. • Metric value "c" is the channel interference the neighbors of the IAP see on the selected channel. • Metric value "d" is the interference the neighbors of the IAP see on the adjacent channel. • To calculate the total Interference Index for a channel add "a+b+c+d".
channel_pair	Displays the list of paired channels.
Pairwise_intf_index	Displays the pairwise interference index.
Interface Name	Displays the interface name.
Current ARM Assignment	Displays the current ARM assignment details.
Covered channels	Displays the number of channels being used by the 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.

Column	Description
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.
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 IAP 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 client, 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 IAP 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 y if the IAP is configured for 802.11 authorization frame types. Otherwise, it displays an n .
assoc	Displays the status of user association. Indicates y if the IAP is configured for 802.11 association frame types. Otherwise, it displays an n .
aid	Indicates 802.11 association ID. A client receives a unique 802.11 association ID when it associates to an 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).

Column	Description
vlan-id	Indicates the VLAN ID associated with the IAP.
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 the Basic Service Set (BSS) of an IAP.

Usage Guidelines

The output of the show ap bss-table command shows the Aruba IAP BSS table for all IAPs. To filter this information and view BSS table data for an individual IAP or a specific port and slot number, include the ap-name, bssid, essid, ip-addr or port keywords.

Example

The following example shows the output of **show ap bss-table** command:

```
Aruba AP BSS Table
-----
bss ess port ip phy type ch/EIRP/max-EIRP cur-cl ap 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:c8: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 d8: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:c8: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 IAP Basic Service Set Identifier (BSSID). This is usually the MAC address of the IAP.
ess	Displays the IAP Extended Service Set Identifier (ESSID).
port	Displays port used by the IAP.
ip	Displays the IP address of an IAP.
phy	Displays an IAP radio type. Possible values are: - a—802.11a - a-HT—802.11a high throughput - g—802.11g - g-HT—802.11g high throughput
type	Shows whether the IAP is working as an access point or air monitor (AM).

Column	Description
ch/EIRP/max-EIRP	Displays the radio channel used by the IAP/current effective Isotropic Radiated Power (EIRP) /maximum EIRP.
cur	Displays the current number of clients 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 cacert

show ap cacert

Description

This command displays the details of the CA certificate on the IAP.

Usage Guidelines

Use this command to view details of the CA certificate uploaded on the IAP.

Example

The following example shows the certificate details displayed in the output of the **show ap cacert** command:

```
Local CA Certificates:
Version          :3
Serial Number    :16:90:C3:29:B6:78:06:07:51:1F:05:B0:34:48:46:CB
Issuer           :/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA
Root
Subject          :/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO High-
Assurance Secure Server CA
Issued On        :Apr 16 00:00:00 2010 GMT
Expires On       :May 30 10:48:38 2020 GMT
Signed Using     :SHA1-RSA
RSA Key size     :2048 bits
Version          :3
Serial Number    :01
Issuer           :/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA
Root
Subject          :/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA
Root
Issued On        :May 30 10:48:38 2000 GMT
Expires On       :May 30 10:48:38 2020 GMT
Signed Using     :SHA1-RSA
RSA Key size     :2048 bits
Version          :3
Serial Number    :02:34:56
Issuer           :/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
Subject          :/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
Issued On        :May 21 04:00:00 2002 GMT
Expires On       :May 21 04:00:00 2022 GMT
Signed Using     :SHA1-RSA
RSA Key size     :2048 bits
Version          :3
Serial Number    :6E:CC:7A:A5:A7:03:20:09:B8:CE:BC:F4:E9:52:D4:91
Issuer           :/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. -
For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5
Subject          :/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at
https://www.verisign.com/rpa (c)10/CN=VeriSign Class 3 Secure Server CA - G3
Issued On        :Feb  8 00:00:00 2010 GMT
Expires On       :Feb  7 23:59:59 2020 GMT
Signed Using     :SHA1-RSA
RSA Key size     :2048 bits
Version          :3
Serial Number    :18:DA:D1:9E:26:7D:E8:BB:4A:21:58:CD:CC:6B:3B:4A
Issuer           :/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. -
For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5
Subject          :/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. -
For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5
Issued On        :Nov  8 00:00:00 2006 GMT
Expires On       :Jul 16 23:59:59 2036 GMT
```

```
Signed Using :SHA1-RSA
RSA Key size :2048 bits
Version      :3
Serial Number :
Issuer       :/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
Subject      :/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
Issued On    :Jun 29 17:06:20 2004 GMT
Expires On   :Jun 29 17:06:20 2034 GMT
Signed Using :SHA1-RSA
RSA Key size :2048 bits
```

The output of this command displays details such as the version, serial number, subject, issue date, expiry date, type of encryption, and RSA key information of the CA certificates uploaded on the IAP.

Command History

Version	Description
Aruba Instant	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-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 (5G)

MAC	RSSI	In Swarm	Flags	Matched	Received
---	---	---	---	---	---
00:27:10:a9:98:60	12	No	4	-	1m:5s
60:f8:1d:ad:7f:f0	18	No	N	-	4s
24:77:03:8f:78:30	24	No	4	-	40s
24:77:03:f7:6d:20	20	No	4	-	17s
00:15:00:5b:3a:50	28	No	4	-	15s
02:36:00:00:00:30	58	No	4	-	45s
0c:84:dc:3b:63:f1	16	No	4	-	3m:27s
6a:10:00:00:00:01	43	No	8	-	2m:33s

Command History

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 IAP 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-match-ssid-table radio-mac

```
show ap client-match-ssid-table radio-mac <mac-address>
```

Description

This command displays the SSID table list over a specific radio for the current IAP and all other neighboring IAPs.

Usage Guidelines

Use this command to view the SSID details stored in the client match database for a specific radio belonging to the current IAP and all its neighboring IAPs.

Parameter	Description
<mac address>	Enter a specific radio belonging to the current IAP and all its neighboring IAPs

Example

The following example shows the output of the **show ap client-match-ssid-table radio-mac** command:

```
(Instant AP)# show ap client-match-ssid-table radio-mac f0:5c:19:1c:92:50
Client Match SSID Table
-----
MAC                SSID Count  SSID Name  Clients  Threshold
---                -
f0:5c:19:1c:92:50  2           CM_zone_a  0        64
CM1_zone_a 0      64
Total 1 Radios
```

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap client-match-ssid-table

show ap client-match-ssid-table

Description

This command displays the SSID table list over the radios of the current IAP and all other neighboring IAPs.

Usage Guidelines

Use this command to view the SSID details stored in the client match database for the radios belonging to the current IAP and all its neighboring IAPs.

Example

The following example shows the output of the **show ap client-match-ssid-table** command:

```
(Instant AP)# show ap client-match-ssid-table
Client Match SSID Table
-----
MAC                SSID Count  SSID Name  Clients  Threshold
---
40:e3:d6:7f:4c:70  2           CM_zone_b  0        64
CM2_zone_b 0      64
40:e3:d6:7f:4c:60  2           CM_zone_b  0        64
CM2_zone_b 0      64
f0:5c:19:1c:92:40  2           CM_zone_a  0        64
CM1_zone_a 0      64
f0:5c:19:1c:92:50  2           CM_zone_a  0        64
CM1_zone_a 0      64
9c:1c:12:3a:e8:e0  2           CM_zone_a  0        64
CM1_zone_a 0      64
9c:1c:12:3a:e8:f0  2           CM_zone_a  0        64
CM1_zone_a 0      64
Total 6 Radios
```

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap client-match-triggers

show ap client-match-triggers

Description

This command displays the configuration conditions that trigger client match events and actions for the clients associated with an IAP.

Usage Guidelines

Use this command to view the clients match trigger records. When the client match feature is enabled on an IAP, the IAP measures the RF health of its associated clients. Based on the following trigger conditions, the clients are moved from one IAP to another for better performance and client experience.

- Dynamic Load Balancing:
- Sticky Clients
- Band Steering
- Channel Utilization
- Client Capability Match

For more information on client match and client match trigger conditions, see *Aruba Instant 6.5.1.0-4.3.1.0 User Guide*.

Example

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

Client Match Triggers

Station		PHY	Target_AP		Reason		STA_CAP	rss	chan	ccnt
cutil	g_ccnt	RSSI	CHAN	CCNT	ROOM	CUTIL				
-----	-----	----	----	-----	-----	-----	-----	----	----	-----
-----	-----	----	----	-----	-----	-----	-----	----	----	-----
A_CCNT	Time									
---	----									
00:15:00:5e:7e:3c	0	9c:1c:12:3a:e9:70	Dynamic Load Balancing	-	25	36+	12			
-	-	44	44+	2	-	-	3h:11m:19s			
5a:15:00:00:00:16	1	9c:1c:12:3a:e9:10	Sticky Client	-	17	6	-			
-	-	34	40-	-	-	-	2h:11m:40s			
00:15:00:5e:77:c8	0	9c:1c:12:3a:e9:10	Dynamic Load Balancing	-	36	48-	19			
-	-	38	40-	0	-	-	2h:11m:34s			
a4:4e:31:97:da:74	0	9c:1c:12:3a:e9:10	Dynamic Load Balancing	-	31	48-	19			
-	-	42	40-	0	-	-	2h:11m:34s			
00:15:00:5b:72:1c	1	9c:1c:12:3a:e9:60	Sticky Client	-	24	5	-			
-	-	35	6	-	-	-	1h:29m:37s			
5a:12:00:00:00:11	0	9c:1c:12:3a:e6:70	Dynamic Load Balancing	-	15	44+	9			
-	-	35	40-	9	-	-	1h:9m:41s			

Total 6 Records

The output of this command displays client match trigger records with details such as station MAC, target AP MAC, trigger condition and so on.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 IAP 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 Received	Channel	RSSI	Clients	Threshold	Channel Util (%)	VC Key	Flags	
---	-----	----	-----	-----	-----	-----	-----	-----

d8:c7:c8:44:50:c0 8m:27s	6	13	1	-	-	-		
d8:c7:c8:44:50:d0	40	8	2	-	-	-	V	1s
d8:c7:c8:44:51:b0 2m:49s	44	40	10	-	-	-	VR	
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 12m:43s	161	7	2	-	-	-	S	
d8:c7:c8:44:4b:80 1m:24s	6	10	3	-	-	-	VR	
d8:c7:c8:44:4b:90 2m:34s	48	17	2	-	-	-	VR	
6c:f3:7f:ee:dc:20	11	32	2	3	0	847face0		3m:6s
d8:c7:c8:44:4c:80 2m:27s	6	24	1	-	-	-	VR	
d8:c7:c8:44:4c:90 2m:34s	36	20	11	-	-	-	VR	
6c:f3:7f:e7:5d:40 14m:24s	1	59	1	3	0	847face0		

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. NOTE: 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-restore-status

```
show ap debug airwave-restore-status
```

Description

This command displays information about the status of the IAP configuration restoration on the AirWave server.

Usage Guidelines

If the IAPs managed by AirWave are not able to connect to the AirWave server, IAP can load the backed up configuration received by AirWave after five minutes. This command displays the restoration status of the IAP configuration for the IAPs managed by AirWave.

Example

The output of the **show ap debug airwave-restore-status** command displays the restoration flag and time. The following example shows the output of this command:

```
Airwave Config Restore
-----
Restore flag Time
-----
No N/A
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	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 VC 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-l3</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 partial output of **show ap debug am-config** command:

```
Channel Number
-----
1
7
Valid 40MHz A-Channel Pairs
-----
Channel Number
-----
36
44
52
60
149
157
AP System Configuration
-----
Parameter Value
-----
AM Scan RF Band all
RF Behavior Configuration
-----
Parameter Value
-----
Station Handoff Assist Disable
RSSI Falloff Wait Time 0
Low RSSI Threshold 0
RSSI Check Frequency 0
Frequent scan action 2
Event Thresholds Configuration
-----
Parameter Value
-----
Detect Frame Rate Anomalies Disable
Bandwidth Rate High Watermark 0
Bandwidth Rate Low Watermark 0
Frame Error Rate High Watermark 0
Frame Error Rate Low Watermark 0
Frame Fragmentation Rate High Watermark 0
Frame Fragmentation Rate Low Watermark 0
Frame Low Speed Rate High Watermark 0
Frame Low Speed Rate Low Watermark 0
Frame Non Unicast Rate High Watermark 0
Frame Non Unicast Rate Low Watermark 0
```



```

Frame Receive Error Rate High Watermark 0
Frame Receive Error Rate Low Watermark 0
Frame Retry Rate High Watermark 0
Frame Retry Rate Low Watermark 0
Interference Configuration
-----
Parameter Value
-----
Detect Interference Disable
Interference Increase Threshold 0
Interference Increase Timeout 0
Interference Wait Time 0
IDS General Configuration

```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	The 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 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 ble-config

show ap debug ble-config

Description

This command displays the BLE configuration details and information such as the update interval for sending beacon management requests to the Beacon Management Console (BMC), BLE token, and the operation mode.

Usage Guidelines

Use this command to view the BLE configuration details.

Examples

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

```
(host)# show ap debug ble-config
BLE Configuration
-----
Item                               Value
----                               -
Master IP                         127.0.0.1
Authorization Token                Not Configured
Endpoint URL                      Not Configured
BLE Ready                         No
Update Intvl (in sec)            300
BLE debug log                     Enabled
Operational Mode                 0 (APB: 0)
Uplink Status                    0 (APB: 0)
APB Connection Status            0
Last BLE Device Update Attempt    00:00:00:00:00:00
Last Update Sent Time            No Update Sent
```

Command History

Release	Modification
Aruba Instant 6.4.4.4-4.2.3	This command was introduced.

Command Information

Platforms	Command Mode
IAP-324/325 IAP-214/215 IAP-224/225 IAP-205H	Privileged Exec mode

show ap debug ble-connect

show ap debug ble-connect

Description

This command displays a log showing the BLE connection details.

Usage Guidelines

Use this command to view the BLE connection details.

Command History

Release	Modification
Aruba Instant 6.4.4.4-4.2.3	This command was introduced.

Command Information

Platforms	Command Mode
IAP-324/325 IAP-214/215 IAP-224/225 IAP-205H	Privileged Exec mode

show ap debug ble-daemon

show ap debug ble-daemon

Description

This command displays the BLE daemon log messages.

Usage Guidelines

Use this command to view the BLE daemon log messages..

Command History

Release	Modification
Aruba Instant 6.4.4.4-4.2.3	This command was introduced.

Command Information

Platforms	Command Mode
IAP-324/325 IAP-214/215 IAP-224/225 IAP-205H	Privileged Exec mode

show ap debug ble-relay

show ap debug ble-relay

Description

This command displays the BLE process logs.

Usage Guidelines

Use this command to view the BLE process logs.

Command History

Release	Modification
Aruba Instant 6.4.4.4-4.2.3	This command was introduced.

Command Information

Platforms	Command Mode
IAP-324/325 IAP-214/215 IAP-224/225 IAP-205H	Privileged Exec mode

show ap debug ble-table

show ap debug ble-table

Description

This command displays beacon details for the BLE devices detected by the IAP.

Usage Guidelines

Use this command to view the beacon details for the BLE devices detected by the IAP.

Examples

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

```
(host)# show ap debug ble-config
BLE Configuration
-----
Item                                Value
----                                -
Master IP                          127.0.0.1
Authorization Token                 Not Configured
Endpoint URL                       Not Configured
BLE Ready                          No
Update Intvl (in sec)              300
BLE debug log                      Enabled
Operational Mode                   0 (APB: 0)
Uplink Status                      0 (APB: 0)
APB Connection Status              0
Last BLE Device Update Attempt     00:00:00:00:00:00
Last Update Sent Time              No Update Sent
```

The following example shows the output of the **show ap debug ble-table** command:

```
BLE Device Table
-----
MAC   HW_Type  FW_Ver  Flags  Status  Batt(%)  RSSI  Major#  Minor#  UUID  Tx_Power  Last
Update  Uptime
---  -
-
Total beacons:0
Note: Battery level for LS-BT1USB devices is indicated as USB.
Note: Uptime is shown as Days hour:minute:second.
Note: Last Update is time in seconds since last heard update.
Status Flags:L:AP's local beacon; I:iBeacon; A: Aruba Beacon; H: Aruba HiPower Beacon
:U:Image Upgrade Pending
```

Command History

Release	Modification
Aruba Instant 6.4.4.4-4.2.3	This command was introduced.

Command Information

Platforms	Command Mode
IAP-324/325 IAP-214/215 IAP-224/225 IAP-205H	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 IAP 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 buffer of the IAP 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 IAP has not transmitted packets in a category type, this data row will not be displayed in the output of the command. Tx WMM [BE]: Best Effort Tx WMM [BK]: Background Tx WMM [VO]: VoIP

Parameter	Description
	Tx WMM [VI]: 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.
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 IAPs 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 IAPs 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 IAPs 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 IAPs 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 IAPs 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 IAPs 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 IAPs 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 IAPs operating in 40 MHz mode.
Frames Received	Shows the number of frames received.
Rx Data Frames	Shows the number of data frames received.
Null Data Frames	Shows the number of null data frames received.
Rx Mgmt Frames	Shows the number of management frames received.
PS Poll Frames	Shows the number of power save poll frames received.

Parameter	Description
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 IAP has not transmitted packets in a category type, this data row will not be displayed in the output of the command. Tx WMM [BE]: Best Effort Tx WMM [BK]: Background Tx WMM [VO]: VoIP Tx WMM [VI]: Video

Command History

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 MAC address of the IAP.
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: none: IAP is a legacy access point that does not support the 802.11n standard. 20Mhz: A high-throughput IAPs using a single 20 Mhz channel. 40Mhz: A high-throughput IAPs using two 20 Mhz channels.

Parameter	Description
AID	Indicates the 802.11 association ID. A client receives a unique 802.11 association ID when it associates to an IAP.
UAPSD	Shows the following values for Unscheduled Automatic Power Save Delivery (UAPSD) in comma-separated format: VO, VI, BK, BE, Max SP, Q Len. VO: If 1, UAPSD is enabled for the VoIP access category. If UAPSD is disabled for this access category, this value is 0. VI: If 1, UAPSD is enabled for the Video access category. If UAPSD is disabled for this access category, this value is 0. BK: If 1, UAPSD is enabled for the Background access category. If UAPSD is disabled for this access category, this value is 0. BE: If 1, UAPSD is enabled for the Best Effort access category. If UAPSD is disabled for this access category, this value is 0. Max SP: The maximum service period is the number of frame sent per trigger packet. This value is value can be 0, 2, 4 or 8. Q Len: The number of frames currently queued for the client, from 0 to 16 frames.
Tx_Pkts	Shows the number of packets transmitted to the client.
Rx_Pkts	Shows the number of packets received from the client.
PS_Qlen	Shows power save queue length, in bytes.
Tx_Rate	Shows the packet rate from the IAP to client.
Rx_Rate	Show the packet rate from the client to IAP.
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 client-frame-history

```
show ap debug client-frame-history client-mac <mac-address> radio {0|1}
```

Description

This command displays the latest Received Signal Strength Indicator (RSSI) information about the incoming packets for a client connected to an IAP.

Syntax

Parameter	Description
client-mac <mac-address>	Allows you to filter the output based on a client MAC address.
radio {0 1}	Allows you to specify the IAP radio ID to which the client is associated.

Usage Guidelines

Use this command to verify if the RSSI information is frequently updated. If the RSSI information is not frequently updated, a client may be steered to an improper new IAP in the cluster.

Example

The following example shows the output of **show ap debug client-frame-history** command:

```
Frame History count: 5
Client Frame History Report
-----
Received Time RSSI Previous RSSI
-----
1s 42 42
1s 42 42
1s 42 42
1s 42 42
1s 42 42
```

Command History

Version	Description
Aruba Instant 6.4.2.0-4.1.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug cloud-server

```
show ap debug cloud-server
```

Description

This command displays if the IAP is managed locally or by a cloud server. If the IAP is managed by a cloud server, the server details are displayed.

Usage Guidelines

Use this command to view information cloud server managing the IAP.

Example

The following example shows the output of **show ap debug cloud-server** command:

```
IAP mgmt mode           :athena-mgmt
Aruba Central server    :jenkins-qa-custom-build-396.test.pdt1.arubathena.com
Aruba Central Protocol  :HTTPS
Aruba Central status    :success
```

Command History

Version	Description
Aruba Instant 6.4.2.3-4.1.2.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug cloud-config-received

show ap debug cloud-config-received

Description

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

Usage Guidelines

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

Example

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

```
wlan ssid-profile test001: OK
inactivity-timeout 1000: OK
exit: OK
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug cloud-data-sent

show ap debug cloud-data-sent

Description

This command displays information about data exchange between the Central server and the IAP.

Usage Guidelines

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

Example

The following example shows the output of the **show ap debug cloud-data-sent** command:

```
(Instant AP) # show ap debug cloud-data-sent
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug cloud-events-pending

show ap debug cloud-events-pending

Description

This command displays the pending Central server events.

Usage Guidelines

Use this command to view the pending Central server events.

Example

The following example shows the partial output of the **show ap debug cloud-events-pending** command:

```
<t11>
<e61>1106</e61>
<e62>807</e62>
<e1005>24:de:c6:be:c6:19</e1005>
<e1006>Cent12-251</e1006>
<e1001>9c:1c:12:c7:ea:7a</e1001>
<e1056>1</e1056>
<e1017>9c:1c:12:c7:ea:7a</e1017>
<e1018>60</e1018>
<e1058>Varbind deprecated</e1058>
</t11>
<t11>
<e61>1106</e61>
<e62>721</e62>
<e1005>24:de:c6:be:be:48</e1005>
<e1006>Cent12-250</e1006>
<e1001>9c:1c:12:c7:ea:7a</e1001>
<e1056>1</e1056>
<e1017>9c:1c:12:c7:ea:7a</e1017>
<e1018>36</e1018>
<e1058>Varbind deprecated</e1058>
</t11>
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

idshow ap debug cloud-signon-key

show ap debug cloud-signon-key

Description

This command displays the Central sign on key used by the administrator to manually authorize the first Virtual Controller for an organization.

Usage Guidelines

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

Example

The following example shows the output of the **show ap debug cloud-signon-key** command:

```
awc_ui_key_new : 4335655801564bbec67e5328865375da248f7539b70eb86d47
awc_ui_key_old : 1bbf60ac01ba24153cdfdcf8db12265bba79f9de27c9631105
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug cloud-restore-status

```
show ap debug cloud-restore-status
```

Description

This command displays information about the status of the IAP configuration restoration on the Central server.

Usage Guidelines

If the IAPs managed by Central are not able to connect to the Central server, IAP can load the backed up configuration received by Central after five minutes. This command displays the restoration status of the IAP configuration for the IAPs managed by Central.

Example

The output of the **show ap debug cloud-restore-status** command displays the restoration flag and time. The following example shows the output of this command:

```
Airwave Config Restore
-----
Restore flag  Time
-----
No           N/A
ac:a3:1e:c2:9c:e2#
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug cloud-state

show ap debug cloud-state

Description

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

Usage Guidelines

Use this command to view the current state of Central events associated with the IAP.

Example

The following example shows the partial output of **show ap debug cloud state**:

```
<MIB_SWARM_TABLE>
MIB_MAC_ADDRESS[1] = 1f26e1f901daf3300416d8351074d5a9869e5078bb4c5e821f
MIB_NAME[2] = instant-C2:9C:E2
MIB_ORGANIZATION[3] =
MIB_IP_ADDRESS[5] = 0.0.0.0
MIB_VERSION[8] = 6.4.3.1-4.2.0.0_50812
MIB_OEM_SHORT_NAME[60] = Aruba
MIB_SINGLE_SIGNON_KEY[79] = 5ea50b3401c25eb1e385aa61e6a2266e1fc51c4eb61823ed64
MIB_CERT_SN_SERVER[63] =
MIB_CERT_SN_CA[64] =
MIB_CONFIG_RCV[67] = <![CDATA[wlan
</MIB_SWARM_TABLE>
<MIB_WLAN_TABLE>
MIB_ESSID[25] = test001
MIB_BSSID_OFFSET[26] = 0
MIB_WLAN_INDEX[116] = 0
MIB_VLAN[27] =
MIB_OPERATION_MODE[28] = 32
MIB_WLAN_TYPE[29] = 1
MIB_BAND[30] = 2
</MIB_WLAN_TABLE>
<MIB_AP_TABLE>
MIB_MAC_ADDRESS[1] = ac:a3:1e:c2:9c:e2
MIB_SERIAL_NUMBER[6] = CM0097540
MIB_SERVICE_TAG[120] = N/A
MIB_NAME[2] = ac:a3:1e:c2:9c:e2
MIB_MODEL[7] = 1.3.6.1.4.1.14823.1.2.68
MIB_MODE[18] = access
MIB_IP_ADDRESS[5] = 10.65.157.254
MIB_CPU_UTILIZATION[15] = 7
MIB_MEMORY_TOTAL[16] = 129269760
MIB_MEMORY_FREE[17] = 25366528
MIB_SWARM_MASTER[13] = 1
MIB_UPTIME[14] = 114314
MIB_MESH_MODE[65] = 0
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug cloud-stats

show ap debug cloud-stats

Description

This command displays the configuration statistics associated with an IAP managed by the Central server.

Usage Guidelines

Use this command to view configuration details of an IAP managed by the Central server.

Example

The following example shows the partial output of the **show ap debug cloud-stats** command:

```
<MIB_SWARM_TABLE>
MIB_MAC_ADDRESS[1] = 1f26e1f901daf3300416d8351074d5a9869e5078bb4c5e821f
MIB_NAME[2] = instant-C2:9C:E2
MIB_ORGANIZATION[3] =
MIB_IP_ADDRESS[5] = 0.0.0.0
MIB_VERSION[8] = 6.4.3.1-4.2.0.0_50812
MIB_OEM_SHORT_NAME[60] = Aruba
MIB_SINGLE_SIGNON_KEY[79] = 5ea50b3401c25eb1e385aa61e6a2266e1fc51c4eb61823ed64
MIB_CERT_SN_SERVER[63] =
MIB_CERT_SN_CA[64] =
MIB_CONFIG_RCV[67] = <![CDATA[wlan
</MIB_SWARM_TABLE>
<MIB_WLAN_TABLE>
MIB_ESSID[25] = test001
MIB_BSSID_OFFSET[26] = 0
MIB_WLAN_INDEX[116] = 0
MIB_VLAN[27] =
MIB_OPERATION_MODE[28] = 32
MIB_WLAN_TYPE[29] = 1
MIB_BAND[30] = 2
</MIB_WLAN_TABLE>
<MIB_AP_TABLE>
MIB_MAC_ADDRESS[1] = ac:a3:1e:c2:9c:e2
MIB_SERIAL_NUMBER[6] = CM0097540
MIB_SERVICE_TAG[120] = N/A
MIB_NAME[2] = ac:a3:1e:c2:9c:e2
MIB_MODEL[7] = 1.3.6.1.4.1.14823.1.2.68
MIB_MODE[18] = access
MIB_IP_ADDRESS[5] = 10.65.157.254
MIB_CPU_UTILIZATION[15] = 7
MIB_MEMORY_TOTAL[16] = 129269760
MIB_MEMORY_FREE[17] = 25366528
MIB_SWARM_MASTER[13] = 1
MIB_UPTIME[14] = 114314
MIB_MESH_MODE[65] = 0
<MIB_RADIO_TABLE>
MIB_MAC_ADDRESS[1] = ac:a3:1e:a9:ce:30
MIB_RADIO_NUM[10] = 0
MIB_RADIO_BAND[11] = 1
MIB_CHANNEL[23] = 140+
MIB_TRANSMIT_POWER[24] = 21
MIB_NOISE_FLOOR[47] = 97
MIB_CHANNEL_BUSY_64[46] = 15
MIB_TX_DROPS[51] = 0
</MIB_RADIO_TABLE>
<MIB_RADIO_TABLE>
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	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 IAP device details to which the client is connected.
Auth-Succs	Displays the number of times the client authenticated successfully.
Auth-Fails	Displays the number of times the client failed to authenticate.
Auth-Timeout	Displays if client authentication timeout details.
Reauths	Displays the reauthentication attempts if any.
Supp-Naks	Displays the number of supplementary NAKs.
UkeyRot	Displays the unicast key rotation details.

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 23:09:03assoc-respd8:c7:c8:c4:29:82 08:ed:b9:e1:51:87 d8:c7:c8:c4:29:82 15Success
May 9 22:02:40 auth d8:c7:c8:c4:29:8b c4:85:08:de:06:d4 d8:c7:c8:c4:29:8b 15Success
May 9 01:25:51 auth 08:ed:b9:e1:51:87 d8:c7:c8:c4:29:8a d8:c7:c8:c4:29:8a 60 -
```

The output of this command includes the following information:

Column	Description
Timestamp	Indicates timestamp for the authentication management frame.
stype	Indicates the type of the packet.
SA	Indicates the source of the packets.
DA	Indicates the destination to which the packets are intended.
BSS	Indicates the BSSID.
Signal	Indicates the signal level.
Misc	Indicates miscellaneous information such as status and other relevant details.

Command History

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 rfc3576-radius-statistics

show ap debug rfc3576-radius-statistics [termination]

Description

This command displays the change of authorization (CoA) statistics for the servers configured on an IAP.

Parameter	Description
termination	Displays termination details.

Usage Guidelines

Use this command to view the CoA details for debugging authentication and authorization related issues.

Example

The following example shows the output of the **show ap debug rfc3576-radius-statistics** command:

RADIUS RFC3576 Statistics

```
-----
Statistics
-----
InternalServer  test      testServer
-----
In Service: Management Auth  Not used    Not used    Not used
In Service: Test1            Up 699292s  Not used    Not used
In Service: ssid1            Up 699292s  Not used    Not used
Disconnect Requests          0           0           0
Disconnect Accepts          0           0           0
Disconnect Rejects          0           0           0
No Secret                   0           0           0
No Session ID               0           0           0
Bad Authenticator           0           0           0
Invalid Request             0           0           0
Packets Dropped             0           0           0
Unknown service             0           0           0
CoA Requests                0           0           0
CoA Accepts                 0           0           0
CoA Rejects                 0           0           0
No permission               0           0           0
SEQ first/last/free         0/0/0       0/0/0       0/0/0
Packets received from unknown clients ::0
Packets received with unknown request ::0
Total RFC3576 packets Received ::0
```

The following example shows the output of the **show ap debug rfc3576-radius-statistics termination** command:

RADIUS RFC3576 Statistics

```
-----
Statistics
-----
t_cpmm      t_HOVCLEARPASS  LDAP-none  free-LDAP
-----
In Service: OCSPTTEST  Not used    Not used    Not used    Not used
In Service: Management Auth  Not used    Not used    Not used    Not used
In Service: IPFHUNTV    Not used    Not used    Not used    Not used
In Service: __wired__eth1  Not used    Not used    Not used    Not used
In Service: IPFHUN      Not used    Not used    Not used    Not used
In Service: IPFHUNGuest  Not used    Not used    Not used    Not used
In Service: booth-psk-225  Not used    Not used    Not used    Not used
In Service: booth-open-205  Not used    Not used    Not used    Not used
In Service: IPFNET      Not used    Not used    Not used    Not used
In Service: booth-cp-225  Not used    Not used    Up 90490s   Up 90490s
```

```

In Service: booth-dot1x-225 Not used Not used Not used Not used
In Service: aaa Not used Not used Not used Not used
Disconnect Requests 0 0 0 0
Disconnect Accepts 0 0 0 0
Disconnect Rejects 0 0 0 0
No Secret 0 0 0 0
No Session ID 0 0 0 0
Bad Authenticator 0 0 0 0
Invalid Request 0 0 0 0
Packets Dropped 0 0 0 0
Unknown service 0 0 0 0
CoA Requests 0 0 0 0
CoA Accepts 0 0 0 0
CoA Rejects 0 0 0 0
No permission 0 0 0 0
SEQ first/last/free 0/0/0 0/0/0 0/0/0 0/0/0
Packets received from unknown clients ::0
Packets received with unknown request ::0
Total RFC3576 packets Received ::0

```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	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 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 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 IAP.
out	Shows the number of packets sent by the IAP.
drop	Shows the number of packets dropped by the IAP.
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 IAP.
BWmgmt	Displays 1 if the bandwidth management feature has been enabled. Otherwise, it displays a 0.
idx	Shows the association index value.
tokens	Represents the credits the station has to transmit tokens.

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 stm-role

show ap debug stm-role

Description

This command displays the station management user roles configured for the SSIDs in an IAP.

Usage Guidelines

Use this command to view the user roles configured for the IAP station management. This includes details of the VLANs assigned to each SSID and also shows if the Calea feature is enabled or disabled.

Example

The following example shows the output of **show ap debug stm-role** command:

```
User Role
-----
Name                Index  Vlan  Calea
-----
Test                 4      0    OFF
wired-instant        2      0    OFF
ssid1                 3      0    OFF
default_wired_port_profile 1      0    OFF
```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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	• IAP uptime	• Boot version
• MTU discovery	• memory usage	• LMS information
• ARP cache	• Kernel slab statistics	• Power status
• Route table	• Interrupts	• CPU type
• Interface Information	• Crash Information	• CPU usage statistics

Command History

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 tacacs-statistics

show ap debug tacacs-statistics

Description

This command displays the TACACS 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.

```
Tacacs Statistics
-----
Statistics
-----
In Service: Management Auth
In Service: Test1
In Service: ssid1
Accounting Requests
Authen Requests
Author Requests
Authen Response Pass
Authen Response Fail
Author Response Pass
Author Response Fail
Accounting Response Pass
Accounting Response Fail
Login Success
Login Failure
Timeouts
AvgRespTime (ms)
Outstanding Auths
SEQ first/last/free
```

Command History

Version	Description
Aruba Instant 6.4.0.2- 4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap dot11k-beacon-report

```
show ap dot11k-beacon-report <mac>
```

Description

This command displays the beacon report details for the 802.11k clients of an IAP.

Syntax

Parameter	Description
<mac>	Allows you to specify the MAC address of the client for which you want to view the beacon report details.

Usage Guidelines

Use this command to view the beacon report details for 802.11k clients connected to an IAP.

Example

The following example shows the output of the **show ap dot11k-beacon-report <mac>** command:

```
(Instant AP)# show ap dot11k-beacon-report 70:11:24:56:02:72
Client: 70:11:24:56:02:72
Status: Success
Nbr count: 4
Last received: 31s
Client 11k Beacon Report
-----
```

BSSID	Channel	RSSI	Antenna
-----	-----	-----	-----
6c:f3:7f:b6:62:f0	38	92	0
6c:f3:7f:b6:69:30	38	94	0
6c:f3:7f:4a:43:d0	46	94	0
6c:f3:7f:b6:66:30	46	92	0

The output of this command displays information on the number of 802.11k neighbors, connection status, and the channel, RSSI and antenna details for the specified MAC address.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap dot11k-nbrs

show ap dot11k-nbrs

Description

This command displays the neighboring details of the 802.11k clients connected to an IAP.

Usage Guidelines

Use this command to view neighbors of the 802.11k clients connected to an IAP.

Example

The following example shows the output of the **show ap dot11k-nbrs** command:

```
Radio: 0
Nbr count: 3
11k Neighbours
-----
BSSID                Channel  Last Update
-----
6c:f3:7f:b6:62:f0    292      1s
6c:f3:7f:b6:69:30    816      6s
6c:f3:7f:b6:66:30    808      5s

Radio: 1
Nbr count: 3
11k Neighbours
-----
BSSID                Channel  Last Update
-----
6c:f3:7f:b6:62:e0     1       13s
6c:f3:7f:b6:66:20     6       33s
6c:f3:7f:b6:69:20     6       33s
```

The output of this command displays information on the number of 802.11k neighbors on each radio of the IAP.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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.

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:10.15.22.255
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 Link
up/down Resel. Switch Other Mgmt
-----
- - - - -
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 IAP or a Child IAP. Each row of data in the Mesh Packet Counters table shows counter values for an individual interface.

Column	Description
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 AP)# 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 mcl
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 IAP names, if available. The IAP names will include [p] (parent), or [c] (child) suffixes to indicate the role of the mesh BSSID.
Channel	Number of a radio channel used by the IAP.
Age	Number of seconds elapsed since the IAP heard from the neighbor.
Hops	Indicates the number of hops it takes traffic from the mesh node to get to the mesh portal. The mesh portal advertises a hop count of 0, while all other mesh nodes advertise a cumulative count based on the parent mesh node.
Cost	A relative measure of the quality of the path from the IAP 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

Parameter	Description
	the sum of the (parent path cost) + (the parent node cost) + (the link cost).
Relation	Shows the relationship between the specified IAP and the IAP on the neighbor list and the amount of time that relationship has existed. • P = Parent • C = Child • N = Neighbor • B = Blacklisted-neighbor
Flags	This parameter shows additional information about the mesh neighbor. The key describing each flag is displayed at the bottom of the neighbor list.
RSSI	The 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 IAP 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 anIAP.

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/Auth pending
a = SAE Accepted; b = SAE Blacklisted-neighbour; e = SAE Enabled; u = portal-unreachable; o =
opensystem
```

The output of this command includes the following information:

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 IAP names, if available. The IAP names will include [p] (parent), or [c] (child) suffixes to indicate the role of the mesh BSSID.
Channel	Number of a radio channel used by the IAP.
Age	Number of seconds elapsed since the IAP heard from the neighbor.
Hops	Indicates the number of hops it takes traffic from the mesh node to get to the mesh portal. The mesh portal advertises a hop count of 0, while all other mesh nodes advertise a cumulative count based on the parent mesh node.
Cost	A relative measure of the quality of the path from the IAP to the VC. 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).

Parameter	Description
Relation	Shows the relationship between the specified IAP and the IAP on the neighbor list and the amount of time that relationship has existed. • P = Parent • C = Child • N = Neighbor • B = Blacklisted-neighbor
Flags	This parameter shows additional information about the mesh neighbor. The key describing each flag is displayed at the bottom of the neighbor list.
RSSI	The 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 IAP 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|
enet-wired-mac <mac>| ids-state <type>| pot-ap-list | pot-sta-list| rogue-ap <mac>| routers|
scan-info| sta-list| state <mac>| stats <mac>| status}
```

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 IAPs that are actively performing policy enforcement containment such as rogue containment. This command can tell us which IAP is sending out deauthorization frames, although it does not specify which IAP is being contained.
ap-list	Shows list of IAPs 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	Shows containment events and counters triggered by the wired containment and wireless containment features configured in the ids. The output of this command shows device and target data for wired containment activity, as well as data for the following counters. Wireless Containment Counters: • Last Deauth Timer Tick • Deauth frames to IAP • Deauth frames to Client • Last Tarpit Timer Tick • Tarpit Frames: Probe Response • Tarpit Frames: Association Response • Tarpit Frames: Authentication • Tarpit Frames: Data from IAP • Tarpit Frames: Data from Client • Last Enhanced Adhoc Containment Timer Tick • Enhanced Adhoc Containment: Frames To Data Sender • Enhanced Adhoc Containment: Frames To Data Receiver • Enhanced Adhoc Containment: Response to Request Enhanced Adhoc Containment: Replay Response Wired Containment Counters: • Last Wired Containment Timer Tick • Last Tagged Wired Containment Timer Tick • Spoof frames sent • Spoof frames sent on tagged VLAN

Parameter	Description
enet-wired-mac	Shows Wired MAC Addresses learned.
ids-state <type>	Shows IDS State.
pot-ap-list	Display the Potential IAP table. The Potential IAP table shows the following data: • bssid: The Basic Service Set Identifier of the IAP. • channel: The current radio channel of the IAP. • phy type: The radio's PHY type. Possible values are 802.11a, 802.11a-HT-40, 802.11b/g, 802.11b/g-HT-20. • num-beacons: Number of beacons seen during a 10-second scan • tot-beacons: Total number of beacons seen since the last reset. • num-frames: Total number of frames seen since the last rest. • mt: Monitor time; the number of timer ticks elapsed since the first IAP is recognized. • at: Active time, in timer ticks. • ibss: Shows if ad-hoc BSS is enabled or disabled. It will be enabled if the bssid has detected an ad-hoc BSS (an ibss bit in an 802.11 frame). • rssi: The 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.
pot-sta-list	Shows the Potential client table. The Potential Client table shows the following values: • last-bssid: the Last BSSID to which the client associated. • from-bssid, • to-bssid • mt: Monitor time; the number of timer ticks elapsed since the first client is recognized. • it: Client Idle time, expressed as a number of timer ticks.
rogue-ap <mac>	Displays rogue IAPs information for the current IAP.
routers	Shows the Router MAC Addresses that were learned. The output of this command includes the router's MAC address, IP address and uptime.
scan-info	Shows scanned information for the IAP.
sta-list	Shows the configuration and status of monitor information of the IAP.
state	Shows the IAP monitoring state.
stats	Shows the IAP monitoring statistics.

Parameter	Description
status	Shows the status of the IAP monitoring.

Examples

show ap monitor active-laser-beams

The following example shows the output of **show ap monitor active-laser-beams** command:

```
Active Laser Beam Sources
-----
bssid channel rssi ap name lms ip master ip inactive time
-----
```

show ap monitor ap-list

The following example shows the output of **show ap monitor ap-list** command:

```
Monitored AP Table
-----
bssid essid chan ap-type 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 0 20 0 no
00:24:6c:80:7d:11 NTT-SPOT 1 interfering 80211b/g disable 3897/3897 9/8 wep 0 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 0
42 41 0 no
00:24:6c:80:7d:12 docomo 1 interfering 80211b/g disable 3779/3779 1/0 wep 0 8 7 0 no
6c:f3:7f:b6:74:32 syelburgi 40 interfering 80211a-HT-40 disable 3729/612 34/0 wpa2-psk-aes 0
59 59 0 no
00:0b:86:51:02:28 kannan-01 44 interfering 80211a disable 3613/1212 10/0 wpa2-psk-aes 0 36 33
3 no
00:0b:86:51:02:2b kannan-03 44 interfering 80211a disable 3555/1154 10/0 wpa2-psk-aes 0 38 35
0 no
00:0b:86:51:02:29 ssid-2 44 interfering 80211a disable 3518/1117 10/0 wpa2-psk-aes 0 37 33 0
no
00:0b:86:51:02:2c kannan-04 44 interfering 80211a disable 3494/1093 10/0 open 0 38 35 0 no
00:0b:86:51:02:2a kannan-02 44 interfering 80211a disable 3459/1058 10/0 open 0 38 34 0 no
00:0b:86:51:02:2d kannan-05 44 interfering 80211a disable 3459/1058 10/0 open 0 37 34 0 no
00:0b:86:51:02:2e kannan-06 44 interfering 80211a disable 3459/1058 10/0 open 0 37 33 0 no
00:0b:86:51:02:2f kannan-07 44 interfering 80211a disable 3459/1058 10/0 open 0 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 0 24
0 no
6c:f3:7f:56:81:00 7SPOT 1 interfering 80211b/g-HT-20 disable 3308/3308 72/71 open 0 0 10 0 no
00:0b:86:51:02:21 ssid-2 11 interfering 80211b/g disable 3277/764 101/0 wpa2-psk-aes 0 0 28 0
no
00:0b:86:51:02:22 kannan-02 11 interfering 80211b/g disable 3271/958 58/0 open 0 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 vlanid age
```

```

--- --
d8:c7:c8:cb:d4:20 10.17.88.188 0 1s
d8:c7:c8:cb:d3:d4 10.17.88.186 0 1s
00:0b:86:40:1c:a0 10.17.88.129 0 1m:18s

```

show ap monitor containment-info

The following example shows the output of **show ap monitor containment-info** command:

```

br0:10.17.88.188
ARP Cache Table
-----
mac ip vlanid age
--- --
d8:c7:c8:cb:d4:20 10.17.88.188 0 1s
d8:c7:c8:cb:d3:d4 10.17.88.186 0 1s
00:0b:86:40:1c:a0 10.17.88.129 0 1m:18s

```

show ap monitor enet-wired-mac

The following example shows the output of **show ap monitor enet-wired-mac** command:

```

Wired MAC Table
-----
mac age

```

show ap monitor ids-state

Use this command to view information about the Intrusion Detection System (IDS) the following detection policies:

- 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 enhanced-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 AP)# show ap monitor stats d8:c7:c8:cb:d4:22
Aggregate Stats
-----
retry low-speed non-unicast recv-error frag bwidth
-----
0 0 0 0 0 0
RSSI
-----
avg-signal low-signal high-signal count duration (sec)
-----
40 40 40 748 70
AP Impersonation State
-----
beacons prev-beacons exp-beacons beacon-interval imp-time imp-active wait-time
-----
0 11 11.00 100 0 0 0
AP Non-beacon-Frames:0
AP Tarpit Fake Channel:0
Raw Stats
-----
tx-pkt tx-byte rx-pkt rx-byte tx-retry-pkt rx-retry-pkt tx-frag-pkt rx-frag-pkt short-hdr-pkt
long-hdr-pkt
-----
2662202 830665629 31438 440132 0 0 0 0 2662202 0
Frame Type Stats
-----
type mgmt-pkt mgmt-byte ctrl-pkt ctrl-byte data-pkt data-byte
-----
tx 2662202 830665629 0 0 0 0
rx 0 0 31438 440132 0 0
Dest Addr Type Stats
-----
bcast-pkt bcast-byte mcast-pkt mcast-byte ucast-pkt ucast-byte
-----
0 0 0 0 0 0
Frame Size Packet Stats

```

```

-----
type 0-63 64-127 128-255 256-511 512-1023 1024+
-----
tx 0 0 0 0 0 0
rx 0 0 0 0 0 0
Frame Rate Stats
-----
type pkt-6m byte-6m pkt-9m byte-9m pkt-12m byte-12m pkt-18m byte-18m pkt-24m byte-24m 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 enhanced-cm-ev-
time
-----
0 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-l
-- -- -- -- --
256 288 45 136 26 2 256
Other Parameters
-----
key value
--- ---
Classification enable
Wireless Containment disable
Wired Containment disable
Rogue Containment disable
System OUI Table
-----
oui
---
RTLS Configuration and State
-----
Type Server IP Port Freq Active Rpt-Tags Tag-Mcast-Addr Tags-Sent Rpt-Sta Incl-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
Aer scout 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 IAPs 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 IAPs 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 6.4.2.3-4.1.2.0	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 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
Received
-----
-----
00:db:df:0a:57:4e Adopted    1           1           Yes   00:24:6c:07:44:c8 (Local 0)  47
59s
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
20s
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 app-services

show app-services

Description

This command displays the list of application services available 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 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 IAP 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 VC.

Usage Guidelines

Use this command to view the ARP messages sent or received by the VC.

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 IAP.
HW address	Displays the MAC address of the device.
Mask	Displays the network mask or the IP address range.
Device	Displays the device used to send ARP requests and replies.

Command History

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 auth-survivability

```
show auth-survivability {cached-info| debug-log [<count>]| time-out}
```

Description

This command displays the authentication survivability information for an IAP.

Syntax

Command/Parameter	Description
cached-info	Displays authentication credentials cached by the IAP.
debug-log [<count>]	Displays the log details for troubleshooting. The count attribute allows you to specify the number of logs to display.
time-out	Displays the duration configured for the cache expiry.

Usage Guidelines

Use this command to view the information cache expiry duration, cached information, and log details to debug when the authentication survivability feature is enabled. The authentication survivability feature supports a survivable authentication framework against the remote link failure when working with the external authentication servers. When enabled, this feature allows the IAPs to authenticate the previously connected clients against the cached credentials if the connection to the authentication server is temporarily lost.

Example

The following example shows the output of the **show 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 of the client whose credentials are cached.
Remaining Cache-Time	Displays the remaining duration for cache expiry.
Auth Survivability time out	Indicates the configured duration for cache expiry.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 backup-config

show backup-config

Description

This command displays the backup configuration information on an IAP.

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 backup-config** command output:

```
version 6.4.0.0-4.1.0
virtual-controller-country IN
virtual-controller-key 0cb5770401cdeb6e4363c25fdfe17d907c4b095a9be5e4258
name instant-C4:42:98
terminal-access
clock timezone none 00 00
rf-band all
allow-new-aps
allowed-ap d8:c7:c8:c4:42:98
arm
wide-bands 5ghz
80mhz-support
min-tx-power 18
max-tx-power 127
band-steering-mode prefer-5ghz
air-time-fairness-mode fair-access
client-aware
scanning
client-match
syslog-level warn ap-debug
syslog-level warn network
syslog-level warn security
syslog-level warn system
syslog-level warn user
syslog-level warn user-debug
syslog-level warn wireless
mgmt-user admin 82c496d47485380deb0a01d41345d3f1
wlan access-rule default_wired_port_profile
index 1
rule any any match any any any permit
wlan access-rule wired-instant
index 2
rule masterip 0.0.0.0 match tcp 80 80 permit
rule masterip 0.0.0.0 match tcp 4343 4343 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit
wlan access-rule test
index 3
rule any any match any any any deny
wlan external-captive-portal
server localhost
port 80
url "/"
auth-text "Authenticated"
auto-whitelist-disable
https
```

```
blacklist-time 3600
auth-failure-blacklist-time 3600
ids classification
ids
wireless-containment none
airgroup
disable
airgroupservice airplay
disable
description AirPlay
airgroupservice airprint
disable
description AirPrint
```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show banner

show banner

Description

This command displays the current login banner of an IAP.

Usage Guidelines

Use this command to review the banner message that appears when you first log in to the command-line interface of the IAP.

Example

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

```
(Instant AP)# show banner

#####welcome to login instant#####
###please start to input admin and password#####
###Don't leak the password###
```

Command History

IAP Platform	Command Mode
Aruba Instant 6.5.0.0-4.3.0.0	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.

Syntax

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.

Parameter	Description
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 ble-config

show ble-config

Description

This command displays the BLE configuration details.

Syntax

Parameter	Description
ble-config	Displays the BLE configuration details.

Usage Guidelines

Use this command to view the BLE configuration.

Examples

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

```
(host)# show ble-config
BLE Configuration
-----
Item Value
----
Master IP 127.0.0.1
Authorization Token Not Configured
Endpoint URL Not Configured
BLE Ready No
Update Intvl (in sec) 300
BLE debug log Enabled
Operational Mode 0 (APB: 0)
Uplink Status 0 (APB: 0)
APB Connection Status 0
Last BLE Device Update Attempt 00:00:00:00:00:00
Last Update Sent Time No Update Sent
```

Command History

Release	Modification
Aruba Instant 6.4.3.4-4.2.1.0	This command was introduced.

Command Information

Platforms	Command Mode
IAP-324/325 IAP-214/215 IAP-224/225 IAP-205H	Privileged Exec mode

show calea config

show calea config

Description

This command displays the details configured for CALEA server integration on an IAP.

Usage Guidelines

Use this command to CALEA configuration details.

Example

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

```
(Instant AP)# 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 an 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 AP)# 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.

Parameter	Description
Internal Captive Portal Redirect URL External Captive Portal Redirect URL	Displays the URL that the users are redirected to, after a successful authentication.
Server	Displays the external Captive port server.
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 example shows the partial output of the **show cellular config** command:

```
No Comm USB Plugged in
Cellular configuration
-----
Type                Value
----                -
4g-usb-type
usb-type
usb-dev
usb-tty
usb-init
usb-auth-type
usb-user
usb-passwd
usb-dial
usb-modeswitch
modem-isp
modem-country
Supported Modem Types
-----
Modem Type          Driver Used
-----
option              option
acm                  acm
airprime             airprime
hso                   hso
sierra-evdo           sierra-evdo
sierra-gsm            sierra-gsm
pantech-uml290        pantech-3g
novatal-mc551         ether-3g
sierra-net            sierra-net
franklin-u770         rndis-u770
rndis-l800            rndis-l800
huawei-cdc             huawei-cdc
novatel-u620          novatel-u620
pantech-uml295        rndis-uml295
sierra-gobi           sierra-gobi
```


Supported Country list

Country list

France
NZ
Israel
HK
Sweden
Spain
China
UK
norway
Germany
Croatia
Saudi-Arabia
US
Japan
Aus
Canada
India

The output of this command includes the following parameters:

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 SIM PIN
---- ----- ---- -----
Not-present Not-detect Linkdown AT+CPIN Error

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.
SIM PIN	Displays the SIM PIN of the model.

Command History

Version	Description
Aruba Instant 6.4.3.4-4.2.1.0	The output of the show cellular status command was modified to display the SIM PIN details of the cellular modems connected to an IAP.
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, OU=GT28470348, OU=See www.geotrust.com/resources/cps (c)11, OU=Domain Control Validated - QuickSSL(R) Premium, CN=securelogin.arubanetworks.com

Issued On :2011-05-11 01:22:10

Expires On :2017-08-11 04:40:59

Signed Using :SHA1

RSA Key size :2048 bits

Default CP Server Certificate:

Version :3

Serial Number :01:DA:52

Issuer :C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA

Subject :0x05=1LUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US, O=securelogin.arubanetworks.com, OU=GT28470348, OU=See www.geotrust.com/resources/cps (c)11, OU=Domain Control Validated - QuickSSL(R) Premium, CN=securelogin.arubanetworks.com

Issued On :2011-05-11 01:22:10

Expires On :2017-08-11 04:40:59

Signed Using :SHA1

RSA Key size :2048 bits

The output of this command displays details such as the version, serial number, subject, issue date, expiry date, type of encryption, and RSA key information for the certificates uploaded to the 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 clarity config

show clarity config

Description

This command displays the status of the clarity configuration parameters on the IAP.

Usage Guidelines

Use this command to view the status of the inline monitoring statistics configured on the IAP.

Example

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

```
Clarity config
-----
Parameter          Value
-----
inline Sta stats    enabled
inline Auth stats   enabled
inline DHCP stats   enabled
inline DNS stats    enabled
```

The output of this command provides the following information:

Parameter	Description
inline Sta stats	Indicates the status of the station passive monitor statistics.
inline Auth stats	Indicates the status of the authentication statistics.
inline DHCP stats	Indicates the status of the DHCP statistics.
inline DNS stats	Indicates the status of the DNS statistics.

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show clarity history

show clarity history {auth|dhcp|dns}

Description

This command displays the history of the clarity configuration parameters.

Parameter	Description
auth	Displays the history of the authentication statistics generated by inline monitoring.
dhcp	Displays the history of the DHCP related statistics generated by inline monitoring.
dns	Displays the history of the DNS statistics generated by inline monitoring.

Usage Guidelines

Use this command to view the history of the clarity configuration parameters.

Example

The following example shows the output of **show clarity history auth** command:

Clarity Auth Trace Buffer

```
-----
Jan  1 15:47:33 DOT1X_EVENT 00:db:df:0a:41:6e ac:a3:1e:c9:32:31 192.168.0.118 3 4
AUTHSERVER_TIMEOUT
Jan  1 15:47:59 DOT1X_EVENT 00:db:df: 0a:41:6e ac:a3:1e:c9:32:31 192.168.0.118 3 6
AUTHSERVER_TIMEOUT
Jan  1 16:05:03 DOT1X_EVENT 00:db:df:0a:41:6e ac:a3:1e:c9:32:31 192.168.0.118 3 6
AUTHSERVER_TIMEOUT
Jun 21 09:25:27 DOT1X_EVENT 00:db:df:0a:41:6e ac:a3:1e:c9:32:21 192.168.0.118 3 13
AUTHSERVER_TIMEOUT
Jun 21 09:25:48 DOT1X_EVENT 00:db:df:0a:41:6e ac:a3:1e:c9:32:31 192.168.0.118 3 4
AUTHSERVER_TIMEOUT
Jun 21 09:26:49 DOT1X_EVENT 00:db:df:0a:41:6e ac:a3:1e:c9:32:31 192.168.0.118 3 5
AUTHSERVER_TIMEOUT
```

The following example shows the output of **show clarity history dns** command:

DNS Server Stats Table ---- In Transaction

```
-----
Server Ip    Max Delay  Min Delay  Avg Delay  RCODE0  RCODE1  RCODE2  RCODE3  RCODE4  RCODE5
Last Query  Last Resp  Samples    Anomaly Cnt Anomaly Ip  RCODE History
-----
10.65.6.33   7758       7758       7758       1        0        0        0        0        0
107870       4799346    1          1          10.65.66.110 1 0 0 0 0 0
Total dns servers in transaction: 1
```

DNS Server Stats Table ---- In Pending Send

```
-----
Server Ip    Max Delay  Min Delay  Avg Delay  RCODE0  RCODE1  RCODE2  RCODE3  RCODE4  RCODE5
Last Query  Last Resp  Samples    Anomaly Cnt Anomaly Ip  RCODE History
-----
```

Total pending send: 0

The following example shows the output of **show clarity history dhcp** command:

DHCP Server Stats Table ---- In Transaction

Client Mac Ip	Sequence	Timestamp	Time Diff1	Time Diff2	Time Diff3	Time Diff4	Server
88:32:9b:a5:59:0c 0.0.0.0	1	552762	0	0	0	0	

Total dhcp clients in transaction: 1

DHCP Server Stats Table ---- In Pending Send

Client Mac	Sequence	Timestamp	Time Diff1	Time Diff2	Time Diff3	Time Diff4	Server Ip

Total pending send: 0

The output of this command provides the following information:

Parameter	Description
inline Sta stats	Indicates the status of the station passive monitor statistics.
inline Auth stats	Indicates the status of the authentication statistics.
inline DHCP stats	Indicates the status of the DHCP statistics.
inline DNS stats	Indicates the status of the DNS statistics.

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	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  
[debug]]
```

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   ESSID      Access Point
----                -
132-15-Auto-PC-Change 10.17.133.241  08:ed:b9:e1:51:7b rev_ipv6 ac:a3:1e:cd:46:94

Channel Type  Role      IPv6 Address      Signal      Speed (mbps)
-----
36+          AN        rev_ipv6  2001:470:36:5c3:ffff:ffff:ffff:64  0 (poor)    0 (poor)
\

Number of Clients      :1
Info timestamp         :605085
```

A similar output is displayed for the **show clients wired** command.

The client list in the command output for both wireless and wired clients provides the following information:

Column	Description
Name	Displays the name of the client
IP address	Displays the IP address of the client.
MAC address	Displays the MAC address of the client.
OS	Indicates the OS running on the client system.
Network	Indicates the SSID and network to which the client is connected.
Access Point	Indicates the IP address of the Access Point to which the client is connected.
Channel	Indicates the channel assigned to the client.
Type	Indicates the type of the Wi-Fi client device.
Role	Indicates the role assigned to the client.
Signal	Indicates the current signal strength of the client, as detected by the IAP.
Speed (Mbps)	Indicates the current speed at which data is transmitted. When the client is associated with an IAP, it constantly negotiates the speed of data transfer. A value of 0 means that the IAP has not received any packets from the client for some time.

show clients <diff>

The **show clients <diff>** command displays the change in the clients table data that occurred during the specified interval. For example, if the value specified for <diff> parameter is 10 seconds, the client table displays the changes such as signal strength or speed that occurred since the last 10 seconds.

show accounting <mac>

The **show accounting <mac>** command displays the accounting information such as status and session ID for a specific client MAC address.

show checksum <mac>

The following output is displayed for the **show checksum <mac>** command:

```
Mac Address:08:ed:b9:e1:51:7d
Basic info
-----
mac
---
08 ed b9 e1 51 7d
bssid
d8 c7 c8 3d 3d 52
ap_ip
0a 11 58 ba
name
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00
ssid
73 72 6f 79 2d 73 6f 6d 65 74 68 69 6e 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00
```



```

auth_failure_count
00
acl
00 8a
acct_session
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
user_role
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
swarm_basic_client_t
08 ed b9 e1 51 7d d8 c7 c8 3d 3d 52 0a 11 58 ba 73 72 6f 79 2d 73 6f 6d 65 74 68 69 6e 67 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8a a9 fe 5a 9a 03 e8 00 00
checksum
02 ec ba ec

```

The **show checksum <mac>** command displays the checksum errors associated with the IAP clients.

show clients debug and show clients wired debug

The **show clients debug** command displays detailed information about the clients MAC and IP addresses, client role, authentication aging time, and accounting intervals, ESSID and BSSID details, VLAN and multicast groups to which the client is associated, and DHCP roles and options associated with the client. The **show clients wired debug** command displays a similar output.

The following example shows the **show clients debug** command output:

Client List

Name	IP Address	MAC Address	OS	ESSID	Access Point
132-15-Auto-PC-Change	10.17.133.241	08:ed:b9:e1:51:7b		rev_ipv6	ac:a3:1e:cd:46:94

Channel	Type	Role	IPv6 Address	Signal	Speed (mbps)	Reauth Age
36+	AN	rev_ipv6	2001:470:36:5c3:ffff:ffff:ffff:64	0 (poor)	0 (poor)	0

Reauth Interval	Reauth ESSID	Auth Type	Authenticated	DEL	Age	Vlan	ESSID
0		N/A	no	no	9	1 (SSID)	()

Private role info	Accounting Session Name	BSSID	Idle Timeout	csum	mcast groups
0 (0-0)	132-15-Auto-PC-Change	ac:a3:1e:54:69:50	1000	0000	(0)

Acct Interval	Class Attribute	Dhcp-Opt Vlan	Dhcp-Opt role	Intercept	Offline	FB Token
0	null	0, (null)	,0,0-0	no	no	null

FB RxBytes	FB TxBytes	SLAAC IP Address	Link Local IP Address
null	null	2001:470:36:5c3:406b:7c14:9d1d:142d	fe80::9198:30aa:5217:d22a

DHCP Status	DHCP v6 Status
Completed	Soliciting

show clients status

The **show clients status <mac>** command displays the status of an IAP client.

show clients roaming

The **show clients roaming** command displays the MAC address and IP address details of IAP from which the client has roamed and IP address of the IAP to which the client is roamed.

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 november 02:00
Baja-California UTC-08 MDT first sunday april 02:00 last sunday october 02:00
Pacific-Time UTC-08 PDT second sunday march 02:00 first sunday november 02:00
Arizona UTC-07
Chihuahua UTC-07 MDT first sunday april 02:00 last sunday october 02:00
La-Paz UTC-07 MDT first sunday april 02:00 last sunday october 02:00
Mazatlan UTC-07 MDT first sunday april 02:00 last sunday october 02:00
Mountain-Time UTC-07 MDT second sunday march 02:00 first sunday november 02:00
Central-America UTC-06
Central-Time UTC-06 CDT second sunday march 02:00 first sunday november 02:00
Guadalajara UTC-06 CDT first sunday april 02:00 last sunday october 02:00
Mexico-City UTC-06 CDT first sunday april 02:00 last sunday october 02:00
Monterrey UTC-06 CDT first sunday april 02:00 last sunday october 02:00
Saskatchewan UTC-06
Bogota UTC-05
Lima UTC-05
Quito UTC-05
Eastern-Time UTC-05 EDT second sunday march 02:00 first sunday november 02:00
Indiana(East) UTC-05 EDT second sunday march 02:00 first sunday november 02:00
```

The output of this command includes the following information:

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 Hour
-----
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
clock timezone	Configures timezones for the IAP.	Config mode
clock summer-time	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 cluster-security

show cluster-security [connections] [peers] [stats]

Description

This command displays cluster security configuration details for all the IAPs in the cluster.

Command/Parameter	Description
cluster-security	Displays the status of the DTLS configuration and DTLS state, whether enabled or disabled.
connections	Displays the total number of connections monitored in the swarm by cluster security dtls.
peers	Displays the details and status of the peers monitored by cluster security dtls.
stats	Displays the cluster security dtls monitoring stats for the cluster

Usage Guidelines

Use this command to view information about the cluster security configuration and monitoring statistics for the IAPs in the cluster.

Example

The following output is displayed for the **show cluster-security** command:

Cluster Security Profile

```
-----
Parameter      Value
-----
DTLS config     Enabled
DTLS state      Enabled
Reboot required No
```

The following output is displayed for the **show cluster-security connections** command:

```
-----
IDX          :Connection Index
Flags        :I-Initiator, R-Responder
Inactivity   :Time remaining till inactivity timeout
Re-Neg       :Time remaining till Re-negotiation
-----
Cluster Security DTLS Connections
-----
Local IDX  Remote IDX  State  Flags  Local Address  Peer Address  Rx bytes  Tx
bytes Age          Inactivity Re-Neg
-----
-----
19bb00b0   7df90024   connected  R      10.17.142.77[4434]  10.17.142.74[4434]  673511
138016 05h:04m:32s 01m:55s 01h:54m:37s
19bb00b1   4db20024   connected  R      10.17.142.77[4434]  10.17.142.73[4434]  394516
80788 02h:58m:17s 01m:53s 04h:21m:06s
19bb00b2   1f6e0024   connected  R      10.17.142.77[4434]  10.17.142.76[4434]  354332
74632 02h:44m:18s 01m:57s 03h:55m:52s
19bb00b3   7d6f0024   connected  I      10.17.142.77[4434]  10.17.142.71[4434]  269882
57304 02h:09m:39s 01m:57s 04h:33m:12s
19bb00b4   57fd0024   connected  R      10.17.142.77[4434]  10.17.142.75[4434]  90933
18544 40m:59s      01m:52s 05h:56m:43s
```

Total connections count:5

The following output is displayed for the **show cluster-security peers** command:

```
-----
IDX          :Connection Index
-----
Cluster Security DTLS Peers
-----
Peer Address      State   Local IDX
-----
10.17.142.76[4434] active 19bb00b2
10.17.142.73[4434] active 19bb00b1
10.17.142.75[4434] active 19bb00b4
10.17.142.74[4434] active 19bb00b0
10.17.142.71[4434] active 19bb00b3
Total peers count:5
```

The following output is displayed for the **show cluster-security stats** command:

```
Cluster Security Statistics
-----
Statistic Name                               Counts
-----
No resource                                0
Dropped messages                          0
New connection alloc success/fail/free    180/0/175
New connection establishment success/fail  180/0
Connection lookup fail                     0
Connection init attempts                   83
Connection renegotiations attempts         83
Connection init request fail               0
Connection response attempts              97
New peers alloc success/fail/freed         5/0/0
Peer init response fail                    0
Peer connection slots full                 0
Signing module not init/async fail         3/0
Entropy not available                     0
Retrieve date-time fail                    0
Inits retried                             3
Connection timeouts                       0
Connection timeouts (inactivity)           0
Connection responses timeouts              0
Handshake fail after retransmit            0
Handshake fail after signing in retries    0
Signing module op attempts/success/fail/busy 180/180/0/1
Socket msgs rx success/fail                1221386/0
Discovery msg tx success/fail              0/0
Discovery msg rx (allowed)                 0
Msg rx on old ports (dropped)              0
Unsecure msg tx success/fail               0/0
Unsecure msg rx allow/drop                 586369/0
Loopback msg sent to AP's uplink IP        0
18:64:72:cf:ec:9a# show cluster-security connections stats
Cluster Security Connections Statistics for: Local Idx = 19bb00b0
-----
Statistic Name                               Counts
-----
IO Send success/fail                       1835/0
IO Receive success/fail                    2583/0
IO Receive peek fail                       0
Peer connection mismatch                   1
Handshake success after signing in retries 0
Signing still in progress (dropped)        0
Negotiate msg rx success/fail              5/0
```

```

Peer init request tx/response rx          0/0
Signing module op attempts/success/fail  1/1/0
Signing in module busy                    0
Verify peer mac address fail              0
Verify peer certificate fail              0
Retransmitted handshakes                  0
SSL msg write fail (out of resources)     0
SSL msg write fail (error)                0
SSL msg read fail (out of resources)      0
SSL msg read fail (error)                 0
Total DTLS msg tx/rx                     1825/2575
Cluster Security Connections Statistics for: Local Idx = 19bb00b1
-----

```

Statistic Name	Counts
-----	-----
IO Send success/fail	1082/0
IO Receive success/fail	1522/0
IO Receive peek fail	0
Peer connection mismatch	0
Handshake success after signing in retries	0
Signing still in progress (dropped)	0
Negotiate msg rx success/fail	5/0
Peer init request tx/response rx	0/0
Signing module op attempts/success/fail	1/1/0
Signing in module busy	0
Verify peer mac address fail	0
Verify peer certificate fail	0
Retransmitted handshakes	0
SSL msg write fail (out of resources)	0
SSL msg write fail (error)	0
SSL msg read fail (out of resources)	0
SSL msg read fail (error)	0
Total DTLS msg tx/rx	1072/1514
Cluster Security Connections Statistics for: Local Idx = 19bb00b2	

Statistic Name	Counts
-----	-----
IO Send success/fail	1001/0
IO Receive success/fail	1424/0
IO Receive peek fail	0
Peer connection mismatch	0
Handshake success after signing in retries	0
Signing still in progress (dropped)	0
Negotiate msg rx success/fail	5/0
Peer init request tx/response rx	0/0
Signing module op attempts/success/fail	1/1/0
Signing in module busy	0
Verify peer mac address fail	0
Verify peer certificate fail	0
Retransmitted handshakes	0
SSL msg write fail (out of resources)	0
SSL msg write fail (error)	0
SSL msg read fail (out of resources)	0
SSL msg read fail (error)	0
Total DTLS msg tx/rx	991/1416
Cluster Security Connections Statistics for: Local Idx = 19bb00b3	

Statistic Name	Counts
-----	-----
IO Send success/fail	772/0
IO Receive success/fail	1086/0
IO Receive peek fail	0


```

Peer connection mismatch                0
Handshake success after signing in retries 0
Signing still in progress (dropped)      0
Negotiate msg rx success/fail           5/0
Peer init request tx/response rx         1/1
Signing module op attempts/success/fail 1/1/0
Signing in module busy                   0
Verify peer mac address fail             0
Verify peer certificate fail             0
Retransmitted handshakes                 0
SSL msg write fail (out of resources)    0
SSL msg write fail (error)               0
SSL msg read fail (out of resources)     0
SSL msg read fail (error)               0
Total DTLS msg tx/rx                    763/1077
Cluster Security Connections Statistics for: Local Idx = 19bb00b4
-----

```

Statistic Name	Counts
IO Send success/fail	263/0
IO Receive success/fail	384/0
IO Receive peek fail	0
Peer connection mismatch	0
Handshake success after signing in retries	0
Signing still in progress (dropped)	0
Negotiate msg rx success/fail	6/0
Peer init request tx/response rx	0/0
Signing module op attempts/success/fail	1/1/0
Signing in module busy	0
Verify peer mac address fail	0
Verify peer certificate fail	0
Retransmitted handshakes	0
SSL msg write fail (out of resources)	0
SSL msg write fail (error)	0
SSL msg read fail (out of resources)	0
SSL msg read fail (error)	0
Total DTLS msg tx/rx	253/376

```

18:64:72:cf:ec:9a# show cluster-security peers stats
Cluster Security Peers' Statistics for: Remote Address = 10.17.142.76
-----

```

Statistic Name	Counts
Peer collisions occurred/resolved	0/0
Peer connections active/connected/recv data/close notify/shutdown	36/16/0/20/0
Peer connections being renegotiated	15

Cluster Security Peers' Statistics for: Remote Address = 10.17.142.73

Statistic Name	Counts
Peer collisions occurred/resolved	0/0
Peer connections active/connected/recv data/close notify/shutdown	36/21/0/15/0
Peer connections being renegotiated	20

Cluster Security Peers' Statistics for: Remote Address = 10.17.142.75

Statistic Name	Counts
Peer collisions occurred/resolved	0/0
Peer connections active/connected/recv data/close notify/shutdown	36/17/0/19/0
Peer connections being renegotiated	16

Cluster Security Peers' Statistics for: Remote Address = 10.17.142.74

Statistic Name	Counts

```

-----
Peer collisions occurred/resolved                                0/0
Peer connections active/connected/recv data/close notify/shutdown 36/18/0/18/0
Peer connections being renegotiated                             17
Cluster Security Peers' Statistics for: Remote Address = 10.17.142.71
-----
Statistic Name                                                  Counts
-----
Peer collisions occurred/resolved                                0/0
Peer connections active/connected/recv data/close notify/shutdown 36/16/0/20/0
Peer connections being renegotiated

```

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	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 config-status

show config-status

Description

This command displays the details about the configuration status of an IAP.

Usage Guidelines

Use this command to view the current configuration status of the IAP in flash memory.

Example

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

```
Config Status
-----
Config Name Compressed
-----
Primary No
Backup No
```

The backup configuration is used when the primary configuration is lost. And the **Compressed** option indicates that the configuration file has been compressed if the file size is large.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show console-settings

show console-settings

Description

This command displays the details about the console settings of an IAP.

Usage Guidelines

Use this command to view if the access to IAP console is enabled or disabled.

Example

The following example shows the output of the **show console-settings** command:

```
(Instant AP)# show console-settings
Console Setting
-----
Status
-----
enabled
```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 list of supported country codes for the IAP.

Usage Guidelines

Use this command to view a list of the supported country codes.

Example

The following example shows a partial output of the **show country-codes** command .

```
CA:Canada
DE:Germany
NL:Netherlands
IT:Italy
PT:Portugal
LU:Luxembourg
NO:Norway
SE:Sweden
FI:Finland
DK:Denmark
CH:Switzerland
CZ:Czech Republic
BE:Belgium
ES:Spain
GB:United Kingdom
KR:Republic of Korea (South Korea)
CN:China
FR:France
HK:Hong Kong
SG:Singapore
TW:Taiwan
MY:Malaysia
BR:Brazil
SA:Saudi Arabia
LB:Lebanon
AE:United Arab Emirates
ZA:South Africa
AR:Argentina
AU:Australia
AT:Austria
BO:Bolivia
CL:Chile
GR:Greece
HU:Hungary
IS:Iceland
IN:India
IE:Ireland
KW:Kuwait
LV:Latvia
LI:Liechtenstein
LT:Lithuania
MX:Mexico
MA:Morocco
NZ:New Zealand
PL:Poland
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 6.4.3.1-4.2	The output of the command displays a list of supported country codes only.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show cpcert

show cpcert

Description

This command displays the details of the captive portal server certificate used by the IAP for guest authentication.

Usage Guidelines

Use this command to view information about the captive portal server certificate uploaded on n IAP.

Example

The following example shows the default certificate details of the captive portal server in the output of the **show cpcert** command:

```
Default Server Certificate:
Version      :3
Serial Number :01:DA:52
Issuer       :C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA
Subject      :0x05=1LUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US, O=securelogin.arubanetworks.com,
OU=GT28470348, OU=See www.geotrust.com/resources/cps (c)11, OU=Domain Control Validated -
QuickSSL(R) Premium, CN=securelogin.arubanetworks.com
Issued On    :2011-05-11 01:22:10
Expires On   :2017-08-11 04:40:59
Signed Using :SHA1
RSA Key size :2048 bits
```

The output of this command describes details such as the version, serial number, subject, issue date, expiry date, type of encryption, and RSA key information for the captive portal certificates uploaded to the IAP.

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 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|ipv6 {session|user}|dmo-session|dmo-station <mac>|mcast|nat-pool  
<ID>|route|session[ucc|dpi <verbose>]|statistics|user|vlan}
```

Descriptions

This command shows the system statistics for your 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 ACL table allocation details.
acl-rule <rule>	Displays the name of the ACL.
acl-rule-detail <acl>	Displays the ACL rule details.
bridge	Shows bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for anIAP.
ipv6 session	Displays datapath for IPv6 session table.
ipv6 user	Displays datapath statistics for IPv6 users.
dmo-session	Displays details of a DMO session.
dmo-station <mac>	Displays details of a DMO station.
mcast	Displays multicast table statistics for the IAP.
nat-pool <ID>	Displays the contents of the datapath NAT entries table. It displays NAT pools as configured in the datapath. Statistics include pool, SITP start, SIP end and DIP.
route	Displays datapath route table statistics.
session {ucc dpi<verbose>}	Displays datapath session statistics.
statistics	Displays datapath station association table statistics.
user	Displays datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users and maximum link length.
vlan	Displays VLAN table information such as VLAN memberships inside the datapath including L2 tunnels which tunnel L2 traffic.

Usage Guidelines

Use the show **datapath** command to display various datapath statistics for debugging purposes

Examples

show datapath acl

The following example shows the output of **show datapath acl** command.

Datapath ACL 3 Entries

```
-----
Flags: P - permit, L - log, E - established, M/e - MAC/etype filter
S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror
I - Invert SA, i - Invert DA, H - high prio, O - set prio, C - Classify Media
A - Disable Scanning, B - black list, T - set TOS, 4 - IPv4, 6 - IPv6
-----
```

show datapath acl-all

The following example shows the output of **show datapath acl-all** command.

```
ACL Name {magic-vlan} Number {106}
1: any any 17 0-65535 8209-8211 P4
2: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 any P4
3: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 any P4
4: 192.168.10.0 255.255.254.0 any any PS4
5: any any any P4 hits 2127
-----
ACL Name {internal-cp-magic} Number {107}
1: any 192.168.10.1 255.255.255.255 6 0-65535 80-80 PSD4
2: any 192.168.10.1 255.255.255.255 6 0-65535 443-443 PSD4
3: any any 6 0-65535 80-80 PSD4
4: any any 6 0-65535 443-443 PSD4
5: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 17 0-65535 67-68 P4
6: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 17 0-65535 67-68 P4
7: 192.168.10.0 255.255.254.0 any 17 0-65535 67-68 PS4
8: any any 17 0-65535 67-68 P4
9: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 17 0-65535 53-53 P4
10: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 17 0-65535 53-53 P4
11: 192.168.10.0 255.255.254.0 any 17 0-65535 53-53 PS4
12: any any 17 0-65535 53-53 P4
13: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 6 0-65535 8081-8081 P4
14: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 6 0-65535 8081-8081 P4
15: 192.168.10.0 255.255.254.0 any 6 0-65535 8081-8081 PS4
16: any any 6 0-65535 8081-8081 P4
17: any any any 4
-----
ACL Name {external-cp-magic} Number {108}
1: any 192.168.10.1 255.255.255.255 6 0-65535 80-80 PSD4
2: any 192.168.10.1 255.255.255.255 6 0-65535 443-443 PSD4
3: any any 6 0-65535 80-80 PSD4
4: any any 6 0-65535 443-443 PSD4
5: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 17 0-65535 67-68 P4
6: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 17 0-65535 67-68 P4
7: 192.168.10.0 255.255.254.0 any 17 0-65535 67-68 PS4
8: any any 17 0-65535 67-68 P4
9: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 17 0-65535 53-53 P4
10: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 17 0-65535 53-53 P4
11: 192.168.10.0 255.255.254.0 any 17 0-65535 53-53 PS4
12: any any 17 0-65535 53-53 P4
13: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 6 0-65535 8081-8081 P4
14: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 6 0-65535 8081-8081 P4
```



```

15: 192.168.10.0 255.255.254.0 any 6 0-65535 8081-8081 PS4
16: any any 6 0-65535 8081-8081 P4
17: any any any 4
-----

```

show datapath acl-allocation

The following example shows the output of **show datapath acl-allocation** command.

```

ACL ACE Start ACE Block Size
-----
105 3200 32
103 3234 16
107 3250 32
104 3282 16
108 3298 32
100 3330 2
101 3332 4
102 3336 4
134 3340 4
135 3344 8
136 3352 4
143 3360 8
145 3372 8
130 3380 16
131 3412 16
132 3444 16
133 3476 16
137 3508 8
139 3520 8
141 3532 8
146 3540 4
147 3544 8
148 3552 4
149 3556 8
150 3564 4
151 3568 4
152 3572 4
153 3576 4
138 3580 8
140 3588 8
142 3596 8
144 3604 8
106 3612 8

```

show datapath acl-rule

The following example shows the output of **show datapath acl-rule** command.

```

Datapath SSID: test ACL Entries
-----
Flags: P - permit, L - log, E - established, M/e - MAC/etype filter
S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror
I - Invert SA, i - Invert DA, H - high prio, O - set prio, C - Classify Media
A - Disable Scanning, B - black list, T - set TOS, 4 - IPv4, 6 - IPv6
-----
ACL Name {test 0} Number {142}
1: any any 17 0-65535 8209-8211 P4
2: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 any P4
3: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 any P4
4: 192.168.10.0 255.255.254.0 any any PS4
5: any any any P4
-----
ACL Name {test 1} Number {143}

```

```

1: any any 17 0-65535 8209-8211 P4
2: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 any P4
3: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 any P4
4: 192.168.10.0 255.255.254.0 any any PS4
5: any any any P4
-----
ACL Name {test 2} Number {144}
1: any any 17 0-65535 8209-8211 P4
2: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 any PT4
3: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 any PT4
4: 192.168.10.0 255.255.254.0 any any PST4
5: any any any PT4
-----
ACL Name {test 3} Number {145}
1: any any 17 0-65535 8209-8211 P4
2: 192.168.10.0 255.255.254.0 192.168.10.0 255.255.254.0 any PT4
3: 192.168.10.0 255.255.254.0 224.0.0.0 224.0.0.0 any PT4
4: 192.168.10.0 255.255.254.0 any any PST4
5: any any any PT4
-----

```

show datapath bridge

The following example shows the output of **show datapath bridge** command.

```

Datapath Bridge Devices
-----
Flags: F - source-filter, T - trusted, Q - tagged, I - IP
S - split-tunnel, B - bridge, M - mesh, P - PPPoE
C - content-filter, O - corp-access, h - to HAP, f - to FAP
h - dhcp-redirect
Dev Name VLANs PVID ACLs FramesRx FramesTx Flags
---
3 bond0 1 1 0/0 618048 95826 FTQB
8 br0 0 1 105/0 95432 0 IB
11 aruba002 1 1 100/0 0 176788 B
12 aruba102 1 1 100/0 0 140373 B
13 aruba003 1 1 100/0 0 139236 B
14 aruba103 1 1 100/0 0 0 B
Datapath Bridge Table Entries
-----
Flags: P - Permanent, D - Deny, R - Route, M - Mobile, X - Xsec, A - Auth
AP Flags: X - Awaiting 1X reply, B - Block all non-1X traffic, F - Force bridge role
MAC VLAN Assigned VLAN Destination Flags AP Flags Bridge Role ACL
-----
00:1A:1E:0D:7E:D3 1 1 dev3 0
D8:C7:C8:C4:42:98 1 1 local P 0
D8:C7:C8:C4:42:98 3333 3333 local P 0
00:0B:86:40:1C:A0 1 1 dev3 0
6C:F3:7F:C3:5C:12 64 64 dev3 0

```

show datapath ipv6 session

The following example shows the output of the **show datapath ipv6 session** command:

```

Datapath Session Table Entries (v6)
-----
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
I - Deep inspect, U - Locally destined
s - media signal, m - media mon, a - rtp analysis
E - Media Deep Inspect, G - media signal

```

```

A - Application Firewall Inspect
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to master, t - time based
Source IP                               Destination IP Prot SPort Dport
-----
fe80::aea3:1eff:fe4d:4708               ff02::16      58   5782  36608
fe80::6273:5cff:fe65:ee19               ff02::16      58   53973 36608
fe80::9198:30aa:5217:d22a               ff02::16      58   47682 36608
fe80::6273:5cff:fe65:ee19               ff02::d       103   0      0
fe80::6273:5cff:fe65:ee19               ff02::1       58   43684 33280
fe80::f25c:19ff:fe4b:34d0               ff02::16      58   64552 36608
fe80::9198:30aa:5217:d22a               ff02::16      58   30486 36608
fe80::3e97:eff:fe48:9e45                ff02::16      58   59459 36608
fe80::aea3:1eff:fe4d:4694               ff02::16      58   5968  36608
fe80::aea3:1eff:fe4d:471a               ff02::16      58   1289  36608

Cntnr Prio ToS Age Destination TAge  Flags
-----
0      0      0      1      dev8          6e    C
0      0      0      1      dev8          63    C
0      0      0      1      dev8          60    C
0      0      0      0      dev8          8     C
0      0      0      1      dev8          88    C
0      0      0      1      dev8          82    C
0      0      0      1      dev8          6c    C
0      0      0      1      dev8          59    C
0      0      0      1      dev8          62    C
0      0      0      1      local         76    C

```

show datapath ipv6 user

The following example shows the output of the **show datapath ipv6 user** command:

```

Datapath User Table Entries (v6)
-----
Flags: P - Permanent, W - WEP, T- TKIP, A - AESCCM
R - ProxyARP to User, N - VPN, L - local, I - Intercept, D - Deny local routing
FM(Forward Mode): S - Split, B - Bridge, N - N/A
IP                               MAC                               ACLs      Contract      Location      Age
-----
2001:470:36:5c3:ffff:ffff:ffff:5b  AC:A3:1E:CD:47:1A  105/0      0/0           0             0
fe80::aea3:1eff:fe4d:471a          AC:A3:1E:CD:47:1A  105/0      0/0           0             0

Sessions      Flags      Vlan  FM
-----
0/65535          1      N
0/65535          1      N

```

show datapath dmo-session

The following example shows the output of **show datapath dmo-session** command.

```

MCAST Groups:
-----
Source Group Vlan Age[s] BSSs Received Multicast Converted Unicast Dropped _Stas _l2grp _l3grp
DMO queue: size:256, dropped:0, rescheduled:0, length:0, high-water:0
DMO Sessions:
-----

```

show datapath dmo-station

The following example shows the output of **show datapath dmo-station** command.

```

Group Ref_count Position

```

show datapath mcast

The following example shows the output of **show datapath mcast** command.

```
Dev Vlans
-----
dev3 1
dev11 1
dev12 1
dev13 1
dev14 1
```

show datapath nat-pool

The following example shows the output of **show datapath nat-pool** command.

```
Datapath NAT Pool Entries
-----
ID Begin Source IP End Source IP Destination IP Flags
--
```

show datapath route

The following example shows the output of **show datapath route** command.

```
Route Table Entries
-----
Flags: L - Local, P - Permanent, T - Tunnel, I - IPsec, M - Mobile, A - ARP, D - Drop
IP Mask Gateway Cost VLAN Flags
-----
0.0.0.0 0.0.0.0 10.17.88.2 0 0
192.168.10.0 255.255.254.0 192.168.10.1 0 3333 D
0.0.0.0 255.255.255.192 10.17.88.59 0 1 L
Route Cache Entries
-----
Flags: L - local, P - Permanent, T - Tunnel, I - IPsec, M - Mobile, A - ARP, D - Drop
IP MAC VLAN Flags
-----
10.17.88.2 00:0B:86:40:1C:A0 1 A
10.17.88.59 D8:C7:C8:C4:42:98 1 LP
192.168.10.1 D8:C7:C8:C4:42:98 3333 LP
```

show datapath session

The following example shows the partial output of **show datapath session ucc** command.

```
Datapath Session Table Entries
-----
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
I - Deep inspect, U - Locally destined
s - media signal, m - media mon, a - rtp analysis
E - Media Deep Inspect, G - media signal
A - Application Firewall Inspect
L - ALG session
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to master, t - time based

Source IP      Destination IP  Prot SPort Dport Cntr Prio ToS  Destination  Flags Codec
-----
10.17.138.91   10.17.138.90  17   50023 50022 0    0    40   dev18        FHTCVL X_H264UC
10.17.138.90   10.17.138.91  17   50022 50023 0    0    40   dev18        FHTVL  X_H264UC
10.17.138.91   10.17.138.90  17   50012 50014 0    0    48   dev18        FHTCVL SILK
10.17.138.90   10.17.138.91  17   50014 50012 0    0    48   dev18        FHTVL  SILK
```

The following example shows the output of **show datapath session dpi** command.

Datapath Session Table Entries

Flags: F - fast age, S - src NAT, N - dest NAT

D - deny, R - redirect, Y - no syn

H - high prio, P - set prio, T - set ToS

C - client, M - mirror, V - VOIP

I - Deep inspect, U - Locally destined

s - media signal, m - media mon, a - rtp analysis

E - Media Deep Inspect, G - media signal

A - Application Firewall Inspect

L - ALG session

RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to master, t - time based

DPI Flags: a - app extraction done, b - URL extraction done

c - copied to dpimgr, d - dropped reverse session on bca cache miss

w - waiting for classification, e - enforcement done

f - app classification done, g - webcc classification done

DPI WebRep: 1 - High Risk Sites, 2 - Suspicious Sites

3 - Moderate Risk Sites, 4 - Low Risk Sites

5 - Trustworthy Sites

Source IP	Destination IP	Prot	SPort	Dport	App	Webcat
WebRep	Packets	Bytes	PktsDpi	Flags	DPIFlags	
10.20.120.252	173.223.235.19	6	63421	80	linkedin	[305] content-
delivery-ne [65]	5	0	0	1	C	abcdefg
10.20.120.228	10.13.5.200	17	50338	53	incomplete	[6] Web-Not-Class
[0] 0	1	55	1	FCIA	ac	
10.22.152.66	10.20.120.252	6	443	63460	https	[68] Web-Not-Class
[0] 0	0	0	3		acef	
10.20.120.240	132.245.73.194	6	54365	443	office365	[1448] computer-and-
intern [5] 5	0	0	1	CGs	abcefg	
74.125.68.188	10.20.120.228	6	5228	5844	gtalk	[1441] category-unknown
[84] 7	0	0	0		acef	
10.1.10.10	10.20.120.252	6	139	63391	incomplete	[6] category-unknown
[84] 7	0	0	3	F	ace	
15.50.26.221	10.20.120.144	6	5222	50783	App-Not-Class	[0] Web-Not-Class
[0] 0	0	0	0	YA		
10.20.120.187	216.58.197.69	17	57576	443	incomplete	[6] Web-Not-Class
[0] 0	5	220	5	FC	ace	
10.20.120.173	10.22.35.50	6	50162	22	ssh	[198] category-unknown
[84] 7	0	0	1	C	acef	
10.20.120.147	40.113.14.159	6	51324	443	office365	[1448] business-and-
econom [4] 5	0	0	1	CGs	abcefg	
computer-and-intern [5]	5					
10.20.120.187	10.20.50.10	6	55956	135	epm	[37] category-unknown
[84] 7	0	0	1	FC	acef	
10.20.120.198	172.217.26.78	6	56432	443	google	[54] shopping
[7] 5	1	29	1	CGs	abcefg	
news-and-media	[63] 5					
10.20.120.147	10.44.96.64	6	62236	44591	App-Not-Class	[0] Web-Not-Class
[0] 0	0	0	0	C		
132.245.244.146	10.20.120.198	6	443	54673	office365	[1448] computer-and-
intern [5] 5	0	0	0		abcefg	
10.20.120.198	10.1.10.10	6	56463	445	incomplete	[6] category-unknown
[84] 7	3	108	6	FC	ace	
10.20.120.251	59.161.166.108	6	37685	8080	incomplete	[6] category-unknown
[84] 7	0	0	3	C	ace	
132.245.242.114	10.20.120.173	6	443	50119	office365	[1448] computer-and-
intern [5] 5	0	0	0		abcefg	
10.1.8.53	10.20.120.153	6	80	49543	soap	[191] private-ip-
adresse [77] 4	7	354	0	F	abcefg	

10.29.83.170	10.20.120.173	6	22	63997 ssh	[198] category-unknown
[84] 7	1 28 0			acef	
24:77:03:CE:B3:1C		0806		App-Not-Class	[0] Web-Not-Class
[0] 0	0 0	F			
216.58.197.78	10.20.120.228	6	443	8590 google-play	[1122] shareware-and-
freew [30] 5	1 34 0			abcefg	
10.20.120.228	10.53.12.175	6	5017	22 ssh	[198] category-unknown
[84] 7	0 0 0		C	acef	
10.20.120.198	172.217.26.78	6	56433	443 google	[54] search-engines
[50] 5	1 29 1		CGs	abcefg	
10.20.120.252	10.1.8.53	6	63454	80 soap	[191] private-ip-
adresse [77] 4	0 0	2	FC	abcefg	
10.22.152.66	10.20.120.252	6	443	63269 https	[68] Web-Not-Class
[0] 0	0 0 3			acef	
10.22.152.66	10.20.120.252	6	443	63461 https	[68] Web-Not-Class
[0] 0	0 0 3			acef	
10.20.120.240	10.20.120.255	17	137	137 nbns	[128] Web-Not-Class
[0] 0	5 186 1		FC	acef	
10.20.120.173	10.13.5.200	17	60658	53 incomplete	[6] Web-Not-Class
[0] 0	0 0 1		FCIA	ac	
10.1.10.10	10.20.120.252	6	139	63390 incomplete	[6] category-unknown
[84] 7	0 0 5		F	ace	
10.44.96.200	10.20.120.252	6	41050	62338 msrpc	[742] category-unknown
[84] 7	1 34 0			acef	

show datapath statistics

The following example shows the partial output of **show datapath statistics** command.

```
Datapath Counters
-----
Counter Value
-----
Tagged frames dropped on untagged interface 0
Frames dropped for being too short 0
Frames received on port not in VLAN 0
Non-dot1x frames dropped during L2 blocking 0
Frames dropped for ingress change on permanent bridge entry 0
Frames received on port not in VLAN 0
Unicast frames filtered 86
Frames dropped due to FP firewall 6
Frames that failed FP spoofing check 0
Frames dropped with logging 0
Frames dropped due to unknown FP opcode 0
Frames freed by FP 3
Frames that failed SP spoofing check 0
Frames dropped due to excessive user misses 0
Frames dropped due to no buffers 0
Frames dropped due to no 'br0' device 0
Frames dropped due to no stack IP address 0
Frames dropped while user miss pending 0
Frames dropped when user entry creation failed 0
Frames dropped due to unknown FP opcode 0
Frames dropped due to initial IP route lookup failure 0
Frames dropped due to final IP route lookup failure 0
Frames dropped due to ARP processing failure 0
Frames dropped due to illegal device index 0
Frames dropped due to interface being down 0
Unicast frames not bridged due to split-tunnel destination 0
Unicast frames from bridge role user dropped 0
Unicast frames that could not be bridged to split tunnel 0
Frames dropped due to missing PPP device 0
Frames dropped due to pullup failure 0
Frames dropped due to misalignment 0
```

```

Frames received by firewall 715679
DHCP frames on DHCP local VLAN 96041
PPPOE frames to session processing 0
Frames needing bridging 716075
Mesh frames forwarded 0
Thin AP frames forwarded 0
Frames to session processing 718714
Frames to SP 21792
Frames bridged by SP 396
Frames routed by SP 0
Frames for SP session processing 17454
Frames for FP application processing 3942
Frames bridged by FP 0
Frames for FP session processing 2725
Frames routed by FP 18577
FP user misses 73
Frames not tunneled from bridge role user 0
SP user misses 73
Frames to DHCP 18
Frames to DNS 0
Frames held 0
Frames needed routing 715572
Frames needed forwarding 634373
Frames redirected to CSS tunnel 0
Frames sent by firewall 94681
Frames delivered to stack 82061
Frames delivered to CP 0
Frames to be flooded 538842
Frames potentially needing flooding 637659

```

show datapath user

The following example shows the partial output of **show datapath user** command.

Datapath User Table Entries

```

-----
Flags: P - Permanent, W - WEP, T- TKIP, A - AESCCM
R - ProxyARP to User, N - VPN, L - local
FM(Forward Mode): S - Split, B - Bridge, N - N/A
IP MAC ACLs Contract Location Age Sessions Flags Vlan FM
-----
10.17.88.59 D8:C7:C8:C4:42:98 105/0 0/0 0 0 1/65535 1 N
0.0.0.0 D8:C7:C8:C4:42:98 105/0 0/0 0 0 0/65535 P 1 N
192.168.10.1 D8:C7:C8:C4:42:98 105/0 0/0 0 11115 0/65535 P 3333 B

```

show datapath vlan

The following example shows the partial output of **show datapath vlan** command.

Datapath VLAN Table Entries

```

-----
Flags: N - Nat Inside, M - Route Multicast, R - Routing
S - Snoop MLD, G - Snoop IGMP, P - Proxy IGMP
VLAN Flags Ports
----
1 R dev3
1 R dev11
1 R dev12
1 R dev13
1 R dev14

```

The outputs of the **show datapath** command indicates the following:

- ACL table allocation details for the IAP.
- IAP Datapath ACL Tables.
- List of ACL rules configured for the SSID and Ethernet port profiles.
- Bridge table entry statistics including MAC address, VLAN, assigned VLAN, destination and flag information for the IAP.
- Details of a DMO session.
- Multicast table statistics for the IAP.
- Route table statistics for the IAP.
- Datapath session table statistics for the IAP
- Hardware packet statistics for the IAP.
- Datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length for the IAP.
- VLAN table information such as VLAN memberships inside the datapath including L2 tunnels for the IAP.

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	The ucc parameter is added show datapath session.
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 ddns

show ddns [clients]

Description

This command displays the DDNS status of the IAP and the list of DDNS clients.

Usage Guidelines

Use this command to view information about the DDNS clients.

Example

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

```
DDNS Enabled      :Enabled
DDNS Server       :10.17.132.85
DDNS Key          :hmac-sha1:ddns-key:asdfasdfsgdsgs=
DDNS Interval     :900
```

The following output is displayed for the **show ddns clients** command:

```
DDNS Client List
-----
Host Name      Domain Name  IP Address  DHCP profile name  Success Count  Failure Count
-----
iap1-ddns-home test.ddns    192.192.192.17 None               16             22
132-13-Auto-PC test.ddns    192.168.99.18 DistL3             9              3
132-14-Auto-PC test.ddns    192.168.99.4  DistL3             2              0

Last updated   Last update status
-----
7 seconds ago  Success
7 seconds ago  Success
7 seconds ago  Success
```



DHCP profile name is None for the Master IAP update sent.

The output of this command provides the following information:

Command/Parameter	Description
Host Name	Displays the hostname of the DDNS client
Domain Name	Displays the domain name mapped to the DDNS client.
IP Address	Denotes the IP address of the DDNS client.
DHCP profile name	Denotes the profile name of the DHCP server.
Success Count	Indicates the number of times the update sent to the DNS server succeeded.
Failure Count	Indicates the number of times the update sent to the DNS server got failed.

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show delta-config

```
show delta-config cfgid
```

Description

This command displays the difference between the current configuration in the current CLI session and the configuration that is saved on the IAP.

Usage Guidelines

Use this command to view the difference between the current configuration information stored in the IAP flash memory and the configuration information saved in the IAP memory.

Example

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

```
103-Master# show delta-config
IAP delta configuration current_config_id:7
IAP delta configuration top_config_id:7
```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 AP)# show dhcp-allocation
-----/etc/dnsmasq.conf-----
listen-address=127.0.0.1
addn-hosts=/etc/ld_eth_hosts
addn-hosts=/etc/ld_ppp_hosts
dhcp-src=192.168.10.1
dhcp-leasefile=/tmp/dnsmasq.leases
dhcp-authoritative
filterwin2k
#magic-vlan
{
vlan-id=3333
dhcp-range=192.168.10.3,192.168.11.254,255.255.254.0,12h
dhcp-option=1,255.255.254.0
dhcp-option=3,192.168.10.1
dhcp-option=6,10.1.1.50
dhcp-option=54,192.168.10.1
}
-----/tmp/dnsmasq.leases-----
```

Command History

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 dhcpc-opts

show dhcpc-opts

Description

This command displays the DHCP options configured on an IAP.

Usage Guidelines

Use this command to view the current status of the vendor-specific DHCP options configured on an IAP. The DHCP options are configured and enabled for assignment and distribution to DHCP clients based on the type of DHCP server, scope, and clients.

Example

The following output is displayed for the **show dhcpc-opts** command:

```
-----DHCP option43 -----  
Not available
```

The output of this command displays the vendor-specific DHCP option configured for a DHCP scope and the current status of the DHCP option.

Command History

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 DHCP Host
-----
Centralized DHCP Scopes
-----
Name Type VLAN DHCP Relay DHCP Relay Servers DHCP Option 82 VLAN IP VLAN Mask Split
Tunnel
-----
-----

Local DHCP Scopes
-----
Name Type VLAN Network Netmask Exclude Address DNS Server Domain Name Lease Time DHCP Option
-----
local Local 12 12.12.12.0 255.255.255.0 0.0.0.0 0.0.0.0

DHCP Host DNS Cache
-----
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. • Distributed, L2 • Distributed, L3 • Local • Local, L3

Parameter	Description
	Centralized, L2
VLAN	Indicates the VLAN ID assigned to DHCP scope.
Netmask	Displays the subnet mask.
DNS Server	Displays the DNS server IP address.
Domain Name	Displays the domain name configured for the DHCP scope.
Default router	Displays the IP address of the default router.
lease-time	Displays the lease-time configured for the DHCP clients.
IP Address Range	Displays the range of IP addresses configured for the distributed DHCP scopes.
client-count <number>	Displays the number of clients allowed per DHCP branch.
DHCP Option	Displays the DHCP option if configured.
Reserve First and Reserve Last	Displays the first few and the last few IP addresses reserved in the subnet.
Branch ID	Displays the DHCP branch ID.
Branch Netmask	Displays the branch subnet mask.
Branch Router	Displays the IP address if the branch router.
Exclude IP address	Displays the excluded IP address. The value displayed in this determines the exclusion range of the subnet. Based on the size of the subnet, the IP addresses that come before or after the IP address value specified in this field are excluded.
DHCP Relay	Displays the DHCP relay information that enables the IAPs to intercept the broadcast packets and relay DHCP requests directly to corporate network.
DHCP Relay Server	Displays the IP address of the corporate DHCP server for the DHCP request relay.
Split Tunnel	Indicates if the split-tunnel function is enabled or disabled.
DHCP Host	Indicates the DHCP host name if configured.
DNS cache	Indicates if DNS caching is enabled or disabled.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 dhcp subnets

show dhcp subnets

Description

This command displays the subnet details and the gateway IP for Distributed, L2 and Distributed, L3 networks.

Usage Guidelines

Use this command to view the subnet details for the Distributed, L2 and Distributed, L3 networks.

Example

The following example shows the output of the **show dhcp subnets** command:

DHCP Subnet Table

VLAN	Type	Subnet	Mask	Gateway	Mode	Rolemap
532	12	192.168.132.0	255.255.255.0	0.0.0.0	remote,full-tunnel	VLAN532
539	nat	192.168.1.0	255.255.255.0	192.168.1.1	local,split-tunnel	VLAN532
538	13	192.168.2.0	255.255.255.0	192.168.2.1	local,split-tunnel	VLAN532
534	12	0.0.0.0	255.255.255.255	0.0.0.0	remote,full-tunnel	VLAN532

The output of this command displays the following information:

Parameter	Description
VLAN	Displays the VLAN details.
Type	Displays the type of DHCP assignment mode.
Subnet	Displays the subnet details.
Mask	Displays the subnet mask details.
DNS Server	Displays the DNS server IP address.
Gateway	Displays the gateway IP address.
Mode	Displays details of the tunnel mode.
Rolemap	Displays the role assigned to the clients.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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. • Distributed, L2 • Distributed, L3
<sip> <eip>	Filters the branch count information based on an IP address range specified for the starting IP address <sip> and ending IP address parameters. You can specify up to four different ranges of IP addresses to filter the command output.

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 dpi

```
show dpi {app <name> all|appcategory <name> all|debug <statistics>|<status>|qsessions [detail  
[<session_id>]]|webcategory <name> all|webcategory-lookup <url>}
```

Description

This command displays the DPI configuration information.

Syntax

Command/Parameter	Description
app <name> <all>	Displays a list of all applications (with the all keyword) and details such as application name, ID, application category, and default ports when a specific application name is provided.
appcategory <name> <all>	Displays the list of all application categories (with the all keyword) and details of the applications that belong to a specific application category when an application category is specified.
debug {statistics status}	Displays DPI statistics or status that can be used for debugging.
qsessions [detail [<session_id>]]	Displays advanced debug statistics for troubleshooting the DPI issues.
webcategory <name> <all>	Displays the list of web categories.
webcategory-lookup <URL>	Displays the details for a given URL and the reputation score based on security rating. Run this command twice to fetch information from the cloud server.

Usage Guidelines

Use this command to view the DPI configuration details.

Example

show dpi app

The following example shows the output of the **show dpi app <name>** command:

```
(Instant AP)# show dpi app wikipedia
```

```
Pre-defined Application
```

```
-----  
Name      App ID  App Category  Default Ports  
-----  
wikipedia  222     web           tcp 80
```

The output of this command displays details such as the name of the application, application category, default ports configured for deep packet inspection.

show dpi appcategory

The following example shows the output of the **show dpi appcategory all** command:

```
(Instant AP)# show dpi appcategory all  
Pre-defined Application Categories
```

```

-----
Name                               App Category ID
-----
antivirus                          1
authentication                     2
behavioral                         3
cloud-file-storage                 4
collaboration                      5
encrypted                          6
enterprise-apps                    7
gaming                             8
im-file-transfer                   9
instant-messaging                  10
mail-protocols                     11
mobile-app-store                   12
network-service                    13
peer-to-peer                       14
social-networking                  15
standard                           16
streaming                          17
thin-client                        18
tunneling                          19
unified-communications             20
web                                21
webmail                            22
mobile                             23
Total application categories = 23

```

The output of this command displays all application categories.

show dpi debug statistics

The following example shows the output of the **show dpi debug statistics** command.

```

DPI Engine Version      :4.20.0-34 (build date Aug 21 2016)
API Version             :1.190.0
Protocol Bundle Version :1.230.0-20 (build date Aug 21 2016)
Dpimgr Debug Statistics
-----
Key                               Value
---                               -
dpimgr total pkt handled          2043 (1961)
dpimgr total classified            581 (556)
dpimgr qsession total alloc       1026 (981)
dpimgr qsession total uapp alloc   800 (765)
dpimgr qsession total uapp alloc free 799 (764)
dpimgr qsession total session age  1024 (979)
dpimgr qsession classified skipped  73 (73)
dpimgr qsession event param error  16 (16)
dpimgr qsession total classified   562 (537)
dpimgr qsession total request received 1691 (1624)
dpimgr bca total cloud lookup      23 (17)
dpimgr bca total cached lookup     226 (225)
dpimgr bca total request received  258 (242)
dpimgr bca total classified        19 (19)
Dpimgr cloud internal stats
-----
dns/name server configured        :yes
url cloud lookup server reachable :yes
number of cache hits              :227
number of cloud hits               :22
number of cloud lookups            :22
Max time taken for cloud lookups   :0.230000

```



```

number of local database hits           :0
number of uncategorized responses       :1
number of cache entries                 :16
maximum queue depth reached             :1
trusted user rep average                :91
guest user rep average                  :0
total number of lookup errors           :0 (net: 0 + http: 0 + proto: 0)
current major version                   :0
current minor version                   :0
DPI datapath stats
-----
number of pkts send to dpimgr           :1691
number of msg prepare failure           :0
number of visibility stats cpy to dpimgr failure :0
number of cloud dpi session mismatch    :0
number of cloud dpi session unclassified :0
number of bytes in tx socket buffer     :0
number of bytes in rx socket buffer     :0
total number of incomplete session      :0
number of dpi session mismatch          :0
IAP average cpu usage in 10 secs        :20
allowed unclassified session in 10 secs (max=0) :0
unclassified dpi session in 10 secs      :8
total number of unclassified session     :406
DPI debug pkt stats

```

show dpi debug status

The following example shows the output of the **show dpi debug status** command:

```

Dpimgr Running           :TRUE
Dpimgr Hello count       :1
Dpimgr Agent              :All set - App, Webcc & URL
Dpimgr Status value      :0x3b
Dpimgr Platform Status   :App + WebCC + URL
Dpimgr Visibility Status  :App + WebCC
Dpimgr Enforcement Status :None
Dpimgr External Visibility Status :None

```

show dpi webcategory

The following example shows the output of the **show dpi webcategory all** command:

```

(Instant AP)# show dpi webcategory all
Pre-defined BrightCloud Web Categories
-----
Name                               Web Category ID
----                               -
real-estate                        1
computer-and-internet-security     2
financial-services                  3
business-and-economy               4
computer-and-internet-info         5
auctions                           6
shopping                           7
cult-and-occult                    8
travel                             9
abused-drugs                       10
adult-and-pornography              11
home-and-garden                    12
military                           13
social-networking-web              14
dead-sites                         15
individual-stock-advice-and-tools  16

```

training-and-tools	17
dating	18
sex-education	19
religion	20
entertainment-and-arts	21
personal-sites-and-blogs	22
legal	23
local-information	24
streaming-media	25
job-search	26
gambling	27
translation	28
reference-and-research	29
shareware-and-freeware	30
peer-to-peer-web	31
marijuana	32
hacking	33
games	34
philosophy-and-political-advocacy	35
weapons	36
pay-to-surf	37
hunting-and-fishing	38
society	39
educational-institutions	40
online-greeting-cards	41
sports	42
swimsuits-and-intimate-apparel	43
questionable	44
kids	45
hate-and-racism	46
personal-storage	47
violence	48
keyloggers-and-monitoring	49
search-engines	50
internet-portals	51
web-advertisements	52
cheating	53
gross	54
web-based-email	55
malware-sites	56
phishing-and-other-frauds	57
proxy-avoidance-and-anonymizers	58
spyware-and-adware	59
music	60
government	61
nudity	62
news-and-media	63
illegal	64
content-delivery-networks	65
internet-communications	66
bot-nets	67
abortion	68
health-and-medicine	69
spam-urls	71
dynamically-generated-content	74
parked-domains	75
alcohol-and-tobacco	76
private-ip-addresses	77
image-and-video-search	78
fashion-and-beauty	79
recreation-and-hobbies	80
motor-vehicles	81

```
web-hosting                82
category-incomplete       83
category-unknown          84
Total web categories = 81
```

The output of this command displays the list of web categories and the IDs associated with these categories.

show dpi webcategory-lookup

The following example shows the output of the **show dpi webcategory-lookup <url>** command:

```
(Instant AP)# show dpi webcategory-lookup www.yahoo.com
Input URL: www.yahoo.com
Request sent for CLOUD LOOKUP, please try again.
```

On running command again, the following information is retrieved from the cloud server and displayed as the output:

```
Input URL: www.yahoo.com
Found CACHED RESULT:
URL: yahoo.com REP: 81 A1: 0, Serial = 0x200001
Index: 0 Category: internet-portals(51) Confidence level: 98
```

Command History

Version	Description
Aruba Instant6.5.0.0-4.3.0.0	The command is modified.
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show dpi-error-page-url

show dpi-error-page-url

Description

This command displays the list of custom error page URLs that are displayed when web access is blocked by the AppRF policies.

Usage Guidelines

Use this command to view the list of custom error page URLs. The error page URLs are displayed when client access to certain websites is blocked by the AppRF policies configured on the IAP. The custom error page URLs are configured using **dpi-error-page-url** command.

Example

The following example shows the output of the **show dpi-error-page-url** command:

```
(Instant AP)# show dpi-error-page-url
Global DPI error page URLs Config
-----
ID   URL
--  ---
```

The output of this command displays ID and URLs that are blocked.

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show dpi-stats

```
show dpi-stats
  app [id <app> [deny] [full] |user ip <ipaddr> [deny] [full] | [ssid <ssid-name> full | deny
    [full] | full]
  appcategory [id <appcat> [deny] [full] |user ip <ipaddr> [deny] [full] | [ssid <ssid-name>
    full | deny [full] | full]
  session [full]
  webcategory [id <web> [deny] [full] |user ip <ipaddr> [deny] [full] | [ssid <ssid-name>
    full | deny [full] | full]
  webreputation [id <rep> [deny] [full] |user ip <ipaddr> [deny] [full] | [ssid <ssid-name>
    full | deny [full] | full]
```

Description

This command displays the DPI statistics.

Syntax

Command/Parameter	Description
app	Displays application statistics.
appcategory	Displays the DPI statistics for application category.
session	Displays datapath session details for DPI.
webcategory	Displays the DPI statistics for web category.
webreputation	Displays the DPI statistics for web reputation score.
ssid	Displays the DPI statistics for the last 15 minutes from each IAP connected to the SSID in the network.
ssid name	Displays DPI statistics for the last 15 minutes for the specified SSID.
id	Displays DPI statistics for the specified application, application category, web category or web reputation ID.
user ip <ip-addr>	Displays DPI statistics for specified user IP address.
full	Displays the complete DPI statistics for the application, application category, session, web category, and web reputation stored on the IAP since the last 15 minutes.
deny	Displays the blocked URLs and web content related traffic.

Usage Guidelines

Use this command to view the DPI statistics.

Example

show dpi-stats app

The following example shows the output of the **show dpi-stats app full** command:

```
Last snapshot timestamp 17:10:47
```

```

Dpi Top Application list
-----
App           AppId  Total bytes
---           -
apple         306    10172
apns          1118   278
Not-Classified 0     160
-----
Total bytes           :10610
Classification percentage :98

```

show dpi-stats appcategory

The following example shows the output of the **show dpi-stats appcategory full** command:

```

Last snapshot timestamp 17:10:47
Dpi Top Application category list
-----
App Category      App Category Id  Total bytes
-----
web                20              10172
mobile-app-store   11              278
Not-Classified     0              160
-----
Total bytes           :10610
Classification percentage :98

```

show dpi-stats session

The following example shows the output of the **show dpi-stats session full** command:

```

Datapath DPI CDR Session Table Entries
-----
Source IP      App           Webcat           TX Bytes  Rx Bytes  Webrep
-----
172.31.98.103  google-plus (1125)  social-networking-web (14)  trustworthy-sites (5)  8635
3697
172.31.98.103  krb5 (97)          Not-Classified (0)          8237      5998      Not-Classified
172.31.98.189  smb (185)          Not-Classified (0)          886       0         Not-Classified
172.31.98.103  http (67)          Not-Classified (0)          507       4074      Not-Classified
172.31.98.103  https (68)         computer-and-internet-info (5)  trustworthy-sites (5)
449597 644401
172.31.98.103  yahoo (1294)       web-based-email (55)        6044      10818     trustworthy-si
tes (5)
172.31.98.103  gtalk (1441)       Not-Classified (0)          3375      5904      Not-Classified
172.16.100.174  ssdp (197)         Not-Classified (0)          4339      0         Not-Classified
(0)

Datapath DPI CDR Session Table Entries
-----
Source IP      App           Webcat           TX Bytes  Rx Bytes  Webrep
-----
10.17.139.167  ssdp (197)       Not-Classified (0)          6923      0         Not-Classified
(0)
10.17.139.183  ssdp (197)       Not-Classified (0)          5458      0         Not-Classified
(0)

```

```

172.16.100.174  udp (216)          Not-Classified (0)          Not-Classified
                  (0)          152          0
10.17.139.167   windowslive (298)          internet-portals (51)          trustworthy-sites (5)  893
5907
172.31.98.103   http (67)          computer-and-internet-info (5) trustworthy-sites (5)  439
1783
10.17.139.183   http (67)          computer-and-internet-info (5) trustworthy-sites (5)  643
620
Num of Entries:47

```

show dpi-stats webcategory

The following example shows the output of the **show dpi-stats webcategory full** command:

```

Last snapshot timestamp 17:25:43
Dpi Top Web Category list
-----
Web Category          Web Category Id  Total bytes
-----
computer-and-internet-info  5              740
-----
Total bytes              :740

```

show dpi-stats webreputation

The following example shows the output of the **show dpi-stats webreputation full** command:

```

Last snapshot timestamp 15:39:32
Dpi Top Web Reputation list
-----
Web Reputation        Web Reputation Id  Total bytes
-----
trustworthy-sites     5              1211900
moderate-risk-sites   3              2998
-----
Total bytes            :1214898

```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.
Aruba Instant 6.4.0.2-4.1.1	This command is modified.
Aruba Instant 6.4.4.4-4.2.3	This command is modified.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show election

```
show election {statistics}
```

Description

This command shows master IAP election statistics.

Syntax

Parameter	Description
statistics	Shows master election statistics.

Usage Guidelines

Use this command to view the statistics of the IAP selected as VC.

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	Indicates if the IAP is provisioned as master.
master_beacon	Displays the number of beacons transmitted and received by the master IAP.
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
Whitelist Use HTTPs  Server Offload Prevent Frame Overlay In Use Redirect Mode
-----
default   localhost 80    /    Authenticated          Disable          Disable          Enable
          Yes      No
Samuel    localhost 80    /    Authenticated          Disable          Disable          Disable
          No      No
test      localhost 80    /    Authenticated          Disable          Disable          Disable
          No      No
```

The output of this command displays details such as the external captive portal profile name, server name, server port, redirection URL, and automatic whitelisting status.

Command History

Version	Description
Aruba Instant 6.4.3.x-4.2	The output of this command was modified to include server offload and prevent frame overlay configuration settings.
Aruba Instant 6.3.1.1-4.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show facebook

show facebook

Description

This command displays the Facebook configuration details when an IAP successfully registers with Facebook.

Usage Guidelines

Use this command to view Facebook configuration details.

Example

The following example shows the output of **show facebook** command:

```
Facebook Id      :461857943969928
Config Url       :https://www.facebook.com/wifiath/config?gw_id=461857943969928
```

The output of this command displays the Facebook ID and the configuration URL if the IAP registration with Facebook is successful.

Command History

Version	Description
Aruba Instant 6.4.2.x-4.1.1.x	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 firewall

```
show firewall
```

Description

This command displays the status of firewall settings of an IAP.

Usage Guidelines

Use this command to view the firewall configuration details of the IAP.

Example

The following example shows the output of **show firewall** command:

```
Firewall
-----
Type                Value
----                -
Auto topology rules  disable
```

Command History

Version	Description
Aruba Instant 6.4.4.6-4.2.4.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show g-max-clients

```
show g-max-clients <ssid_profile>
```

Description

This command displays the maximum number of clients allowed for an SSID profile on a 2.4 GHz radio channel.

Syntax

Parameter	Description	Range
<ssid_profile>	Denotes the SSID profile for which the maximum clients limit is to be configured.	—

Usage Guidelines

Use this command to view the maximum number of clients allowed for a 2.4 GHz radio channel SSID profile.

Example

The following example configures the maximum number of clients for a 2.4 GHz radio channel:

```
(Instant AP)# show g-max-clients ssid3  
g-max-clients: 77
```

The output of this command displays the maximum number of clients allowed to connect to the SSID profile.

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	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| rogue-ap <mac>}
```

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 a details of the IAP to which the client is connected.
clients	Displays a list of unknown clients detected by the IAP.
phy-types	Displays the PHY details of the IAP.
rap-types	Displays a list of Remote APs (RAPs) detected by the IAP.
rogue-ap <mac>	Displays the list of rogue IAPs detected by the master IAP in the IAP cluster.

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 akvoicel Interfering 6 G 17:38:49
00:24:d7:40:ca:88 akvoicel 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 6.4.2.3-4.1.2.0	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 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-deauth-broadcast disable enable enable enable
signature-deassociation-broadcast disable enable enable enable
detect-adhoc-using-valid-ssid enable disable enable enable
detect-malformed-large-duration enable disable enable enable
detect-ap-impersonation enable disable disable enable
detect-adhoc-network enable disable disable enable
detect-valid-ssid-misuse enable disable disable enable
detect-wireless-bridge disable disable disable enable
detect-ht-40mhz-intolerance disable disable disable enable
detect-ht-greenfield disable disable disable enable
detect-ap-flood disable disable disable enable
detect-client-flood disable disable disable enable
detect-bad-wep disable disable disable enable
detect-cts-rate-anomaly disable disable disable enable
detect-rts-rate-anomaly disable disable disable enable
detect-invalid-addresscombination disable disable disable enable
detect-malformed-htie disable disable disable enable
detect-malformed-assoc-req disable disable disable enable
detect-malformed-frame-auth disable disable disable enable
detect-overflow-ie disable disable disable enable
detect-overflow-eapol-key disable disable disable enable
detect-beacon-wrong-channel disable disable disable enable
detect-invalid-mac-oui disable disable disable enable
client detection level :off
-----
Policies Status Low Medium High
-----
detect-valid-clientmisassociation disable enable enable enable
detect-disconnect-sta disable disable enable enable
detect-omerta-attack disable disable enable enable
detect-fatajack disable disable enable enable
detect-block-ack-attack disable disable enable enable
detect-hotspotter-attack disable disable enable enable
detect-unencrypted-valid disable disable enable enable
detect-power-save-dos-attack disable disable enable enable
detect-eap-rate-anomaly disable disable disable enable
detect-rate-anomalies disable disable disable enable
detect-chopchop-attack disable disable disable enable
detect-tpkip-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: • For RAP-108/109—ArubaInstant_Pegasus_<build-version> • For RAP-155/155P—ArubaInstant_Aries_<build-version> • For all other IAPs—ArubaInstant_Orion_<build-version>

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	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 inbound-firewall-rules

show inbound-firewall-rules

Description

This command displays the details of inbound firewall rules configured on an IAP.

Usage Guidelines

Use this command to view the details of the inbound firewall rules configured for an IAP network.

Example

The following output is displayed for the **show inbound-firewall-rules** command:

```
Access Rules
-----
Src IP   Src Mask  Dest IP   Dest Mask  Dest Match  Protocol (id:sport:eport)  Application
Action  Log   TOS   802.1P   Blacklist  App Throttle (Up:Down)  Mirror  DisScan  ClassifyMedia
-----
-----
any      any      any      any      match      h323-tcp
permit
any      any      192.0.2.0 255.255.255.0 match      h323-udp
permit
```

The output of this command displays information about the inbound firewall access rule configuration parameters, which indicate whether a particular type of traffic is to be allowed to a particular destination from the source subnet, and the service and protocol in use. It also indicates if other options such as logging and prioritizing traffic are enabled when the rule is triggered.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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.

Parameter	Description
Transmitted packets	Shows total number of transmitted packets.
Transmitted bytes	Shows total number of transmitted bytes.
Transmitted dropped	Shows total number of packets dropped.
Transmission errors	Shows total number of errors during packet transmit.
Lost carrier	Shows total number of lost carriers.

Command History

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 VC

Example

The following output is displayed for the **show ip dhcp database** command:

```
DHCP Subnet          :192.0.2.0
DHCP Netmask         :255.255.255.0
DHCP Domain Name     :example.com
DHCP DNS Server      :192.0.2.1
DHCP DNS Cache       :Disabled
```

The output of this command provides the following information:

Column	Description
DHCP subnet	Indicates the network range for the client IP addresses.
DHCP Netmask	Indicates the subnet mask specified for the IP address range for the DHCP subnet.
DHCP Lease Time (m)	Indicates the duration of DHCP lease. The lease time refers to the duration of lease that a DHCP-enabled client has obtained for an IP address from a DHCP server.
DHCP Domain Name	Indicates the domain-name of the DHCP client.
DHCP DNS Server	Indicates the IP address of the DNS server.
DHCP DNS Cache	Indicates if the DNS cache is enabled.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	The output of 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 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.

Parameter	Description
MAC	Indicates the MAC address of member associated with the specified multicast group address.
VLAN	Indicates the VLAN ID associated with the multicast groups or a specific multicast group address.
Destination	Indicates the destination to which the multicast packets are routed.
Age	Indicates the aging time of the forwarding table entries.

Command History

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. • Enabled—up • Disabled—down
Protocol	Displays the status of the IP on the interface. • Enabled—up • Disabled—down

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 ipv6 interface

```
show ipv6 interface {brief|details}
```

Description

Shows IPv6-related information for all interfaces on the IAP.

Syntax

Parameter	Description
brief	Displays a brief summary of the IPv6-related information on all interfaces of an IAP.
details	Displays detailed information on the interfaces that support IPv6.

Usage Guidelines

Use this command to view IPv6 related information on an IAP.

Example

The following example shows the output of the **show ipv6 interface brief** command:

```
IPv6 is enable, link-local address is fe80::aea3:1eff:fe8d:471a/64
br0 is up, line protocol is up
Global unicast address(es):
2001:470:36:5c3:aea3:1eff:fe8d:471a/64, subnet is 2001:470:36:5c3::/64
2001:470:36:5c3:ffff:ffff:ffff:1001/128, subnet is 2001:470:36:5c3:ffff:ffff:ffff:1001/128
2001:470:36:5c3:ffff:ffff:ffff:5b/64, subnet is 2001:470:36:5c3::/64
```

The following example shows the output of the **show ipv6 interface details** command:

```
1: lo: <LOOPBACK,UP,10000> mtu 16436
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
15: br0: <BROADCAST,MULTICAST,UP,10200> mtu 1300 qlen 1000
inet6 2001:470:36:5c3:ffff:ffff:ffff:5b/64 scope global
valid_lft forever preferred_lft forever
inet6 2001:470:36:5c3:aea3:1eff:fe8d:471a/64 scope global dynamic
valid_lft 2963sec preferred_lft 1963sec
inet6 2001:470:36:5c3:ffff:ffff:ffff:1001/128 scope global
valid_lft forever preferred_lft forever
inet6 fe80::aea3:1eff:fe8d:471a/64 scope link
valid_lft forever preferred_lft forever
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is introduced.

Command Information

Platform	Command Mode
IAP-214/215, IAP-224/225, IAP-274/275, IAP-314/315, IAP-324/325, IAP-334/335	Privileged EXEC mode

show ipv6 route

show ipv6 route

Description

This command displays the IPv6 routing table.

Usage Guidelines

Use this command to view the static IPv6 routes configured on the IAP.

Examples

The following example shows the output of the **show ipv6 route** command:

Kernel IPv6 routing table

Destination	Next Hop	Flags	Metric
-----	-----	-----	-----
2001:470:36:5c3:ffff:ffff:ffff:1001/128	::	U	256
2001:470:36:5c3::/64	::	UA	256
fe80::/64	::	U	256
::/0	fe80::6273:5cff:fe65:ee19	UGDA	1024
::1/128	::	U	0
2001:470:36:5c3:aea3:1eff:fe6d:471a/128	::	U	0
2001:470:36:5c3:ffff:ffff:ffff:5b/128	::	U	0
2001:470:36:5c3:ffff:ffff:ffff:1001/128	::	U	0
fe80::aea3:1eff:fe6d:471a/128	::	U	0
ff02::d/128	ff02::d	UC	0
ff02::1:2/128	ff02::1:2	UC	0
ff00::/8	::	U	256
Ref	Use	Iface	
---	-----		
0	0	br0	
0	0	br0	
0	0	br0	
0	0	br0	
0	1	lo	
0	1	lo	
2800	1	lo	
6	1	lo	
6602	1	lo	
12194	0	br0	
2	0	br0	
0	0	br0	

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is introduced.

Command Information

Platform	Command Mode
IAP-214/215, IAP-224/225, IAP-274/275, IAP-314/315, IAP-324/325, IAP-334/335	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 IAP 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, IAP 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
IAP-220 Series	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 AP)# show l2tpv3 config
L2TPV3 Tunnel configuration
-----
Tunnel Profile Primary Peer Backup Peer Peer UDP Port Local UDP Port Hello Interval Host Name
MTU Message Digest Type secret Key Failover Mode Failover Retry Count Retry Interval Checksum
-----
-
test_tunnel 10.0.0.63 10.0.0.65 3000 1701 150 Instant-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 1.1.1.1 255.255.255.0 5 0 0 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 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 AP)# 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 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: aruba1600pop658509.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: aruba1600pop658509.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: aruba1600pop636635.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 6.5.1.0-4.3.1.0	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.

Column	Description
Value	Indicates if a flag is enabled.
Virtual Controller IP	Displays the VC IP address. The VC 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 VC configuration associated with the mobility domain.

show l3-mobility datapath

The following example shows the output of **show l3-mobility datapath** command:

```
L3 Mobility Datapath Home Table
-----
Client Index Client MAC Home Vlan Destinaton Device Index
-----
L3 Mobility Datapath Foreign Table
-----
Client Index Client MAC Home Vlan VAP Vlan Destinaton Device Index HAP IP Virtual Controller
IP Packets Forwarded
-----
L3 Mobility Datapath Tunnel Table
-----
Tunnel Device Remote Protocol Dest IP Clients Idle Time Rx Packets Tx Packets Rx Mcasts Tx
Mcasts ARP Proxy Pkts Tx Jumbo MTU Rx HB Tx HB MTU Reqs MTU Resps HB Mismatch IP Mismatch Type
Vlan Translations
-----
-----
-----
```

The output of this command provides the following information:

Parameter	Description
L3 Mobility Datapath Home Table	Displays details such as client index, client MAC address, VLAN, destination device associated with the L3 mobility home subnet.
L3 Mobility Datapath Foreign Table	Displays details such as client index, client MAC address, VLAN, Destination device, home IAP IP address, VC IP address and packet details associated with the L3 mobility foreign subnet.
L3 Mobility Datapath Tunnel table	Displays the following details about L3 mobility tunnel: • Tunnel - Indicates the tunnel interface. • Device - Displays the device ID. • Remote Protocol - Indicates the remote protocol used by the roaming clients. • Dest IP - Indicates the destination IP address to which the packets are routed. • Clients - Displays the list of clients

Parameter	Description
	• Idle Time - Displays the idle time • Rx Packets - Displays information about packets received. • Tx Packets - Displays information about packets transmitted. • Rx Mcasts - Displays information about multicast packets received. • Tx Mcasts - Displays information about multicast packets transmitted. • ARP Proxy Pkts - Displays information packets resolved to destination IP address by the proxy Address Resolution Protocol (ARP) • Tx Jumbo MTU - Displays information about the Maximum Transmission Unit (MTU) in jumbo frames. • Rx HB • Tx HB • MTU Reqs - Indicates the number of MTU requests sent. • MTU Resps - Indicates the number of MTU responses received. • HB Mismatch • IP Mismatch - Indicates IP address mismatch if any • Type • Vlan Translations - Displays details about VLAN translation.

show l3-mobility events

The following example shows the output of the **show l3-mobility events** command:

```
L3 Mobility Events
-----
Time Client MAC Event IP Dir

----
May 9 23:26:29 08:ed:b9:e1:51:87 Station Offline 10.17.88.59 <-
May 9 23:26:29 08:ed:b9:e1:51:87 Potential Foreign Client10.17.88.59 <-

May 9 23:09:05 08:ed:b9:e1:51:87 This Client is Normal 10.17.88.59 ->

Peer IP Home Vlan VAP Vlan Tunnel ID Old AP IP FAP IP HAP IP VC IP Additional Info
-----
self - 1 - - - - -
self - - - - -
self - 1 - - 10.17.88.59 - 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.

Parameter	Description
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 IAP.
Tunnel ID	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.
VC IP	Indicates the IP address of the VC.
Additional Info	Displays additional information if any.

show l3-mobility status

The following example shows the output of the **show l3-mobility status** command:

```
Roaming Client Table
-----
Client MAC Home Vlan VAP Vlan Tunnel ID Status Virtual Controller IP Peer IP Old AP IP Device
Name
-----
----
Tunnel Table
-----
Peer IP Local Tunnel ID Remote Tunnel ID Use Count Type
-----
Virtual Controller Table
-----
Virtual Controller IP Type HAP IP Local Tunnel ID Remote Tunnel ID
-----
192.0.1.0 C - - -
```

The output of this command provides the following information:

Parameter	Description
Roaming Client Table	Displays details such as client MAC address, Home IAP and Virtual IAP VLAN, Tunnel ID, roaming status, VC 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 VC IP address, type, Home IAP 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 VC.

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 sAMAccountName
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 papi-handler

```
show log papi-handler {count}
```

Description

This command shows the cluster security debugging 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 6.5.1.0-4.3.1.0	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
vlan 0, 1 tid 255 oldapip 0.0.0.0 fapip 10.17.88.59 hapip 0.0.0.0 vcip 0.0.0.0 info l2-timed-
out,test
May 9 01:43:22: Station Offline: mac 08:ed:b9:e1:51:87 rcvd from self vlan 0, 0 tid 255
oldapip 0.0.0.0 fapip 0.0.0.0 hapip 0.0.0.0 vcip 0.0.0.0 info
May 9 01:25:53: This Client is Normal: mac 08:ed:b9:e1:51:87 sent to self vlan 0, 1 tid 255
oldapip 0.0.0.0 fapip 10.17.88.59 hapip 0.0.0.0 vcip 0.0.0.0 info
May 9 01:25:53: Too many retries: mac 08:ed:b9:e1:51:87 rcvd from self vlan 0, 1 tid 255
oldapip 0.0.0.0 fapip 10.17.88.59 hapip 0.0.0.0 vcip 0.0.0.0 info
May 9 01:25:52: Potential Foreign Client Information: mac 08:ed:b9:e1:51:87 rcvd from self
vlan 0, 1 tid 255 oldapip 0.0.0.0 fapip 10.17.88.59 hapip 0.0.0.0 vcip 0.0.0.0 info l2-timed-
out,test
```

The output of this command provides the following information:

Content	Description
Timestamp	Indicates the timestamp of the L3 mobility event.
Client MAC	Indicates the MAC address of the roaming clients.
Event	Provides a description of the mobility event.
Home Vlan	Displays the VLAN ID associated with the home subnet.
VAP Vlan	Displays the VLAN ID associated with the Virtual IAP.
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

Content	Description
	currently connected.
VC IP	Indicates the IP address of the VC.
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 management 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
Hash Management Password :Enabled
Authentication Servers
-----
Name  Type  IP Address  Port  Key  Timeout  Retry Count  NAS IP Address  NAS Identifier
RFC3576
-----
--
Management User Table
-----
Name      Password                                     Type
-----
admin     0603e7ee02ede87d7fb6081270dd548a69df219e8ef4a457f99e190f66cd4298bb97f7afab  Admin
                                                Local
                                                Read-Only
                                                Guest-Mgmt
```

The output of this command provides the following information:

Column	Description
Server Load Balancing	Indicates if load balancing is enabled when two authentication servers are used.
Local User DB Backup	Indicates if the backing up of the local user database is enabled.
Hash Management Password	Indicates if hashing of management user password is enabled or disabled.
Name (Authentication Servers Table)	Indicates the name of the RADIUS server.
Type	Indicates the type of the RADIUS server.
IP address	Indicates the IP address of the RADIUS server.
Port	Indicates the authorization port number of the RADIUS server.
Key	Indicates the key for communicating with the RADIUS server.

Column	Description
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 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 management user
Password	Indicates the password of the admin user.
Type	Indicates if the type of the user (admin, read-only, or guest management user).

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	The output of this command is modified.
Aruba Instant 6.3.1.1-4.0.0.0	The output of this command is modified.
Aruba Instant 6.2.1.0-3.3.0.0	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 network-summary

show network-summary

Description

This command displays the status of the available network configurations on the IAP.

Usage Guidelines

Use this command to view the status of the network configurations.

Examples

The following output is displayed for the **show network-summary** command:

```
Internet reachable :Detection disabled
Active uplink :eth0
Primary VPN :Not configured
Secondary VPN :Not configured
AirWave :Not configured
```

The output of this command provides the following information:

Column	Description
Internet Reachable	Indicates the status of the WLAN network.
Active uplink	Indicates the uplink that is currently active on the IAP.
Primary VPN	Indicates the status of the Primary VPN configuration.
Secondary VPN	Indicates the status of the Secondary VPN connection.
Airwave	Indicates the status of the AirWave configuration.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 out-of-service

show out-of-service

Description

This command displays the details of the out of service operations triggered on the IAP.

Usage Guidelines

Use this command to view the out-of-service operations and the SSID availability based on the out-of-service states detected on the IAP.

Example

The following example shows the output of the **show out-of-service** command:

```
Out of service trigger Status
```

```
-----  
uplink-down   primary-uplink-down  internet-down  vpn-down  
-----  
No            No            -              Yes
```

```
The following out-of-service events got triggered in last out-of-service-hold-on-time(45) sec  
: None
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	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 the **show port status** command:

```
(Instant AP)# 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

IAP Platforms	Command Mode
All platforms	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 d226cccfac5a95cd6bb04ca74f20473eae9085fb16892b66
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/udhcpd -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 AP)# show radio config

Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:0
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Cell Size Reduction:0

5.0 GHz:
Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:2
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Standalone Spectrum Band:5ghz-upper
Cell Size Reduction:0
```

The output of this command provides the following information:

Parameter	Description
Legacy Mode	Indicates if the legacy mode is enabled on the 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 IAP radio profile to improve performance in high-interference environments. For more information on

Parameter	Description
	configuring immunity levels, see rf dot11a-radio-profile and rf dot11g-radio-profile .
Channel Switch Announcement Count	Displays the number of channel switching announcements that are sent before switching to a new channel.
MAX distance	Indicates the maximum distance in meters between a client and anIAP 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 IAPs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.
Standalone Spectrum	Indicates the portion of the channel (upper, middle, or lower) that is being monitored on the 5 GHz band.
Cell Size Reduction	Indicates the Rx sensitivity values configured on the 2.4 GHz and 5.0 GHz radio profiles.

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	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	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
----          -
InternalServer 127.0.0.1       1616  1813      596ff8d50a0662b542e96567bb87db331
208cc412bfb4aade8033ca9b46e5f09f933f89bb374bdd80b9acadcc981fdf5ea5ea13e33e43378f
56913cd3e76dc7a

test          test@abc.com     1812  1813
testServer    test@test.com    1812  1813

Timeout  Retry Count  NAS IP Address  NAS Identifier  In Use  RFC3576
-----  -
5        3
5        3

Airgroup RFC3576-ONLY  Airgroup RFC3576 port  Deadtme  DRP IP  DRP IP Mask
-----  -
Y        5999      5
5

DRP VLAN  DRP Gateway  Radsec  Radsec port
-----  -
Disabled  Disabled
Enabled   2083
```

The output of this command provides the following information:

Parameter	Description
Name	Indicates the name of the RADIUS server.
IP address	Indicates the IP address of the RADIUS server.
Port	Indicates the authorization port number of the RADIUS server.
AcctPort	Indicates the authorization port number of the RADIUS server.
Key	Indicates the key for communicating with the RADIUS server.
Timeout	Indicates timeout value in seconds for one RADIUS request.

Parameter	Description
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.
Airgroup RFC3576 port	Indicates the port number used for sending AirGroup CoA.
Deadtime	Indicates the RADIUS server dead-time.
DRP IP DRP Mask DRP VLAN	Indicates the IP address, net mask, and DRP VLAN configured for Dynamic Proxy Radius (DRP).
RadSec RadSec Port	Indicates if RadSec protocol for the RADIUS communication over TLS is enabled. If RadSec is enabled, the RadSec port number is displayed.

Command History

Version	Description
Aruba Instant 6.4.2.3.-4.1.2	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 status

show radius status

Description

This command displays the status of TLS tunnel between the IAP and RadSec proxy.

Usage Guidelines

Use this command to view the status of TLS tunnel when RADIUS communication over TLS is enabled on an IAP.

Example

The following example shows the output of **show radius status** command:

Radius server status

```
-----
Name                Server IP   Source IP   Server Name   Protocol   Port   Connected sockets
-----
InternalServer      127.0.0.1  10.17.129.253 Not configured RADIUS/UDP 1616   Not Applicable
test                10.0.0.1   10.17.129.253 Not configured RADIUS/UDP 1812   Not Applicable
t_test             127.0.0.1  10.17.129.253 Not configured RADIUS/UDP 2630   Not Applicable
Radius1            10.0.0.2   10.17.129.253 Not configured RADIUS/UDP 1812   Not Applicable
t_Radius1          127.0.0.1  10.17.129.253 Not configured RADIUS/UDP 2632   Not Applicable

Status              Last connection tried at   Next connection at
-----
Not Applicable      Not Applicable              Not Applicable
Not Applicable      2015-07-07 00:00:00.000000  2015-07-07 00:00:05.5000000
Not Applicable      2015-07-07 00:00:00.000000  2015-07-07 00:00:05.5000000
Not Applicable      2015-07-07 00:00:00.000000  2015-07-07 00:00:05.5000000
Not Applicable      2015-07-07 00:00:00.000000  2015-07-07 00:00:05.5000000
```

The output of this command provides the following information:

Parameter	Description
Name	Indicates the name of the RADIUS server.
Server IP	Indicates the IP address of the RADIUS server.
Source IP	Indicates the source IP address.
Server Name	Indicates the name of the server.
Protocol	Indicates the type of protocol used for RADIUS communication with the IAP clients.
Port	Indicates the authorization port number of the RADIUS server.
Connected Sockets	Indicates connected sockets if any.
Status	Indicates status of the server connection.
Last connection tried at	Indicates the time stamp during which the last connection between the server

Parameter	Description
	and client was attempted.
Next connection at	Indicates the time at which the next attempt will be made to establish the connection with the RADIUS server.

Command History

Version	Description
Aruba Instant 6.4.2.3-4.1.2.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show radseccert

show radseccert

Description

This command displays details of the RadSec client and CA certificates uploaded on the IAP.

Usage Guidelines

Use this command to view the RadSec certificate details on the IAP.

Example

The following example shows the output of the **show radseccert** command:

```
Current radsec CA Certificate:
Version          :3
Serial Number    :DE:DF:11:F6:AC:C0:91:00
Issuer           :/C=GB/ST=Berkshire/O=My Company
Ltd/OU=Leon/CN=Leon/emailAddress=lzheng@arubanetworks.com
Subject          :/C=GB/ST=Berkshire/O=My Company
Ltd/OU=Leon/CN=Leon/emailAddress=lzheng@arubanetworks.com
Issued On        :Mar 24 15:14:41 2011 GMT
Expires On       :Mar 21 15:14:41 2021 GMT
Signed Using     :SHA1-RSA
RSA Key size     :1024 bits
Current radsec Certificate:
Version          :3
Serial Number    :DE:DF:11:F6:AC:C0:91:03
Issuer           :/C=GB/ST=Berkshire/O=My Company
Ltd/OU=Leon/CN=Leon/emailAddress=lzheng@arubanetworks.com
Subject          :/C=GB/ST=Berkshire/L=Newbury/O=My Company
Ltd/CN=ClientCert/emailAddress=lzheng@arubanetworks.com
Issued On        :Mar 24 15:25:24 2011 GMT
Expires On       :Mar 21 15:25:24 2021 GMT
Signed Using     :SHA1-RSA
RSA Key size     :1024 bits
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	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 example shows the partial output of the **show running-config** command output:

```
version 6.4.0.0-4.1.0
virtual-controller-country IN
virtual-controller-key 0cb5770401cdeb6e4363c25fdfde17d907c4b095a9be5e
name instant-C4:42:98
terminal-access
clock timezone none 00 00
rf-band all
allow-new-aps
allowed-ap d8:c7:c8:c4:42:98
arm
wide-bands 5ghz
80mhz-support
min-tx-power 18
max-tx-power 127
band-steering-mode prefer-5ghz
air-time-fairness-mode fair-access
client-aware
scanning
client-match
syslog-level warn ap-debug
syslog-level warn network
syslog-level warn security
syslog-level warn system
syslog-level warn user
syslog-level warn user-debug
syslog-level warn wireless
mgmt-user admin aba950f14f5764975371fcb66a72d10f
wlan access-rule default_wired_port_profile
index 1
rule any any match any any any permit
wlan access-rule wired-instant
index 2
rule masterip 0.0.0.0 match tcp 80 80 permit
rule masterip 0.0.0.0 match tcp 4343 4343 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit
wlan access-rule test
index 3
rule any any match any any any deny
wlan ssid-profile test
enable
index 1
type employee
ssid instant
opmode opensystem
```

```

max-authentication-failures 0
rf-band all
captive-portal disable
dtim-period 1
inactivity-timeout 1000
broadcast-filter none
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64
dot11k
dot11v
auth-survivability cache-time-out 24
wlan external-captive-portal
server localhost
port 80
url "/"
auth-text "Authenticated"
auto-whitelist-disable
https
blacklist-time 3600
auth-failure-blacklist-time 3600
ids
wireless-containment none
wired-port-profile wired-instant
switchport-mode access
allowed-vlan all
native-vlan guest
no shutdown
access-rule-name wired-instant
speed auto
duplex auto
no poe
type guest
captive-portal disable
no dot1x
wired-port-profile default_wired_port_profile
switchport-mode trunk
allowed-vlan all
native-vlan 1
shutdown
access-rule-name default_wired_port_profile
speed auto
duplex full
no poe
type employee
captive-portal disable
no dot1x
enet0-port-profile default_wired_port_profile
uplink
preemption
enforce none
failover-internet-pkt-lost-cnt 10
failover-internet-pkt-send-freq 30
failover-vpn-timeout 180
airgroup
disable
airgroupservice airplay
disable
description AirPlay
airgroupservice airprint
disable
description AirPrint

```

Command History

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 VC.

Usage Guidelines

Use this command to view the SNMP information configured on a VC.

Example

The following example shows the output of **show snmp-configuration** command:

```
Engine ID:D8C7C8CBD420
Community Strings
-----
Name
----
Test
SNMPv3 Users
-----
Name      Authentication Type  Encryption Type
-----
hallo     SHA                   NONE
DES       SHA                   DES
SNMP Trap Hosts
-----
IP Address  Version  Name  Port  Inform
-----
192.0.2.1  v3       miro  162   Yes
```

The output of this command includes the following parameters:

Parameter	Description
Engine ID	Displays the SNMP engine ID.
Community Strings	Displays the SNMP community strings..
SNMPv3 Users	Displays details about the SNMPv3 users.
Name	Indicates the name of the SNMP user.
Authentication Type	Indicates the authentication protocol configured for the SNMP users.
Encryption Type	Indicates the encryption type, for example, CBC-DES Symmetric Encryption Protocol (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.

Parameter	Description
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 VC. The spectrum alert messages provide information about the device ID, device type, IP address of the spectrum monitor or hybrid IAP, and the timestamp. The VC 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 speed-test

show speed-test

Description

This command displays the details obtained from the VC speed-test client.

Usage Guidelines

Use this command to view the traffic details obtained from the last speed test run from the VC client.

Examples

The following output is displayed for the **show speed-test** command:

Speed Test Data for traffic : From Client to Server

```
Time of Execution :Mon, 02 Nov 2015 09:18:07 GMT
Server IP :10.17.138.2
Local IP :10.17.138.188
Local Port :51308
Remote Port :5201
Protocol :UDP
Duration :20
Bytes Txferred :249271000
Bandwidth(bps) :99706100
Jitter(millisecond) :0
Datagrams sent :249270
```

Speed Test Data for traffic : From Server to Client

```
Time of Execution :Mon, 02 Nov 2015 09:18:28 GMT
Server IP :10.17.138.2
Local IP :10.17.138.188
Local Port :56423
Remote Port :5201
Protocol :UDP
Duration :20
Bytes Txferred :234013000
Bandwidth(bps) :93603500
Jitter(millisecond) :0
Datagrams sent :234009
```

The output of this command provides the following information:

Command History

Version	Description
Aruba Instant 6.4.3.4-4.2.1	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, VC, 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
[Interfering] Neighboring APs [Rogue] Neighboring Clients [Valid] Neighboring Clients
[Interfering] Clients Throughput [Out] (bps) Throughput [In] (bps)
-----
-----
00:34:46 8 164 4 239 0 1 8 1 93 99
00:34:17 8 164 4 239 0 1 8 1 186 199
0 1 9
RF Trends
-----
Timestamp Utilization [2.4 GHz] (%) Utilization [5.0 GHz] (%) Noise Floor [2.4 GHz]
(dBm) Noise Floor [5.0 GHz] (dBm) 2.4 GHz Frames [Errors] (fps) 5.0 GHz Frames [Errors] (fps)
2.4 GHz Frames [Out] (fps) 5.0 GHz Frames [Out] (fps) 2.4 GHz Frames [In] (fps) 5.0 GHz Frames
[In] (fps) 2.4 GHz Frames [Drops] (fps) 5.0 GHz Frames [Drops] (fps) 2.4 GHz Mgmt Frames [In]
(fps) 5.0 GHz Mgmt Frames [In] (fps) 2.4 GHz Mgmt Frames [Out] (fps) 5.0 GHz Mgmt Frames [Out]
(fps)
-----
-----
-----
00:34:46 59 4 -91 -93 41 0 0 0 68 18 1 1 403 265 1 0
00:34:17 61 5 -92 -93 45 0 0 1 78 21 1 1 408 287 1 1
Client Heatmap
-----
Clients Signal Speed IP Address
-----
AP List
-----
Name IP Address Mode Spectrum Clients Type CPU Utilization %: Memory Free (MB): Serial Number:
Need Antenna Config From Port
-----
-----
d8:c7:c8:cb:d4:20 10.17.88.188 access disable 1 135 8 164 AX0059921 No none

```

show stats client

The following example shows the output for the **show stats client <mac>** command:

```

Name::
IP Address::169.254.90.154
MAC Address::08:ed:b9:e1:51:7d
Access Point::d8:c7:c8:cb:d4:20
Channel::149+
Network::Network1
Connection Time::4h:50m:48s
Type::AN
OS::
Swarm Client Stats
-----
Timestamp Signal (dB) Frames [In] (fps) Frames [Out] (fps) Throughput [In] (bps) Throughput
[Out] (bps) Frames [Retries In] (fps) Frames [Retries Out] (fps) Speed (mbps)
-----
-----
00:32:46 47 0 0 0 170 0 0 6
00:32:16 47 0 0 0 170 0 0 6
00:31:46 47 0 1 0 5946 0 0 6
00:31:16 49 0 0 0 316 0 0 6

Mobility Trail
-----
Association Time Access Point
-----

```

```

11:04:56 d8:c7:c8:cb:d4:20
Client Heatmap
-----
Client Signal Speed IP Address
-----
169.254.90.154 good good 169.254.90.154
Access Point Heatmap
-----
Access Point Utilization Noise Errors
-----
d8:c7:c8:cb:d4:20 good good good
Client List
-----
Name IP Address MAC Address OS Network Access Point Channel Type Role
-----
169.254.90.154 08:ed:b9:e1:51:7d Network1 d8:c7:c8:cb:d4:20 149+ AN Network1
Info timestamp :48662

```

show stats global

The following example shows the output for the **show stats global** command:

```

Swarm Global Stats
-----
Timestamp Clients Frames [Out] (fps) Frames [In] (fps) Throughput [Out] (bps) Throughput [In] (bps)
-----
00:38:05 1 0 0 294 380
00:37:35 1 0 0 98 101
00:37:04 1 0 0 0 0
00:36:33 1 0 0 0 0
00:36:03 1 0 0 0 0
00:35:32 1 0 0 46 49
00:35:01 1 0 0 93 99
00:34:31 1 0 0 186 199
00:34:00 1 0 0 0 0
00:33:29 1 0 0 0 0
00:32:59 1 0 0 0 170
00:32:28 1 0 0 0 170
00:31:58 1 0 1 2961 5946
00:31:27 1 0 0 196 316
00:30:56 1 0 0 196 202
Access Point Heatmap
-----
Access Points Utilization Noise Errors
-----
Client Heatmap
-----
Clients Signal Speed IP Address
-----

```

show stats network

The following example shows the output for the **show stats network <network-name>** command:

```

Swarm Network Stats
-----
Timestamp Clients Frames [Out] (fps) Frames [In] (fps) Throughput [Out] (bps) Throughput [In] (bps)
-----
16:39:25 0 0 0 0 0
16:38:55 0 0 0 0 0

```

```

16:38:25 0 0 0 0 0
16:37:54 0 0 0 0 0
16:37:24 0 0 0 0 0
16:36:54 0 0 0 0 0
16:36:24 0 0 0 0 0
16:35:54 0 0 0 0 0
16:35:23 0 0 0 0 0
16:34:53 0 0 0 0 0
16:34:23 0 0 0 0 0
Access Point Heatmap
-----
Access Points Utilization Noise Errors
-----
d8:c7:c8:c4:42:98 poor good good
Client Heatmap
-----
Clients Signal Speed IP Address
-----
Name :test123
ESSID :test123
Status :Enabled
Mode :wpa2-aes
Band :all
Type :employee
Termination :Disabled
Passphrase :
WEP Key :
WEP Key Index :1
VLAN :
Server Load Balancing :Disabled
MAC Authentication :Disabled
L2 Auth Failthrough :Disabled
Captive Portal :disable
Exclude Uplink :none
Hide SSID :Disabled
Content Filtering :Disabled
Auth Survivability :Disabled
Auth Survivability time-out :24
RADIUS Accounting :Disabled
Interim Accounting Interval :0
Radius Reauth Interval :0
DTIM Interval :1
Inactivity Timeout :1000
Legacy Mode Bands :all
G Minimum Transmit Rate :1
G Maximum Transmit Rate :54
A Minimum Transmit Rate :6
A Maximum Transmit Rate :54
Multicast Rate Optimization :Disabled
LEAP Use Session Key :Disabled
Broadcast-filter :none
Max Authentication Failures :0
Blacklisting :Disabled
WISPr :Disabled
Accounting mode :Authentication
Work without usable uplink :Disabled
Percentage of Airtime: :Unlimited
Overall Limit: :Unlimited
Per-user Limit: :Unlimited
Access Control Type: :Role
Machine-only Role: :test1
User-only Role: :test1

```

```

Dynamic Multicast Optimization :Disabled
DMO Channel Utilization Threshold :90
Local Probe Request Threshold :0
Max Clients Threshold :64
Background WMM Share :0
Best Effort WMM Share :0
Video WMM Share :0
Voice WMM Share :0
Certificate Installed: :No
Internal Radius Users: :0
Internal Guest Users: :0
Role Derivation Rules
-----
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
----
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 subscription-aps

show subscription-aps

Description

This command displays the subscription status of an IAP.

Example

```
(Instant AP) (config) # show subscription-aps
```

```
IAP controlled by Cloud-Server:disable  
subscription enabled by manually :disable  
Subscription Ap List  
-----  
MAC Address Status  
-----  
d8:c7:c8:c4:56:de ACTIVE  
d8:c7:c8:c4:57:06 ACTIVE
```

Command History

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|image-sync}
```

Description

This command displays the various entities associated with the swarm.

Syntax

Parameter	Description
state	Displays the current status of the IAP cluster.
mode	Displays the functioning mode of the IAP cluster.
image-sync	Displays the image-sync IAP list.

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 6.5.0.0-4.3.0.0	The image-sync parameter 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 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 IAP 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. - Emergency—Panic conditions that occur when the system becomes unusable. - Alert—Any condition requiring immediate attention and correction. - Critical—Any critical conditions, for example, hard drive error. - Errors—Error conditions.

Parameter	Description
	- Warning—Warning messages. - Notice—Significant events of a non-critical and normal nature. The default value for all Syslog facilities. - Informational—Messages of general interest to system users. - Debug—Messages containing information useful for debugging.

Command History

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 tacacs-servers

show tacacs-servers

Description

This command displays all the tacacs servers configured on an IAP.

Usage Guidelines

Use this command to view the list of tacacs servers available on an IAP.

Example

The following example shows the output of the **show tacacs-servers** command:

```
TACACS Servers
-----
Name IP Address Port Key Timeout Retry Count In Use
----
tacacs1 10.64.16.240 49 pass123 20 1 Yes
tacacs2 192.168.0.100 49 pass456 10 2 No
```

The output of this command provides the following information:

Parameter	Description
Name	Indicates the list of tacacs server available on an IAP.
IP Address	Displays the IP address for each tacacs server.
Port	Indicates the TCP Port in use for the tacacs server.
key	Indicates the shared secret key used to authenticate and access tacacs server.

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	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 IAP 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 time-profile

show time-profile

Description

This command displays all the time range profiles, the respective SSIDs on which they are applied, and the status (enabled/disabled).

Usage Guidelines

Use this command to view the list of time profiles created on the IAP.

Example

The following example shows the output of the **show time-profile** command:

```
Time Range SSID Profile
-----
Time Profile Name SSID profile Name Enable/Disable
-----
Lunch Break Test123 Enable
```

The output of this command provides the following information:

Parameter	Description
Time Profile Name	Name of the time profile.
SSID Profile	The WLAN SSID profiles for which the time profile is applied.
Enable/Disable	Status of the time range profile on the SSID.

Command History

Version	Description
Aruba Instant 6.4.3.4-4.2.1.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show time-range

show time-range

Description

This command displays a list of the time range profiles configured on the IAP.

Usage Guidelines

Use this command to view the time range profiles configured on an IAP.

Example

The following example shows the output of the **show time-range** command:

```
Time Range Summary
-----
Profile Name  Type  Start Day  Start Time  End Day  End Time  Valid
-----
Lunch Break   absolute 10/28/2014 12:40 10/28/2014 13:00 No
```

The output of this command provides the following information:

Parameter	Description
Profile Name	Indicates the name of Time Profiles created on the IAP.
Type	Indicates the type of time profile created.
Start Day	Indicates the date on which the time profile is enabled on the SSID.
Start Time	Indicates the time at which the time profile is made active on the SSID.
End Day	Indicates the date on which the time profile is disabled on the SSID.
End Time	Indicates the time at which the time profile is disabled on the SSID.
Valid	Indicates if the profile is valid for current time. For example, if a profile is run only during a specific time of the day and is not active when the command is run, the Valid column displays the status as No .

Command History

Version	Description
Aruba Instant 6.4.3.4-4.1.2.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show tspec-calls

show tspec-calls

Description

This command displays the traffic specification (TSPEC) statistics when voice traffic is prioritized and TSPEC function is enabled on an SSID.

Usage Guidelines

Use this command to view the TSPEC statistics.

Example

The following example shows the output of the **show tspec-calls** command:

```
TSPEC Stats
-----
SSID      Total ADDTS   Accepted calls   Refused calls   DELTS Received   DELTS Sent
-----
Aruba-ap  0              0                0                0                0
Aruba-ap  0              0                0                0                0
TSPEC SSIDs
-----
SSID      Radio   Max Bandwidth   Available Bandwidth
-----
Aruba-ap  1       0.00            0.00
TSPEC Calls
-----
Client    Client MAC   Allocated Bandwidth   Active flows
-----
TSPEC SSIDs
-----
SSID      Radio   Max Bandwidth   Available Bandwidth
-----
Aruba-ap  0       0.00            0.00
TSPEC Calls
-----
Client    Client MAC   Allocated Bandwidth   Active flows
-----
```

The output of this command displays information about the voice calls, the SSIDs on which TSPEC is enabled, and the IAP clients connected to the SSIDs with TSPEC enabled.

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	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: - For RAP-108/109, IAP-103, and IAP-114/115—ArubaInstant_Pegasus_<build-version> - For RAP-155/155P—ArubaInstant_Aries_<build-version> - For IAP-224/225 and IAP-274/275—ArubaInstant_Centaurus_<build-version> - For IAP-324/325—ArubaInstant_Hercules_6.5.1.0-4.3.1.0.0_xxxx - For all other IAPs—ArubaInstant_Orion_<build-version>
Status	Indicate the current status of the image upgrade.
Image Info	Indicates the source of image.
Error Detail	Displays errors generated when an upgrade fails.
Auto Reboot	Indicates if automatic rebooting of 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 6.5.0.0-4.3.0.0	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 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 (VCs) 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 url-visibility

show url-visibility [verbose]

Description

This command displays the url visibility status of the outstanding user sessions.

Usage Guidelines

Use this command to view the list of client URLs that are yet to be forwarded to the ALE server.

Example

The following output is displayed for the **show url-visibility** command:

Client URL List

```
-----
SrcIP          DstIP          URL              URL Length  HitCount
-----
172.16.40.254  98.139.183.24  yahoo.com        9           1
172.16.40.254  173.194.203.94 google.co.in/?gfe_rd... 49           1
172.16.40.254  74.125.224.34  youtube.com      11           1
172.16.40.254  74.125.224.39  google.com       10           1
172.16.40.254  173.252.120.68 facebook.com     12           2
172.16.40.254  198.35.26.96  wikipedia.org    13           1
172.16.40.254  74.125.224.41  youtube.com      11           2
172.16.40.254  198.35.26.96  wikipedia.org    13           1
172.16.40.254  206.190.36.105 in.yahoo.com     12           1
172.16.40.254  173.252.90.132 facebook.com     12           1
172.16.40.254  198.35.26.96  wikipedia.org    13           1
172.16.40.254  206.190.36.45  yahoo.com        9           1
Num of Entries:12
Last URL flash timestamp: 00:00:00
Last flash URL session count: 0
Max URL table size: 2097152 bytes
Current URL count: 12
Current URL size: 426 bytes
```

The output of this command provides the following information:

Column	Description
SrcIP	Indicates the source IP.
DstIP	Indicates the destination IP.
URL	Lists the URL of the session.
URL Length	Indicates the length of the URL.
HitCount	Indicates the number of hits on the URL.

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show usb status

show usb status

Description

This command displays the status of the cellular modem link on the IAP.

Usage Guidelines

The USB devices connected to an IAP can be enabled or disabled according to uplink configuration settings. The **show usb status** command displays the status of the USB connected to the IAP.

Example

The following example shows the output of the **show usb status** command:

```
cellular status
-----
card          detect      link
----          -
Not-present   Not-detect   Linkdown
```

The output of this command indicates the connection status of a 3G or 4G USB modem.

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	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: 225), Version 6.4.4.3-4.2.2.0  
Website: http://www.arubanetworks.com  
Copyright (c) 2002-2015, Aruba Networks, an HP company.  
Compiled on 2015-12-18 at 23:46:04 PST (build 53034) by p4build  
FIPS Mode :disabled  
AP uptime is 2 days 3 hours 44 minutes 55 seconds  
Reboot Time and Cause: unknown
```

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|tunnels}
```

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.
tunnels	Displays the IAP-VPN retry counter statistics.

Example

The following example shows the output displayed for **show vpn config** command:

```
Concentrator
-----
Type Value
----
VPN Primary Server
VPN Backup Server
VPN Preemption disable
VPN Fast Failover disable
VPN Hold Time 600
VPN Monitor Pkt Send Freq 5
VPN Monitor Pkt Lost Cnt 2
VPN Ikepsk
VPN Username
VPN Password 95a5624fbf08dfb3e794ac2c6686e330
GRE outside vpn disable
GRE Server
GRE IP Address 0.0.0.0
GRE Type 1
GRE Per AP Tunnel disable
Reconnect User On Failover disable
Reconnect Time On Failover 60
Routing Table
-----
Destination Netmask Gateway Type
-----
```

The output displayed for this command provides information on the parameters configured for the VPN concentrator.

For more information on the VPN configuration parameters, see the following commands:

- [vpn primary](#)
- [vpn backup](#)
- [vpn preemption](#)
- [vpn fast-failover](#)
- [vpn gre-outside](#)
- [vpn hold-time](#)

- [vpn monitor-pkt-lost-cnt](#)
- [vpn monitor-pkt-send-freq](#)
- [vpn ikepsk](#)
- [gre 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 6.4.0.2-4.1	The tunnels keyword was added.
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.

Parameter	Description
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 Trusted
-----
auto    Yes  Yes    None Yes
full    No   Yes    None No

Port Profile Assignments
-----
Port  Profile Name
-----
0     default_wired_port_profile
1     example1-crash
2     wired-instant
3     wired-instant
4     wired-instant
```

The output of this command provides the following information:

Column	Description
Name	Indicates the name of the wired port profile.
VLAN Mode	Indicates the name of switchport mode for the wired profiles. The VLAN modes can be Access or Trunk .
Allowed VLAN	Indicates the list of allowed VLANs. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
Native VLAN	Indicates the values assigned for Native VLAN. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN.
Admin Status	Indicates the status of admin port.
Role	Indicates the role assigned to the wired profile users.
Speed	Indicates the speed of wired client traffic.

Column	Description
duplex	Indicates if the client traffic duplexing full, half, or automatically assigned based on the capabilities of the client, the IAP, 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.
Trusted	Indicates if a trusted port is supported in an IAP.
Port	Indicates the port number to which a wired profile is assigned.
Profile	Indicates the name of wired profile assigned to a wired port.

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	The parameter Trusted is introduced.
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

show xml-api-server

show xml-api-server config

Description

This command displays the XML API server configuration details.

Usage Guidelines

Use this command to view the XML API server configuration details.

Example

The following example shows the output of the **show xml-api-server** command:

```
ip :192.0.2.5  
key :user1234
```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

snmp-server

```
snmp-server
  community <address>
  engine-id <engineID>
  host <ipaddr> version {1 <name> udp-port <port>}|{2c|3 <name> [inform] [udp-port <port>]}
  user <name> <auth-prot> <password> <priv-prot> <password>
```

Description

This command configures SNMP parameters.

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 <ipaddr>	Configures the IP address of the host to which SNMP traps are sent. This host needs to be running a trap receiver to receive and interpret the traps sent by the controller.	—	—
version	Configures the SNMP version and security string for notification messages.	1,2c,3	—
inform	Sends SNMP inform messages to the configured host.	—	—
udp-port	Indicates the port number to which notification messages are sent.	—	162
user	Configures an SNMPv3 user profile for the specified username.	—	—
auth-prot	Indicates the authentication protocol for the user, either HMAC-MD5-98 Digest Authentication Protocol (MD5) or HMAC-SHA-98 Digest Authentication Protocol (SHA), and the password to use with the designated protocol.	MD5/SHA	SHA
priv-prot	Indicates the privacy protocol for the user and the password to use with the designated protocol. CBC-DES Symmetric Encryption Protocol (DES) is the default option.	DES	DES

Usage Guidelines

This command configures SNMP on the IAPs only.

Example

The following example configures an SNMP host and community string:

```
(Instant AP) (config)# snmp-server community user123
(Instant AP) (config)# snmp-server host 10.0.0.1 version 2c udp-port 162 inform
```

Command History

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

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

speed test

```
speed-test
  bandwidth <bandwidth>
  include-reverse
  on-boot
  protocol [<tcp>|<udp>]
  sec-to-measure <secs>
  server-ip <server>
  server-port <port>
  time-interval <interval>
  no
```

Description

This command enables the user to configure an iperf3 client on the VC to run each time the IAP boots up and additionally configure time intervals at which it is executed periodically.

Syntax

Parameter	Description	Range	Default
speed test	Enables speed-test configuration sub-mode for speed-test profile configuration.	—	—
bandwidth <bandwidth>	Configures the bandwidth length in Mbps.	—	—
include-reverse	The direction of traffic is reversed and sent from the server to the client. This option enables Iperf to run the speed test for an extended duration.	—	—
on-boot	Configures the IAP to run the speed test during boot up.	—	—
protocol [<tcp> <udp>]	Configures the speed test profile to be executed using the UDP or TCP protocol.	—	tcp
sec-to-measure <secs>	Configures the duration of the speed test.	0-20 secs	10 secs
server-ip <server>	Denotes the IP address of the Iperf server which is used to run the speed test.	—	—
server-port <port>	Denotes the server port that the client needs to connect to execute the speed test.	—	5201

Parameter	Description	Range	Default
time-interval <internal>	Configures a time interval (secs) to run the speed test on a regular basis. The minimum time interval is 60 secs.	—	—
no	Removes the speed-test profile configuration.	—	—

Usage Guidelines

Use this command to run a speed test on the Master IAP.

Examples

The following example configures the speed test profile:

```
(Instant AP) (config) # speed-test
(Instant AP) (speed-test) # server-ip 10.17.138.2
(Instant AP) (speed-test) # server-port 5201
(Instant AP) (speed-test) # sec-to-measure 20
(Instant AP) (speed-test) # include-reverse
(Instant AP) (speed-test) # protocol udp
(Instant AP) (speed-test) # bandwidth 100
(Instant AP) (speed-test) # time-interval 600
(Instant AP) (speed-test) # end
(Instant AP) (speed-test) # commit apply
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3.0	This command is modified.
Aruba Instant 6.4.3.4-4.2.1.0	This command is introduced.

Command Information

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

speed test <server>

```
speed-test {<server> <protocol> [<bandwidth>|<include-reverse>|<sec-to-measure>|<server-port>]}
```

Description

This command enables the user to run a speed test on the lperf server at any point in time. The speed test configuration is not saved and can be executed only once.

Syntax

Parameter	Description	Range	Default
server	Enter the IP address of the lperf server on which the speed test needs to be run.	—	—
protocol [<tcp> <udp>]	Enter the protocol type used for executing the speed test.	—	tcp
bandwidth <bandwidth>	Enter the bandwidth length in Mbps.	—	—
include-reverse	The direction of traffic is reversed and sent from the server to the client. This option enables lperf to run the speed test for an extended duration.	—	—
sec-to-measure <secs>	Specify a duration (in secs) for the speed test.	0-20 secs	10 secs
server-port <port>	Enter the server port that the client needs to connect to execute the speed test.	—	5201

Usage Guidelines

Use this command to run a speed test on the lperf server at any instant.

Examples

The following example runs a speed test on the lperf server:

```
(Instant AP) # speed-test 10.17.138.2 udp bandwidth 100 sec-to-measure 20 server-port 5201
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3.0	This command is modified.
Aruba Instant 6.4.3.4-4.2.1.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

subscription-ap

```
subscription-ap <MAC-address> status <status>  
no...
```

Description

This command configures the subscription status for an IAP.

Syntax

Command/Parameter	Description
<MAC-address>	Enter the MAC address of the IAP.
<status>	Enter the subscription status for the IAP.
no...	Removes the configuration.

Usage Guidelines

Use this command to subscribe the IAP based on its MAC address.

Example

```
(Instant AP) (config) # subscription-ap a1:b2:c3:d4:42:98 status
```

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

subscription-ap-enable

subscription-ap-enable
no...

Description

This command enables the subscription of an IAP.

Syntax

Command/Parameter	Description
subscription-ap-enable	Enables the subscription for an IAP.
no	Removes the configuration.

Usage Guidelines

Use this command to enable the subscription of the IAP.

Example

```
(Instant AP) (config) # subscription-ap-enable
```

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

swarm-mode

swarm-mode <mode>

Description

This command allows you to provision an IAP in the standalone or cluster mode.

Syntax

Parameter	Description	Range
<mode>	Provisions the IAP in the standalone or cluster mode. The swarm-mode standalone command converts the IAP to the standalone mode, whereas the swarm-mode cluster command converts it to the cluster mode.	standalone or cluster

Usage Guidelines

When an IAP is converted to the standalone mode, it cannot join a cluster of IAPs even if the IAP is in the same VLAN. If the IAP is in the cluster mode, it can form a cluster with other VC IAPs in the same VLAN.

Example

The following command allows you to convert an IAP to a standalone IAP:

```
(Instant AP)# swarm-mode standalone
```

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.

syslocation

syslocation <syslocation>
no...

Description

This command allows you to define the physical location for the IAP.

Syntax

Command/Parameter	Description
<syslocation>	Allows you to specify a physical location.
no	Removes the configuration.

Usage Guidelines

Use this command to define the physical location of the IAP.

Example

The following example sets the physical location of the IAP to Sunnyvale:

```
(Instant AP) (config) # syslocation <Sunnyvale>
```

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

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
<code>syslog-level <level></code>	Configures the Syslog facility level. You can configure any of the following logging levels: - Emergency—Panic conditions that occur when the system becomes unusable. - Alert—Any condition requiring immediate attention and correction. - Critical—Any critical conditions such as a hard drive error. - Errors—Error conditions. - Warning—Warning messages. - Notice—Significant events of a non-critical and normal nature. The default value for all Syslog facilities. - Informational—Messages of general interest to system users. - Debug—Messages containing information useful for debugging.	Emergency, Alert, Critical, Errors, Warning, Notice, Informational, Debug	Notice
<code>ap-debug</code>	Generates a log for the IAP device for debugging purposes.	—	—
<code>network</code>	Generates a log when there is a change in the network, for example, when a new IAP is added to a network.	—	—
<code>security</code>	Generates a log for network security, for example, when a client connects using wrong password.	—	—
<code>system</code>	Generates a log about the system configuration and status.	—	—
<code>user</code>	Generates a log for the IAP clients.	—	—
<code>user-debug</code>	Generates a detailed log about the clients for	—	—

Parameter	Description	Range	Default
	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 AP) (config) # syslog-level error ap-debug
(Instant AP) (config) # end
(Instant AP) # 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 AP) (config) # syslog-server 192.0.2.9  
(Instant AP) (config) # end  
(Instant AP) # 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

```
telnet <host> telnet-port <port>
```

Description

This command initiates a telnet session with external servers from the Instant command line interface (CLI).

Syntax

Command/Parameter	Description
host	The IP address of the destination server.
<telnet-port>	The physical port number of the server to which a connection needs to be established through Telnet.

Usage Guidelines

Use this command to Telnet an external server using the Instant CLI.

Example

The following example initiates a telnet session with external servers:

```
(Instant AP) telnet 10.0.0.1 23
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This port parameter was introduced.
Aruba Instant 6.3.1.1-4.0	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC 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 AP) (config) # telnet-server  
(Instant AP) (config) # end  
(Instant AP) # 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 AP) (config) # terminal-access
(Instant AP) (config) # end
(Instant AP) # 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 AP) (config) # tftp-dump-server <IP-address>  
(Instant AP) (config) # end  
(Instant AP) # 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

time-range

```
time-range <name> {absolute start <startday> <starttime> end <endday> <endtime>| periodic  
{daily | weekday | weekend} <starttime> to <endtime> | <startday <starttime> to <endday>  
<endtime>}  
no time-range <name>
```

Description

This command allows you to create time range profiles on an IAP to enable or disable access to an SSID during a specific period of time.

Syntax

Command/Parameter	Description
name	Enter the profile name for the time range profile.
absolute start {<startdate> <starttime>} end {<enddate> <endtime>}	The SSID is made available only during the specified date and time range. Configure the following time range parameters: - startday—Enter the start date in the mm/dd/yyyy format. - starttime—Enter the start time in the hh:mm format. - endday—Enter the end date in the mm/dd/yyyy format. - endtime—Enter the end time in the hh:mm format.
periodic {<startday> <starttime>} to {<endday> <endtime>}	The availability of the SSID will be periodically changed based on the time range set in the profile. Configure the following time range parameters: - startday—Specify any day of the week from Monday to Sunday - starttime—Enter the start time in the hh:mm format. - endday—Enter the end day for the time range profile. - endtime—Enter the end time in the hh:mm format.
periodic <daily> [<starttime> to <endtime>]	- daily—The time range profile is applied on the SSID on a daily basis. - starttime—Enter the start time in the hh:mm format. - endtime—Enter the end time in the hh:mm format.
periodic <weekday> [<starttime> to <endtime>]	- weekday—The time range profile is applied only during the weekday - starttime—Enter the start time in the hh:mm format. - endtime—Enter the end time in the hh:mm format.
periodic <weekend> [<starttime> to <endtime>]	- weekend—The time range profile is applied only during the weekend. - starttime—Enter the start time in the hh:mm format. - endtime—Enter the end time in the hh:mm format.
no time-range <name>	Removes the time range configuration.

Usage Guidelines

Use this command to create a Time Range Profile using the Instant CLI. You can create an absolute time profile to execute once during a specific date and time configured in the profile or create a periodic profile to execute at regular intervals based on the periodicity specified in the configuration. These time based profiles can be applied to existing SSIDs in the IAP.

Example

The following example creates an absolute time range profile :

```
(Instant AP) (config) # time-range test1234 absolute start 10/20/2013 10:40 end 10/20/2015 10:50
```

The following example creates a periodic time range profile that executes on the specified day of the week:

```
(Instant AP) (config) # time-range test1234 periodic monday 10:40 to tuesday 10:50
```

The following example creates a periodic time range profile that executes daily:

```
(Instant AP) (config) # time-range testshs12 periodic daily 10:20 to 10:35
```

The following example creates a periodic time range profile that executes during the weekday:

```
(Instant AP) (config) # time-range test123 periodic weekday 10:20 to 10:35
```

The following example creates a periodic time range profile that executes during the weekend:

```
(Instant AP) (config) # time-range test12 periodic weekend 10:20 to 10:30
```

The following example removes the time range configuration:

```
(Instant AP) (config) # no time-range testshs12
```

Command History

Version	Description
Aruba Instant 6.4.3.4-4.2.1.0	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. You can also use this command to upgrade images for multi-class IAP cluster.
upgrade-image2-no-reboot	Uploads an 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 an 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 RAP-108/109, IAP-103, and IAP-114/115—ArubaInstant_Pegasus_<build-version>
- For RAP-155/155P—ArubaInstant_Aries_<build-version>
- For IAP-204/205 and IAP-205H—ArubaInstant_Taurus_6.5.1.0-4.3.1.0.0_xxxx
- For IAP-224/225, IAP-228, IAP-274/275, and IAP-277—ArubaInstant_Centaurus_<build-version>
- For IAP-324/325—ArubaInstant_Hercules_6.5.1.0-4.3.1.0.0_xxxx
- For all other IAPs—ArubaInstant_Orion_<build-version>

Example

The following examples upgrade an IAP by using an image file from the FTP server:

```
(Instant AP) # upgrade-image ftp://192.0.2.7/Aruba_Orion_6.2.1.0-4.0.0.0_xxxx  
(Instant AP) # upgrade-image2-no-reboot ftp://192.0.2.7/Aruba_Orion_6.2.1.0-4.0.0.0_xxxx
```

To upgrade images for a multi-class IAP cluster:

```
(Instant AP) # upgrade-image2  
Orion@tftp://192.168.0.1/mips32.ari;Cassiopeia@tftp://192.168.0.1/armv5te.ari
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is modified.
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-ip <ip>
  failover-internet-check-timeout
  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...
no uplink
```

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: • ethernet • cellular • wifi • none	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

Parameter	Description	Range	Default
failover-internet-ip	Allows you to configure the IP address to which the ICMP packets are sent in the event of Internet failure. If the out-of-service feature is enabled for the Internet down event in the SSID and the Internet is down, the ICMP packets are sent to the configured IP address to verify if the Internet is reachable from current uplink. By default, the master IAPs send the ICMP packets to 8.8.8.8 IP address to verify if the Internet is reachable.	Any IP address	8.8.8.8
failover-internet-check-timeout	Configures the number of seconds after which the Internet based uplink verification times out.	0-3600	10
failover-internet-pkt-lost-cnt <count>	Configures the number of packets that are to be lost when verifying the uplink availability using the Internet.	1—1000	10
failover-internet-pkt-send-freq <frequency>	Configures the frequency in seconds, at which the ICMP packets are sent to verify the uplink availability using the Internet.	1—3600	30
failover-vpn-timeout <seconds>	Configures a duration to wait for an uplink switch based on VPN status.	—	180 seconds
preemption	Enables pre-emption when no uplinks are enforced. When enabled, if the current uplink is active, the 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>]}	Sets an uplink priority. You can specify the type of	Integer	Eth0

Parameter	Description	Range	Default
wifi <priority>}	uplink to configure and assign a priority. If Ethernet uplink needs to be prioritized, specify the interface port number.		
no...	Disables the parameters configured under the uplink command.	—	—
no uplink	Removes the uplink 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 as the primary uplink regardless of uplink preemption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured and uplink is enabled on the wired profiles, the 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. The uplink with the highest priority is used as the primary uplink. For example, if WiFi-sta has the highest priority, it is used as the primary uplink.
- When no uplink is enforced and preemption is enabled, and if the current uplink fails, the IAP tries to find an available uplink based on 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 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 AP) (uplink) # uplink-priority ethernet port 0 1
(Instant AP) (uplink) # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	The failover-internet-ip parameter was added.
Aruba Instant 6.4.0.2-4.1	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 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 (VCs) to the same port on an upstream switch (for example, AirWave server).

Example

The following example configures uplink management VLAN:

```
(Instant AP) # 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

url-visibility

url-visibility
no...

Description

This command enables url visibility on the IAP and extracts the full URL information of the http and https sessions along with the session-ip and periodically logs them on the ALE server.

Syntax

Parameter	Description
url-visibility	Enables URL visibility on the IAP.
no	Disables URL visibility.

Usage Guidelines

Use this command to determine the frequency of hits on a specific URL. To verify if the configuration has been applied correctly, use the **show dpi debug status** command.

Example

The following example enables url visibility:

```
(Instant AP) (config)# url-visibility
(Instant AP) (config)# end
(Instant AP)# commit apply
```

The following example shows the output of the show dpi debug status command:

```
Dpimgr Running :TRUE
Dpimgr Hello count :1
Dpimgr Agent :App
Dpimgr Status value :0x17d
Dpimgr Visibility Status :URL + App
Dpimgr Enforcement Status :App
Dpimgr External Visibility Status :AMP
```

Command History

Version	Description
Aruba Instant 6.4.4.4-4.2.3	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode.

usb-port-disable

usb-port-disable
no...

Description

This command disables the USB port on the IAP.

Usage Guidelines

Use this command to disable the USB port. To re-enable the port, run the **no usb-port-disable** command. Reboot the IAP after changing the USB port status.

Example

The following example shows how to disable the USB port on the IAP:

```
(Instant AP) # usb-port-disable
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	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 IAPs 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 AP) (config)# user user1 password123 radius
(Instant AP) (config)# end
(Instant AP)# 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 an 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 AP) (config)# virtual-controller-country US
(Instant AP) (config)# end
(Instant AP)# 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-dnsip

```
virtual-controller-dnsip <addr>  
no...
```

Description

This command configures the VC DNS IP address.

Syntax

Parameter	Description
<code>virtual-controller-ip <IP-address></code>	Configures the DNS IP address for the VC.
<code>no...</code>	Removes the configuration.

Usage Guidelines

Use this command to configure a DNS IP address for the VC.

Example

The following example configures a DNS IP address for the VC:

```
(Instant AP) (config)# virtual-controller-dnsip 192.0.2.2  
(Instant AP) (config)# end  
(Instant AP)# commit apply
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	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 VC.

Syntax

Parameter	Description
virtual-controller-ip <IP-address>	Assigns an IP address for the VC.

Usage Guidelines

Use this command to configure an IP address for the VC.

Example

The following example assigns an IP address for the VC:

```
(Instant AP) (config)# virtual-controller-ip 192.0.2.2
(Instant AP) (config)# end
(Instant AP) # 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-ipv6

virtual-controller-ipv6 <IPv6 address>

Description

This command configures an IPv6 address for the VC.

Syntax

Parameter	Description
virtual-controller-ipv6 <IPv6 address>	Assigns an IPv6 address for the VC.

Usage Guidelines

Use this command to configure an IPv6 address for the VC.

Example

The following example assigns an IP address for the VC:

```
(Instant AP) (config)# virtual-controller-ipv6 10.17.154.132
(Instant AP) (config)# end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	This command is introduced.

Command Information

IAP Platform	Command Mode
IAP-214/215, IAP-224/225, IAP-274/275, IAP-314/315, IAP-324/325, IAP-334/335	Configuration mode

virtual-controller-key

virtual-controller-key <name>

Description

This command configures a unique name for the VC.

Syntax

Parameter	Description
virtual-controller-key <name>	Defines a unique name for the VC.

Usage Guidelines

Use this command to assign a name for the VC.

Example

```
(Instant AP) (config)# virtual-controller-key <name>
(Instant AP) (config)# virtual-controller-ip <IP-address>
(Instant AP) (config)# virtual-controller-vlan <Vlan-ID> <Mask> <Gateway-IP-address>
(Instant AP) (config)# end
(Instant AP)# 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 VC.

Syntax

Parameter	Description
virtual-controller-vlan <virtual-controller-vlan>	Associates a VLAN ID with the VC.
<virtual-controller-mask>	Configures a subnet mask for the VC.
<virtual-controller-gateway>	Configures a gateway for the VC.
no...	Removes the configuration.

Usage Guidelines

Use this command to configure VLAN, Netmask, and Gateway for the VC.

Example

The following example configures VLAN for the VC:

```
(Instant AP) (config) # virtual-controller-vlan <Vlan-ID> <Mask> <Gateway-IP-address>  
(Instant AP) (config) # end  
(Instant AP) # 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 a the primary VPN server is not available.

Example

The following example configures a backup server for VPN connections:

```
(Instant AP) (config)# vpn backup <name>
(Instant AP) (config)# end
(Instant AP) # commit apply
```

Command History

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 AP) (config)# fast-failover
(Instant AP) (config)# end
(Instant AP)# 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 AP) (config) # vpn gre-outside  
(Instant AP) (config) # end  
(Instant AP) # 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 AP) (config) # hold-time <seconds>  
(Instant AP) (config) # end  
(Instant AP) # 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 AP) (config)# vpn ikepsk secretKey username User1 password password123  
(Instant AP) (config)# end  
(Instant AP)# 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 AP) (config)# vpn monitor-pkt-lost-cnt <count>  
(Instant AP) (config)# end  
(Instant AP)# 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 AP) (config)# vpn monitor-pkt-send-freq 10  
(Instant AP) (config)# end  
(Instant AP)# 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 AP) (config)# vpn primary <name>
(Instant AP) (config)# end
(Instant AP)# 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>  
no...
```

Description

This command defines a period after which the VPN connection can be reestablished when the primary VPN tunnel fails.

Syntax

Parameter	Description
<code>vpn reconnect-time-on-failover <down-time></code>	Configures a time period in minutes after which the VPN is reconnected when the primary VPN tunnel fails.
<code>no...</code>	Removes the configuration.

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 AP) (config)# vpn reconnect-time-on-failover 20  
(Instant AP) (config)# end  
(Instant AP) # 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 AP) (config)# vpn reconnect-user-on-failover
(Instant AP) (config)# end
(Instant AP) # 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

web-server

```
web-server
  ssl-protocol {all|tlsv1|tlsv1.1|tlsv1.2}
  no...
```

Description

This command allows you to configure web server and enable or disable the TLS protocol.

Syntax

Parameter	Description
ssl-protocol	Enables SSL protocol for secure communication with the web server.
all	Enables all versions of Transport Layer Security (TLS) protocol for secure communication with the web server.
tlsv1	Enables TLS v1 protocol.
tlsv1.1	Enables TLS v1.1 protocol.
tlsv1.2	Enables TLS v1.2 protocol.
no...	Removes the configuration.

Usage Guidelines

Use the **web-server** command to enable secure communication with the web server through the TLS protocol.

Example

The following example shows how to enable TLS v1.0:

```
(Instant AP) (config) # web-server
(Instant AP) (web-server) # ssl-protocol tlsv1
(Instant AP) (web-server) # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This command was 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>	Configures the IAP to function in any of the following modes: • Access— In Access mode, the IAP serves clients, while also monitoring for rogue IAPs in the background. • Monitor—In Monitor mode, the IAP acts as a dedicated monitor, scanning all channels for rogue IAPs and clients. • Spectrum Monitor— In Spectrum Monitor mode, the IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring IAPs or from non-WiFi devices such as microwaves and cordless phones. NOTE: In Monitor and Spectrum Monitor modes, the IAP does not provide access services to clients.	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 AP) # 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>	Configures the IAP to function in any of the following modes: • Access— In Access mode, the IAP serves clients, while also monitoring for rogue IAPs in the background. • Monitor—In Monitor mode, the IAP acts as a dedicated monitor, scanning all channels for rogue IAPs and clients. • Spectrum Monitor— In Spectrum Monitor mode, the IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring IAPs or from non-WiFi devices such as microwaves and cordless phones. NOTE: In Monitor and Spectrum Monitor modes, the IAP does not provide access services to clients.	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 AP) # 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>] | external [Profile <name>] [exclude-uplink
  <types>]}
  content-filtering
  dot1x
  duplex <duplex>
  inactivity-timeout <interval>
  l2-auth-failthrough
  mac-authentication
  native-vlan <vlan>
  poe
  radius-accounting
  radius-accounting-mode {user-association|user-authentication}
  radius-interim-accounting-interval <minutes>
  radius-reauth-interval <minutes>
  server-load-balancing
  set-role <attribute>{{equals|not-equal|starts-with|ends-with|contains}<operator>
  <role>|value-of}
  set-role-mac-auth <mac-only>
  set-role-machine-auth <machine-only> <user-only>
  set-role-pre-auth <role>
  set-role-unrestricted
  set-vlan <attribute>{equals|not-equals|starts-with|ends-with|contains} <operator> <VLAN-
  ID>|value-of}
  shutdown
  spanning-tree
  speed <speed>
  switchport-mode <mode>
  trusted
  type <type>
  uplink-enable
  no...
no wired-port-profile <port>
```

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.	—	—

Command/Parameter	Description	Range	Default
	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>[exclude-uplink <types>] external [exclude-uplink <types> profile <name>[exclude-uplink <types>]]}	Enables internal or external captive portal authentication for the wired profile users. You can also disable redirection to the captive portal based on the type of current uplink. If the external captive profiles are created, you can specify the profile name by using the external and profile keywords and associated parameters.	—	—
content-filtering	Enables content filtering.	—	—
dot1x	Enables 802.11X authentication for the Wired profile users.	—	Disabled
duplex <duplex>	Assigns a value for duplexing client traffic based on the capabilities of the client, the IAP, and the cable. You can specify full , half , or auto .	full, half, auto	auto
inactivity-timeout <interval>	Configures a timeout value for the inactive client sessions. When a client session is inactive for the specified duration, the session expires and the clients are required to log in again.	60-86400 seconds	1000 seconds
l2-auth-failthrough	Allows the clients to use 802.1X authentication when MAC authentication fails.	—	Disabled
mac-authentication	Enables MAC authentication.	—	Disabled
native-vlan <vlan>	Configures a value for Native VLAN. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN.	1-4093	—

Command/Parameter	Description	Range	Default
poe	Enables power over Ethernet	—	Enabled
radius-accounting	Enables accounting for the RADIUS server authentication. When enabled, the IAPs post accounting information to the Radius server at the specified accounting interval.	—	—
radius-accounting-mode {user-association user-authentication}	Configures an accounting mode for the captive portal users. You can configure any of the following modes for accounting: user-authentication—when configured, the accounting starts only after client authentication is successful and stops when the client logs out of the network. user-association—When configured, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.	—	user-authentication
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.	0-60	—
radius-reauth-interval <minutes>	Configures a reauthentication interval at which all associated and authenticated clients must be reauthenticated.	0-32768	—
server-load-balancing	Enables load balancing across two RADIUS servers if two authentication servers are configured for the SSID.	—	Enabled
set-role <attribute> {{equals not-equal starts-with ends-with contains}operator}> <role> value-of}	Assigns a user role to the clients. The first rule that matches the configured condition is applied.	—	—

Command/Parameter	Description	Range	Default
	You can specify any of the following conditions: - contains—The rule is applied only if the attribute value contains the specified string. - ends-with—The rule is applied only if the attribute value ends with the specified string. - equals—The rule is applied only if the attribute value is equal to the specified string. - not-equals—The rule is applied only if the attribute value is not equal to the specified string. - starts-with—The rule is applied only if the attribute value begins with the specified string. - value-of - This rule sets the 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.		
<code>set-role-machine-auth <machine-only><user-only></code>	Configures a machine authentication rule. You can assign different rights to clients based on whether their hardware device supports machine authentication. Machine authentication is only supported on Windows devices, so this can be used to distinguish between Windows devices and other devices such as iPads.	—	—
<code>set-role-mac-auth <mac-only></code>	Configures a MAC authentication based user role.	—	—
<code>set-role-pre-auth <role></code>	Configures a pre-authentication role to allow some access to the guest users before the client authentication.	—	—

Command/Parameter	Description	Range	Default
set-role-unrestricted	Configures unrestricted access control.	—	—
set-vlan <attribute> {equals not-equals starts-with ends-with contains} <operator> <VLAN-ID> value-of}	Assigns a VLAN to the clients. The first rule that matches the configured condition is applied. You can specify any of the following conditions: - contains—The rule is applied only if the attribute value contains the specified string. - ends-with—The rule is applied only if the attribute value ends with the specified string. - equals—The rule is applied only if the attribute value is equal to the specified string. - not-equals—The rule is applied only if the attribute value is not equal to the specified string. - starts-with—The rule is applied only if the attribute value begins with the specified string. - value-of - This rule sets the VLAN to the value of the attribute returned. To set a user role, the value of the attribute must already be configured on the IAP.	—	—
shutdown	Shuts down the admin status port.	up, down	up
spanning-tree	Enables Spanning Tree Protocol on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on IAPs with three or more ports. By default Spanning Tree is disabled on wired profiles.	—	—

Command/Parameter	Description	Range	Default
<code>speed <speed></code>	Assigns a value for indicating speed of client traffic based on the capabilities of the client, the IAP, and the cable.	10,100,200, auto	auto
<code>switchport-mode <mode></code>	Defines the switchport mode for the wired profile. You can specify any of the following modes: • Access—Use this mode to allow the port to carry a single VLAN specified as the native VLAN. • Trunk—Use this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.	access, trunk	trunk
<code>trusted</code>	Supports trusted ports to enable wired users in an L3 mode to connect to a switch or a router that is connected to the downlink port of an IAP. In this mode, <code>mac-authentication</code> , <code>dot1x</code> , and <code>captive-portal</code> parameters will not take any effect.	—	No
<code>type <type></code>	Defines the primary usage of the wired profile	employee, guest	employee
<code>uplink-enable</code>	Enables uplink for the wired profile	—	—
<code>no...</code>	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 AP) (config)# wired-port-profile employeeWired1
(Instant AP) (wired ap profile"employeeWired1")# type employee
(Instant AP) (wired ap profile"employeeWired1")# speed auto
(Instant AP) (wired ap profile"employeeWired1")# duplex auto
(Instant AP) (wired ap profile"employeeWired1")# no shutdown
(Instant AP) (wired ap profile"employeeWired1")# poe
(Instant AP) (wired ap profile"employeeWired1")# uplink-enable
```

```
(Instant AP) (wired ap profile"employeeWired1")# content-filtering
(Instant AP) (wired ap profile"employeeWired1")# switchport-mode trunk
(Instant AP) (wired ap profile"employeeWired1")# allowed-vlan 2,3,5
(Instant AP) (wired ap profile"employeeWired1")# native-vlan 1
(Instant AP) (wired ap profile"employeeWired1")# mac-authentication
(Instant AP) (wired ap profile"employeeWired1")# dot1x
(Instant AP) (wired ap profile"employeeWired1")# l2-auth-failthrough
(Instant AP) (wired ap profile"employeeWired1")# auth-server server1
(Instant AP) (wired ap profile"employeeWired1")# server-load-balancing
(Instant AP) (wired ap profile"employeeWired1")# radius-reauth-interval 20
(Instant AP) (wired ap profile"employeeWired1")# access-rule-name wiredACL
(Instant AP) (wired ap profile"employeeWired1")# set-role Group-Name contains wired wired-
instant
(Instant AP) (wired ap profile"employeeWired1")# set-vlan ap-name equals test 400
(Instant AP) (wired ap profile"employeeWired1")# trusted
(Instant AP) (wired ap profile"employeeWired1")# end
(Instant AP) # commit apply
```

The following example configures a guest wired profile:

```
(Instant AP) (config)# wired-port-profile guestWired1
(Instant AP) (wired ap profile"guestWired1")# type guest
(Instant AP) (wired ap profile"guestWired1")# speed auto
(Instant AP) (wired ap profile"guestWired1")# duplex auto
(Instant AP) (wired ap profile"guestWired1")# no shutdown
(Instant AP) (wired ap profile"guestWired1")# poe
(Instant AP) (wired ap profile"guestWired1")# uplink-enable
(Instant AP) (wired ap profile"guestWired1")# content-filtering
(Instant AP) (wired ap profile"guestWired1")# switchport-mode trunk
(Instant AP) (wired ap profile"guestWired1")# allowed-vlan 200,201,400
(Instant AP) (wired ap profile"guestWired1")# native-vlan 1
(Instant AP) (wired ap profile"guestWired1")# captive-portal external exclude-uplink Ethernet
(Instant AP) (wired ap profile"guestWired1")# mac-authentication
(Instant AP) (wired ap profile"guestWired1")# auth-server server1
(Instant AP) (wired ap profile"guestWired1")# server-load-balancing
(Instant AP) (wired ap profile"guestWired1")# access-rule-name wiredACL
(Instant AP) (wired ap profile"guestWired1")# set-role Group-Name contains wired wired-instant
(Instant AP) (wired ap profile"guestWired1")# set-vlan ap-name equals test 200
(Instant AP) (wired ap profile"guestWired1")# trusted
(Instant AP) (wired ap profile"guestWired1")# end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	The parameter Trusted is introduced.
Aruba Instant 6.4.3.1-4.2	The inactivity-timeout and accounting parameters (radius-accounting , radius-accounting-mode , and radius-interim-accounting-interval) were added.
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}
    dpi-error-page-url <idx>
    index <index>
    rule <dest> <mask> <match> {<protocol> <start-port> <end-port> {permit|deny|src-nat [vlan
    <vlan id>|tunnel <tunnel ip>]|dst-nat{<IP-address> <port>| <port>}}| app <app> {permit|
    deny}}| appcategory <appgrp>| webcategory <webgrp> {permit| deny}}| webreputation <webrep>}}
    [<opt1...opt11>]
    redirect-blocked-https-traffic
    vlan <vlan-id>
    no...
no wlan access-rule <name>
```

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>}}	Assign bandwidth contracts to user roles. 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. If you want to assign a bandwidth contract specific for each user, you can run the command with peruser parameter. The bandwidth contract will not be applicable to the user traffic on the bridged out (same subnet) destinations. NOTE: In the earlier releases, bandwidth contract could be assigned per SSID. In the current release, the bandwidth contract can also be assigned per SSID user. If the bandwidth contract is assigned for an SSID in Instant 6.2.1.0-3.4.0.0 image	1-65535 Kbps	—

Command/Parameter	Description	Range	Default
	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.		
calea	Creates an access rule for CALEA integration.	—	—
captive-portal {external [profile <name>] internal}	Configures a captive-portal role, to assign to the users role after a successful authentication.	—	—
dpi-error-page-url <idx>	Creates an access rule to display a specific error page when clients access the HTTP websites blocked by AppRF policies.	—	—
<index>	Creates an index entry for access rules.	—	—
rule	Creates an access rule. You can create up to 128 access control entries in an ACL for a user role. However, it is recommended to delete any existing configuration and apply changes at regular intervals.	—	—
<dest>	Allows you to specify the destination IP address.	—	—
<mask>	Specifies the subnet mask for the destination IP address.	—	—
<match>	match—Indicates if the rule specific to the destination IP address and subnet mask matches the value specified for protocol. invert— Indicates if the rule allows or denies traffic with an exception to the specified destination IP address and subnet mask.	match invert	—

Command/Parameter	Description	Range	Default
<protocol>	Configures any of the following: - Protocol number between 0-255 - any: any protocol - tcp: Transmission Control Protocol - udp: User Datagram Protocol	1-255	—
<sport>	Specifies the starting port number from which the rule applies.	1-65534	—
<eport>	Specifies the ending port number until which the rule applies	1-65534	—
dst-nat	Allows the IAP to perform destination NAT on packets.	—	—
src-nat [vlan <vlan id> tunnel]	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). vlan - All client based traffic will be directed to the specified uplink VLAN using the IP address of the interface that IAP has on that VLAN; if the interface is not found, this option has no effect. tunnel - The traffic from the Network Assigned clients is directed to the VPN tunnel.	—	—
<dst-nat-IP-address>	Specifies the destination-NAT IP address for the specified packets when dst-nat action is configured.	—	—
<dst-nat-port>	Specifies the destination-NAT port for the specified packets when dst-nat action is	—	—

Command/Parameter	Description	Range	Default
	configured.		
app <app>	Specifies a rule to allow or deny access to a specific type of application.	To view the list of applications, run the show dpi app all command.	—
appcategory <appgrp>	Specifies a rule to allow or deny access to a specific category of application.	To view the list of application categories, run the show dpi appcategory all command.	—
webcategory <webgrp>	Specifies a rule to allow or deny access to websites based on website category.	To view the list of website categories, run the show dpi webcategory all command.	—
webreputation <webrep>	Specifies a rule to allow or deny access to websites based on security rating.	• trustworthy-sites • low-risk-sites • moderate-risk-sites • suspicious-sites • high-risk-sites	—
permit	Creates a rule to allow the specified packets.	—	—
deny	Creates a rule to reject the specified packets	—	—
<opt0...opt11>	Allows you to specify up to 10 options for network ACLs and up to 12 options for DPI ACLs. You can configure any of the following options: • Log—Creates a log entry when this rule is triggered. • Blacklist—Blacklists the	—	—

Command/Parameter	Description	Range	Default
	client when this rule is triggered. - Classify-media—Performs a packet inspection on all non-NAT traffic and marks the critical traffic. - Disable-scanning—Disables ARM scanning when this rule is triggered. - DSCP tag—Specifies a DSCP value to prioritize traffic when this rule is triggered. 802.1p priority—Sets an 802.1p priority. - Application throttling: To set a bandwidth limit based on application, application category, web category or website reputation, you can configure application throttling by using the throttle-downstream and throttle-up options. For example, you can limit the bandwidth rate for video streaming applications such as Youtube or Netflix, or set a low bandwidth for suspicious websites.		
<code>redirect-blocked-https-traffic</code>	Configures an access rule to redirect users to a custom error page URL when accessing blocked HTTPS websites for the WLAN SSID or Wired profile.		
<code>vlan <vlan-id></code>	Configures an access rule for VLAN assignment.	1-4093	—
<code>no...</code>	Removes the definition of parameters under wlan access-rule command.	—	—
<code>no wlan access-rule</code>	Removes the WLAN access rule 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.



If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.

Example

The following example configures access rules for the wireless network:

```
(Instant AP) (config)# wlan access-rule WirelessRule
(Instant AP) (Access Rule "WirelessRule")# rule 192.0.2.2 255.255.255.0 match 6 4343 4343 log
classify-media
(Instant AP) (Access Rule "WirelessRule")# rule 192.0.2.2 255.255.255.0 192.0.2.7 255.255.255.0
match tcp 21 21 deny
(Instant AP) (Access Rule "WirelessRule")# rule 192.0.2.2 255.255.255.0 192.0.2.7 255.255.255.0
match udp 21 21 deny
(Instant AP) (Access Rule "WirelessRule")# rule any any match app youtube permit throttle-
downstream 256 throttle-up 256
(Instant AP) (Access Rule "WirelessRule")# rule any any match appcategory webmail permit
throttle-downstream 256 throttle-up 256
(Instant AP) (Access Rule "WirelessRule")# rule any any match webcategory gambling deny
(Instant AP) (Access Rule "WirelessRule")# rule any any match webcategory training-and-tools
permit
(Instant AP) (Access Rule "WirelessRule")# rule any any match webreputation high-risk-sites
deny
(Instant AP) (Access Rule "WirelessRule")# end
(Instant AP)# commit apply
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	The redirect-blocked-https-traffic parameter is added.
Aruba Instant 6.4.4.6-4.2.4.0	The src-nat parameter is added
Aruba Instant 6.4.3.1-4.2	The dpi-error-page-url parameter is added
Aruba Instant 6.4.0.2-4.1	This command is modified.
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 <time>
  drp-ip <IP> <mask> vlan <vlan> gateway <gateway>
  ip <host>
  key <key>
  nas-id <ID>
  nas-ip <IP-address>
  port <port>
  radsec [port <port>]
  retry-count <count>
  rfc3576
  rfc5997 {auth-only|acct-only}
  timeout <value>
  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 <time>	Configures a dead time interval for the authentication server.	1—1440 minutes	5

Command/Parameter	Description	Range	Default
	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.		
drp-ip <IP-address> <mask> vlan <vlan> gateway <gateway-IP-address>	Configures the IP address, net mask and VLAN, which will be used as source address and VLAN for RADIUS packets. Before configuring DRP IP address, ensure that dynamic RADIUS proxy is enabled, and a static VC IP is configured.	—	—
ip <host>	Configures the IP address or the host name of the RADIUS server.	—	—
key <key>	Configures a shared key communicating with the external RADIUS server.	—	—
nas-id <ID>	Configures Network Attached Storage (NAS) identifier strings for RADIUS attribute 32, which is sent with RADIUS requests to the RADIUS server.	—	—
nas-ip <IP>	Configures the VC IP address as the NAS address which is sent in data packets.	—	—
port <port>	Configures the authorization port number of the external RADIUS server.	—	1812
radsec [port <port>]	The RadSec command enables secure communication between the RADIUS server and IAP clients by creating a TLS tunnel between the IAP and the server. When RadSec is enabled, the port command can be used for specifying the communication port number for RadSec TLS connection. By default, the port number is set to 2083.	1-65534	2083

Command/Parameter	Description	Range	Default
<code>retry-count <count></code>	Configures the maximum number of authentication requests that can be sent to the server group.	1-5	3
<code>rfc3576</code>	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
<code>rfc5997 {auth-only acct-only}</code>	When enabled, allows the IAP to send a status-server request to determine the actual status of the authentication or accounting server. This proves useful when there is a authentication or request time rfc5997—RFC5997 support enabled for both authentication and accounting on the authentication server. auth-only—RFC5997 support enabled for authentication only. acct-only—RFC5997 support enabled for accounting only no rfc5997—Disables RFC5997 support for the authentication server.	—	Disabled
<code>timeout <value></code>	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
<code>no...</code>	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 AP) (config)# wlan auth-server RADIUS1
(Instant AP) (Auth Server <RADIUS1>)# ip 192.0.0.5
(Instant AP) (Auth Server <RADIUS1>)# key SecretKey
(Instant AP) (Auth Server <RADIUS1>)# port 1812
(Instant AP) (Auth Server <RADIUS1>)# acctport 1813
(Instant AP) (Auth Server <RADIUS1>)# rfc3576
(Instant AP) (Auth Server <RADIUS1>)# rfc5997 auth-only
(Instant AP) (Auth Server <RADIUS1>)# no nas-id
(Instant AP) (Auth Server <RADIUS1>)# no nas-ip
(Instant AP) (Auth Server <RADIUS1>)# drp-ip 192.0.2.11 255.255.255.255 vlan 200 gateway
192.0.2.15
(Instant AP) (Auth Server <RADIUS1>)# timeout 10
(Instant AP) (Auth Server <RADIUS1>)# retry-count 3
(Instant AP) (Auth Server <RADIUS1>)# end
(Instant AP)# commit apply
```

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	The rfc5997 parameter is added.
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...
no wlan captive-portal
```

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 authenticated text is used for indicating that the authentication mode is enabled for the internal captive portal users. When the authentication mode is enabled, the 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.	—	—

Command/Parameter	Description	Range	Default
<code>redirect-url <url></code>	Configures a URL to redirect the users after a successful authentication. NOTE: By default, after entering the requested info at the splash page, the users are redirected to the URL that was originally requested. When a URL is configured for redirection, it overrides the user's original request and redirects them to URL configured for redirection.	—	—
<code>terms-of-use <terms-of-use-text></code>	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
<code>use-policy <policy-text></code>	Configures usage policy text for splash page.	Text string	Please read terms and conditions before using Guest Network
<code>no...</code>	Removes the definition of parameters configured under the wlan captive-portal command.	—	—
<code>no wlan captive-portal</code>	Removes the captive portal 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 AP) (config)# wlan captive-portal
(Instant AP) (Captive Portal)# authenticated
(Instant AP) (Captive Portal)# background-color 13421772
(Instant AP) (Captive Portal)# banner-color 16750848
(Instant AP) (Captive Portal)# banner-text "Welcome to Guest Network"
(Instant AP) (Captive Portal)# no decoded-texts
(Instant AP) (Captive Portal)# redirect-url example1.com
(Instant AP) (Captive Portal)# terms-of-use "This network is not secure, and use is at your own risk"
(Instant AP) (Captive Portal)# use-policy "Please read terms and conditions before using Guest Network"
(Instant AP) (Captive Portal)# end
(Instant AP)# commit apply
```


Command History

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>
  prevent-frame-overlay
  redirect-url <redirection-url>
  server <server-name>
  server-fail-through
  switch-ip
  server-offload
  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.	—	—
https	Enables HTTPS for client connections.	—	—
Port <port>	Configures the port to use for communication with the external captive portal server.	—	80
prevent-frame-overlay	Prevents overlay of frames. when configured, a frame displays a page only if it is in the same domain as the main page.	—	—
redirect-url <redirection-url>	Configures a URL to redirect the users after a successful authentication. NOTE: By default, after entering the requested info at the splash page, the users are redirected to the URL that was originally requested. When a URL is	—	—

Command/Parameter	Description	Range	Default
	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.	—	—
server-fail-through	Allows the guest clients to access the Internet when the external captive portal server is not available.	—	Disabled
switch-ip	Sends the IP address of the VC in the redirection URL when external captive portal servers are used.	—	Disabled
server-offload	Enables the server-offload feature to reduce the load on the external captive portal server by allowing the IAP to use a Meta tag to redirect HTTP and HTTPS requests from the client. When enabled, this feature prevents the non-browser client applications from following unnecessary 302-redirects generated by their background HTTP or HTTPS requests.	—	—
url <url>	Configures the URL of the external captive portal server.	—	—
no...	Removes the 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 AP) (config) # wlan external-captive-portal AuthText1
(Instant AP) (External Captive Portal "AuthText1") # auth-text authenticated
(Instant AP) (External Captive Portal "AuthText1") # port 80
(Instant AP) (External Captive Portal "AuthText1") # redirect-url http://www.example1.com
(Instant AP) (External Captive Portal "AuthText1") # server CPServer1
(Instant AP) (External Captive Portal "AuthText1") # url "/aruba.php"
(Instant AP) (External Captive Portal "AuthText1") # server-fail-through
(Instant AP) (External Captive Portal "AuthText1") # switch-ip
(Instant AP) (External Captive Portal "AuthText1") # no auto-whitelist-disable
(Instant AP) (External Captive Portal "AuthText1") # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.5.1.0-4.3.1.0	The switch-ip parameter was introduced.
Aruba Instant 6.5.1.0-4.3.1.0 6.4.3.1-4.2	The prevent-frame-overlay and server-offload parameters were added.
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>
  deadtime <time>
  filter <filter>
  key-attribute <key-attribute>
  ip <IP-address>
  port <port-name>
  timeout <seconds>
  retry-count <count>
no...
```

Description

This command configures a Lightweight Directory Access Protocol (LDAP) server for user authentication on the VC.

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.	—	—
deadtime <time>	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 minutes	5

Command/Parameter	Description	Range	Default
filter <filter>	Configures the filter to apply when searching for a user in the LDAP database.	strings	(objectclass=*)
key-attribute <key-attribute>	Configures the attribute to use as a key when searching for the LDAP server. For Active Directory, the value is sAMAccountName	—	—
ip <IP-address>	Configures the IP address of the LDAP server.	—	—
port <port>	Configures the authorization port number of the LDAP server.	—	389
timeout <seconds>	Configures a timeout value for LDAP requests from the clients	1-30 seconds	5
retry-count <count>	Defines the number of times that the clients can attempt to connect to the server.	1-5	3
no...	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 AP) (config)# wlan ldap-server Server1
(Instant AP) (LDAP Server <name>)# ip 192.0.1.5
(Instant AP) (LDAP Server <name>)# port 389
(Instant AP) (LDAP Server <name>)# admin-dn cn=admin
(Instant AP) (LDAP Server <name>)# admin-password password123
(Instant AP) (LDAP Server <name>)# base-dn dc=example, dc=com
(Instant AP) (LDAP Server <name>)# filter (objectclass=*)
(Instant AP) (LDAP Server <name>)# key-attribute sAMAccountName
(Instant AP) (LDAP Server <name>)# timeout 5
(Instant AP) (LDAP Server <name>)# retry-count 3
(Instant AP) (LDAP Server <name>)# end
(Instant AP)# commit apply
```

Command History

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 <ssid_profile>
  a-basic-rates <rate>
  a-max-tx-rate <rate>
  a-min-tx-rate <rate>
  a-tx-rates <rate>
  accounting-server <name>
  air-time-limit <limit>
  auth-pkt-mac-format {delimiter|upper-case}
  auth-req-thresh <threshold>
  auth-server <name>
  auth-survivability
  bandwidth-limit <limit>
  blacklist
  broadcast-filter {All|ARP|Unicast-ARP-Only|Disabled}
  called-station-id {type{ap-group|ap-name|ipaddr|macaddr|clan-id} |include-ssid [delimiter]}
  captive-portal {<type> [exclude-uplink <types>] | external [Profile <name>] [exclude-uplink
<types>]}
  captive-portal-proxy-server <ip> <port>
  content-filtering
  deny-inter-user-bridging
  deny-local-routing
  disable
  dmo-channel-utilization-threshold <threshold>
  dot11k
  dot11r
  dot11v
  dot1x-timer-idrequest-period
  dot1x-wpa-key-period
  dot1x-wpa-key-retries
  dtim-period <value>
  dynamic-multicast-optimization
  enable
  enforce-dhcp
  essid <ssid>
  explicit-ageout-client
  external-server
  g-basic-rates
  g-min-tx-rate <rate>
  g-max-tx-rate <rate>
  g-tx-rates
  hide-ssid
  hotspot-profile <name>
  inactivity-timeout <interval>
  index <idx>
  key-duration <duration>
  l2-auth-failthrough
  leap-use-session-key
  local-probe-req-thresh <threshold>
  mac-authentication
  mac-authentication-delimiter <delim>
  mac-authentication-upper-case
  max-authentication-failures <limit>
  max-clients-threshold <Max_clients>
  max-retries
  mfp-capable
  mfp-required
  multicast-rate <rate>
  multicast-rate-optimization
  mpdu-agg-disable
  okc
```



```

okc-disable
opmode <opmode>
out-of-service <def> <name>
per-user-bandwidth-limit <limit>
radius-accounting
radius-accounting-mode {user-association|user-authentication}
radius-interim-accounting-interval <minutes>
radius-reauth-interval <minutes>
rf-band <band>
rrm-quiet-ie
server-load-balancing
set-role <attribute> {{contains|ends-with|equals|matches-regular-expression|not-
equals|starts-with} <operand> <role>|value-of}
set-role-by-ssid
set-role-mac-auth <mac_only>
set-role-machine-auth {<machine_only>|<user_only>}
set-role-pre-auth <role>
set-role-unrestricted
set-vlan <attribute> {{contains|ends-with|equals|matches-regular-expression|not-
equals|starts-with} <operand> <vlan>|value-of}
short-preamble-disable
strict-svp
supported-mcs-set
temporal-diversity
termination
time-range <name> {enable| disable}
tspec
tspec-bandwidth
type {employee|voice|guest}
use-ip-for-calling-station
utf8
very-high-throughput-disable
vht-supported-mcs-map
vht-txbf-explicit-enable
vlan <vlan>
wep-key <wep-key>
wispr
wmm-background-dscp <dscp>
wmm-background-share <share>
wmm-best-effort-dscp <dscp>
wmm-best-effort-share <share>
wmm-uapsd-disable
wmm-video-dscp <dscp>
wmm-video-share <share>
wmm-voice-dscp <dscp>
wmm-voice-share <share>
work-without-uplink
wpa-passphrase <wpa-passphrase>
zone <zone>
no...

```

Description

This command configures a WLAN SSID profile.

Syntax

Command/Parameter	Description	Range	Default
wlan ssid-profile <ssid_profile>	Creates a WLAN SSID profile.	—	—
a-basic-rates	Allows you to define a set of modulation rates to use for the clients on the 5 GHz radio band.	6,9,12,18,24,36,48,54 in Mbps	6, 12, 24
a-max-tx-rate <rate>	Configures the specify the maximum transmission rate for the 5 GHz band.	6,9,12,18,24,36,48,54 in Mbps	54
a-min-tx-rate <rate>	Configures the specify the minimum transmission rate for the 5 GHz band.	6,9,12,18,24,36,48,54 in Mbps	6
a-tx-rate <rate>	Allows you to configure specific transmission rate at which IAP can transmit data to the clients connected on 5 GHz band.	6,9,12,18,24,36,48,54 in Mbps	All
accounting-server <name>	This command configures a server for accounting purpose.	—	—
air-time-limit <limit>	Configures an aggregate amount of airtime that all clients using this SSID can use for sending and receiving data.	—	—
auth-pkt-mac-format {delimiter upper-case}	Configures a delimiter and upper-case characters in a MAC Address string of authentication packet or the username and password of the client. The delimiter and upper-case parameters in this command are available for all authentication methods. And without the mac-authentication-delimiter and mac-authentication-upper-case configuration, it works on the username and password for MAC Authentication.	—	—
auth-req-thresh	Allows you to set a threshold for authentication requests for the SSID profile.	—	—
auth-server <name>	Configures an authentication server for the SSID users.	—	—
auth-survivability	Enables the authentication survivability feature.	—	—

Command/Parameter	Description	Range	Default
	NOTE: The authentication survivability feature requires ClearPass Policy Manager 6.0.2 or later, and is applicable only when external servers such as RADIUS are configured for the SSID. When enabled, Instant authenticates the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily lost. The Authentication survivability feature is not applicable when a RADIUS server is configured as an internal server.		
bandwidth-limit <limit>	Configures an aggregate amount of bandwidth that each radio is allowed to provide for the connected clients.	1—65535	—
blacklist	Enables dynamic blacklisting of clients.	—	—
broadcast-filter {All ARP Unicast-ARP-Only Disabled}	Configures broadcast filtering parameters: You can configure any of the following filtering parameters: • All — When set to All, the IAP drops all broadcast and multicast frames except DHCP, ARP, igmp-group queries, and IPv6 neighbor discovery protocol. • ARP — When set to ARP, the IAP drops all broadcast and multicast frames except ARP, DHCP, igmp-group queries, IPv6 neighbor discovery protocol, and additionally converts ARP frames to unicast. • Unicast-ARP-Only — When set to Unicast-ARP-Only, the IAP allows all broadcast and multicast frames as it is, however the ARP requests are converted to unicast frames and sends them to the associated clients. • Disabled — When set to Disabled, the IAP routes all the broadcast and multicast frames to the wireless interfaces.	All, ARP, Unicast-ARP-Only, Disabled	ARP

Command/Parameter	Description	Range	Default
called-station-id {type{ap-group ap-name ipaddr macaddr vlan-id} include-ssid [delimiter]}	Configures the following called-station-id types: • ap-group — The VC name is used as the called-station-id. • ap-name — The IAP hostname is used as the called-station-id. • vlan-id — The VLAN ID of the client is used as the called-station-id. • ipaddr — The IP address of the IAP is used as the called-station-id. • macaddr — The MAC address of the IAP is used as the calling-station-id. • include-ssid {delimiter <delimiter>} — The SSID is appended to the original called-station-id. You can optionally set a delimiter at the end.		called-station-id {type <macaddr>}
captive-portal {<type>[exclude-uplink <types>] external[exclude-uplink <types>] profile <name> [exclude-uplink <types>]]}	Configures captive portal authentication for the SSID. If the external captive profiles are created, you can specify the profile name by using the external and profile keywords and associated parameters.	—	—
	You can also exclude an uplink type for the captive portal based SSID profiles. When an uplink type is selected for the exclude-uplink option, redirection to the captive portal based on the type of specified uplink is disabled.	3G,4G, wifi,ethernet	—
captive-portal-proxy-server <ip> <port>	Allows you to specify an IP address and port number that match the proxy configuration of your browser.	—	—
content-filtering	Routes all DNS requests for the non-corporate domains to OpenDNS on this network.	—	Disabled

Command/Parameter	Description	Range	Default
deny-inter-user-bridging	Disables the bridging traffic between two clients connected to the same SSID on the same VLAN. When inter-user bridging is disabled, the clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.	—	—
deny-local-routing	Disables the routing traffic between two clients connected to the same SSID on different VLANs. When local routing is disabled, the clients can connect to the Internet, but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision.	—	—
disable	Disables the SSID. By default all SSIDs are enabled.	—	—
dmo-channel-utilization-threshold <threshold>	Sets a threshold for DMO channel utilization. IAP sends multicast traffic over the wireless link.	1–100 percentage value	90
dot11k	Enables 802.11k roaming on the SSID profile. The 802.11k protocol enables IAPs and clients to dynamically measure the available radio resources. When 802.11k is enabled, IAPs and clients send neighbor reports, beacon reports, and link measurement reports to each other.	—	—
dot11r	Enables 802.11r on the SSID profile. 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.	—	—

Command/Parameter	Description	Range	Default
	Fast BSS Transition is operational only if the wireless client supports 802.11r standard. If the client does support 802.11r standard, it falls back to normal WPA-2 authentication method.		
dot11v	Enables 802.11v based BSS transition.	—	—
dtim-period <value>	Configures the Delivery Traffic Indication Message (DTIM) interval for the SSID profile. The DTIM interval determines how often the IAP should deliver the buffered broadcast and multicast frames to associated clients in the powersaving mode. 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.	1–10 beacons	1
dynamic-multicast-optimization	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. NOTE: When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.	—	Disabled
enable	Re-enables the deactivated SSIDs.	—	Enabled
enforce-dhcp	Blocks IAP traffic to the clients that do obtain IP address from DHCP.	—	Disabled
essid <ssid>	Defines a name that uniquely identifies a wireless network.	—	—
external-server	Configures an external RADIUS server for authentication.	—	—

Command/Parameter	Description	Range	Default
<code>explicit-ageout-client</code>	Allows the IAP to send a deauthentication frame to the client and clear client entry.	—	Disabled
<code>g-basic-rates</code>	Allows you to define a set of modulation rates to use for the clients on the 2.4 GHz radio band.	1,2,5,6,9,11,12,18,24,36,48,54 in Mbps	1, 2
<code>g-min-tx-rate <rate></code>	Configures the specify the minimum transmission rate for the 2.4 GHz band.	1,2,5,6,9,11,12,18,24,36,48,54 in Mbps	1
<code>g-max-tx-rate <rate></code>	Configures the specify the maximum transmission rate for the 2.4 GHz band.	1,2,5,6,9,11,12,18,24,36,48,54 in Mbps	54
<code>g-tx-rates</code>	Allows you to configure specific transmission rate at which the IAP can transmit data to the clients connected on 2.4 GHz band.	1,2,5,6,9,11,12,18,24,36,48,54	All
<code>hide-ssid</code>	Hides the SSID. When enabled, the SSID will not be visible for the users.	—	Disabled
<code>hotspot-profile <name></code>	Associates a hotspot profile with the WLAN SSID profile.	—	—
<code>inactivity-timeout <interval></code>	Configures a timeout value for the inactive client sessions. When a client session is inactive for the specified duration, the session expires and the clients are required to log in again.	60-86400 seconds	1000
<code>index <idx></code>	Assigns an index value for the SSID.	—	—
<code>12-auth-failthrough</code>	Allows the clients to use 802.1X authentication when MAC authentication fails.	—	Disabled
<code>leap-use-session-key</code>	Allows the users to derive session keys for Lightweight Extensible Authentication Protocol (LEAP) authentication. Configure this command for old printers that use dynamic WEP and if you do not want use a session key from the RADIUS Server to derive pair wise	—	Disabled

Command/Parameter	Description	Range	Default
	unicast keys.		
<code>local-probe-req-thresh <threshold></code>	Configures a Received signal strength indication (RSSI) threshold value to limit the number of incoming probe requests. When enabled, this command controls the system response to the broadcast probe requests sent by clients to search for the available SSIDs and ignores the probe request if required,	0-100 dB	—
<code>mac-authentication</code>	Enables MAC authentication for clients that use this SSID profile.	—	Disabled
<code>mac-authentication-delimiter <delim></code>	Allows you to set a delimiter that can be used in the MAC address string for MAC authentication. You can specify colon or dash for delimiter. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. If you specify colon for the delimiter, the MAC addresses in the xx:xx:xx:xx:xx:xx format are used.	colon or dash	—
<code>mac-authentication-upper-case</code>	Enables the IAP to use uppercase letters in MAC address string for MAC authentication.	—	—
<code>max-authentication-failures <limit></code>	Configures the maximum number of authentication failures to dynamically blacklist the users. The users who exceed the number of authentication failures configured through this command are dynamically blacklisted.	—	—
<code>max-retries</code>	Denotes the maximum number of retries the IAP attempts when the client is not responding to the 802.11 frames.	1-128	8
<code>mfp-capable</code>	When enabled, the SSID supports management frame protection (MFP) capable clients and non-MFP clients.	—	Disabled

Command/Parameter	Description	Range	Default																																																																																
mfp-required	When enabled, the SSID supports only the clients that exhibit the MFP functionality	—	Disabled																																																																																
multicast-rate <rate>	Increases the video transmission rate of the IAP. The IAPs can select the rate for video multicast frames. Ensure that you tag the multicast traffic with video priority. You can configure Modulation Coding Scheme (MCS) rates as well. MCS is an important setting because it provides a greater throughput. The following information displays the MCS rate of the IAP: <table> <tr> <th>MCS</th><th>Streams</th><th>20 MHz</th><th>20 MHz</th></tr> <tr> <th>SGI</th><th></th><th></th><th></th></tr> <tr> <td>---</td><td>-----</td><td>-----</td><td>-----</td></tr> <tr> <td>----</td><td></td><td></td><td></td></tr> <tr> <td>0</td><td>1</td><td>6.5</td><td>7.2</td></tr> <tr> <td>1</td><td>1</td><td>13.0</td><td>14.4</td></tr> <tr> <td>2</td><td>1</td><td>19.5</td><td>21.7</td></tr> <tr> <td>3</td><td>1</td><td>26.0</td><td>28.9</td></tr> <tr> <td>4</td><td>1</td><td>39.0</td><td>43.3</td></tr> <tr> <td>5</td><td>1</td><td>52.0</td><td>57.8</td></tr> <tr> <td>6</td><td>1</td><td>58.5</td><td>65.0</td></tr> <tr> <td>7</td><td>1</td><td>65.0</td><td>72.2</td></tr> <tr> <td>8</td><td>2</td><td>13.0</td><td>14.4</td></tr> <tr> <td>9</td><td>2</td><td>26.0</td><td>28.9</td></tr> <tr> <td>10</td><td>2</td><td>39.0</td><td>43.3</td></tr> <tr> <td>11</td><td>2</td><td>52.0</td><td>57.8</td></tr> <tr> <td>12</td><td>2</td><td>78.0</td><td>86.7</td></tr> <tr> <td>13</td><td>2</td><td>104.0</td><td>115.6</td></tr> <tr> <td>14</td><td>2</td><td>117.0</td><td>130.0</td></tr> <tr> <td>15</td><td>2</td><td>130.0</td><td>144.4</td></tr> </table> The MCS rates for video multicast are supported in all the 802.11n-capable IAPs, and in the IAP-2xx access points which are 802.11ac-capable. NOTE: This parameter is not supported on IAP-300 series access points.	MCS	Streams	20 MHz	20 MHz	SGI				---	-----	-----	-----	----				0	1	6.5	7.2	1	1	13.0	14.4	2	1	19.5	21.7	3	1	26.0	28.9	4	1	39.0	43.3	5	1	52.0	57.8	6	1	58.5	65.0	7	1	65.0	72.2	8	2	13.0	14.4	9	2	26.0	28.9	10	2	39.0	43.3	11	2	52.0	57.8	12	2	78.0	86.7	13	2	104.0	115.6	14	2	117.0	130.0	15	2	130.0	144.4	default, 6, 9, 12, 18, 24, 36, 48, 54 Mbps mcs0-mcs15	default
MCS	Streams	20 MHz	20 MHz																																																																																
SGI																																																																																			
---	-----	-----	-----																																																																																

0	1	6.5	7.2																																																																																
1	1	13.0	14.4																																																																																
2	1	19.5	21.7																																																																																
3	1	26.0	28.9																																																																																
4	1	39.0	43.3																																																																																
5	1	52.0	57.8																																																																																
6	1	58.5	65.0																																																																																
7	1	65.0	72.2																																																																																
8	2	13.0	14.4																																																																																
9	2	26.0	28.9																																																																																
10	2	39.0	43.3																																																																																
11	2	52.0	57.8																																																																																
12	2	78.0	86.7																																																																																
13	2	104.0	115.6																																																																																
14	2	117.0	130.0																																																																																
15	2	130.0	144.4																																																																																
multicast-rate-optimization	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.	—	Disabled																																																																																

Command/Parameter	Description	Range	Default
	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.		
<code>mpdu-agg-disable</code>	Disables MAC Protocol Data Unit (MPDU) aggregation.	—	—
<code>okc</code>	Enables opportunistic key caching (OKC).	—	—
<code>okc-disable</code>	Disables opportunistic key caching (OKC). In the OKC based roaming, the IAP 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. NOTE: 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 WPA-2-AES Enterprise network only.	—	—
<code>opmode <opmode></code>	Configures the layer-2 authentication and encryption for this SSID to protect access and ensure the privacy of the data transmitted to and from the network. You can configure any of the following types of encryption: • opensystem—No authentication and encryption. • wpa2-aes—WPA-2 with AES encryption and dynamic keys using 802.1X. • wpa2-psk-aes—WPA-2 with AES encryption using a preshared key. • wpa-tkip—WPA with TKIP encryption and dynamic keys using 802.1X. • wpa-psk-tkip—WPA with TKIP encryption using a pre-shared key.	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
	- wpa-tkip, wpa2-aes—WPA with TKIP and WPA-2 with AES encryption. - wpa-psk-tkip,wpa2-psk-aes - WPS with TKIP and WPA-2 with AES encryption using a pre-shared key. - static-wep—WEP with static keys. - dynamic-wep—WEP with dynamic keys.		
out-of-service <def> <name>	Enables or disables the SSID based on any of the out of service states of the IAP: - VPN down - Uplink down - Internet down - Primary uplink down The network will be out of service when selected event occurs and the SSID is enabled or disabled as per the configuration settings applied. For example, if you select the VPN down option from the dropdown and set the status to enabled, the SSID is enabled when the VPN connection is down and is disabled when the VPN connection is restored.	For out-of-service states,any of the following valies is allowed: vpn-down uplink-down internet-down primary-uplink-down For SSID status, select enable or disable.	—
per-user-bandwidth-limit <limit>	Configures a bandwidth limit in Kbps for the SSID users. NOTE: The bandwidth contracts can also be applied per SSID user.	1—65535 Kbps	—
radius-accounting	Enables accounting for the RADIUS server authentication. When enabled, the IAPs post accounting information to the Radius server at the specified accounting interval.	—	—
radius-accounting-mode {user-association user-authentication}	Configures an accounting mode for the captive portal users. You can configure any of the following modes for accounting: user-authentication—when configured, the accounting starts	—	user-authentication

Command/Parameter	Description	Range	Default
	only after client authentication is successful and stops when the client logs out of the network. • user-association—When configured, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.		
radius-interim-accounting-interval <minutes>	Configures an interval for posting accounting information as RADIUS INTERIM accounting records to the RADIUS server. When configured, the IAP sends interim-update messages with current user statistics to the RADIUS server at regular intervals.	0–60	—
radius-reauth-interval <minutes>	Allows you to configure an interval after which the IAPs can redo the RADIUS transaction to reauthenticate clients. If the reauthentication interval is configured: • On an SSID performing L2 authentication (MAC or 802.1X authentication): When reauthentication fails, the clients are disconnected. If the SSID is performing only MAC authentication and has a pre-authentication role assigned to the client, the client will get a post-authentication role only after a successful reauthentication. If reauthentication fails, the client retains the pre-authentication role. • On an SSID performing both L2 and L3 authentication (MAC with captive portal authentication): When reauthentication succeeds, the client retains the role that is already assigned. If reauthentication fails, a pre-authentication role is assigned to the client. • On an SSID performing only L3	Any integer value in minutes	—

Command/Parameter	Description	Range	Default
	authentication (captive portal authentication): When reauthentication succeeds, a pre-authentication role is assigned to the client that is in a post-authentication role. Due to this, the clients are required to go through captive portal to regain access.		
rf-band <band>	Configures the radio frequency band on which this SSID will be broadcast. You can select either 2.4GHz, 5 GHz, or all to specify both bands.	2.4 GHz, 5 GHz, all	
rts-threshold <threshold>	Configures a threshold to trigger the RTS/CTS handshake. The RTS (Request to Send)/CTS (Clear to Send) mechanism allows devices to reserve the RF medium and minimizes frame collisions introduced by the hidden stations. When RTS is enabled, a higher number of retransmissions occurring on the WLAN trigger the RTS/CTS handshake and the transmitter station sends an RTS frame to the receiver station. The receiver station responds with a CTS frame. Typically, the RTS/CTS frames are not sent, unless the packet size exceeds the RTS threshold. By default, the RTS threshold is set to 2333 octets. When the size of the packets sent by the transmitter exceeds the configured threshold, RTS frames are sent.	0-2347	2333
server-load-balancing	Enables load balancing across two RADIUS servers if two authentication servers are configured for the SSID.	—	Enabled
set-role {contains ends-with equals matches- regular-expression not-equals starts- with} <operand> <role> value-of}	Assigns a user role to the clients. The first rule that matches the configured condition is applied. You can set any of the following conditions: contains—The rule is applied only if the attribute value contains the specified string.	—	—

Command/Parameter	Description	Range	Default
	- ends-with—The rule is applied only if the attribute value ends with the specified string. - equals—The rule is applied only if the attribute value is equal to the specified string. - not-equals—The rule is applied only if the attribute value is not equal to the specified string. - starts-with—The rule is applied only if the attribute value begins with the specified string. - value-of - This rule sets the user role to the value of the attribute returned. To set a user role, the value of the attribute must already be configured on the IAP. - 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 mac-address-and-dhcp-options attribute is selected in the Attribute drop-down.		
set-role-by-ssid	Configures a user role based on the type of SSID configured.	—	—
set-role-mac-auth <mac-only>	Configures a MAC authentication based user role.	—	—
set-role-machine-auth <machine_only> <user_only>	Configures a machine authentication rule. You can assign different rights to clients based on whether their hardware device supports machine authentication. Machine authentication is only supported on Windows devices, so this can be used to distinguish between Windows devices and other devices such as iPads.	—	—
set-role-pre-auth <role>	Configures a pre-authentication role to allow some access to the guest users before the client authentication.	—	—

Command/Parameter	Description	Range	Default
set-role-unrestricted	Configures unrestricted access control.	—	—
set-vlan <attribute> {contains ends-with equals matches- regular-expression not-equals starts- with} <operand> <vlan> value-of}	Assigns a VLAN to the clients. The first rule that matches the configured condition is applied. You can specify any of the following conditions: - contains—The rule is applied only if the attribute value contains the specified string. - ends-with—The rule is applied only if the attribute value ends with the specified string. - equals—The rule is applied only if the attribute value is equal to the specified string. - not-equals—The rule is applied only if the attribute value is not equal to the specified string. - starts-with—The rule is applied only if the attribute value begins with the specified string. - value-of - This rule sets the VLAN to the value of the attribute returned. To set a user role, the value of the attribute must already be configured on the IAP. - 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 mac-address-and-dhcp-options attribute is selected in the Attribute drop-down.	—	—
short-preamble-disable	Disables the transmission and reception of short preamble frames for the clients connected to an SSID. By default, short preamble is enabled.	—	—
strict-svp	Enables Strict Spectralink Voice Protocol (SVP) and prioritizes voice traffic for SVP handsets.	—	—

Command/Parameter	Description	Range	Default
<code>supported-mcs-set</code>	Allows you to define a set of Modulation and Coding Scheme (MCS) rates for High Throughput (HT) channels.	0-23	0-23
<code>temporal-diversity</code>	Shows if the temporal diversity feature has been enabled or disabled. When this feature is enabled and the client is not responding to 802.11 packets, the IAP attempts two hardware retries. If the hardware retries are not successful, it attempts software retries. When this feature is disabled, the IAP attempts only hardware retries.	enable, disable	disable
<code>tspec</code>	Allows the IAPs to prioritize time-sensitive traffic such as voice traffic initiated by the client.	—	—
<code>tspec-bandwidth</code>	Reserves the configured bandwidth for prioritizing voice traffic when traffic specification (TSPEC) is enabled.	200–600000 Kbps	2000 Kbps
<code>termination</code>	Configures the EAP portion of 802.1X authentication on the IAP, instead of the RADIUS server. When enabled, this command reduces network traffic to the external RADIUS server by terminating the authorization protocol on the 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.	—	Disabled
<code>time-range <name> {enable disable}</code>	Specify the time range profile name to apply. When a time range profile is enabled on SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00 to 13:00, the SSID becomes	—	—

Command/Parameter	Description	Range	Default
	available only between 12 PM to 1 PM on a given day. If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if configured time-range is 14:00 to 17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.		
type {employee voice guest}	Configures the type of network such as employee, voice, guest network.	—	—
use-ip-for-calling-station	The IP address of the client will be used as the calling-station-id.	—	—
utf8	Encodes the SSID. When enabled, the SSID name is displayed in the UTF-8 format. SSIDs are not encoded by default.	—	—
very-high-throughput-disable	Disables very high throughput (VHT) for clients connecting the WLAN SSID profile.	—	—
vht-mu-txbf-disable	Disables MU-MIMO. The MU-MIMO feature allows the 802.11ac Wave 2 IAPs to send multiple frames to multiple clients simultaneously over the same frequency spectrum. With MU-MIMO, APs can support simultaneous directional Radio Frequency (RF) links and up to four simultaneous full-rate Wi-Fi connections (For example, smart phone, tablet, laptop, multimedia player or other client device). The MU-MIMO feature is enabled by default on WLAN SSIDs.	—	—
vht-supported-mcs-map	Allows you to define a combination of VHT MCS and spatial streams as a VHT MCS rate set.	0-7 0-8 0-9	0-9 for each spatial stream
vht-txbf-explicit-disable	Disables VHT TX beamforming on the IAP-2xx Series access points. This feature is available only on the IAP-2xx Series devices.		

Command/Parameter	Description	Range	Default
<code>vlan <vlan></code>	Allows the administrators to assign a VLAN to the SSID users.	1–4095	—
<code>wep-key <wep-key></code>	Static WEP key associated with the key index. The WEP key values can be 10 or 26 hexadecimal characters in length.	—	—
<code>wispr</code>	Enables WISPr authentication for the SSID profile.	—	—
<code>wmm-background-dscp <dscp></code>	Allows you to specify the DSCP mapping value for the background traffic.	0—63	—
<code>wmm-background-share <share></code>	Allocates bandwidth for background traffic such as file downloads or print jobs.	—	—
<code>wmm-best-effort-dscp <dscp></code>	Allows you to specify the DSCP mapping value for the best effort traffic.	0—63	—
<code>wmm-best-effort-share <share></code>	Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS.	—	—
<code>wmm-uapsd-disable</code>	Disables Unscheduled Automatic Power Save Delivery (UAPSD) on all WMM access categories (ACs). By default, UAPSD or WMM power save is enabled.	—	—
<code>wmm-video-dscp <dscp></code>	Allows you to specify the DSCP mapping value for the video traffic.	0—63	—
<code>wmm-video-share <share></code>	Allocates bandwidth for video traffic generated from video streaming.	—	—
<code>wmm-voice-dscp <dscp></code>	Allows you to specify the DSCP mapping value for the voice traffic.	0—63	—
<code>wmm-voice-share <share></code>	Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication.	—	—
<code>work-without-uplink</code>	Allows the SSID to be used without an uplink connection.	—	—

Command/Parameter	Description	Range	Default
	NOTE: In Instant 6.4.4.4-4.2.3 release, the work-without-uplink is not operational. To configure SSID availability based on the uplink connection status, use the out-of-service parameter.		
wpa-passphrase <passphrase>	Defines a WPA passphrase with which you can generate a pre-shared key (PSK).	—	—
zone <zone>	Allows you to specify a zone for SSID. If an SSID belongs to a zone, it is not broadcast on any IAP which does not belong to the zone.		

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 AP) (config)# wlan ssid-profile employee1
(Instant AP) (SSID Profile "employee1")# type employee
(Instant AP) (SSID Profile "employee1")# essid employee1
(Instant AP) (SSID Profile "employee1")# enable
(Instant AP) (SSID Profile "employee1")# vlan 1
(Instant AP) (SSID Profile "employee1")# wpa-passphrase user@123
(Instant AP) (SSID Profile "employee1")# opmode wpa2-psk-aes
(Instant AP) (SSID Profile "employee1")# max-authentication-failures 0
(Instant AP) (SSID Profile "employee1")# mac-authentication
(Instant AP) (SSID Profile "employee1")# l2-auth-failthrough
(Instant AP) (SSID Profile "employee1")# termination
(Instant AP) (SSID Profile "employee1")# blacklist
(Instant AP) (SSID Profile "employee1")# mac-authentication
(Instant AP) (SSID Profile "employee1")# auth-server InternalServer
(Instant AP) (SSID Profile "employee1")# rf-band all
(Instant AP) (SSID Profile "employee1")# dtim-period 1
(Instant AP) (SSID Profile "employee1")# inactivity-timeout 1000
(Instant AP) (SSID Profile "employee1")# broadcast-filter none
(Instant AP) (SSID Profile "employee1")# use-ip-for-calling-station
(Instant AP) (SSID Profile "employee1")# dmo-channel-utilization-threshold 90
(Instant AP) (SSID Profile "employee1")# local-probe-req-thresh 0
(Instant AP) (SSID Profile "employee1")# max-clients-threshold 64
(Instant AP) (SSID Profile "employee1")# set-role Group-Name contains wireless employee
(Instant AP) (SSID Profile "employee1")# set-vlan mac-address-and-dhcp-options matches-regular-expression ..link 200
(Instant AP) (SSID Profile "employee1")# no wmm-background-dscp
(Instant AP) (SSID Profile "employee1")# wmm-best-effort-dscp 21
(Instant AP) (SSID Profile "employee1")# no wmm-video-dscp
(Instant AP) (SSID Profile "employee1")# wmm-voice-dscp 46,44,42,41
(Instant AP) (SSID Profile "employee1")# zone Zone1
(Instant AP) (SSID Profile "employee1")# end
(Instant AP)# commit apply
```

The following example configures a guest WLAN SSID profile:

```
(Instant AP) (config)# wlan ssid-profile guestNetwork
(Instant AP) (SSID Profile "guestNetwork")# type guest
(Instant AP) (SSID Profile "guestNetwork")# essid guestNetwork
(Instant AP) (SSID Profile "guestNetwork")# enable
(Instant AP) (SSID Profile "guestNetwork")# opmode opensystem
(Instant AP) (SSID Profile "guestNetwork")# rf-band all
(Instant AP) (SSID Profile "guestNetwork")# dtim-period 1
(Instant AP) (SSID Profile "guestNetwork")# g-min-tx-rate 1
(Instant AP) (SSID Profile "guestNetwork")# g-max-tx-rate 54
(Instant AP) (SSID Profile "guestNetwork")# a-min-tx-rate 6
(Instant AP) (SSID Profile "guestNetwork")# a-max-tx-rate 54
(Instant AP) (SSID Profile "guestNetwork")# inactivity-timeout 1000
(Instant AP) (SSID Profile "guestNetwork")# vlan 1
(Instant AP) (SSID Profile "guestNetwork")# dmo-channel-utilization-threshold 90
(Instant AP) (SSID Profile "guestNetwork")# max-clients-threshold 64
(Instant AP) (SSID Profile "guestNetwork")# local-probe-req-thresh 0
(Instant AP) (SSID Profile "guestNetwork")# blacklist
(Instant AP) (SSID Profile "guestNetwork")# max-authentication-failures 3
(Instant AP) (SSID Profile "guestNetwork")# radius-interim-accounting-interval 10
(Instant AP) (SSID Profile "guestNetwork")# radius-reauth-interval 30
(Instant AP) (SSID Profile "guestNetwork")# captive-portal external
(Instant AP) (SSID Profile "guestNetwork")# mac-authentication
(Instant AP) (SSID Profile "guestNetwork")# auth-server server1
(Instant AP) (SSID Profile "guestNetwork")# set-role-by-ssid
(Instant AP) (SSID Profile "guestNetwork")# set-role-pre-auth test1
(Instant AP) (SSID Profile "guestNetwork")# end
(Instant AP)# commit apply
```

Command History

Version	Description
Aruba Instant 6.5.0.0-4.3.0.0	The following parameters are added: • multicast-rate • use-ip-for-calling-station • called-station-id • broadcast-filtering <unicast-arp-only> • max-retries • temporal-diversity • mfp-capable • mfp-required
Aruba Instant 6.4.4.4-4.2.3.0	The out-of-service parameter is added.
Aruba Instant 6.4.3.4-4.2.1.0	The time-range parameter is added.
Aruba Instant 6.4.3.1-4.2	The following parameters are added: • captive-portal-proxy-server <ip> <port> • explicit-ageout-client • mpdu-agg-disable • strict-svp

Version	Description
	• tspec • tspec-bandwidth • vht-txbf-explicit-enable
Aruba Instant 6.4.0.2-4.1.1	This command is modified.
Aruba Instant 6.4.0.2-4.1	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 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: • clear —To clear a cipher suite • wpa-tkip-psk —To use WPA with TKIP encryption along with Pre-shared key (PSK). • wpa2-ccmp-psk—To use WPA-2 with Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption mode with strong security.	—	—
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 AP) (config) # wlan sta-profile
(Instant AP) (sta uplink) # uplink-band dot11a
(Instant AP) (sta uplink) # uplink-band dot11a
(Instant AP) (sta uplink) # cipher-suite wpa-tkip-psk
(Instant AP) (sta uplink) # wpa-passphrase user@123
```

Command History

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 tacacs-server

```
wlan tacacs-server <profile-name>
    deadtime <minutes>
    ip <IP-address>
    key <key>
    no
    port <port>
    retry-count <number>
    session-authorization
    timeout <seconds>
    no...
no tacacs-server <profile-name>
```

Description

This command is used to configure a TACACS server for management users.

Syntax

Command/Parameter	Description	Default
wlan tacacs-server	Configures the TACACS server profile.	-
deadtime <minutes>	Configures an interval	
ip <IP-address>	Configures the IP address of the TACACS server.	-
port <port>	Configures the TCP port for the server	49
key	Configures a shared secret key to authenticate communication between the TACACS+ client and server.	-
timeout <seconds>	Configures a timeout value for TACACS+ requests from the management users	20
retry-count <number>	Configures the maximum number of authentication requests that are sent to the server	3
session-authorization	Enables session authorization for the admin users. By default, session authorization is disabled.	—
no...	Removes the specified configuration parameter.	—

Usage Guidelines

Use this command to configure a TACACS server as an external authentication server. This configuration applies only for management users in Instant and not for the other SSID or wired profiles.

Example

The following example configures the TACACS protocols:

```
(Instant AP) (config)# wlan tacacs-server Server1
(Instant AP) (TACACS Server < Server1>) # ip <10.17.121.54>
(Instant AP) (TACACS Server <Server1>) # port <49>
(Instant AP) (TACACS Server <Server1>) # key <pass123>
(Instant AP) (TACACS Server <Server1>) # timeout <30>
```



```
(Instant AP) (TACACS Server <Server1>) # retry-count <4>
(Instant AP) (TACACS Server <Server1>) # deadtime <30>
(Instant AP TACACS Server <Server1>) # end
(Instant AP) # commit apply
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	The deadtime and session authorization parameters were added.
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and TACACS server profile sub-mode.

wlan walled-garden

```
wlan walled-garden
    white-list <domain>
    black-list <domain>
    no...
no wlan walled-garden
```

Description

This command configures a walled garden 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, yahoo.com/* to provide access to various domains such as news.yahoo.com , travel.yahoo.com and finance.yahoo.com . Similarly, the www.apple.com/library/test is only allow a subset of www.apple.com site corresponding to path /library/test/* .	URLs, URLs with POSIX regular expression (regex(7))	—
black-list <domain>	Configures a blacklist to prevent the users from accessing the websites in a specific domain. You can specify the URLs for which the user access is denied. When a URL specified in blacklist is accessed by an unauthenticated user, IAP sends an HTTP 403 response to the client with a simple error message.	URLs	—
no...	Removes the configuration settings of the wlan walled-garden command parameters .	—	—
no wlan walled-garden	Deletes the walled garden 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 AP) (config)# wlan walled-garden
(Instant AP) (Walled Garden)# white-list <domain>
(Instant AP) (Walled Garden)# black-list <domain>
(Instant AP) (Walled Garden)# end
(Instant AP)# commit apply
```

Command History

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 and <http://www.itu.int>).

Example

The following commands configure a WISPr authentication profile:

```
(Instant AP) (config) # wlan wispr-profile
(Instant AP) (WISPr) # wispr-location-id-ac 408
(Instant AP) (WISPr) # wispr-location-id-cc 1
(Instant AP) (WISPr) # wispr-location-id-isocc US
(Instant AP) (WISPr) # wispr-location-id-network wispr
(Instant AP) (WISPr) # wispr-location-name-location airport
(Instant AP) (WISPr) # wispr-location-name-operator-name KNP
(Instant AP) (WISPr) # end
(Instant AP) # commit apply
```

Command History

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
<code>erase <all> <reboot></code>	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.
<code>memory</code>	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

xml-api-server

```
xml-api-server [<xml_api_server_profile>]
  ip <addr> [mask <mask>]
  key <key>
  no...
no xml-api-server [<xml_api_server_profile>]
```

Description

This command integrates an XML API interface to the IAP.

Syntax

Command/Parameter	Description
xml-api-server	Displays the sub-mode for configuring the XML API interface parameters.
<xml_api_server_profile>	Creates an XML API server profile.
ip <subnet> mask [<mask>]	Configures the subnet of the XML API server. You can optionally configure the subnet mask for the XML API server.
key <shared-key>	Configures the key required for accessing the XML API interface.
no...	Removes the parameter definition configured under the xml-api-server command.
no xml-api-server [<xml_api_server_profile>]	Removes the XML API configuration.

Usage Guidelines

Use this command to integrate an IAP with an external XML API interface.

Example

The following command configures the XML API Server details on an IAP:

```
(Instant AP) (config)# xml-api-server test-xml
(Instant AP) (xml-api-server "test-xml")# ip 12.0.132.61
(Instant AP) (xml-api-server "test-xml")# key123
(Instant AP) (xml-api-server "test-xml")# end
(Instant AP)# commit apply
```

Command History

Version	Description
Aruba Instant 6.4.3.1-4.2	This command is modified.
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

zonename

zonename <name>
no...

Description

This command configures a zone name for the IAP. You can configure zone settings on an IAP and the SSID profile, to assign an SSID to a specific IAP.

Syntax

Parameter	Description
zonename <name>	Configures zone on an IAP.
no...	Removes the configuration.

Usage Guidelines

Use this command to configure an IAP zone. To assign an SSID to a specific IAP, the IAP zone name must be configured on the WLAN SSID profile.

The following constraints apply to the IAP zone configuration:

- An IAP can belong to only one zone and only one zone can be configured on an SSID.
- If an SSID belongs to a zone, all IAPs in this zone can broadcast this SSID. If no IAP belongs to the zone configured on the SSID, the SSID is not broadcast.
- If an SSID does not belong to any zone, all IAPs can broadcast this SSID.

Example

The following example configures a zone name on an IAP:

```
(Instant AP) # zonename zoneA
```

Command History

Version	Description
Aruba Instant 6.4.0.2-4.1	This command is introduced.

Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

Glossary

The following table lists the terms and their definitions used in this document.

Table 12: *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.
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.

Table 12: *List of Terms*

Term	Definition
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 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.
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.

Table 12: *List of Terms*

Term	Definition
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: • Endspan— The switch that an AP is connected for power supply. • Midspan— A device can sit between the switch and APs 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.
TACACS	Family of protocols that handle remote authentication and related services for network access control through a centralized server.
TACACS+	Derived from TACACS but an entirely new and separate protocol to handle AAA services. TACACS+ uses TCP and is not compatible with TACACS. Because it encrypts password, username, authorization, and accounting, it is less vulnerable than RADIUS.
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.

Table 12: *List of Terms*

Term	Definition
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.
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.

Acronyms and Abbreviations

The following table lists the abbreviations used in this document.

Table 13: *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	Instant Access Point
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
LEAP	Lightweight Extensible Authentication Protocol
MX	Mail Exchanger
MAC	Media Access Control
NAS	Network Access Server
NAT	Network Address Translation

Table 13: *List of abbreviations*

Abbreviation	Expansion
NS	Name Server
NTP	Network Time Protocol
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 document.

Table 14: *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.

Table 14: *List of Terms*

Term	Definition
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.
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 track of computers connected to the network. This database helps in preventing any two computers from being configured with the same IP address.

Table 14: *List of Terms*

Term	Definition
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.
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: • Endspan— The switch that an AP is connected for power supply. • Midspan— A device can sit between the switch and APs

Table 14: *List of Terms*

Term	Definition
	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.
TACACS	Family of protocols that handle remote authentication and related services for network access control through a centralized server.
TACACS+	Derived from TACACS but an entirely new and separate protocol to handle AAA services. TACACS+ uses TCP and is not compatible with TACACS. Because it encrypts password, username, authorization, and accounting, it is less vulnerable than RADIUS.
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.
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.

Table 14: *List of Terms*

Term	Definition
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.