Dell PowerConnect ArubaOS 6.0 Command Line Interface

Reference Guide

Copyright

© 2010 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, and other registered marks are trademarks of Aruba Networks, Inc. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. Any other trademarks appearing in this manual are the property of their respective companies.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

The ArubaOS command line interface (CLI) allows you to configure and manage your controllers. The CLI is accessible from a local console connected to the serial port on the controllers or through a Telnet or Secure Shell (SSH) session from a remote management console or workstation.

Note: Telnet access is disabled by default on Dell controllers. To enable Telnet access, enter the telnet cli command from a serial connection or an SSH session, or in the WebUI navigate to the **Configuration > Management > General** page.

What's New In ArubaOS 6.0

The following commands have been added in the ArubaOS 6.0 Command Line Interface.

Command	Description
`aaa dns-query-period`	Configure how often the controller should generate a DNS request to cache the IP address for a RADIUS server identified via its fully qualified domain name (FQDN).
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
`ipv6 enable`	This command enables IPv6 packet processing globally. This option is disabled by default.
`local-userdb-remote-node`	This command adds a Remote Node to the Remote Node whitelist. You can also delete the whitelist entry using this command.
`remote-node-localip`	This command configures the switch-IP address and preshared key for the local Remote Node on a master Remote Node.
`remote-node-masterip`	This command configures the IP address and preshared key for the master Remote Node on a local Remote Node.
`remote-node-profile`	The remote-node-profile command lets you create a Remote Node profile. Once in Remote Node profile configuration mode, you can issue any of the following commands to define the values you want to assign to that profile.
`rf am-scan-profile`	Configure an Air Monitor (AM) scanning profile.
`rf spectrum-profile`	Define the spectrum band and device ageout times used by a spectrum monitor radio.
`show ap debug crash-info`	Show crash log information (if it exists) for an individual AP. The stored information is cleared from the flash after the AP reboots.
`show ap spectrum ap-list`	This command shows spectrum data seen by an access point that has been converted to a spectrum monitor.
`show ap spectrum channel-metrics`	This command shows channel quality, availability and utilization metrics as seen by a spectrum monitor.
`show ap spectrum channel-summary`	This command displays a summary of the 802.11a or 802.11g channels seen by a spectrum monitor.
`show ap spectrum client-list`	This command shows details for clients seen by a specified spectrum monitor.
`show ap spectrum debug monitors`	Show a detailed description of all spectrum monitors on the controller.

Command	Description
show ap spectrum debug fft	Save FFT (Fast Fourier Transform) power data to a file on the spectrum monitor.
show ap spectrum debug status	This command shows detailed status and statistics for a spectrum monitor.
show ap spectrum device-history	This command shows the history of the last 256 non-Wi-Fi devices.
show ap spectrum device-summary	This command shows the numbers of wi-fi and non-Wi-Fi device types on each channel monitored by a spectrum monitor.
show ap spectrum interference-power	This command shows the interference power detected by a 802.11a or 80211g radio on a spectrum monitor.
show ap spectrum monitors	This command shows a list of APs terminating on the controller that are currently configured as spectrum monitors.
show ap spectrum-load-balancing	Show spectrum load balancing information for an AP with this feature enabled.
show master-configpending	Displays the list of global commands which are not saved and are not sent to the local controller.
show remote-node	Shows configuration and other information about the remote node.
show remote-node-profile	The output of this command shows Remote Node profile configuration information.
show remote-node-dhcp-pool	The output of this command lists shows Remote Node DHCP pool summary information.
show voice configurations	Displays the details of the voice related configurations on your controller.
show voice logging	Displays the MAC address of the voice client that has logging enabled.
show voice real-time-analysis	Displays the call quality parameters based on the call quality analysis on the RTP media streams for voice calls.
show voice real-time-analysis-config	Displays the status of Real Time Call Quality Analysis configuration.
show voice sip	Displays the SIP settings on the controller.
show voice sip-midcall-req-timeout	Displays the status of the SIP mid-call request timeout configuration on the controller.
spanning-tree mode	Set the spanning tree mode to either Rapid Spanning Tree (802.1w) or PVST+ (Per VLAN Spanning Tree).
spanning-tree vlan (PVST+)	Configure PVST+ on a VLAN.
spanning-tree vlan range (PVST+)	Configure PVST+ on a VLAN.
vlan-bwcontract-explist	Use this command to add entries to or remove entries from the MAC exception list for bandwidth contracts on broadcast/multicast traffic.
voice dialplan-profile	This command allows you to create a dial plan profile and configure dial plans to the profile.
voice logging	This command allows you to enable logging for a voice client.
voice real-time-config	This command enables the controller to analyze the call quality of the voice calls based on the RTP media streams.

Command	Description
voice sip	This command allows you to enable SIP session timer and associate a dial plan profile to the SIP ALG.

Modified Commands

The following commands were modified in ArubaOS 6.0.

Command	Parameter Description
aaa authentication captive-portal <profile>max-authentication-failures <number>	The max-authentication-failures parameter no longer requires a license.
aaa authentication-server radius host <ipaddr>|<FQDN>	Identify the RADIUS server either by its IP address or fully qualified domain name.
aaa authentication-server tacacs	Enables TACACS+ authorization.Session-authorization turns on the optional authorization session for admin users.
ap system-profile am-scan-rf-band [a | g | all]	Added option for scanning band for multiple RF radios
clear aaa	tacacs—to clear TACACS server statistics.
interface vlan	The pppoe-max-segment-site, pppoe-password, pppoe-service-name and pppoe-password parameters were introduced.
ip mobile domain	A new parameter, description is added for providing more information about a HAT entry.
netservice	The list parameter for defining non-contiguous ports was introduced.
rf dot11a-radio-profile am-scan-profile <profile-name>	Configure an Air Monitor (AM) scanning profile.
rf dot11g-radio-profile am-scan-profile <profile-name>	Configure an Air Monitor (AM) scanning profile.sss
shape-mcast	Enables multicast optimization and provides excellent streaming quality regardless of the amount of VLANs or IP IGMP groups that are used.
show aaa authentication-server tacacs	The Statistics parameter was introduced.
show ap debug system-status	Show crash information for an AP with a specified name.
show ip mobile	Description of the HAT entry.
show spanning-tree	Added PVST+ in the display output
show spantree	Added PVST+ in the display output
show switches	The version column in the output of this command was expanded to include both the version and the build number for controllers running ArubaOS 6.0 and later releases.
show voice call-cdrs	The cid and rtpa parameters were introduced.
show voice call-quality	The rtpa and sta parameters were introduced.

Command	Parameter Description
show voice client-status	The sta parameter was introduced.
show voice trace	The trace output included the BSSID parameter.
show whitelist-db cpsec-local-switch-list	The cpsec-local-ctrlr-list parameter was modified to cpsec-local-switch-list
show whitelist-db cpsec-local-switch-list	The cpsec-master-ctrlr-list parameter was modified to cpsec-master-switch-list
spanning-tree (Configuration Interface)	Added support for PVST+ and VLAN range
stm purge-blacklist-client	Clear the entire client blacklist.
uplink	Set the priority of the wired uplink. Each uplink type has an associated priority; wired ports having the highest priority by default.
vlan <id> wired aaa-profile <profile>	Assign an AAA profile to a VLAN to enable role-based access for wired clients connected to an untrusted VLAN or port on the controller. This parameter applies to wired clients only.
voice rtcp-inactivity	This was part of the voip command in the earlier version. voip command is now deprecated.
voice sip-midcall-req-timeout	This was part of the voip command in the earlier version. voip command is now deprecated.
whitelist-db cpsec add	The controller-cert parameter was modified to switch-cert.
whitelist-db cpsec modify	The cpsec-local-ctlr-list parameter was modified to cpsec-local-switch-list
whitelist-db cpsec-local-switch-list	The cpsec-local-ctlr-list parameter was modified to cpsec-local-switch-list
whitelist-db cpsec-master-switch-list	The cpsec-master-ctrlr-list parameter was modified to cpsec-master-switch-list
wlan virtual-ap <profile> steering-mode band-balancing|force-5ghz|prefer-5ghz	Band steering supports three different band steering modes.
wms ap bssid mode	Updated the mode names and deprecated the dos mode.

Deprecated Commands

The following commands were deprecated in ArubaOS 6.0.

Command	Description
show ap debug association-failure (deprecated)	Display association failure information that can be used to troubleshoot problems on an AP
show user_session_count (deprecated)	Show the number of users using an ESSID for different time intervals.

About this Guide

This guide describes the ArubaOS command syntax. The commands in this guide are listed alphabetically.

The following information is provided 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, including license requirements for specific parameters if needed. The applicable ranges and default values, if any, are also included.
- 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 ArubaOS in which the command was first introduced. Modifications and changes to the command are also noted
- Command Information—This table describes any licensing requirements, command modes and platforms for which this command is applicable. For more information about available licenses, see the "Software Licenses" chapter in the *ArubaOS User Guide*.

Connecting to the Controller

This section describes how to connect to the controller to use the CLI.

Serial Port Connection

The serial port is located on the front panel of the controller. Connect a terminal or PC/workstation running a terminal emulation program to the serial port on the controller to use the CLI. Configure your terminal or terminal emulation program to use the following communication settings.

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

Telnet or SSH Connection

Telnet or SSH access requires that you configure an IP address and a default gateway on the controller and connect the controller to your network. This is typically performed when you run the Initial Setup on the controller, as described in the *Dell Quick Start Guide*. In certain deployments, you can also configure a loopback address for the controller; see the "Deploying a Basic Dell User-Centric System" chapter in the *ArubaOS User Guide* for more information.

Configuration changes on Master Controllers

Some commands can only be issued when connected to a master controller. If you make a configuration change on a master controller, all connected local controllers will subsequently update their configurations as well. You can manually synchronize all of the controllers at any time by saving the configuration on the master controller.

CLI Access

When you connect to the controller using the CLI, the system displays its host name followed by the login prompt. Log in using the admin user account and the password you entered during the Initial Setup on the controller (the password displays as asterisks). For example:

```
(host)
User: admin
Password: *****
```

When you are logged in, the *user* mode CLI prompt displays. For example:

```
(host) >
```

User mode provides only limited access for basic operational testing such as running **`ping`** and **`traceroute`**.

Certain management functions are available in *enable* (also called "privileged") mode. To move from user mode to enable mode requires you to enter an additional password that you entered during the Initial Setup (the password displays as asterisks). For example:

```
(host) > enable
Password: ******
```

When you are in enable mode, the > prompt changes to a pound sign (#):

```
(host) #
```

Configuration commands are available in *config* mode. Move from enable mode to config mode by entering **configure terminal** at the # prompt:

```
(host) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
```

When you are in basic config mode, (config) appears before the # prompt:

```
(host) (config) #
```

Note: There are several other sub- command modes that allow users to configure individual interfaces, subinterfaces, loopback addresses, GRE tunnels and cellular profiles. For details on the prompts and the available commands for each of these modes, see "Appendix A: Command Modes" on page 1237

Command Help

You can use the question mark (?) to view various types of command help.

When typed at the beginning of a line, the question mark lists all the commands available in your current mode or sub-mode. A brief explanation follows each command. For example:

```
(host) > ?

enable            Turn on Privileged commands
logout            Exit this session. Any unsaved changes are lost.
ping              Send ICMP echo packets to a specified IP address.
traceroute        Trace route to specified IP address.
```

When typed at the end of a possible command or abbreviation, the question mark lists the commands that match (if any). For example:

```
(host) > c?

clear                   Clear configuration
clock                   Configure the system clock
configure               Configuration Commands
copy                    Copy Files
```

If more than one item is shown, type more of the keyword characters to distinguish your choice. However, if only one item is listed, the keyword or abbreviation is valid and you can press tab or the spacebar to advance to the next keyword.

When typed in place of a parameter, the question mark lists the available options. For example:

```
(host) # write ?
erase                   Erase and start from scratch
file                    Write to a file in the file system
memory                  Write to memory
terminal                Write to terminal
<cr>
```

The <cr> indicates that the command can be entered without additional parameters. Any other parameters are optional.

Command Completion

To make command input easier, you can usually abbreviate each key word in the command. You need type only enough of each keyword to distinguish it from similar commands. For example:

```
(host) # configure terminal
```

could also be entered as:

```
(host) # con t
```

Three characters (**con**) represent the shortest abbreviation allowed for **configure**. Typing only **c** or **co** would not work because there are other commands (like **copy**) which also begin with those letters. The configure command is the only one that begins with **con**.

As you type, you can press the spacebar or tab to move to the next keyword. The system then attempts to expand the abbreviation for you. If there is only one command keyword that matches the abbreviation, it is filled in for you automatically. If the abbreviation is too vague (too few characters), the cursor does not advance and you must type more characters or use the help feature to list the matching commands.

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 enable or config prompt followed by the question mark. For example:

  ```
  (host) (config) # no?
  ```
- To delete a configuration, use the no form of a configuration command. For example, the following command removes a configured user role:

  ```
  (host) (config) # no user-role <name>
  ```
- To negate a specific configured parameter, use the **no** parameter within the command. For example, the following commands delete the DSCP priority map for a priority map configuration:

  ```
  (host) (config) # priority-map <name>
  (host) (config-priority-map) # no dscp priority high
  ```

Saving Configuration Changes

Each Dell controller contains two different types of configuration images.

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

  ```
  (host) # show running-config
  ```
- The *startup config* holds the configuration which will be used the next time the controller is rebooted. It contains all the options last saved using the **write memory** command. To view the startup-config, use the following command:

  ```
  (host) # show startup-config
  ```

When you make configuration changes via the CLI, those changes affect the current running configuration only. If the changes are not saved, they will be lost after the controller reboots. To save your configuration changes so they are retained in the startup configuration after the controller reboots, use the following command in enable mode:

```
(host) # write memory
Saving Configuration...
```

Saved Configuration

Both the startup and running configurations can also be saved to a file or sent to a TFTP server for backup or transfer to another system.

Commands That Reset the Controller or AP

If you use the CLI to modify a currently provisioned and running radio profile, those changes take place immediately; you do not reboot the controller or the AP for the changes to affect the current running configuration. Certain commands, however, automatically force the controller or AP to reboot. You may want to consider current network loads and conditions before issuing these commands, as they may cause a momentary disruption in service as the unit resets. Note also that changing the **lms-ip** parameter the in an AP system profile associated with an AP group will cause all APs in that AP group to reboot.

Commands that reset an AP

- ap-regroup
- ap-rename
- apboot
- apflash
- provision-ap reprovision
- ap wired-ap-profile <profile> forward-mode {bridge|split-tunnel|tunnel}
- wlan virtual-ap <profile> {aaa-profile <profile>|forward-mode {tunnel|bridge|split-tunnel|decrypt-tunnel}|ssid-profile <profile>|vlan <vlan>...}
- ap system-profile <profile> {bootstrap-threshold <number>|lms-ip <ipaddr>|master-ip <ipaddr>}
- wlan ssid-profile <profile> {battery-boost|deny-bcast|essid|opmode|strict-svp|wepkey1 <key>|wepkey2 <key>|wepkey3 <key>|wepkey4 <key>|weptxkey <index>|wmm|wmm-be-dscp <best-effort>|wmm-bk-dscp <background>|wmm-ts-min-inact-int <milliseconds>|wmm-vi-dscp <video>|wmm-vo-dscp <voice>|wpa-hexkey <psk>|wpa-passphrase <string>}
- wlan dotllk <profile> {bcn-measurement-mode|dot11k-enable|force-dissasoc}

Commands that reset a controller

- reload

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 to move back through the list and the *down* arrow key to forward. To reissue a specific command, press **Enter** when the command appears in the command history. You can even 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 table below lists the editing controls: To use key shortcuts, press and hold the **Ctrl** button while you press a letter key.

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.

Typographic Conventions

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

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
Boldface	This style is used to emphasize 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.

Type Style	Description
`{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.

Specifying Addresses and Identifiers in Commands

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

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, 10.4.1.258). For subnetwork addresses, specify a netmask in dotted decimal notation (for example, 255.255.255.0).
Netmask address	For subnetwork addresses, specify a netmask in dotted decimal notation (for example, 255.255.255.0).
Media Access Control (MAC) address	For any command that requires entry of a device's hardware address, use the hexadecimal format (for example, 00:05:4e:50:14:aa).
Service Set Identifier (SSID)	A unique character string (sometimes referred to as a network name), consisting of no more than 32 characters. The SSID is case-sensitive (for example, WLAN-01).
Basic Service Set Identifier (BSSID)	This entry is the unique hard-wireless MAC address of the AP. A unique BSSID applies to each frequency— 802.11a and 802.11g—used from the AP. Use the same format as for a MAC address.
Extended Service Set Identifier (ESSID)	Typically the unique logical name of a wireless network. If the ESSID includes spaces, you must enclose the name in quotation marks.
Fast Ethernet or Gigabit Ethernet interface	Any command that references a Fast Ethernet or Gigabit Ethernet interface requires that you specify the corresponding port on the controller in the format <slot>/<port>: **<slot>** is always 1. **<port>** refers to the network interfaces that are embedded in the front panel of the W-3000 Controller Series Multi-Service Controller. Port numbers start at 0 from the left-most position. Use the **show port status** command to obtain the interface information currently available from a controller.

aaa authentication captive-portal

```
aaa authentication
aaa authentication captive-portal <profile>
   clone <source-profile>
   default-guest-role <role>
   default-role <role>
   enable-welcome-page
   guest-logon
   login-page <url>
   logon-wait {cpu-threshold <percent>}|{maximum-delay <seconds>}|{minimum-delay <secs>}
   logout-popup-window
   max-authentication-failures <number>
   no ...
   protocol-http
   redirect-pause <secs>
   server-group <group-name>
   show-acceptable-use-policy
   show-fqdn
   single-session
   switch-in-redirection-url <ipaddr>
   sygate-on-demand-agent
   use-chap
   user-logon
   welcome-page <url>
```

Description

This command configures a Captive Portal authentication profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing Captive Portal profile from which parameter values are copied.	—	—
`default-guest-role`	Role assigned to guest.	—	guest
`default-role <role>`	Role assigned to the Captive Portal user upon login. When both user and guest logon are enabled, the default role applies to the user logon; users logging in using the guest interface are assigned the guest role.	—	guest
`enable-welcome-page`	Displays the configured welcome page before the user is redirected to their original URL. If this option is disabled, redirection to the web URL happens immediately after the user logs in.	enabled/ disabled	enabled
`guest-logon`	Enables Captive Portal logon without authentication.	enabled/ disabled	disabled
`login-page <url>`	URL of the page that appears for the user logon. This can be set to any URL.	—	/auth/index. html
`logon-wait`	Configure parameters for the logon wait interval	1-100	60%
`cpu-threshold <percent>`	CPU utilization percentage above which the Logon wait interval is applied when presenting the user with the logon page.	1-100	60%
`maximum-delay <seconds>`	Maximum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter.	1-10	10 seconds
`minimum-delay <secs>`	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter.	1-10	5 seconds
`logout-popup-window`	Enables a pop-up window with the Logout link for the user to logout after logon. If this is disabled, the user remains logged in until the user timeout period has elapsed or the station reloads.	enabled/ disabled	enabled
`max-authentication-failures <number>`	Maximum number of authentication failures before the user is blacklisted.	0-10	0
`no`	Negates any configured parameter.	—	—
`protocol-http`	Use HTTP protocol on redirection to the Captive Portal page. If you use this option, modify the captive portal policy to allow HTTP traffic.	enabled/ disabled	disabled (HTTPS is used)
`redirect-pause <secs>`	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link.	1-60	10 seconds
`server-group <group-name>`	Name of the group of servers used to authenticate Captive Portal users. See "aaa server-group" on page 70.	—	—

Parameter	Description	Range	Default
show-fqdn	Allows the user to see and select the fully-qualified domain name (FQDN) on the login page. The FQDNs shown are specified when configuring individual servers for the server group used with captive portal authentication.	enabled/ disabled	disabled
show-acceptable-use-policy	Show the acceptable use policy page before the logon page.	enabled/ disabled	disabled
single-session	Allows only one active user session at a time.	—	disabled
switch-in-redirection-url	Sends the controller's IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the controller from which a request originated by parsing the 'switchip' variable in the URL.	enabled/ disabled	disabled
sygate-on-demand-agent	Enables client remediation with Sygate-on-demand-agent (SODA). **NOTE**: This parameter requires the PEFNG license.	enabled/ disabled	disabled
use-chap	Use CHAP protocol. You should not use this option unless instructed to do so by an Dell representative.	enabled/ disabled	disabled (PAP is used)
user-logon	Enables Captive Portal with authentication of user credentials.	enabled/ disabled	enabled
welcome-page <url>	URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL.	—	/auth/ welcome.html

Usage Guidelines

You can configure the Captive Portal authentication profile in the base operating system or with the Next Generation Policy Enforcement Firewall (PEFNG) license installed. When you configure the profile in the base operating system, the name of the profile must be entered for the initial role in the AAA profile. Also, when you configure the profile in the base operating system, you cannot define the default-role.

Example

The following example configures a Captive Portal authentication profile that authenticates users against the controller's internal database. Users who are successfully authenticated are assigned the auth-guest role.

To create the auth-guest user role shown in this example, the PEFNG license must be installed in the controller.

```
aaa authentication captive-portal guestnet
   default-role auth-guest
   user-logon
   no guest-logon
   server-group internal
```

Command History

Version	Description
ArubaOS 3.0	Command introduced.
ArubaOS 6.0	The **max-authentication-failures** parameter no longer requires a license.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system, except for noted parameters	Config mode on master controllers

aaa authentication dot1x

```
aaa authentication dot1x {<profile>|countermeasures}
   ca-cert <certificate>
   clear
   clone <profile>
   eapol-logoff
   framed-mtu <mtu>
   heldstate-bypass-counter <number>
   ignore-eap-id-match
   ignore-eapolstart-afterauthentication
   machine-authentication blacklist-on-failure|{cache-timeout <hours>}|enable|
     {machine-default-role <role>}|{user-default-role <role>}
   max-authentication-failures <number>
   max-requests <number>
   multicast-keyrotation
   no ...
   opp-key-caching
   reauth-max <number>
   reauthentication
   server {server-retry <number>|server-retry-period <seconds>}
   server-cert <certificate>
   termination {eap-type <type>}|enable|enable-token-caching|{inner-eap-type (eap-
     gtc|eap-mschapv2)}|{token-caching-period <hours>}
   timer {idrequest_period <seconds>}|{mkey-rotation-period <seconds>}|{quiet-period
     <seconds>}|{reauth-period <seconds>}|{ukey-rotation-period <seconds>}|{wpa-
     groupkey-delay <seconds>}|{wpa-key-period <milliseconds>}|wpa2-key-delay
     <milliseconds>
   tls-guest-access
   tls-guest-role <role>
   unicast-keyrotation
   use-session-key
   use-static-key
   validate-pmkid
   voice-aware
   wep-key-retries <number>
   wep-key-size {40|128}
   wpa-fast-handover
   xSec-mtu <mtu>
```

Description

This command configures the 802.1x authentication profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`clear`	Clear the Cached PMK, Role and VLAN entries. This command is available in enable mode only.	—	—
`countermeasures`	Scans for message integrity code (MIC) failures in traffic received from clients. If there are more than 2 MIC failures within 60 seconds, the AP is shut down for 60 seconds. This option is intended to slow down an attacker who is making a large number of forgery attempts in a short time.	—	disabled
`ca-cert <certificate>`	CA certificate for client authentication. The CA certificate needs to be loaded in the controller.	—	—
`clone <profile>`	Name of an existing 802.1x profile from which parameter values are copied.	—	—
`eapol-logoff`	Enables handling of EAPOL-LOGOFF messages.	—	disabled
`framed-mtu <MTU>`	Sets the framed MTU attribute sent to the authentication server.	500-1500	1100
`heldstate-bypass-counter <number>`	(This parameter is applicable when 802.1x authentication is terminated on the controller, also known as AAA FastConnect.) Number of consecutive authentication failures which, when reached, causes the controller to not respond to authentication requests from a client while the controller is in a held state after the authentication failure. Until this number is reached, the controller responds to authentication requests from the client even while the controller is in its held state.	0-3	0
`ignore-eap-id-match`	Ignore EAP ID during negotiation.	—	disabled
`ignore-eapol start-afterauthentication`	Ignores EAPOL-START messages after authentication.	—	disabled
`machine-authentication`	(For Windows environments only) These parameters set machine authentication: **NOTE**: This parameter requires the PEFNG license.		
`blacklist-on-failure`	Blacklists the client if machine authentication fails.	—	disabled
`cache-timeout <hours>`	The timeout, in hours, for machine authentication.	1-1000	24 hours (1 day)
`enable`	Select this option to enforce machine authentication before user authentication. If selected, either the machine-default-role or the user-default-role is assigned to the user, depending on which authentication is successful.	—	disabled
`machine-default-role <role>`	Default role assigned to the user after completing only machine authentication.	—	guest
`user-default-role <role>`	Default role assigned to the user after 802.1x authentication.	—	guest

Parameter	Description	Range	Default
`max-authentication-failures <number>`	Number of times a user can try to login with wrong credentials after which the user is blacklisted as a security threat. Set to 0 to disable blacklisting, otherwise enter a non-zero integer to blacklist the user after the specified number of failures. **NOTE**: The RF Protect license must be installed.	0-5	0 (disabled)
`max-requests <number>`	Maximum number of times ID requests are sent to the client.	1-10	3
`multicast-key rotation`	Enables multicast key rotation	—	disabled
`no`	Negates any configured parameter.	—	—
`opp-key-caching`	Enables a cached pairwise master key (PMK) derived with a client and an associated AP to be used when the client roams to a new AP. This allows clients faster roaming without a full 802.1x authentication. **NOTE**: Make sure that the wireless client (the 802.1x supplicant) supports this feature. If the client does not support this feature, the client will attempt to renegotiate the key whenever it roams to a new AP. As a result, the key cached on the controller can be out of sync with the key used by the client.	—	enabled
`reauth-max <number>`	Maximum number of reauthentication attempts.	1-10	3
`reauthentication`	Select this option to force the client to do a 802.1x reauthentication after the expiration of the default timer for reauthentication. (The default value of the timer is 24 hours.) If the user fails to reauthenticate with valid credentials, the state of the user is cleared. If derivation rules are used to classify 802.1x-authenticated users, then the reauthentication timer per role overrides this setting.	—	disabled
`reload-cert`	Reload Certificate for 802.1X termination. This command is available in enable mode only.	—	—
`server`	Sets options for sending authentication requests to the authentication server group.		
`server-retry <number>`	Maximum number of authentication requests that are sent to server group.	0-3	2
`server-retry-period <seconds>`	Server group retry interval, in seconds.	5-65535	30 seconds
`server-cert <certificate>`	Server certificate used by the controller to authenticate itself to the client.	—	—
`termination`	Sets options for terminating 802.1x authentication on the controller.		
`eap-type <type>`	The Extensible Authentication Protocol (EAP) method, either EAP-PEAP or EAP-TLS.	eap-peap/ eap-tls	eap-peap
`enable`	Enables 802.1x termination on the controller.	—	disabled
`enable-token-caching`	If you select EAP-GTC as the inner EAP method, you can enable the controller to cache the username and password of each authenticated user. The controller continues to reauthenticate users with the remote authentication server, however, if the authentication server is not available, the controller will inspect its cached credentials to reauthenticate users.	—	disabled

Parameter	Description	Range	Default
`inner-eap-type eap-gtc|eap-mschapv2`	When EAP-PEAP is the EAP method, one of the following inner EAP types is used: **EAP-Generic Token Card (GTC)**: Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the controller as a backup to an external authentication server. **EAP-Microsoft Challenge Authentication Protocol version 2 (MS-CHAPv2)**: Described in RFC 2759, this EAP method is widely supported by Microsoft clients.	eap-gtc/ eap-mschapv2	eap-mschap v2
`token-caching-period <hours>`	If you select EAP-GTC as the inner EAP method, you can specify the timeout period, in hours, for the cached information.	(any)	24 hours
`timer`	Sets timer options for 802.1x authentication:		
`idrequest-period <seconds>`	Interval, in seconds, between identity request retries.	1-65535	30 seconds
`mkey-rotation-period <seconds>`	Interval, in seconds, between multicast key rotation.	60-864000	1800 seconds
`quiet-period <seconds>`	Interval, in seconds, following failed authentication.	1-65535	30 seconds
`reauth-period <seconds>`	Interval, in seconds, between reauthentication attempts, or specify **server** to use the server-provided reauthentication period.	60-864000	86400 seconds (1 day)
`ukey-rotation-period <seconds>`	Interval, in seconds, between unicast key rotation.	60-864000	900 seconds
`wpa-groupkey -delay <milliseconds>`	Interval, in milliseconds, between unicast and multicast key exchanges.	0-2000	0 ms (no delay)
`wpa-key-period <milliseconds>`	Interval, in milliseconds, between each WPA key exchange.	1000-5000	3000 ms
`wpa2-key-delay <milliseconds>`	Set the delay between EAP-Success and unicast key exchange.	1-2000	0 ms (no delay)
`tls-guest-access`	Enables guest access for EAP-TLS users with valid certificates.	—	disabled
`tls-guest-role <role>`	User role assigned to EAP-TLS guest. **NOTE**: This parameter requires the PEFNG license.	—	guest
`unicast-keyrotation`	Enables unicast key rotation.	—	disabled
`use-session-key`	Use RADIUS session key as the unicast WEP key.	—	disabled
`use-static-key`	Use static key as the unicast/multicast WEP key.	—	disabled
`validate-pmkid`	This parameter instructs the controller to check the pairwise master key (PMK) ID sent by the client. When this option is enabled, the client must send a PMKID in the associate or reassociate frame to indicate that it supports OKC or PMK caching; otherwise, full 802.1x authentication takes place. (This feature is optional, since most clients that support OKC and PMK caching do not send the PMKID in their association request.)	—	disabled

Parameter	Description	Range	Default
`voice-aware`	Enables rekey and reauthentication for VoWLAN clients. **NOTE**: The Next Generation Policy Enforced Firewall license must be installed.	—	enabled
`wep-key-retries <number>`	Number of times WPA/WPA2 key messages are retried.	1-5	3
`wep-key-size`	Dynamic WEP key size, either 40 or 128 bits.	40 or 128	128 bits
`wpa-fast-handover`	Enables WPA-fast-handover. This is only applicable for phones that support WPA and fast handover.	—	disabled
`xSec-mtu <mtu>`	Sets the size of the MTU for xSec.	1024-1500	1300 bytes

Usage Guidelines

The 802.1x authentication profile allows you to enable and configure machine authentication and 802.1x termination on the controller (also called "AAA FastConnect").

In the AAA profile, you specify the 802.1x authentication profile, the default role for authenticated users, and the server group for the authentication.

Examples

The following example enables authentication of the user's client device before user authentication. If machine authentication fails but user authentication succeeds, the user is assigned the restricted "guest" role:

```
aaa authentication dot1x dot1x
   machine-authentication enable
   machine-authentication machine-default-role computer
   machine-authentication user-default-role guest
```

The following example configures an 802.1x profile that terminates authentication on the controller, where the user authentication is performed with the controller's internal database or to a "backend" non-802.1x server:

```
aaa authentication dot1x dot1x
   termination enable
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system. The voice-aware parameter requires the PEFNG license	Config mode on master controllers

aaa authentication mac

```
aaa authentication mac <profile>
   case upper|lower
   clone <profile>
   delimiter {colon|dash|none}
   max-authentication-failures <number>
   no ...
```

Description

This command configures the MAC authentication profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`case`	The case (upper or lower) used in the MAC string sent in the authentication request. If there is no delimiter configured, the MAC address in lower case is sent in the format xxxxxxxxxxxx, while the MAC address in upper case is sent in the format XXXXXXXXXXXX.	upper|lower	lower
`clone <profile>`	Name of an existing MAC profile from which parameter values are copied.	—	—
`delimiter`	Delimiter (colon, dash, or none) used in the MAC string.	colon|dash|none	none
`max-authentication-failures <number>`	Number of times a client can fail to authenticate before it is blacklisted. A value of 0 disables blacklisting.	0-10	0 (disabled)
`no`	Negates any configured parameter.	—	—

Usage Guidelines

MAC authentication profile configures authentication of devices based on their physical MAC address. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to all other devices. Users may be required to authenticate themselves using other methods, depending upon the network privileges.

Example

The following example configures a MAC authentication profile to blacklist client devices that fail to authenticate.

```
aaa authentication mac mac-blacklist
   max-authentication-failures 3
```

Command History:

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3.1.8	The max-authentication-failures parameter was allowed in the base operating system. In earlier versions of ArubaOS, the max-authentication-failures parameter required the Wireless Intrusion Protection license

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa authentication mgmt

```
aaa authentication mgmt
   default-role {guest-provisioning|location-api|network-operations|no-access|read-
   only|root}
   enable
   no ...
   server-group <group>
```

Description

This command configures authentication for administrative users.

Syntax

Parameter	Description	Range	Default
`default-role`	Select a predefined management role to assign to authenticated administrative users:	—	default
`default`	Default superuser role		
`guest-provisioning`	Guest provisioning role		
`location-api`	Location API role		
`network-operations`	Network operations role		
`no-access`	No commands are accessible for this role		
`read-only`	Read-only role		
`enable`	Enables authentication for administrative users.	enabled| disabled	disabled
`no`	Negates any configured parameter.	—	—
`server-group <group>`	Name of the group of servers used to authenticate administrative users. See “aaa server-group” on page 70.	—	default

Usage Guidelines

If you enable authentication with this command, users configured with the **mgmt-user** command must be authenticated using the specified server-group.

You can configure the management authentication profile in the base operating system or with the PEFNG license installed.

Example

The following example configures a management authentication profile that authenticates users against the controller’s internal database. Users who are successfully authenticated are assigned the read-only role.

```
aaa authentication mgmt
   default-role read-only
   server-group internal
```

Command History:

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	The network-operations role was introduced.
ArubaOS 3.3	The location-api-mgmt role was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa authentication stateful-dot1x

```
aaa authentication stateful-dot1x
   default-role <role>
   enable
   no ...
   server-group <group>
   timeout <seconds>
```

Description

This command configures 802.1x authentication for clients on non-Dell APs.

Syntax

Parameter	Description	Range	Default
`default-role <role>`	Role assigned to the 802.1x user upon login. **NOTE**: The PEFNG license must be installed.	—	guest
`enable`	Enables 802.1x authentication for clients on non-Dell APs. Use **no enable** to disable this authentication.	—	enabled
`no`	Negates any configured parameter.	—	—
`server-group <group>`	Name of the group of RADIUS servers used to authenticate the 802.1x users. See “aaa server-group” on page 70.	—	—
`timeout <seconds>`	Timeout period, in seconds.	1-20	10 seconds

Usage Guidelines

This command configures 802.1x authentication for clients on non-Dell APs. The controller maintains user session state information for these clients.

Example

The following command assigns the employee user role to clients who successfully authenticate with the server group corp-rad:

```
aaa authentication stateful-dot1x
   default-role employee
   server-group corp-rad
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa authentication stateful-dot1x clear

```
aaa authentication stateful-dot1x clear
```

Description

This command clears automatically-created control path entries for 802.1x users on non-Dell APs.

Syntax

No parameters.

Usage Guidelines

Run this command after changing the configuration of a RADIUS server in the server group configured with the **aaa authentication stateful-dot1x** command. This causes entries for the users to be created in the control path with the updated configuration information.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa authentication stateful-ntlm

```
aaa authentication stateful-ntlm
   default-role <role>
   enable
   server-group <server-group>
   timeout <timeout>
```

Description

This command configures stateful NT LAN Manager (NTLM) authentication.

Syntax

Parameter	Description	Range	Default
`default-role`	Select an existing role to assign to authenticated users.	—	guest
`no`	Negates any configured parameter.	—	—
`server-group <server-group>`	Name of a server group.	—	default
`timeout <timeout>`	NTLM authentication request, timeout period, in seconds.	1-20 seconds	10 seconds

Usage Guidelines

NT LAN Manager (NTLM) is a suite of Microsoft authentication and session security protocols. You can use a stateful NTLM authentication profile to configure an Dell controller to monitor the NTLM authentication messages between clients and an authentication server. The controller can then use the information in the Server Message Block (SMB) headers to determine the client's username and IP address, the server IP address and the client's current authentication status. If the client successfully authenticates via an NTLM authentication server, the controller can recognize that the client has been authentication and assign that client a specified user role. When the user logs off or shuts down the client machine, the user will remain in the authenticated role until the user's authentication is aged out.

The Stateful NTLM Authentication profile requires that you specify a server group which includes the servers performing NTLM authentication, and a default role to be assigned to authenticated users. For details on defining a windows server used for NTLM authentication, see aaa authentication-server windows.

Example

The following example configures a stateful NTLM authentication profile that authenticates clients via the server group "Windows1." Users who are successfully authenticated are assigned the "guest2" role.

```
aaa authentication stateful-ntlm
   default-role guest2
   server-group Windows1
```

Command History

Command introduced in ArubaOS 3.4.1

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa authentication via auth-profile

```
aaa authentication via auth-profile <profile>
   clone <source>
   default-role <default-role>
   desc <description>
   max-authentication-failures <max-authentication-failures>
   no
   server-group <server-group>
```

Description

This command configures the VIA authentication profile.

Syntax

Parameter	Description	Default
`clone <source>`		
`default-role <default-role>`	Name of the default VIA authentication profile.	-
`desc <description>`	Description of this profile for reference.	-
`max-authentication-failures <max-authentication-failures>`	Number of times VIA will prompt user to login due to incorrect credentials. After the maximum authentication attempts failures VIA will exit.	3
`server-group <server-group>`	Server group against which the user is authenticated.	-

Usage Guidelines

Use this command to create VIA authentication profiles and associate user roles to the authentication profile.

Example

```
(host) (config) #aaa authentication via auth-profile default
(host) (VIA Authentication Profile "default") #default-role example-via-role
(host) (VIA Authentication Profile "default") #desc "Default VIA Authentication
Profile"
```

(host) (VIA Authentication Profile "default") #server-group "via-server-group"

Command History

Command introduced in 5.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master or local controllers

aaa authentication via connection-profile

```
aaa authentication via connection-profile <profile>
   allow-user-disconnect
   auth-profile <auth-profile>
   auto-login
   auto-upgrade
   client-logging
   client-netmask <client-netmask>
   client-wlan-profile <client-wlan-profile> position <position>
   clone
   controller addr <addr> internal-ip <internal-ip> desc <description>
   csec-gateway-url <URL>
   csec-http-ports <comma separated port numbers>
   dns-suffix-list <dns-suffix-list>
   enable-csec
   ext-download-url <ext-download-url>
   force-ssl-fallback
   ike-policy <ike-policy>
   ipsec-cryptomap map <map> number <number>
   max-reconnect-attempts <max-reconnect-attempts>
   max-timeout value <value>
   no
   save-passwords
   split-tunneling
   support-email
   tunnel
   validate-server-cert
   windows-credentials
```

Description

This command configures the VIA connection profile.

Syntax

Parameter	Description	Default
`allow-user-disconnect`	Enable or disable users to disconnect their VIA sessions.	on
`auth-profile <auth-profile>`	This is the list of VIA authentication profiles that will be displayed to users in the VIA client.	
`auto-login`	Enable or disable VIA client to auto login and establish a secure connection to the controller.	Enabled
`auto-upgrade`	Enable or disable VIA client to automatically upgrade when an updated version of the client is available on the controller.	Enabled
`client-logging`	Enable or disable VIA client to auto login and establish a secure connection to the controller.	Enabled
`client-netmask <client-netmask>`	The network mask that has to be set on the client after the VPN connection is established.	255.255.255.255
`client-wlan-profile <client-wlan-profile>`	A list of VIA client WLAN profiles that needs to be pushed to the client machines that use Windows Zero Config (WZC) to configure or manage their wireless networks.	
`position <position>`		
`clone`	Create a copy of connection profile from an another VIA connection profile.	
`controller`	• *Address*: This is the public IP address or the DNS hostname of the VIA controller. Users will connect to remote server using this IP address or the hostname. • Internal IP Address: This is the IP address of any of the VLAN interface IP addresses belongs to this controller. • Description: This is a human-readable description of the controller.	
`addr <addr>`		
`<internal-ip <internal-ip>`		
`desc <description>`		
`csec-gateway-url`	Specify the content security service providers URL here. You must provide a fully qualified domain name.	
`csec-http-ports`	Specify the ports (separated by comma) that will be monitored by the content security service provider. Do not add space before or after the comma.	
`dns-suffix-list <dns-suffix-list>`	The DNS suffix list (comma separated) that has be set on the client once the VPN connection is established. .	None
`enable-csec`	Use this option to enable the content security service.	
`ext-download-url <ext-download-url>`	End users will use this URL to download VIA on their computers.	
`ike-policy <ike-policy>`	List of IKE policies that the VIA Client has to use to connect to the controller.	
`ipsec-cryptomap`	List of IPSec Crypto Map that the VIA client uses to connect to the controller. These IPSec Crypto Maps are configured in CLI using the `crypto-local ipsec-map <ipsec-map-name>` command.	
`map <map>`		
`number <number>`		
`max-reconnect-attempts <max-reconnect-attempts>`	The maximum number of re-connection attempts by the VIA client due to authentication failures.	3
`max-timeout value <value>`	The maximum time (minutes) allowed before the VIA session is disconnected.	1440 min
`save-passwords`	Enable or disable users to save passwords entered in VIA.	Enabled

Parameter	Description	Default
`split-tunneling`	Enable or disable split tunneling. • If enabled, all traffic to the VIA tunneled networks will go through the controller and the rest is just bridged directly on the client. • If disabled, all traffic will flow through the controller.	off
`support-email`	The support e-mail address to which VIA users will send client logs.	None
`tunnel address <address>`	A list of network destination (IP address and netmask) that the VIA client will tunnel through the controller. All other network destinations will be reachable directly by the VIA client. Enter tunneled IP address and its netmask.	
`address <address>`		
`netmask <netmask>`		
`validate-server-cert`	Enable or disable VIA from validating the server certificate presented by the controller.	Enabled
`windows-credentials`	Enable or disable the use of the Windows credentials to login to VIA. If enabled, the SSO (Single Sign-on) feature can be utilized by remote users to connect to internal resources.	Enabled

Usage Guidelines

Issue this command to create a VIA connection profile. A VIA connection profile contains settings required by VIA to establish a secure connection to the controller. You can configure multiple VIA connection profiles. A VIA connection profile is always associated to a user role and all users belonging to that role will use the configured settings. If you do not assign a VIA connection profile to a user role, the default connection profile is used.

Example

The following example shows a simple VIA connection profile:

```
(host) (config) #aaa authentication via connection-profile "via"
(host) (VIA Connection Profile "via") #controller addr 202.100.10.100 internal-ip
10.11.12.13 desc "VIA Primary Controller" position 0
(host) (VIA Connection Profile "via") #auth-profile "default" position 0
(host) (VIA Connection Profile "via") #tunnel address 10.0.0.0 netmask 255.255.255.0
(host) (VIA Connection Profile "via") #split-tunneling
(host) (VIA Connection Profile "via") #windows-credentials
(host) (VIA Connection Profile "via") #client-netmask 255.0.0.0
(host) (VIA Connection Profile "via") #dns-suffix-list mycorp.com
(host) (VIA Connection Profile "via") #dns-suffix-list example.com
(host) (VIA Connection Profile "via") #support-email via-support@example.com
```

Command History

Command introduced in 5.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master or local controllers

aaa authentication via web-auth

```
aaa authentication via web-auth default
   auth-profile <auth-profile> position <position>
   clone <source>
   no
```

Description

A VIA web authentication profile contains an ordered list of VIA authentication profiles. The web authentication profile is used by end users to login to the VIA download page (*https://<server-IP-address>/via*) for downloading the VIA client. Only one VIA web authentication profile is available. If more than one VIA authentication profile is configured, users can view this list and select one during the client login.

Syntax

Parameter	Description	Default
`auth-profile <auth-profile>`		
`position <position>`		
`clone <source>`		

Example

```
(host) (config) #aaa authentication via web-auth default
```

(host) (VIA Web Authentication "default") #auth-profile default position 0

Command History

Command introduced in 5.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master or local controllers

aaa authentication vpn

```
aaa authentication vpn <profile-name>
   clone <source>
   default-role <guest>
   max-authentication-failures <number>
   no ...
   server-group <group>
```

Description

This command configures VPN authentication settings.

Syntax

Parameter	Description	Default
`<profile-name>`	There are three VPN profiles: **default**, **default-rap** or **default-cap**. This allows users to use different AAA servers for VPN, RAP and CAP clients. **NOTE:** The **default** and **default-rap** profiles are configurable. The **default-cap** profile is not configurable and is predefined with the default settings.	—
`default-role <role>`	Role assigned to the VPN user upon login. **NOTE:** This parameter requires the Policy Enforcement Firewall for VPN Users (PEFV) license.	guest
`clone <source>`	Copies data from another VPN authentication profile. Source is the profile name from which the data is copied.	—
`max-authentication-failures <number>`	Maximum number of authentication failures before the user is blacklisted. A value of 0 disables blacklisting. **NOTE**: The RF Protect license must be installed.	0 (disabled)
`no`	Negates any configured parameter.	—
`server-group <group>`	Name of the group of servers used to authenticate VPN users. See “aaa server-group” on page 70.	internal

Usage Guidelines

This command configures VPN authentication settings for VPN, RAP and CAP clients.

Use the **vpdn group** command to enable and configure Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPsec) or Point-to-Point Tunneling Protocol (PPTP) VPN connection. (See “vpdn group l2tp” on page 1188.)

Example

The following command configures VPN authentication settings for the default-rap profile:

```
aaa authentication vpn default-rap
   default-role guest
   clone default
   max-authentication-failures 0
   server-group vpn-server-group
```

The following message appears when a user tries to configure the non-configurable default-cap profile:

```
(host) (config) #aaa authentication vpn default-cap
Predefined VPN Authentication Profile "default-cap" is not editable
```

Command History

Version	Description
ArubaOS 3.0	Command introduced.
ArubaOS 5.0	The **default-cap** and **default-rap** profiles were introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system, except for noted parameters. The **default-role** parameter requires the Policy Enforcement Firewall for VPN Users (PEFV) license.	Config mode on master controllers

aaa authentication wired

```
aaa authentication wired
   no ...
   profile <aaa-profile>
```

Description

This command configures authentication for a client device that is directly connected to a port on the controller.

Syntax

Parameter	Description
no	Negates any configured parameter.
profile <aaa-profile>	Name of the AAA profile that applies to wired authentication. This profile must be configured for a Layer-2 authentication, either 802.1x or MAC. See “aaa profile” on page 63.

Usage Guidelines

This command references an AAA profile that is configured for MAC or 802.1x authentication. The port on the controller to which the device is connected must be configured as untrusted.

Example

The following commands configure an AAA profile for dot1x authentication and a wired profile that references the AAA profile:

```
aaa profile sec-wired
   dot1x-default-role employee
   dot1x-server-group sec-svrs
aaa authentication wired
   profile sec-wired
```

Related Commands

Command	Description
vlan wired aaa-profile <profile>	Assign an AAA profile to an individual VLAN to enable role-based access for wired clients connected to an untrusted VLAN or port on the controller.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa authentication wispr

```
aaa authentication wispr
   default-role <role>
   logon-wait {cpu-threshold|maximum-delay|minimum-delay}
   no ...
   server-group <server-group>
   wispr-location-id-ac <wispr-location-id-ac>
   wispr-location-id-cc <wispr-location-id-cc>
   wispr-location-id-isocc <wispr-location-id-isocc>
   wispr-location-id-network <wispr-location-id-network>
   wispr-location-name-location <wispr-location-name-location>
   wispr-location-name-operator-name <wispr-location-name-operator>
```

Description

This command configures WISPr authentication with an ISP's WISPr RADIUS server.

Syntax

Parameter	Description
`default-role`	Default role assigned to users that complete WISPr authentication.
`logon-wait`	Configure the CPU utilization threshold that will trigger logon wait maximum and minimum times
`CPU-threshold`	Percentage of CPU utilization at which the maximum and minimum login wait times are enforced. Range: 1-100%.Default: 60%.
`maximum-wait`	If the controller's CPU utilization has surpassed the **CPU-threshold** value, the **maximum-wait** parameter defines the minimum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 10 seconds.
`minimum-wait`	If the controller's CPU utilization has surpassed the **CPU-threshold** value, the **minimum-wait** parameter defines the minimum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 5 seconds.
`wispr-location-id-ac <wispr-location-id-ac>`	The E.164 Area Code in the WISPr Location ID.
`wispr-location-id-cc <wispr-location-id-cc>`	The 1-3 digit E.164 Country Code in the WISPr Location ID.
`wispr-location-id-isocc <wispr-location-id-isocc>`	The ISO Country Code in the WISPr Location ID.
`wispr-location-id-network <wispr-location-id-network>`	The SSID/network name in the WISPr Location ID.
`wispr-location-name-location <wispr-location-name-location>`	A name identifying the hotspot location. If no name is defined, the default ap-name is used.
`wispr-location-name-operator-name <wispr-location-name-operator>`	A name identifying the hotspot operator.

Usage Guidelines

WISPr authentication allows a "smart client" to remain authenticated on the network when they roam between Wireless Internet Service Providers, even if the wireless hotspot uses an ISP for which the client may not have an account.

If you are hotstpot operator using WISPr authentication, and a client that has an account with your ISP attempts to access the Internet at your hotspot, then your ISP's WISPr AAA server authenticates that client directly, and

allows the client access on the network. If, however, the client only has an account with a *partner* ISP, then your ISP's WISPr AAA server will forward that client's credentials to the partner ISP's WISPr AAA server for authentication. Once the client has been authenticated on the partner ISP, it will be authenticated on your hotspot's own ISP, as per their service agreements. Once your ISP sends an authentication message to the controller, the controller assigns the default WISPr user role to that client.

ArubaOS supports the following smart clients, which enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) *redirect*, *proxy*, *authentication* and *logoff* messages within HTLM messages to the controller.

- iPass
- Bongo
- Trustive
- weRoam
- AT&T

A WISPr authentication profile includes parameters to define RADIUS attributes, the default role for authenticated WISPr users, maximum numbers of authenticated failures and logon wait times. The WISPr-Location-ID sent from the controller to the WISPr RADIUS server will be the concatenation of the ISO Country Code, E.164 Country Code, E.164 Area Code and SSID/Zone parameters configured in this profile

The parameters to define WISPr RADIUS attributes are specific to the RADIUS server your ISP uses for WISPr authentication; contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU web sites (www.iso.org and http://www.itu.int.)

Note: A Boingo smart client uses a NAS identifier in the format <CarrierID>_<VenueID> for location identification. To support Boingo clients, you must also configure the **NAS identifier** parameter in the Radius server profile for the WISPr server

Example

The following commands configure an WISPr authentication profile:

```
aaa authentication wispr
   default-role authuser
   max-authentication-failure 5
   server-group wispr1
   wispr-location-id-ac 408
   wispr-location-id-cc 1
   wispr-location-id-isocc us
   wispr-location-id-network <wispr-location-id-network>
   wispr-location-name-location <wispr-location-name-location>
   wispr-location-name-operator-name <wispr-location-name-location>
```

Command History

This command was available in ArubaOS 3.4.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master or local controllers

aaa authentication-server internal

```
aaa authentication-server internal use-local-switch
```

Description

This command specifies that the internal database on a local controller be used for authenticating clients.

Usage Guidelines

By default, the internal database in the *master* controller is used for authentication. This command directs authentication to the internal database on the *local* controller where you run the command.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master or local controllers

aaa authentication-server ldap

```
aaa authentication-server ldap <server>
   admin-dn <name>
   admin-passwd <string>
   allow-cleartext
   authport <port>
   base-dn <name>
   clone <server>
   enable
   filter
   host <ipaddr>
   key-attribute <string>
   no ...
   preferred-conn-type ldap-s|start-tls|clear-text
   timeout <seconds>
```

Description

This command configures an LDAP server.

Syntax

Parameter	Description	Range	Default
`<server>`	Name that identifies the server.	—	—
`admin-dn <name>`	Distinguished name for the admin user who has read/search privileges across all of the entries in the LDAP database (the user does not need write privileges but should be able to search the database and read attributes of other users in the database).	—	—
`admin-passwd <string>`	Password for the admin user.	—	—
`allow-cleartext`	Allows clear-text (unencrypted) communication with the LDAP server.	enabled| disabled	disabled
`authport <port>`	Port number used for authentication. Port 636 will be attempted for LDAP over SSL, while port 389 will be attempted for SSL over LDAP, Start TLS operation and clear text.	1-65535	389
`base-dn <name>`	Distinguished Name of the node which contains the entire user database to use.	—	—
`clone <server>`	Name of an existing LDAP server configuration from which parameter values are copied.	—	—
`enable`	Enables the LDAP server.	—	
`filter`	Filter that should be applied to search of the user in the LDAP database (default filter string is: ì(objectclass=*)î).	—	(objectclass =)*
`host <ip-addr>`	IP address of the LDAP server, in dotted-decimal format.	—	—
`key-attribute <string>`	Attribute that should be used as a key in search for the LDAP server. For Active Directory, the value is sAMAccountName.	—	sAMAccount Name
`no`	Negates any configured parameter.	—	—
`preferred-conn-type`	Preferred connection type.The default order of connection type is: 1. ldap-s 2. start-tls 3. clear-text The controller will first try to contact the LDAP server using the preferred connection type, and will only attempt to use a lower-priority connection type if the first attempt is not successful. **NOTE:** You enable the **allow-cleartext** option before you select **clear-text** as the preferred connection type. If you set clear-text as the preferred connection type but do not allow clear-text, the controller will only use ldap-s or start-tls to contact the LDAP server.	ldap-s start-tls clear-text	ldap-s
`timeout <seconds>`	Timeout period of a LDAP request, in seconds.	1-30	20 seconds

Usage Guidelines

You configure a server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see “aaa server-group” on page 70).

Example

The following command configures and enables an LDAP server:

```
aaa authentication-server ldap ldap1
   host 10.1.1.243
   base-dn cn=Users,dc=1m,dc=corp,dc=com
```

```
admin-dn cn=corp,cn=Users,dc=1m,dc=corp,dc=com
admin-passwd abc10
key-attribute sAMAccountName
filter (objectclass=*)
enable
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa authentication-server radius

```
aaa authentication-server radius <server>
   acctport <port>
   authport <port>
   clone <server>
   enable
   host <ipaddr>|<FQDN>
   key <psk>
   nas-identifier <string>
   nas-ip <ipaddr>
   no ...
   retransmit <number>
   timeout <seconds>
   use-md5
```

Description

This command configures a RADIUS server.

Syntax

Parameter	Description	Range	Default
`<server>`	Name that identifies the server.	—	—
`acctport <port>`	Accounting port on the server.	1-65535	1813
`authport <port>`	Authentication port on the server	1-65535	1812
`clone <server>`	Name of an existing RADIUS server configuration from which parameter values are copied.	—	—
`enable`	Enables the RADIUS server.		
`host`	Identify the RADIUS server either by its IP address or fully qualified domain name.	—	—
`<ipaddr>`	IP address of the RADIUS server.	—	—
`<FQDN>`	Fully qualified domain name (FQDN) of the RADIUS server. The maximum supported length is 63 characters.	—	—
`key <psk>`	Shared secret between the controller and the authentication server. The maximum length is 128 characters.	—	—
`nas-identifier <string>`	Network Access Server (NAS) identifier to use in RADIUS packets.	—	—
`nas-ip <ip-addr>`	NAS IP address to send in RADIUS packets. You can configure a "global" NAS IP address that the controller uses for communications with all RADIUS servers. If you do not configure a server-specific NAS IP, the global NAS IP is used. To set the global NAS IP, enter the **ip radius nas-ip** *ipaddr* command.	—	—
`no`	Negates any configured parameter.	—	—
`retransmit <number>`	Maximum number of retries sent to the server by the controller before the server is marked as down.	0-3	3
`timeout <seconds>`	Maximum time, in seconds, that the controller waits before timing out the request and resending it.	1-30	5 seconds
`use-md5`	Use MD5 hash of cleartext password.	—	disabled

Usage Guidelines

You configure a server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see "aaa server-group" on page 70).

Example

The following command configures and enables a RADIUS server:

```
aaa authentication-server radius radius1
   host 10.1.1.244
   key qwERtyuIOp
   enable
```

Command History

Version	Modification
ArubaOS 3.0	Command introduced.
ArubaOS 6.0	RADIUS server can be identified by its qualified domain name (FQDN).

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa authentication-server tacacs

```
aaa authentication-server tacacs <server>
   clone <server>
   enable
   host <ipaddr>
   key <psk>
   no ...
   retransmit <number>
   session-authorization
   tcp-port <port>
   timeout <seconds>
```

Description

This command configures a TACACS+ server.

Syntax

Parameter	Description	Range	Default
`<server>`	Name that identifies the server.	—	—
`clone <server>\`	Name of an existing TACACS server configuration from which parameter values are copied.	—	—
`enable`	Enables the TACACS server.	—	
`host <ip-addr>`	IP address of the TACACS server.	—	—
`key`	Shared secret to authenticate communication between the TACACS+ client and server.	—	—
`no`	Negates any configured parameter.	—	—
`retransmit <number>`	Maximum number of times a request is retried.	0-3	3
`session-authorization`	Enables TACACS+ authorization.Session-authorization turns on the optional authorization session for admin users.	—	disabled
`tcp-port <port>`	TCP port used by the server.	1-65535	49
`timeout <timeout>`	Timeout period of a TACACS request, in seconds.	1-30	20 seconds

Usage Guidelines

You configure a server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see “aaa server-group” on page 70).

Example

The following command configures, enables a TACACS+ server and enables session authorization:

```
aaa authentication-server tacacs tacacs1
   clone default
   host 10.1.1.245
   key qwERtyuIOp
   enable
   session-authorization
```

Command History

Version	Description
ArubaOS 3.0	Command introduced.
ArubaOS 6.0	session-authorization parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa authentication-server windows

```
aaa authentication-server windows <windows_server_name>
   clone <source>
   enable
   host <ipaddr>
```

Description

This command configures a windows server for stateful-NTLM authentication.

Syntax

Parameter	Description
`<windows_server_name>`	Name of the windows server. You will use this name when you add the windows server to a server group.
`clone <source>`	Name of a Windows Server from which you want to make a copy.
`enable`	Enables the Windows server.
`host <ipaddr>`	IP address of the Windows server.

Usage Guidelines

You must define a Windows server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see “aaa server-group” on page 70). Windows servers are used for stateful-NTLM authentication.

Example

The following command configures and enables a windows server:

```
aaa authentication-server windows IAS_1
   host 10.1.1.245
   enable
```

Command History

This command was available in ArubaOS 3.4.1

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa bandwidth-contract

```
aaa bandwidth-contract <name> {kbits <kbits>|mbits <mbits>}
```

Description

This command configures a bandwidth contract.

Syntax

Parameter	Description	Range
<name>	Name that identifies this bandwidth contract.	—
kbits <bits>	Limit the traffic rate for this bandwidth contract to a specified number of kilobits per second.	256-2000000
mbits <bits>	Limit the traffic rate for this bandwidth contract to a specified number of megabits per second.	1-2000

Usage Guidelines

You can apply a configured bandwidth contract to a user role or to a VLAN. When you apply a bandwidth contract to a user role (see “user-role” on page 1172), you specify whether the contract applies to upstream traffic (from the client to the controller) or downstream traffic (from the controller to the client). You can also specify whether the contract applies to all users in a specified user role or per-user in a user role.

When you apply a bandwidth contract to a VLAN (see “interface vlan” on page 262), the contract limits multicast traffic and does not affect other data. This is useful because an AP can only send multicast traffic at the rate of the slowest associated client. Thus excessive multicast traffic will fill the buffers of the AP, causing frame loss and poor voice quality. Generally, every system should have a bandwidth contract of 1 Mbps or even 700 Kbps and it should be applied to all VLANs with which users are associated, especially those VLANs that pass through the upstream router. The exception are VLANs that are used for high speed multicasts, where the SSID is configured without low data rates.

Example

The following command creates a bandwidth contract that limits the traffic rate to 1 Mbps:

```
aaa bandwidth-contract mbits 1
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa derivation-rules

```
aaa derivation-rules user <name>
   no ...
   set {role|vlan} condition <rule-type> <condition> <value> set-value {<role>|<vlan>}
   [description <rule description>][position <number>]
```

Description

This command configures rules by which the role or VLAN assigned to a client is derived from the client's association with an AP.

The PEFNG must be installed for a user role to be assigned.

Syntax

Parameter	Description
`<name>`	Name that identifies this set of user derivation rules.
`no`	Negates a configured rule.
`set {role|vlan}`	Specify whether the action of the rule is to set the role or the VLAN.
`condition`	Condition that should be checked to derive role/VLAN
`<rule-type>`	Specify one of the following rule types for this user derivation rule. • **bssid**: BSSID of access point. • **dhcp-option-77**: Enable DHCP packet processing. • **encryption-type**: Encryption method used by station. • **essid**: ESSID of access point. • **location**: user location (ap name). • **macaddr**: MAC address of user.
`<condition>`	Specify one of the following conditions: • **contains**: Check if attribute *contains* the operand value. • **ends-with**: Check if attribute *ends with* the operand value. • **equals**: Check if attribute *equals* the operand value. • **not-equals**: Check if attribute *is not equal* to the operand value. • **starts-with**: Check if attribute *starts with* the operand value.
`set-value <role>|<vlan>`	Specify the user role or VLAN ID to be assigned to the client if the above condition is met.
`description`	Describes the user derivation rule. This parameter is optional and has a 128 character maximum.
`position`	Position of this rule relative to other rules that are configured.

Usage Guidelines

The user role can be derived from attributes from the client's association with an AP. You configure the user role to be derived by specifying condition rules; when a condition is met, the specified user role is assigned to the client. You can specify more than one condition rule; the order of rules is important as the first matching condition is applied. You can also add a description of the rule.

User-derivation rules are executed *before* the client is authenticated.

Example

The following command sets the client's user role to "guest" if the client associates to the "Guest" ESSID. The rule description indicates that is was created for special customers.

```
aaa derivation-rules user derive1
   set role condition essid equals Guest set-value guest description
   createdforspecialcustomers
```

Command History

Version	Description
ArubaOS 3.0	Command introduced.
ArubaOS 6.0	Description parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system. The PEFNG license must be installed for a user role to be assigned.	Config mode on master controllers

aaa dns-query-period

```
aaa dns-query-period <minutes>
```

Description

Configure how often the controller should generate a DNS request to cache the IP address for a RADIUS server identified via its fully qualified domain name (FQDN).

Syntax.

Parameter	Description
<minutes>	Specify, in minutes, the interval between DNS requests sent from the controller to the DNS server. By default, DNS requests are sent every 15 minutes. Range: 1-1440 minutes

Usage Guidelines

If you define a RADIUS server using the FQDN of the server rather than its IP address, the the controller will periodically generate a DNS request and cache the IP address returned in the DNS response. Issue this command to configure the frequency of these requests.

Example

This command configures a DNS query interval of 30 minutes.

```
(host) # aaa dns-query-period 30
```

Related Commands

To view the current DNS query interval, issue the command show aaa dns-query-period.

Command History

This command was available in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on local and master controllers

aaa inservice

```
aaa inservice <server-group> <server>
```

Description

This command designates an “out of service” authentication server to be “in service”.

Syntax

Parameter	Description
<server-group>	Server group to which this server is assigned.
<server>	Name of the configured authentication server.

Usage Guidelines

By default, the controller marks an unresponsive authentication server as “out of service” for a period of 10 minutes (you can set a different time limit with the **aaa timers dead-time** command). The **aaa inservice** command is useful when you become aware that an “out of service” authentication server is again available before the dead-time period has elapsed. (You can use the **aaa test-server** command to test the availability and response of a configured authentication server.)

Example

The following command sets an authentication server to be in service:

```
aaa inservice corp-rad rad1
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa ipv6 user add

```
aaa ipv6 user add <ipv6addr> [authentication-method {dot1x|mac|stateful-
dot1x|vpn|web}][mac <macaddr>] [name <username>]
[profile <aaa-profile>] [role <role>]
```

Description

This command manually assigns a user role or other values to a specified IPv6 client.

Syntax

Parameter	Description
`<ipv6addr>`	IPv6 address of the user to be added.
`authentication-method`	Authentication method for the user.
`dot1x`	802.1x authentication.
`mac`	MAC address of the user.
`stateful-dot1x`	Stateful 802.1x authentication.
`vpn`	VPN authentication
`web`	Captive Portal authentication
`mac <macaddr>`	Name for the user.
`name <username>`	Name for the user.
`profile <aaa-profile>`	AAA profile for the user.
`role <role>`	Role for the user.

Usage Guidelines

This command should only be used for troubleshooting issues with a specific IPv6 client. This command allows you to manually assign a client to a role. For example, you can create a role “debugging” that includes a policy to mirror session packets to a specified destination for further examination, then use this command to assign the “debugging” role to a specific client. Use the **aaa ipv6 user delete** command to remove the client or device from the role.

Note that issuing this command does not affect ongoing sessions that the client may already have. For example, if a client is in the “employee” role when you assign them to the “debugging” role, the client continues any sessions allowed with the “employee” role. Use the **aaa ipv6 user clear-sessions** command to clear ongoing sessions.

Example

The following commands create a role that logs HTTPS traffic, then assign the role to a specific IPv6 client:

```
ipv6 access-list session ipv6-log-https
   any any svc-https permit log
user-role ipv6-web-debug
   session-acl ipv6-log-https
   In enable mode:
aaa ipv6 user add 2002:d81f:f9f0:1000:e409:9331:1d27:ef44 role ipv6-web-debug
```

Command History

This command was available in ArubaOS 3.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa ipv6 user clear-sessions

```
aaa ipv6 user clear-sessions <ipaddr>
```

Description

This command clears ongoing sessions for the specified IPv6 client.

Syntax

Parameter	Description
`<ipaddr>`	IPv6 address of the user.

Usage Guidelines

This command clears any ongoing sessions that the client already had before being assigned a role with the **aaa ipv6 user add** command.

Example

The following command clears ongoing sessions for an IPv6 client:

```
aaa user clear-sessions 2002:d81f:f9f0:1000:e409:9331:1d27:ef44
```

Command History

This command was available in ArubaOS 3.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa ipv6 user delete

```
aaa ipv6 user delete {<ipaddr>|all|mac <macaddr>|name <username>|role <role>}
```

Description

This command deletes IPv6 clients, users, or roles.

Syntax

Parameter	Description
`<ipv6addr>`	IPv6 address of the client to be deleted.
`all`	Deletes all connected IPv6 clients.
`mac`	MAC address of the IPv6 client to be deleted.
`name`	Name of the IPv6 client to be deleted.
`role`	Role of the IPv6 client to be deleted.

Usage Guidelines

This command allows you to manually delete clients, users, or roles. For example, if you used to the **aaa ipv6 user add** command to assign a user role to an IPv6 client, you can use this command to remove the role assignment.

Example

The following command a role:

```
aaa ipv6 user delete role web-debug
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa ipv6 user logout

```
aaa ipv6 user logout <ipaddr>
```

Description

This command logs out an IPv6 client.

Syntax

Parameter	Description
<ipv6addr>	IPv6 address of the client to be logged out.

Usage Guidelines

This command logs out an authenticated IPv6 client. The client must reauthenticate.

Example

The following command logs out an IPv6 client:

```
aaa user logout 2002:d81f:f9f0:1000:e409:9331:1d27:ef44
```

Command History

This command was available in ArubaOS 3.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa password-policy mgmt

```
aaa password-policy mgmt
   enable
   no
   password-lock-out
   password-lock-out-time
   password-max-character-repeat.
   password-min-digit
   password-min-length
   password-min-lowercase-characters
   password-min-special-character
   password-min-uppercase-characters
   password-not-username
```

Description

Define a policy for creating management user passwords.

Syntax

Parameter	Description
`enable`	enable the password management policy
`password-lock-out`	The number of failed attempts within a 3 minute window that causes the user to be locked out for the period of time specified by the password-lock-out-time parameter. Range: 0-10 attempts. By default, the password lockout feature is disabled, and the default value of this parameter is 0 attempts.
`password-lock-out-time`	The number of minutes a user who has exceeded the maximum number of failed password attempts is locked out of the network. After this period has passed, the lockout is cleared without administrator intervention. Range: 1 min to 1440 min (24 hrs). Default: 3. **NOTE:** When a management user gets locked out, that event is logged in the controller log file. The management user lockout warning message can have any one of the following warning IDs. • 125060 = Password policy locked out a management user created via the **mgmt-user** command in the serial console CLI. • 125061 = Password policy locked out a management user created via the WebUI or the **mgmt-user** command in the Telnet/SSH CLI. • 133109 = Password policy locked out a management user created via the **local-userdb** command in the CLI.
`password-max-character-repeat`	The maximum number of consecutive repeating characters allowed in a management user password. Range: 0-10 characters. By default, there is no limitation on the numbers of character that can repeat within a password, and the parameter has a default value of 0 characters.
`password-min-digit`	The minimum number of numeric digits required in a management user password. Range: 0-10 digits. By default, there is no requirement for numerical digits in a password, and the parameter has a default value of 0.
`password-min-length`	The minimum number of characters required for a management user password Range: 6-64 characters. Default: 6.
`password-min-lowercase-characters`	The minimum number of lowercase characters required in a management user password. Range: 0-10 characters. By default, there is no requirement for lowercase letters in a password, and the parameter has a default value of 0.
`password-min-special-character`	The minimum number of special characters required in a management user password. Range: 0-10 characters. By default, there is no requirement for special characters in a password, and the parameter has a default value of 0. See Usage Guidelines below for a list of allowed and disallowed special characters
`password-min-uppercase-characters`	The minimum number of uppercase characters required in a management user password. Range: 0-10 characters. By default, there is no requirement for uppercase letters in a password, and the parameter has a default value of 0.
`password-not-username`	Password cannot be the management users' current username or the username spelled backwards.

Usage Guidelines

By default, the password for a management user has no requirements other than a minimum length of 6 alphanumeric or special characters.You do not need to configure a different management user password policy

unless your company enforces a best practices password policy for management users with root access to network equipment.

The table below lists the special characters allowed and not allowed in any management user password

Allowed Characters	Disallowed Characters
exclamation point: !	Parenthesis: ( )
underscore: _	apostrophe: '
at symbol: @	semi-colon: ;
pound sign: #	dash: -
dollar sign: $	equals sign: =
percent sign: %	slash: /
caret: ^	question mark: ?
ampersand: &	
star: *	
greater and less than symbols: < >	
curled braces: { }	
straight braces: [ ]	
colon :	
period: .	
pipe: |	
plus sign: +	
tilde: ~	
comma: ,	
accent mark: `	

Example

The following command sets a management password policy that requires the password to have a minimum of nine characters, including one numerical digit and one special character:

```
aaa password-policy mgmt
   enable
   password-min-digit 1
   password-min-length 9
   password-min-special-characters 1
```

Related Commands

Command	Description	Mode
`show aaa password-policy mgmt`	Use `show aaa password-policy mgmt` to show the current management password policy	Enable mode

Command History

This command was available in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa profile

```
aaa profile <profile>
   authentication-dot1x <dot1x-profile>
   authentication-mac <mac-profile>
   clone <profile>
   dot1x-default-role <role>
   dot1x-server-group <group>
   initial-role <role>
   mac-default-role <role>
   mac-server-group <group>
   no ...
   radius-accounting <group>
   rfc-3576-server <ipaddr>
   sip-authentication-role <role>
   user-derivation-rules <profile>
   wired-to-wireless-roam
   xml-api-server <ipaddr>
```

Description

This command configures the authentication for a WLAN.

Syntax

Parameter	Description	Default
`<profile>`	Name that identifies this instance of the profile. The name must be 1-63 characters.	"default"
`authentication-dot1x <dot1x-profile>`	Name of the 802.1x authentication profile associated with the WLAN. See "aaa authentication dot1x" on page 17.	—
`authentication-mac <mac-profile>`	Name of the MAC authentication profile associated with the WLAN. See "aaa authentication mac" on page 22.	—
`clone <profile>`	Name of an existing AAA profile configuration from which parameter values are copied.	—
`dot1x-default-role <role>`	Configured role assigned to the client after 802.1x authentication. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role. **NOTE**: This parameter requires the PEFNG license.	guest
`dot1x-server-group <group>`	Name of the server group used for 802.1x authentication. See "aaa server-group" on page 70.	—
`initial-role <role>`	Role for unauthenticated users.	logon
`mac-default-role <role>`	Configured role assigned to the user when the device is MAC authenticated. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role. **NOTE:** This parameter requires the PEFNG license.	guest
`mac-server- <group> group`	Name of the server group used for MAC authentication. See "aaa server-group" on page 70.	—
`no`	Negates any configured parameter.	—
`radius-accounting <group>`	Name of the server group used for RADIUS accounting. See "aaa server-group" on page 70.	—
`rfc-3576-server <ip-addr>`	IP address of a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576, "Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)". See "aaa rfc-3576-server" on page 69. **NOTE**: This parameter requires the PEFNG license.	—
`sip-authentication-role <role>`	Configured role assigned to a session initiation protocol (SIP) client upon registration. **NOTE**: This parameter requires the PEFNG license.	guest
`user-derivation-rules <profile>`	User attribute profile from which the user role or VLAN is derived.	—
`wire-to-wireless-roam`	Keeps user authenticated when roaming from the wired side of the network.	enabled
`xml-api-server <ip-addr>`	IP address of a configured XML API server. See "aaa xml-api" on page 85. **NOTE**: This parameter requires the PEFNG license.	—

Usage Guidelines

The AAA profile defines the user role for unauthenticated users, the default user role for MAC or 802.1x authentication, and user derivation rules. The AAA profile contains the authentication profile and authentication server group.

There are predefined AAA profiles available: default-dot1x, default-mac-auth, and default-open, that have the parameter values shown in the following table.

Parameter	default-dot1x	default-mac-auth	default-open
authentication-dot1x	default	N/A	N/A
authentication-mac	N/A	default	N/A
dot1x-default-role	authenticated	guest	guest
dot1x-server-group	N/A	N/A	N/A
initial-role	logon	logon	logon
mac-default-role	guest	authenticated	guest
mac-server-group	default	default	default
radius-accounting	N/A	N/A	N/A
rfc-3576-server	N/A	N/A	N/A
user-derivation-rules	N/A	N/A	N/A
wired-to-wireless roam	enabled	enabled	enabled

Example

The following command configures an AAA profile that assigns the "employee" role to clients after they are authenticated using the 802.1x server group "radiusnet".

```
aaa profile corpnet
   dot1x-default-role employee
   dot1x-server-group radiusnet
```

Command History

Version	Description
ArubaOS 3.0	Command introduced.
ArubaOS 3.4.1	License requirements changed in ArubaOS 3.4.1, so the **sip-authentication-role** parameter required the Policy Enforcement Firewall license instead of the Voice Services Module license required in earlier versions.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system, except for noted parameters	Config mode on master controllers

aaa query-server

```
aaa query-server <ldap-server-name> <user-name>
```

Description

Troubleshoot an LDAP authentication failure by verifying that the user exists in the ldap server database.

Syntax

Parameter	Description
`<ldap-server-name>`	Name of an LDAP server.
`<user-name>`	Name of a user whose LDAP record you want to view.

Usage Guidelines

If the Admin-DN binds successfully but the wireless user fails to authenticate, issue this command to troubleshoot whether the problem is with the wireless network, the controller, or the ldap server. The **aaa query-user <ldap_server_name> <username>** command to makes the controller send a search query to find the user. If that search fails in spite of the user being in the LDAP database, it is most probable that the base DN where the search was started was not correct. In such case, it is advisable to make the base DN at the root of the ldap tree.

Example

The example below shows part of the output for an LDAP record for the username JDOE.

```
(host) #aaa query-user eng JDOE


objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: John Doe
sn: Doe
userCertificate: 0\202\005\2240\202\004|\240\003\002\001\002\002\012H\011\333K
userCertificate: 0\202\005\2240\202\004|\240\003\002\001\002\002\012]\350\346F
userCertificate: 0\202\005\2240\202\004|\240\003\002\001\002\002\012\023\001\017\240
userCertificate: 0\202\005\2240\202\004|\240\003\002\001\002\002\012\031\224/\030
userCertificate: 0\202\005~0\202\004f\240\003\002\001\002\002\012\031\223\246\022
userCertificate: 0\202\005\2240\202\004|\240\003\002\001\002\002\012\037\177\374\305
givenName: JDE
distinguishedName: CN=John Doe,CN=Users,DC=eng,DC=net
instanceType: 4
whenCreated: 20060516232817.0Z
whenChanged: 20081216223053.0Z
displayName: John Doe
uSNCreated: 24599
memberOf: CN=Cert_Admins,CN=Users,DC=eng,DC=net
memberOf: CN=ATAC,CN=Users,DC=eng,DC=net
uSNChanged: 377560
department: eng
name: John Doe
...
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa radius-attributes

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

Description

This command configures RADIUS attributes for use with server derivation rules.

Syntax

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

Usage Guidelines

Add RADIUS attributes for use in server derivation rules. Use the **show aaa radius-attributes** command to display a list of the current RADIUS attributes recognized by the controller. To add a RADIUS attribute to the list, use the **aaa radius-attributes** command.

Example

The following command adds the VSA "Dell-User-Role":

```
aaa radius-attributes add Dell-User-Role 1 string vendor Dell 14823
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa rfc-3576-server

```
aaa rfc-3576-server <ipaddr>
   clone <server>
   key <psk>
   no ...
```

Description

This command configures a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576, “Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)”.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the server.
`clone <server>`	Name of an existing RFC 3576 server configuration from which parameter values are copied.
`key <psk>`	Shared secret to authenticate communication between the RADIUS client and server.
`no`	Negates any configured parameter.

Usage Guidelines

The server configured with this command is referenced in the AAA profile for the WLAN (see “aaa profile” on page 63).

Example

The following command configures an RFC 3576 server:

```
aaa rfc-3576-server 10.1.1.245
   clone default
   key asdfjkl;
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa server-group

```
aaa server-group <group> allow-fail-through
   auth-server <name> [match-authstring contains|equals|starts-with <string>] [match-
   fqdn <string>] [position <number>] [trim-fqdn]
   clone <group>
   no ...
   set role|vlan condition <attribute> contains|ends-with|equals|not-equals|starts-with
   <string> set-value <set-value-str> [position <number>]
```

Description

This command allows you to add a configured authentication server to an ordered list in a server group, and configure server rules to derive a user role, VLAN ID or VLAN name from attributes returned by the server during authentication.

Syntax

Parameter	Description	Default
<group>	Name that identifies the server group. The name must be 32 characters or less.	—
allow-fail-through	When this option is configured, an authentication failure with the first server in the group causes the controller to attempt authentication with the next server in the list. The controller attempts authentication with each server in the ordered list until either there is a successful authentication or the list of servers in the group is exhausted.	disabled
auth-server <name>	Name of a configured authentication server.	—
match-authstring	This option associates the authentication server with a match rule that the controller can compare with the user/client information in the authentication request. With this option, the user/client information in the authentication request can be in any of the following formats: <domain>\<user> <user>@<domain> host/<pc-name>.<domain> An authentication request is sent to the server only if there is a match between the specified match rule and the user/client information.You can configure multiple match rules for an authentication server.	—
contains	**contains**: The rule matches if the user/client information contains the specified string.	
equals	The rule matches if the user/client information exactly matches the specified string.	
starts-with	The rule matches if the user/client information starts with the specified string.	
match-fqdn <string>	This option associates the authentication server with a specified domain. An authentication request is sent to the server only if there is an exact match between the specified domain and the <domain> portion of the user information sent in the authentication request. With this option, the user information must be in one of the following formats: <domain>\<user> <user>@<domain>	—
position <number>	Position of the server in the server list. 1 is the top.	(last)
trim-fqdn	This option causes the user information in an authentication request to be edited before the request is sent to the server. Specifically, this option: removes the <domain>\ portion for user information in the <domain>\<user> format removes the @<domain> portion for user information in the <user>@<domain> format	—
clone	Name of an existing server group from which parameter values are copied.	—
no	Negates any configured parameter.	—
set role|vlan	Assigns the client a user role, VLAN ID or VLAN name based on attributes returned for the client by the authentication server. Rules are ordered: the first rule that matches the configured condition is applied. VLAN IDs and VLAN names cannot be listed together.	—
condition	Attribute returned by the authentication server.	—
contains	The rule is applied if and only if the attribute value contains the specified string.	—

Parameter	Description	Default
`ends-with`	The rule is applied if and only if the attribute value ends with the specified string.	—
`equals`	The rule is applied if and only if the attribute value equals the specified string.	—
`not-equals`	The rule is applied if and only if the attribute value is not equal to the specified string.	—
`starts-with`	The rule is applied if and only if the attribute value begins with the specified string.	—
`set-value`	User role or VLAN applied to the client when the rule is matched.	—
`value-of`	Sets the user role or VLAN to the value of the attribute returned. The user role or VLAN ID returned as the value of the attribute must already be configured on the controller when the rule is applied.	—

Usage Guidelines

You create a server group for a specific type of authentication or for accounting. The list of servers in a server group is an ordered list, which means that the first server in the group is always used unless it is unavailable (in which case, the next server in the list is used). You can configure servers of different types in a server group, for example, you can include the internal database as a backup to a RADIUS server. You can add the same server to multiple server groups. There is a predefined server group “internal” that contains the internal database.

Example

The following command configures a server group “corp-servers” with a RADIUS server as the main authentication server and the internal database as the backup. The command also sets the client’s user role to the value of the returned “Class” attribute.

```
aaa server-group corp-servers
   auth-server radius1 position 1
   auth-server internal position 2
   set role condition Class value-of
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa sygate-on-demand

```
aaa sygate-on-demand remediation-failure-role <role>
```

Description

This command configures the user role assigned to clients that fail Sygate On-Demand Agent (SODA) remediation.

Syntax

Parameter	Description	Default
`<role>`	User role assigned to the client upon failure of client remediation.	guest

Usage Guidelines

When you enable SODA client remediation in a captive portal profile, you can specify a user role to clients that fail the remediation. The default role for such clients is the guest role.

Example

The following command assigns the logon role to users who fail remediation:

```
aaa sygate-on-demand remediation-failure-role logon
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Client Integrity Module license	Config mode on master controllers

aaa tacacs-accounting

```
aaa tacacs-accounting server-group <group> [command {action|all|configuration|show}]
[mode {enable|disable}]
```

Description

This command configures reporting of commands issued on the controller to a TACACS+ server group.

Syntax

Parameter	Description	Range	Default
`server-group <group>`	The TACACS server group to which the reporting is sent.	—	—
`command`	The types of commands that are reported to the TACACS server group.	—	—
`action`	Reports action commands only.	—	—
`all`	Reports all commands.	—	—
`configuration`	Reports configuration commands only	—	—
`show`	Reports show commands only	—	—
`mode`	Enables accounting for the server group.	enable/ disable	disabled

Usage Guidelines

You must have previously configured the TACACS+ server and server group (see "aaa authentication-server tacacs" on page 46 and "aaa server-group" on page 70).

Example

The following command enables accounting and reporting of configuration commands to the server-group "tacacs1":

```
aaa tacacs-accounting server-group tacacs1 mode enable command configuration
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa test-server

```
aaa test-server {mschapv2|pap} <server> <username> <passwd>
```

Description

This command tests a configured authentication server.

Syntax

Parameter	Description
`mschapv2`	Use MSCHAPv2 authentication protocol.
`pap`	Use PAP authentication protocol.
`<server>`	Name of the configured authentication server.
`<username>`	Username to use to test the authentication server.
`<passwd>`	Password to use to test the authentication server.

Usage Guidelines

This command allows you to check a configured RADIUS authentication server or the internal database. You can use this command to check for an “out of service” RADIUS server.

Example

The following commands adds a user in the internal database and verifies the configuration:

```
local-userdb add kgreen lkjHGfds
aaa test-server pap internal kgreen lkjHGfds

Authentication successful
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa timers

```
aaa timers {dead-time <minutes>|idle-timeout <number>|logon-lifetime <0-255>}
```

Description

This command configures the timers that you can apply to clients and servers.

Syntax

Parameter	Description	Range	Default
`dead-time <minutes>`	Maximum period, in minutes, that the controller considers an unresponsive authentication server to be "out of service". This timer is only applicable if there are two or more authentication servers configured on the controller. If there is only one authentication server configured, the server is never considered out of service and all requests are sent to the server. If one or more backup servers are configured and a server is unresponsive, it is marked as out of service for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as down for the dead time.	0-50	10 minutes
`idle-timeout <1-15300>`	Maximum number of minutes after which a client is considered idle if there is no user traffic from the client. The timeout period is reset if there is a user traffic. After this timeout period has elapsed, the controller sends probe packets to the client; if the client responds to the probe, it is considered active and the User Idle Timeout is reset (an active client that is not initiating new sessions is not removed). If the client does not respond to the probe, it is removed from the system. If the keyword **seconds** is not specified, the value defaults to minutes.	1 to 255 minutes (30 to 15300 seconds)	5 minutes (300 seconds)
`logon-lifetime`	Maximum time, in minutes, that unauthenticated clients are allowed to remain logged on.	0-255	5 minutes

Usage Guidelines

These parameters can be left at their default values for most implementations.

Example

The following command changes the idle time to 10 minutes:

```
aaa timers idle-timeout 10
```

Related Commands

```
(host) (config) #show aaa timers
(host) (config) #show datapath user table
```

Command History

Version	Description
ArubaOS 3.0	available in ArubaOS 3.0
ArubaOS 3.4.	Idle timeout values and defaults changed

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa trusted-ap

```
aaa trusted-ap <macaddr>
```

Description

This command configures a trusted non-Dell AP.

Syntax

Parameter	Description
<macaddr>	MAC address of the AP

Usage Guidelines

This command configures a non-Dell AP as a trusted AP.

Example

The following configures a trusted non-Dell AP:

```
aaa trusted-ap 00:40:96:4d:07:6e
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa user add

```
aaa user add <ipaddr> [<number>] [authentication-method {dot1x|mac|stateful-dot1x|vpn|
 web}] [mac <macaddr>] [name <username>] [profile <aaa_profile>] [role <role>]
```

Description

This command manually assigns a user role or other values to a specified client or device.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the user to be added.
`<number>`	Number of users to create starting with <ipaddr>.
`authentication-method`	Authentication method for the user.
`dot1x`	802.1x authentication.
`mac`	MAC authentication.
`stateful-dot1x`	Stateful 802.1x authentication.
`vpn`	VPN authentication.
`web`	Captive portal authentication.
`mac <macaddr>`	MAC address of the user.
`name <username>`	Name for the user.
`profile <aaa_profile>`	AAA profile for the user.
`role <role>`	Role for the user.

Usage Guidelines

This command should only be used for troubleshooting issues with a specific client or device. This command allows you to manually assign a client or device to a role. For example, you can create a role “debugging” that includes a policy to mirror session packets to a specified destination for further examination, then use this command to assign the “debugging” role to a specific client. Use the **aaa user delete** command to remove the client or device from the role.

Note that issuing this command does not affect ongoing sessions that the client may already have. For example, if a client is in the “employee” role when you assign them to the “debugging” role, the client continues any sessions allowed with the “employee” role. Use the **aaa user clear-sessions** command to clear ongoing sessions.

Example

The following commands create a role that logs HTTPS traffic, then assign the role to a specific client:

```
ip access-list session log-https
   any any svc-https permit log
user-role web-debug
   session-acl log-https
```

In enable mode:

```
aaa user add 10.1.1.236 role web-debug
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa user clear-sessions

```
aaa user clear-sessions <ipaddr>
```

Description

This command clears ongoing sessions for the specified client.

Syntax

Parameter	Description
`<ip-addr>`	IP address of the user.

Usage Guidelines

This command clears any ongoing sessions that the client already had before being assigned a role with the **aaa user add** command.

Example

The following command clears ongoing sessions for a client:

```
aaa user clear-sessions 10.1.1.236
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa user delete

```
aaa user delete {<ipaddr>|all|mac <macaddr>|name <username>|role <role>}
```

Description

This command deletes clients, users, or roles.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the client to be deleted.
`all`	Deletes all connected clients.
`mac`	MAC address of the client to be deleted.
`name`	Name of the client to be deleted.
`role`	Role of the client to be deleted.

Usage Guidelines

This command allows you to manually delete clients, users, or roles. For example, if you used to the **aaa user add** command to assign a user role to a client, you can use this command to remove the role assignment.

Example

The following command a role:

```
aaa user delete role web-debug
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa user fast-age

```
aaa user fast-age
```

Description

This command enables fast aging of user table entries.

Syntax

No parameters.

Usage Guidelines

When this feature is enabled, the controller actively sends probe packets to all users with the same MAC address but different IP addresses. The users that fail to respond are purged from the system. This command enables quick detection of multiple instances of the same MAC address in the user table and removal of an “old” IP address. This can occur when a client (or an AP connected to an untrusted port on the controller) changes its IP address.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

aaa user logout

```
aaa user logout <ipaddr>
```

Description

This command logs out a client.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the client to be logged out.

Usage Guidelines

This command logs out an authenticated client. The client must reauthenticate.

Example

The following command logs out a client:

```
aaa user logout 10.1.1.236
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

aaa xml-api

```
aaa xml-api server <ipaddr>
   clone <server>
   key <key>
   no ...
```

Description

This command configures an external XML API server.

Syntax

Parameter	Description
`server`	IP address of the external XML API server.
`clone`	Name of an existing XML API server configuration from which parameter values are copied.
`key`	Preshared key to authenticate communication between the controller and the XML API server.
`no`	Negates any configured parameter.

Usage Guidelines

XML API is used for authentication and subscriber management from external agents. This command configures an external XML API server. For example, an XML API server can send a blacklist request for a client to the controller. The server configured with this command is referenced in the AAA profile for the WLAN (see “aaa profile” on page 63). Contact your Dell representative for more information about using the XML API.

Example

The following configures an XML API server:

```
aaa xml-api server 10.210.1.245
   key qwerTYuiOP
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config mode on master controllers

acceleration

```
aaa authentication
acceleration head-end ip-address <ip-address>
```

Description

This command configures a RAP for the Application Acceleration module. The Application Acceleration module improves application performance.

Syntax

Parameter	Description	Range	Default
`head-end`	Configures the head-end device. The head-end device is the Application Acceleration server.	—	—
`ip-address <ip-address>`	The IP address of the Application Acceleration server (head-end) device.	—	—

Usage Guidelines

Configure the head-end device on the RAP by entering the device's IP address. The head-end device is the Application Acceleration server (AAS). You need to install and configure the Application Acceleration server before you can configure the RAP.

Refer to the *ArubaOS Application Acceleration Server Installation and Quick Start Guide* and the *ArubaOS Application Acceleration Module 1.0 Administration Guide* for detailed information about configuring this server.

Example

This example configures the RAP so that it intercepts the client request and forwards it to the head-end device (AAS).

`(host)(config)#` acceleration head-end ip-address 10.1.22.200

Related Commands

View acceleration statistics using the command `show acceleration`.

Command History

Release	Modification
ArubaOS 5.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Application-Acceleration license	Config mode on master controllers

adp

```
adp discovery {disable|enable} igmp-join {disable|enable} igmp-vlan <vlan>
```

Description

This command configures the Dell Discovery Protocol (ADP).

Syntax

Parameter	Description	Range	Default
`discovery`	Enables or disables ADP on the controller.	enabled/ disabled	enabled
`igmp-join`	Enables or disables sending of Internet Group Management Protocol (IGMP) join requests from the controllers.	enabled/ disabled	enabled
`igmp-vlan`	VLAN to which IGMP reports are sent.	—	0 (default route VLAN used)

Usage Guidelines

Dell APs send out periodic multicast and broadcast queries to locate the master controller. If the APs are in the same broadcast domain as the master controller and ADP is enabled on the controller, the controller automatically responds to the APs' queries with its IP address. If the APs are not in the same broadcast domain as the master controller, you need to enable multicast on the network. You also need to make sure that all routers are configured to listen for IGMP join requests from the controller and can route the multicast packets. Use the **show adp config** command to verify that ADP and IGMP join options are enabled on the controller.

Example

The following example enables ADP and the sending of IGMP join requests on the controller:

```
adp discovery enable igmp-join enable
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

am

```
am scan <ipaddr> <channel> [bssid <bssid>]
am test <ipaddr> {suspect-rap bssid <bssid> match-type <match-type> match-method
<method>|wired-mac {add|remove {bssid <bssid>|enet-mac <enet-mac>} mac <mac>}
```

Description

These commands enable channel scanning or testing for the specified air monitor.

Syntax

Parameter	Description	Range
`scan`	IP address of the air monitor to be scanned.	—
`<channel>`	Channel to which the scanning is tuned. Set to 0 to enable scanning of all channels.	—
`bssid`	BSSID of the air monitor.	—
`test`	IP address of the air monitor to be tested.	—
`suspect-rap`	Tests suspect-rap feature.	—
`match-type`	Match type.	eth-wm | ap-wm | eth-gw-wm
`match-method`	Match method.	equal | plus-one | minus-one
`wired-mac`	Tests the rogue AP classification feature. Specifies the Wired MAC table.	—
`enet-mac`	Specifies the Ethernet MAC table.	—
`mac`	Specifies the MAC entry to add/remove from either the Wired MAC table or the Ethernet MAC table.	—

Usage Guidelines

These commands are intended to be used with an Dell AP that is configured as an air monitor. You should not use the **am test** command unless instructed to do so by an Dell representative.

Example

The following command sets the air monitor to scan all channels:

```
(host) (config) #am scan 10.1.1.244 0
```

Command History:

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3.1	Support for the **wired-mac** and **associated** parameters was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

ap authorization-profile

```
ap authorization-profile <profile>
   authorization-group <profile>
```

Description

This command defines a temporary configuration profile for remote APs that are not yet authorized on the network.

Syntax

Parameter	Description	Range	Default
`authorization-profile <profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`authorization-group <profile>`	Name of a configuration profile to be assigned to the group unauthorized remote APs.	—	"NoAuthAp Group"

Usage Guidelines

The AP authorization-profile specifies which configuration should be assigned to a remote AP that has been provisioned but not yet authenticated at the remote site. By default, these yet-unauthorized APs are put into the temporary AP group **authorization-group** and assigned the predefined profile **NoAuthApGroup**. This configuration allows a user to connect to an unauthorized remote AP via a wired port then enter a corporate username and password. Once a valid user has authorized the remote AP, the AP will be permanently marked as authorized on the network and will will then download the configuration assigned to that AP by it's permanent AP group.

Example

The following command creates a new authorization profile with a non-default configuration for unauthorized remote APs:

```
ap authorization-profile default2
   authorization-group NoAuthApGroup2
```

Command History

Release	Modification
ArubaOS 5.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master or local controllers

ap enet-link-profile

```
ap enet-link-profile <profile>
   clone <profile>
   duplex {auto|full|half}
   no ...
   speed {10|100|1000|auto}
```

Description

This command configures an AP Ethernet link profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing Ethernet Link profile from which parameter values are copied.	—	—
`duplex`	The duplex mode of the Ethernet interface, either full, half, or auto-negotiated.	full/half/auto	auto
`no`	Negates any configured parameter.	—	—
`speed`	The speed of the Ethernet interface, either 10 Mbps, 100 Mbps, 1000 Mbps (1 Gbps), or auto-negotiated.	10/100/1000/auto	auto

Usage Guidelines

This command configures the duplex and speed of the Ethernet port on the AP. The configurable speed is dependent on the port type.

Example

The following command configures the Ethernet link profile for full-duplex and 100 Mbps:

```
ap enet-link-profile enet
   duplex full
   speed 100
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3	Support for 1000 Mbps (1 Gbps) Ethernet port speed was introduced.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master controllers

ap mesh-cluster-profile

```
ap mesh-cluster-profile <profile>
   clone <profile>
   cluster <name>
   no ...
   opmode [opensystem | wpa2-psk-aes]
   rf-band {a | g}
   wpa-hexkey <wpa-hexkey>
   wpa-passphrase <wpa-passphrase>
```

Description

This command configures a mesh cluster profile used by mesh nodes.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”
`clone`	Name of an existing mesh cluster profile from which parameter values are copied.	—	—
`cluster`	Indicates the mesh cluster name. The name can have a maximum of 32 characters, and is used as the MSSID for the mesh cluster. When you first create a new mesh cluster profile, the profile uses the default cluster name “Dell-mesh”. Use the **cluster** parameter to define a new, unique MSSID before you assign APs or AP groups to the mesh cluster profile. **NOTE:** If you want a mesh cluster to use WPA2-PSK-AES encryption, *do not use spaces in the mesh cluster name*, as this may cause errors in mesh points associated with that mesh cluster. To view existing mesh cluster profiles, use the CLI command show ap mesh-cluster-profile.	—	“Dell-mesh”
`no`	Negates any configured parameter.	—	—
`opmode`	Configures one of the following types of data encryption. • **opensystem**—No authentication or encryption. • **wpa2-psk-aes**—WPA2 with AES encryption using a pershared key. Best practices are to select wpa2-psk-aes and use the **wpa-passphrase** parameter to select a passphrase. Keep the passphrase in a safe place.	opensystem wpa2-psk-aes	opensystem
`rf-band`	Configures the RF band in which multiband mesh nodes should operate: a = 5 GHz g = 2.4 GHz Best practices are to use 802.11a radios for mesh deployments.	a g	a
`wpa-hexkey`	Configures a WPA pre-shared key.	—	—
`wpa-passphrase`	Sets the WPA password that generates the PSK.	—	—

Usage Guidelines

Mesh cluster profiles are specific to mesh nodes (APs configured for mesh) and provide the framework of the mesh network. You must define and configure the mesh cluster profile before configuring an AP to operate as a mesh node.

You can configure multiple mesh cluster profiles to be used within a mesh cluster. You must configure different priority levels for each mesh cluster profile. See “ap-group” on page 125 or “ap-name” on page 128 for more information about priorities.

Cluster profiles, including the “default” profile, are not applied until you provision your APs for mesh.

Example

The following command configures a mesh cluster profile named “cluster1” for the mesh cluster “headquarters:”

```
ap mesh-cluster-profile cluster1
   cluster headquarters
```

Related Commands

To view a complete list of mesh cluster profiles and their status, use the following command:

```
show ap mesh-cluster-profile
```

To view the settings of a specific mesh cluster profile, use the following command:

show ap mesh-cluster-profile <name>

Command History

This command was introduced in ArubaOS 3.2.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on master controllers

ap mesh-ht-ssid-profile

```
ap mesh-ht-ssid-profile <profile-name>
   clone <source>
   40MHz-enable
   high-throughput-enable
   legacy-stations
   max-rx-a-mpdu-size
   max-tx-a-mpdu-size
   min-mpdu-start-spacing
   mpdu-agg
   no
   short-guard-intvl-40Mhz
   supported-mcs-set
```

Description

This command configures a mesh high-throughput SSID profile used by mesh nodes.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Enter the name of an existing mesh high-throughput SSID profile to modify that profile, or enter a new name or create a new mesh high-throughput profile. The mesh high-throughput profile can have a maximum of 32 characters. To view existing high-throughput SSID radio profiles, use the command **show ap mesh-radio-profile**.		default
`clone <source>`	Copy configuration information from a source profile into the currently selected profile		
`40MHz-enable`	Enable or disable the use of 40 MHz channels. This parameter is enabled by default.		enabled
`high-throughput-enable`	Enable or disable high-throughput (802.11n) features on this SSID. This parameter is enabled by default.		enabled
`legacy-stations`	Allow or disallow associations from legacy (non-HT) stations. By default, this parameter is enabled (legacy stations are allowed).		enabled
`mpdu-agg`	Enable or disable MAC protocol data unit (MPDU) aggregation. High-throughput mesh APs are able to send aggregated MAC protocol data units (MDPUs), which allow an AP to receive a single block acknowledgment instead of multiple ACK signals. This option, which is enabled by default, reduces network traffic overhead by effectively eliminating the need to initiate a new transfer for every MPDU.		enabled
`max-tx-a-mpdu-size`	Maximum size of a transmitted aggregate MPDU, in bytes.	1576 -65535	65535 bytes
`max-rx-a-mpdu-size`	Maximum size of a received aggregate MPDU, in bytes.	8191, 16383, 32767, 65535	65535 bytes
`min-mpdu-start-spacing`	Minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds.	0 (No restriction on MDPU start spacing), .25 µsec, .5 µsec, 1 µsec, 2 µsec, 4 µsec	0 usec
`supported-mcs-set`	A list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20MHz vs. 40MHz) and the number of spatial streams used by the mesh node. The default value is 1-15; the complete set of supported values. To specify a smaller range of values, enter a hyphen between the lower and upper values. To specify a series of different values, separate each value with a comma. Examples: 2-10 1,3,6,9,12 Range: 0-15.	1-15	1-15

Parameter	Description	Range	Default
`short-guard-intvl-40Mhz`	Enable or disable use of short (400ns) guard interval in 40 MHz mode. A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput. This parameter is enabled by default.		enabled

Guidelines

The mesh high-throughput profile defines settings unique to 802.11n-capable, high-throughput APs. If none of the APs in your mesh deployment are 802.11n-capable APs, you do not need to configure a high-throughput SSID profile.

If you modify a currently provisioned and running high-throughput SSID profile, your changes take affect immediately. You do not reboot the controller or the AP.

Example

The following command configures a mesh high-throughput SSID profile named “HT1” and sets some non-default settings for MAC protocol data unit (MPDU) aggregation:

```
(host) (config) #ap mesh-ht-ssid-profile HT1
   max-rx-a-mpdu-size 32767
   max-tx-a-mpdu-size 32767
   min-mpdu-start-spacing .25
```

Related Commands

To view a complete list of mesh high-throughput SSID profiles and their status, use the following command:

```
(host) (config) #show ap mesh-ht-ssid-profile
```

To view the settings of a specific mesh radio profile, use the following command:

(host) (config) #show ap mesh-ht-ssid-profile <name>

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

ap mesh-radio-profile

```
ap mesh-radio-profile <profile>
   a-tx rates [6|9|12|18|24|36|48|54]
   allowed-vlans <vlan-list>
   children <children>
   clone <profile>
   g-tx rates [1|2|5|6|9|11|12|18|24|36|48|54]
   heartbeat-threshold <count>
   hop-count <hop-count>
   link-threshold <count>
   mesh-ht-ssid-profile
   max-retries <max-retries>
   mesh-mcast-opt
   metric-algorithm {best-link-rssi|distributed-tree-rssi}
   mpv <vlan-id>
   no ...
   reselection-mode {reselect-anytime|reselect-never|startup-subthreshold|
      subthreshold-only}
   rts-threshold <rts-threshold>
```

Description

This command configures a mesh radio profile used by mesh nodes.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`allowed-vlans`	Specify a list of VLAN IDs that can be used by a mesh link on APs associated with this mesh radio profile		
`<vlan-list>`	A comma-separated list of VLAN IDs. You can also specify a range of VLAN IDs using a dash (for example, 1–4095)		
`a-tx rates`	Indicates the transmit rates for the 802.11a radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
`children`	Indicates the maximum number of children a mesh node can accept.	1-64	64
`clone`	Name of an existing mesh radio profile from which parameter values are copied.	—	—
`g-tx rates`	Indicates the transmit rates for the 802.11b/g radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
`heartbeat-threshold`	Indicates the maximum number of heartbeat messages that can be lost between neighboring mesh nodes.	1-255	10
`hop-count`	Indicates the maximum hop count from the mesh portal.	1-32	8
`link-threshold`	Indicates the minimal RSSI value. If the RSSI value is below this threshold, the link may be considered a sub-threshold link. A sub-threshold link is a link whose average RSSI value falls below the configured threshold. If this occurs, the mesh node may try to find a better link on the same channel and cluster (only neighbors on the same channel are considered). The supported threshold is hardware dependent, with a practical range of 10-90.	hardware dependent	12
`mesh-ht-ssid-profile`	High-throughput SSID Profile for the mesh feature.		default
`max-retries`	Maximum number of times a mesh node can re-send a packet.	0-15	4 times
`mesh-mcast-opt`	Enables or disables scanning of all active stations currently associated to a mesh point to select the lowest transmission rate based on the slowest connected mesh child. When enabled, this setting dynamically adjusts the multicast rate to that of the slowest connected mesh child. Multicast frames are not sent if there are no mesh children. Best practices are to use the default value.		enabled
`metric-algorithm`	Specifies the algorithm used by a mesh node to select its parent. Best practices are to use the default value distributed-tree-rssi.	—	distributed-tree-rssi
`best-link-rssi`	Selects the parent with the strongest RSSI, regardless of the number of children a potential parent has.	—	—

Parameter	Description	Range	Default
`distributed-tree-rssi`	Selects the parent based on link-RSSI and node cost based on the number of children. This option evenly distributes the mesh points over high quality uplinks. Low quality uplinks are selected as a last resort.	—	—
`mpv`	This parameter is experimental and reserved for future use.	0-4094	0 (disabled)
`no`	Negates any configured parameter.	—	—
`reselection-mode`	Specifies the method used to find a better mesh link. Best practices are to use the default value startup-subthreshold.	(see below)	startup-sub threshold
`reselect-anytime`	Mesh points using the **reselect-anytime** reselection mode perform a single topology readjustment scan within 9 minutes of startup and 4 minutes after a link is formed. If no better parent is found, the mesh point returns to its original parent. This initial scan evaluates more distant mesh points before closer mesh points, and incurs a dropout of 5-8 seconds for each mesh point. After the initial startup scan is completed, connected mesh nodes evaluate mesh links every 30 seconds. If a mesh node finds a better uplink, the mesh node connects to the new parent to create an improved path to the mesh portal.	—	—
`reselect-never`	Connected mesh nodes do not evaluate other mesh links to create an improved path to the mesh portal.	—	—
`startup-subthreshold`	Mesh points using the **startup-subthreshold** reselection mode perform a single topology readjustment scan within 9 minutes of startup and 4 minutes after a link is formed. If no better parent is found, the mesh point returns to its original parent. This initial startup scan evaluates more distant mesh points before closer mesh points, and incurs a dropout of 5-8 seconds for each mesh point. After that time, each mesh node evaluates alternative links if the existing uplink falls below the configured threshold level (the link becomes a sub-threshold link). Best practices are to use the default **startup-subthreshold** value. **NOTE:** Starting with ArubaOS 3.4.1, if a mesh point using the **startup-subthreshold** mode reselects a more distant parent because its original, closer parent falls below the acceptable threshold, then as long as that mesh point is connected to that more distant parent, it will seek to reselect a parent at the earlier distance (or less) with good link quality. For example, if a mesh point disconnects from a mesh parent 2 hops away and subsequently reconnects to a mesh parent 3 hops away, then the mesh point will continue to seek a connection to a mesh parent with both an acceptable link quality and a distance of two hops or less, even if the more distant parent also has an acceptable link quality.	—	—

Parameter	Description	Range	Default
`subthreshold-only`	Connected mesh nodes evaluate alternative links only if the existing uplink becomes a sub-threshold link. **NOTE:** Starting with ArubaOS 3.4.1, if a mesh point using the **subthreshold-only** mode reselects a more distant parent because its original, closer parent falls below the acceptable threshold, then as long as that mesh point is connected to that more distant parent, it will seek to reselect a parent at the earlier distance (or less) with good link quality. For example, if a mesh point disconnects from a mesh parent 2 hops away and subsequently reconnects to a mesh parent 3 hops away, then the mesh point will continue to seek a connection to a mesh parent with both an acceptable link quality and a distance of two hops or less, even if the more distant parent also has an acceptable link quality.	—	—
`rts-threshold`	Defines the packet size sent by mesh nodes. Mesh nodes transmitting frames larger than this threshold must issue request to send (RTS) and wait for other mesh nodes to respond with clear to send (CTS) to begin transmission. This helps prevent mid-air collisions.	256-2,346	2,333 bytes

Usage Guidelines

Mesh radio profiles are specific to mesh nodes (APs configured for mesh) and determine the radio frequency/ channel used by mesh nodes to establish mesh links and the path to the mesh portal. You can configure multiple radio profiles; however, you select and deploy only one radio profile per mesh cluster.

Radio profiles, including the "default" profile, are not active until you provision your APs for mesh. If you modify a currently provisioned and running radio profile, your changes take place immediately. You do not reboot the controller or the AP.

Example

The following command creates a mesh radio profile named "radio2" and associates a mesh high-throughput profile named meshHT1:

```
(host) (config) #ap mesh-radio-profile radio2
   mesh-ht-ssid-profile meshHT1
```

Related Commands

To view a complete list of mesh radio profiles and their status, use the following command:

```
(host) (config) #show ap mesh-radio-profile
```

To view the settings of a specific mesh radio profile, use the following command:

```
(host) (config) #show ap mesh-radio-profile <name>
```

Command History

Release	Modification
ArubaOS 3.2	Command introduced.
ArubaOS 3.2.0.x, 3.3.1.x	The **tx-power** default increased from 14 to 30 dBm.
ArubaOS 3.3	The **heartbeat-threshold** default increased from 5 to 10 heartbeat messages.
ArubaOS 3.3.2	The **mesh-mcast-opt** parameter was introduced.
ArubaOS 3.4	The **mesh-ht-ssid-profile** parameter was introduced The **11a-portal-channel**, **11g-portal-channel**, **beacon-period** and **tx-power** parameters were deprecated. These settings can now be configured via the **rf dot11a-radio-profile and rf dot11g-radio-profile** commands.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

ap provisioning-profile

```
ap provisioning-profile
   clone <source>
   domain-name <name>
   link-priority-cellular <link-priority-cellular>
   link-priority-ethernet <link-priority-ethernet>
   master clear|{set <masterstr>}}
   no ...
   pppoe-passwd <string>
   pppoe-service-name <name>
   pppoe-user <name>
   remote-ap
   reprovision
   usb-dev <usb-dev>
   usb-dial <usb-dial>
   usb-init <usb-init>
   usb-passwd <usb-passwd>
   usb-tty <usb-tty>
   usb-type <usb-type>
   usb-user <usb-user>
```

Description

This command defines a provisioning profile for an AP or group of APs.

Syntax

Parameter	Description	Range	Default
`clone <source>`	Clone an existing ap provisioning profile	—	—
`domain-name`	Domain name for the AP or AP group.	—	—
`link-priority-cellular <link-priority-cellular>`	Set the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary controller link.	0-255	0
`link-priority-ethernet <link-priority-ethernet>`	Set the priority of the wired uplink. Each uplink type has an associated priority; wired ports having the highest priority by default.	0-255	0
`master`	Change the FQDN or IP address for the master controller.	—	—
`set <masterstr>`	Specify the or IP address or FQDN for the master controller.	—	—
`clear`	Clear the definition for the master controller in this profile.	—	—
`no`	Negates any configured parameter.	—	—
`pppoe-passwd`	Point-to-Point Protocol over Ethernet (PPPoE) password for the AP.	—	—
`pppoe-service-name`	PPPoE service name for the AP.	—	—
`pppoe-user`	PPPoE username for the AP.	—	—
`remote-ap`	Specifies that the profile is to be associated with a remote AP using certificates.	—	—
`reprovision`	Provisions one or more APs with the values in the provisioning profile.	—	—
`reset-bootinfo`	Restores factory default provisioning parameters to the specified AP. **NOTE:** This parameter can only be used on the master controller.	—	—
`usb-dev`	The USB device identifier.		
`usb-dial`	The dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.		
`usb-init`	The initialization string for the USB modem. This parameter only needs to be specified if the default string is not correct.		
`usb-passwd`	A PPP password, if provided by the cellular service provider		
`usb-tty`	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.		
`usb-type`	The USB driver type.		
`usb-user`	The PPP username provided by the cellular service provider		

Usage Guidelines

The AP provisioning profile allows you to define a set of provisioning parameters to an AP group. These settings

can be saved or assigned to an AP group via the command **ap-group <group> provisioning-profile <profile>**.

Related Commands

Command	Description
`provision-ap`	Change provisioning parameters for an individual AP. This command does not save the provisioning parameters settings in a reusable profile.

Example

The following commands create a provisioning profile named **profile_branch**, in which the cellular link is the primary uplink because it has a higher priority than the ethernet link:

```
(host) (config) #ap provision-profile profile_branch
   link-priority-cellular 2
   link-priority-ethernet 1
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4	The **link-priority-cellular** and **link-priority-ethernet** parameters introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

ap provisioning-profile

```
ap provisioning-profile
   clone <source>
   domain-name <name>
   link-priority-cellular <link-priority-cellular>
   link-priority-ethernet <link-priority-ethernet>
   master clear|{set <masterstr>}}
   no ...
   pppoe-passwd <string>
   pppoe-service-name <name>
   pppoe-user <name>
   remote-ap
   reprovision
   usb-dev <usb-dev>
   usb-dial <usb-dial>
   usb-init <usb-init>
   usb-passwd <usb-passwd>
   usb-tty <usb-tty>
   usb-type <usb-type>
   usb-user <usb-user>
```

Description

This command defines a provisioning profile for an AP or group of APs.

Syntax

Parameter	Description	Range	Default
`clone <source>`	Clone an existing ap provisioning profile	—	—
`domain-name`	Domain name for the AP or AP group.	—	—
`link-priority-cellular <link-priority-cellular>`	Set the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary controller link.	0-255	0
`link-priority-ethernet <link-priority-ethernet>`	Set the priority of the wired uplink. Each uplink type has an associated priority; wired ports having the highest priority by default.	0-255	0
`master`	Change the FQDN or IP address for the master controller.	—	—
`set <masterstr>`	Specify the or IP address or FQDN for the master controller.	—	—
`clear`	Clear the definition for the master controller in this profile.	—	—
`no`	Negates any configured parameter.	—	—
`pppoe-passwd`	Point-to-Point Protocol over Ethernet (PPPoE) password for the AP.	—	—
`pppoe-service-name`	PPPoE service name for the AP.	—	—
`pppoe-user`	PPPoE username for the AP.	—	—
`remote-ap`	Specifies that the profile is to be associated with a remote AP using certificates.	—	—
`reprovision`	Provisions one or more APs with the values in the provisioning profile.	—	—
`reset-bootinfo`	Restores factory default provisioning parameters to the specified AP. **NOTE:** This parameter can only be used on the master controller.	—	—
`usb-dev`	The USB device identifier.		
`usb-dial`	The dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.		
`usb-init`	The initialization string for the USB modem. This parameter only needs to be specified if the default string is not correct.		
`usb-passwd`	A PPP password, if provided by the cellular service provider.		
`usb-tty`	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.		
`usb-type`	The USB driver type.		
`usb-user`	The PPP username provided by the cellular service provider.		

Usage Guidelines

The AP provisioning profile allows you to define a set of provisioning parameters to an AP group. These settings can be saved or assigned to an AP group via the command **ap-group <group> provisioning-profile <profile>**.

Related Commands

Command	Description
provision-ap	Change provisioning parameters for an individual AP. This command does not save the provisioning parameters settings in a reusable profile.

Example

The following commands create a provisioning profile named **profile_branch**, in which the cellular link is the primary uplink because it has a higher priority than the ethernet link:

```
(host) (config) #ap provision-profile profile_branch
   link-priority-cellular 2
   link-priority-ethernet 1
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4	The **link-priority-cellular** and **link-priority-ethernet** parameters introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

ap regulatory-domain-profile

```
ap regulatory-domain-profile <profile>
   clone <profile>
   country-code <code>
   no ...
   valid-11a-40mhz-channel-pair <valid-11a-40mhz-channel-pair>
   valid-11a-channel <num>
   valid-11g-40mhz-channel-pair <valid-11g-40mhz-channel-pair>
   valid-11g-channel <num>
```

Description

This command configures an AP regulatory domain profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	—
`clone`	Name of an existing regulatory domain profile from which parameter values are copied.	—	—
`country-code`	Code that represents the country in which the APs will operate. The country code determines the 802.11 wireless transmission spectrum. Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions for operators of wireless networks with devices set to improper country codes.	—	country code configured on the master controller during initial setup
`no`	Negates any configured parameter.	—	—
`valid-11a-40mhz-channel-pair`	Specify a channel pair valid for 40 MHz operation in the 802.11a frequency band for the specified regulatory domain. The two channels must be separated by a dash. Example: 36-40 44-48 52-56	country code determines supported channel pairs **Note:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.	
`valid-11a-channel`	Enter a single 802.11a channel number for 20 MHz operation within the specified regulatory domain.	country code determines supported channels **Note:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.	
`valid-11g-40mhz-channel-pair`	Specify a channel pair valid for 40 MHz operation in the 802.11g frequency band for the specified regulatory domain. The two channels must be separated by a dash. Example: 1-5 2-6 7-11	country code determines supported channel pairs **Note:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.	
`valid-11g-channel`	Enter a single 802.11g channel number for 20 MHz operation within the specified regulatory domain.	country code determines supported channels **Note:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.	

Usage Guidelines

This profile configures the country code and valid channels for operation of APs. The list of valid channels only affects the channels that may be selected by ARM or by the controller when no channel is configured. Channels that are specifically configured in the AP radio settings profile (see "rf dot11a-radio-profile" on page 411 or "rf dot11g-radio-profile" on page 417) must be valid for the country and the AP model.

A controller shipped to certain countries, such as the U.S. and Israel, cannot terminate APs with regulatory domain profiles that specify different country codes from the controller. For example, if a controller is designated for the U.S., then only a regulatory domain profile with the "US" country code is valid; setting APs to a regulatory domain profile with a different country code will result in the radios not coming up. For controllers in other countries, you can mix regulatory domain profiles on the same controller; for example, one controller can support APs in Japan, Taiwan, China, and Singapore.

In order for an AP to boot correctly, the country code configured in the AP regulatory domain profile must match the country code of the LMS. If none of the channels supported by the AP have received regulatory approval by the country whose country code you selected, the AP will revert to Air Monitor mode.

Examples

The following command configures the regulatory domain profile for APs in Japan:

```
(host) (config) #ap regulatory-domain-profile rd1
   country-code JP
```

The following command configures a regulatory domain profile for APs in the United States and specifies that the channel pair of 36 and 40, is allowed for 40 MHz mode of operation on the 5 GHz frequency band:

```
(host) (config) #ap regulatory-domain-profile usa1
   country-code US
   valid-11a-40mhz-channel-pair 36-40
```

The following command configures a regulatory domain profile for APs in the United States and specifies that the channel pair of 5 and 1, is allowed for 40 MHz mode of operation on the 2.4 GHz frequency band:

```
(host) (config) #ap regulatory-domain-profile usa1
   country-code US
   valid-11g-40mhz-channel-pair 1-5
```

Related Commands

To view the supported channels, use the **show ap allowed-channels** command.

AP configuration settings related to the IEEE 802.11n standard are configurable for Dell's W-AP120 series access points, which are IEEE 802.11n standard compliant devices.

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3	Support for the IEEE 802.11n standard, including channel pairs for 40 MHz mode of operation, was introduced
ArubaOS 5.0	The **valid-11g-40mhz-channel-pair** and **valid-11g-40mhz-channel-pair** parameters no longer support the + and - parameters that allowed you to define a primary and backup channel within the channel pair.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

ap snmp-profile (deprecated)

Description

This command configures an SNMP profile for APs.

Command History

Version	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4	Command deprecated

ap snmp-user-profile (deprecated)

```
ap snmp-user-profile <profile>
   auth-passwd <password>
   auth-prot {md5|none|sha}
   clone <profile>
   no ...
   priv-passwd <password>
   user-name <name>
```

Description

This command configures an SNMPv3 user profile for APs.

Command History

Version	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4	Command deprecated

ap spectrum clear-webui-view-settings

```
ap spectrum clear-webui-view-settings
```

Description

Clear a saved spectrum dashboard view.

Syntax

no parameters

Usage Guidelines

If your client is unable to load a saved spectrum view in the spectrum dashboard, issue the CLI command **ap spectrum clear-webui-view-settings** to delete the saved spectrum view.

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	RF Protect license	Config mode on master or local controllers

ap spectrum local-override

```
no
override ap-name <ap-name>
spectrum-band 2ghz|5ghz-lower|5ghz-middle|5ghz-upper
```

Description

Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.

Syntax

Parameter	Description	Range	Default
`override ap-name <ap-name>`	name of an AP whose radio should be converted to a spectrum monitor radio	—	—
`spectrum band`	Spectrum band or portion of the band to be monitored by the spectrum monitor radio	**2GHz** (channels 1-14) **5GHz-lower** (channels 36-64) **5GHz-middle** (channels 100-140) **5GHz-upper** (channels 149-165).	2Ghz

Usage Guidelines

There are two ways to change an AP model W-AP120 Series, W-AP105, or W-AP90 Series into a spectrum monitor. You can assign that AP to a 802.11a and 802.11g radio profile that is already set to spectrum mode, or you can temporarily change the AP into a spectrum monitor using a local spectrum override profile. When you use a local spectrum override profile to override an AP's mode setting, that AP will begin to operate as a spectrum monitor, but will remain associated with its previous 802.11a and 802.11g radio profiles. If you change any parameter (other than the overridden mode parameter) in the spectrum monitor's 802.11a or 802.11 radio profiles, the spectrum monitor will immediately update with the change. When you remove the local spectrum override, the spectrum monitor will revert back to its previous mode, and remain assigned to the same 802.11a and 802.11 radio profiles as before.

Related Commands

Command	Description	Mode
`show ap spectrum local-override`	This command shows a list of AP radios currently converted to spectrum monitors via the spectrum local-override list	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	RF Protect license	Config mode on master controllers

ap system-profile

```
ap system-profile <profile>
   aeroscout-rtls-server ip-addr <ipaddr> port <port>
   am-scan-rf-band [a | g | all]
   bkup-lms-ip <ipaddr>
   bootstrap-threshold <number>
   clone <profile>
   dns-domain <domain>
   double-encrypt
   dump-server <server>
   heartbeat-dscp <number>
   keepalive-interval <seconds>
   led-mode normal|off
   lms-hold-down-period <seconds>
   lms-ip <ipaddr>
   lms-preemption
   maintenance-mode
   master-ip <ipaddr>
   max-request-retries <number>
   mtu <bytes>
   native-vlan-id <vlan>
   no ...
   ortronics-high-temp <ortronics-high-temp>
   ortronics-led-to
   ortronics-low-temp <ortronics-low-temp>
   ortronics-walljack
   rap-bw-total
   rap-bw-resv-1
   rap-bw-resv-2
   rap-bw-resv-3
   rap-dhcp-default-router <ipaddr>
   rap-dhcp-dns-server <ipaddr>
   rap-dhcp-lease <days>
   rap-dhcp-pool-end <ipaddr>
   rap-dhcp-pool-netmask <netmask>
   rap-dhcp-pool-start <ipaddr>
   rap-dhcp-server-id <ipaddr>
   rap-dhcp-server-vlan <vlan>
   rap-local-network-access
   request-retry-interval <seconds>
   rf-band <band>
   rfprotect-bkup-server <ipaddr>
   rfprotect-server-ip <ipaddr>
   rtls-server ip-addr <ipaddr> port <port> key <key> station-message-frequency
      <seconds>
   session-acl <acl>
   syscontact <name>
   telnet
```

Description

This command configures an AP system profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”
`aeroscout-rtls-server`	Enables the AP to send RFID tag information to an AeroScout real-time asset location (RTLS) server.	—	—
`am-scan-rf-band`	Scanning band for multiple RF radios	a, g, all	all
`a`	Set the scanning band to 802.11a only	—	all
`g`	Set the scanning band to 802.11g only	—	all
`all`	Set the scanning band to apply to all bands	—	all
`ip-addr`	IP address of the AeroScout server to which location reports are sent.	—	—
`port`	Port number on the AeroScout server to which location reports are sent.	—	—
`bkup-lms-ip`	In multi-controller networks, specifies the IP address of a *backup* to the IP address specified with the lms-ip parameter.	—	—
`bootstrap-threshold`	Number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP rebootstraps. On the controller, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.	1-65535	8
`clone`	Name of an existing AP system profile from which parameter values are copied.	—	—
`dns-domain`	Name of domain that is resolved by corporate DNS servers. Use this parameter when configuring split tunnel.	—	—
`double-encrypt`	This parameter applies only to remote APs. Use double encryption for traffic to and from a wireless client that is connected to a tunneled SSID. When enabled, all traffic is re-encrypted in the IPsec tunnel. When disabled, the wireless frame is only encapsulated inside the IPsec tunnel. All other types of data traffic between the controller and the AP (wired traffic and traffic from a split-tunneled SSID) are always encrypted in the IPsec tunnel.	—	disabled
`dump-server`	(For debugging purposes.) Specifies the server to receive a core dump generated when an AP process crashes.	—	—
`heartbeat-dscp`	DSCP value of AP heartbeats.	0-63	0
`keepalive-interval`	Time, in seconds, between keepalive messages from the AP.	30-65535	60 seconds
`led-mode`	The operating mode for the AP LEDs (W-AP120, W-AP124 and W-AP125 only)		normal
`normal`	Display LEDs in normal mode.		
`off`	Turn off all LEDs.		
`lms-hold-down-period`	Time, in seconds, that the primary LMS must be available before an AP returns to that LMS after failover.	1-3600	600 seconds

Parameter	Description	Range	Default
lms-ip	In multi-controller networks, specifies the IP address of the local management switch (LMS)—the Dell controller—which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. This can be the IP address of the local or master controller. When using redundant controllers as the LMS, set this parameter to be the VRRP IP address to ensure that APs always have an active IP address with which to terminate sessions.	—	—
lms-preemption	Automatically reverts to the primary LMS IP address when it becomes available.	—	disabled
maintenance-mode	Enable or disable AP maintenance mode. This setting is useful when deploying, maintaining, or upgrading the network. If enabled, APs stop flooding unnecessary traps and syslog messages to network management systems or network operations centers when deploying, maintaining, or upgrading the network. The controller still generates debug syslog messages if debug logging is enabled.		disabled
master-ip	In multi-controller networks, specifies the IP address of the master controller. This address must be reachable by the APs.	—	—
max-request-retries	Maximum number of times to retry AP-generated requests, including keepalive messages. After the maximum number of retries, the AP either tries the IP address specified by the bkup-lms-ip (if configured) or reboots.	1-65535	10
mtu	MTU, in bytes, on the wired link for the AP.	1024-1578	—
native-vlan-id	Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).	—	1
no	Negates any configured parameter.	—	—
ortronics-high-temp <ortronics-high-temp>	Temperature (in degrees Celsius) at which to decrease transmit power on Ortronics APs.		110 C
ortronics-led-to	Enable or disable the LED off timeout feature for Ortronics APs.		Enabled
ortronics-low-temp <ortronics-low-temp>	Temperature (in degrees Celsius) at which to restore configured power on Ortronics APs.		100 C
ortronics-walljack	Enable or disable the wall jack on Ortronics DuoWJ APs		Enabled
rap-bw-total	This is the total reserved uplink bandwidth (in Kilobits per second).		
rap-bw-resv-1	Session ACLs with uplink bandwidth reservation in kilobits per second. You can specify up to three session ACLs to reserve uplink bandwidth. The sum of the three uplink bandwidths should not exceed the rap-bw-total value.		
rap-bw-resv-2			
rap-bw-resv-3			
rap-dhcp-default-router	IP address for the default DHCP router.		192.168.11.1
rap-dhcp-dns-server	IP address of the DNS server.		192.168.11.1

Parameter	Description	Range	Default
rap-dhcp-lease	The amount of days that the assigned IP address is valid for the client. Specify the lease in <days>. 0 indicates the IP address is always valid; the lease does not expire.	0-30	0
rap-dhcp-pool-end	Configures a DHCP pool for remote APs. This is the last IP address of the DHCP pool.		192.168.11.254
rap-dhcp-pool-netmask	Configures a DHCP pool for remote APs. This is the netmask used for the DHCP pool.		255.255.255.0
rap-dhcp-pool-start	Configures a DHCP pool for remote APs. This is the first IP address of the DHCP pool.		192.168.11.2
rap-dhcp-server-id	IP address used as the DHCP server identifier.		192.168.11.1
rap-dhcp-server-vlan	VLAN ID of the remote AP DHCP server used if the controller is unavailable. This VLAN enables the DHCP server on the AP (also known as the remote AP DHCP server VLAN). If you enter the native VLAN ID, the DHCP server is unavailable.	—	—
rap-local-network-access	Enable or disable local network access across VLANs in a Remote-AP.	—	disabled
request-retry-interval	Interval, in seconds, between the first and second retries of AP-generated requests. If the configured interval is less than 30 seconds, the interval for subsequent retries is increased up to 30 seconds.	1-65535	10 seconds
rf-band	For APs that support both a and b/g RF bands, RF band in which the AP should operate: • g = 2.4 GHz • a = 5 GHz	a/g	g
rfprotect-bkup-server	IP address of the backup Dell RFprotect server. The AP or AP group to which this profile applies operates as an RFprotect sensor.	—	—
rfprotect-server-ip	IP address of the Dell RFprotect server. The AP or AP group to which this profile applies operates as an RFprotect sensor.	—	—
rtls-server	Enables the AP to send RFID tag information to an RTLS server.	—	—
ip-addr	IP address of the server to which location reports are sent.	—	—
port	Port number on the server to which location reports are sent.	—	—
key	Shared secret key.	—	—
station-message-frequency	Indicates how often packets are sent to the server.	5-3600	30 seconds
session-acl	Session ACL configured with the ip access-list session command. **NOTE:** This parameter requires the PEFNG license.	—	—
syscontact	SNMP system contact information.	—	—
telnet	Enable or disable telnet to the AP.	—	disabled

Usage Guidelines

The AP system profile configures AP administrative operations, such as logging levels.

Example

The following command sets the LMS IP address in an AP system profile:

```
(host) (config) #ap system-profile local1
   lms-ip 10.1.1.240
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	Support for additional RTLS servers, remote AP enhancements was introduced
ArubaOS 3.3.2	• Maintenance-mode parameter was introduced. • Multiple remote AP DHCP server enhancements were introduced. • Support for RFprotect server and backup server configuration was introduced. • The mms-rtls-server parameter was deprecated in ArubaOS 3.3.2. To configure the Mobility Manager server as an RTLS server, see “mobility-manager” on page 356.
ArubaOS 6.0	Added support for the option to set the RF scanning band (am-scan-rf-band)

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system, except for noted parameters	Config mode on master controllers

ap wipe out flash

```
ap wipe out flash
   ap-name <ap-name>
   ip-addr <ip-addr>
```

Description

Overwrite the entire AP compact flash, destroying its contents (including the current image file).

Syntax

Parameter	Description	Range	Default
`ap-name`	Wipe out the flash of the AP with the specified name.	—	—
`ip-addr`	Wipe out the flash of the AP with the specified IP address.	—	—

Usage Guidelines

Use this command only under the supervision of Dell technical support. If you delete the current image in the AP's flash memory, the AP will not function until you reload another image.

Command History

This command was introduced in ArubaOS 3.3.2.

Command Information

Platforms	Licensing	Command Mode
All platforms running ArubaOS 3.3.2.x-FIPS or later.	Base operating system	Config mode on master controllers

ap wired-ap-profile

```
ap wired-ap-profile <profile>
   clone <profile>
   forward-mode {bridge|split-tunnel|tunnel}
   no ...
   switchport access vlan <vlan> | {mode access|trunk} |trunk {allowed vlan <list>|
   add <list> | except <list> | remove <list>}| native vlan <vlan>
   trusted
   wired-ap-enable
```

Description

This command configures a wired AP profile.

Syntax

Parameter	Description
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.
`clone`	Name of an existing wired AP profile from which parameter values are copied.
`forward-mode`	This parameter controls whether data is tunneled to the controller using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the controller, and Internet access remains local). All forwarding modes support band steering, TSPEC/TCLAS enforcement, 802.11k and station blacklisting.
`tunnel`	In this default forwarding mode, the AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames and EAPOL frames over a GRE tunnel to the controller for processing. The controller removes or adds the GRE headers, decrypts or encrypts 802.11 frames and applies firewall rules to the user traffic as usual.
`bridge`	802.11 frames are bridged into the local Ethernet LAN. When a remote AP or campus AP is in bridge mode, the AP handles all 802.11 association requests and responses, encryption/decryption processes, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. An AP in bridge mode supports only the 802.1x authentication type. **NOTE:** Virtual APs in bridge mode using static WEP should use key slots 2-4 on the controller. Key slot 1 should only be used with Virtual APs in tunnel mode.
`split-tunnel`	802.11 frames are either tunneled or bridged, depending on the destination (corporate traffic goes to the controller, and Internet access remains local). An AP in split-tunnel mode supports only the 802.1x authentication type. An AP in split-tunnel forwarding mode handles all 802.11 association requests and responses, encryption/decryption, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. **NOTE:** Virtual APs in split-tunnel mode using static WEP should use key slots 2-4 on the controller. Key slot 1 should only be used with Virtual APs in tunnel mode.
`no`	Negates any configured parameter.
`switchport`	Configures the switching mode characteristics for the port.
`access`	The VLAN to which the port belongs. The default is VLAN 1.
`mode`	The mode for the port, either access or trunk mode. The default is access mode.
`trunk allowed`	Allows multiple VLANs on the port interface. You must define this parameter using VLAN IDs or VLAN names VLAN IDs and VLAN names cannot be listed together.
`trunk native`	The native VLAN for the port (frames on the native VLAN are not tagged with 802.1q tags).
`trusted`	Sets port as either trusted or untrusted. The default setting is untrusted.
`wired-ap-enable`	Enables the wired AP. The wired AP is disabled by default.

Usage Guidelines

This command is only applicable to Dell APs that support a second Ethernet port. The wired AP profile configures the second Ethernet port (enet1) on the AP.

For mesh deployments, this command is applicable to all Dell APs configured as mesh nodes. If you are using mesh to join multiple Ethernet LANs, configure and enable bridging on the mesh point Ethernet port.

Mesh nodes only support bridge mode and tunnel mode on their wired ports (enet0 or enet1). Split tunnel mode is not supported.

Use the bridge mode to configure bridging on the mesh point Ethernet port. Use tunnel mode to configure secure jack operation on the mesh node Ethernet port.

When configuring the Ethernet ports on APs with multiple ethernet ports, note the following requirements:

- If configured as a mesh portal, connect enet0 to the controller to obtain an IP address. The wired AP profile controls enet1.Only enet1 supports secure jack operation.
- If configured as a mesh point, the same wired AP profile will control both enet0 and enet1.

Example

The following command configures the enet1 port on a multi-port AP as a trunk port:

```
(host) (config) #ap wired-ap-profile wiredap1
   switchport mode trunk
   switchport trunk allowed 4,5
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	The **split-tunnel** forwarding mode was introduced.
ArubaOS 6.0	Wired ports on campus APs support bridge forwarding mode.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system, except for noted parameters	Config mode on master controllers

ap-group

```
ap-group <group>
   ap-system-profile <profile>
   clone <profile>
   dot11a-radio-profile <profile>
   dot11a-traffic-mgmt-profile <profile>
   dot11g-radio-profile <profile>
   dot11g-traffic-mgmt-profile <profile>
   enet0-profile <profile>
   enet1-profile <profile>
   event-thresholds-profile <profile>
   ids-profile <profile>
   mesh-cluster-profile <profile> priority <priority>
   mesh-radio-profile <profile>
   no ...
   regulatory-domain-profile <profile>
   rf-optimization-profile <profile>
   virtual-ap <profile>
   voip-cac-profile <profile>
   wired-ap-profile <profile>
```

Description

This command configures an AP group.

Syntax

Parameter	Description	Range	Default
`<group>`	Name that identifies the AP group. The name must be 1-63 characters. NOTE: You cannot use quotes (") in the AP group name.	—	"default"
`ap-system-profile`	Configures AP administrative operations, such as logging levels. See "ap system-profile" on page 116.	—	"default"
`clone`	Name of an existing AP group from which profile names are copied.	—	—
`dot11a-radio-profile`	Configures 802.11a radio settings and load balancing for the AP group; contains the ARM profile. See "rf dot11a-radio-profile" on page 411.	—	"default"
`dot11a-traffic-mgmt-profile`	Configures bandwidth allocation. See "wlan traffic-management-profile" on page 1228.	—	—
`dot11g-radio-profile`	Configures 802.11g radio settings and load balancing for the AP group; contains the ARM profile. See "rf dot11a-radio-profile" on page 411.	—	"default"
`dot11g-traffic-mgmt-profile`	Configures bandwidth allocation. See "wlan traffic-management-profile" on page 1228.	—	—
`enet0-profile`	Configures the duplex and speed of the Ethernet 0 interface on the AP. See "ap enet-link-profile" on page 91.	—	"default"
`enet1-profile`	Configures the duplex and speed of the Ethernet 1 interface on the AP. See "ap enet-link-profile" on page 91.	—	"default"
`event-thresholds-profile`	Configures Received Signal Strength Indication (RSSI) metrics. See "rf event-thresholds-profile" on page 423.	—	"default"
`ids-profile`	Configures Dell's Intrusion Detection System (IDS). See "ids profile" on page 234.	—	"default"
`mesh-cluster-profile`	Configures the mesh cluster profile for mesh nodes that are members of the AP group. There is a "default" mesh cluster profile; however, it is not applied until you provision the mesh node. See "ap mesh-cluster-profile" on page 92.	—	"default"
`priority`	Configures the priority of the mesh cluster profile. If more than two mesh cluster profiles are configured, mesh points use this number to identify primary and backup profile(s). The lower the number, the higher the priority.	1-16	1
`mesh-radio-profile`	Configures the 802.11g and 802.11a radio settings for mesh nodes that are members of the AP group. See "ap mesh-ht-ssid-profile" on page 95. Commands to configure mesh for outdoor APs require the Outdoor Mesh license.	—	"default"
`no`	Negates any configured parameter.	—	—
`regulatory-domain-profile`	Configures the country code and valid channels. See "ap regulatory-domain-profile" on page 109.	—	"default"
`rf-optimization-profile`	Configure coverage hole and interference detection. See "rf optimization-profile" on page 428.	—	"default"
`virtual-ap`	One or more profiles, each of which configures a specified WLAN. See "wlan virtual-ap" on page 1230.	—	"default"

Parameter	Description	Range	Default
`voip-cac-profile`	Configures voice over IP (VoIP) call admission control (CAC) options. See “wlan voip-cac-profile” on page 1236. This parameter requires the PEFNG license.	—	“default”
`wired-ap-profile`	Configures the second Ethernet port (enet1) on the AP. See “ap wipe out flash” on page 121.	—	“default”

Usage Guidelines

AP groups are at the top of the configuration hierarchy. An AP group collects virtual AP definitions and configuration profiles, which are applied to APs in the group.

Example

The following command configures a virtual AP profile to the “default” AP group:

```
(host)(config) #ap-group default
   virtual-ap corpnet
```

Related Commands

View AP group settings using the command show ap-group.

Command History:

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	Support for the mesh parameters was introduced
ArubaOS 3.4.1	The **voip-cac-profile** parameter required the PEF license.
ArubaOS 5.0	The **voip-cac-profile** parameter requires the PEFV license.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system, except for noted parameters	Config mode on master controllers

ap-name

```
ap-name <name>
   ap-system-profile <profile>
   clone <profile>
   dot11a-radio-profile <profile>
   dot11a-traffic-mgmt-profile <profile>
   dot11g-radio-profile <profile>
   dot11g-traffic-mgmt-profile <profile>
   enet0-profile <profile>
   enet1-profile <profile>
   event-thresholds-profile <profile>
   exclude-mesh-cluster-profile-ap <profile>
   exclude-virtual-ap <profile>
   ids-profile <profile>
   mesh-cluster-profile <profile> priority <priority>
   mesh-radio-profile <profile>
   no ...
   regulatory-domain-profile <profile>
   rf-optimization-profile <profile>
   snmp-profile <profile>
   virtual-ap <profile>
   voip-cac-profile <profile>
   wired-ap-profile <profile>
```

Description

This command configures a specific AP.

Syntax

Parameter	Description	Default
<name>	Name that identifies the AP. By default, an AP's name can either be the AP's Ethernet MAC address, or if the AP has been previously provisioned with an earlier version of ArubaOS, a name in the format <building>.<floor>.<location>. The name must be 1-63 characters. NOTE: You cannot use quotes (") in the AP name.	—
ap-system-profile	Configures AP administrative operations, such as logging levels. See "ap system-profile" on page 116.	"default"
clone	Name of an existing AP name from which profile names are copied.	—
dot11a-radio-profile	Configures 802.11a radio settings for the AP group; contains the ARM profile. See "rf dot11a-radio-profile" on page 411.	"default"
dot11a-traffic-mgmt-profile	Configures bandwidth allocation. See "wlan traffic-management-profile" on page 1228.	—
dot11g-radio-profile	Configures 802.11g radio settings for the AP group; contains the ARM profile. See "rf dot11a-radio-profile" on page 411.	"default"
dot11g-traffic-mgmt-profile	Configures bandwidth allocation. See "wlan traffic-management-profile" on page 1228.	—
enet0-profile	Configures the duplex and speed of the Ethernet 0 interface on the AP. See "ap enet-link-profile" on page 91.	"default"
enet1-profile	Configures the duplex and speed of the Ethernet 1 interface on the AP. See "ap enet-link-profile" on page 91.	"default"
event-thresholds-profile	Configures Received Signal Strength Indication (RSSI) metrics. See "rf event-thresholds-profile" on page 423.	"default"
exclude-mesh-cluster-profile-ap	Excludes the specified mesh cluster profile from this AP. The Secure Enterprise Mesh license must be installed.	—
exclude-virtual-ap	Excludes the specified virtual AP profiles from this AP.	
ids-profile	Configures Dell's Intrusion Detection System (IDS). See "ids profile" on page 234.	"default"
mesh-cluster-profile	Configures the mesh cluster profile for the AP (mesh node). There is a "default" mesh cluster profile; however, it is not applied until you provision the mesh node. See "ap mesh-cluster-profile" on page 92. The Secure Enterprise Mesh license must be installed.	"default"
priority	Configures the priority of the mesh cluster profile. If more than two mesh cluster profiles are configured, mesh points use this number to identify primary and backup profile(s). The supported range of values is 1-16. The lower the number, the higher the priority.	1
mesh-radio-profile	Configures the 802.11g and 802.11a radio settings for the AP (mesh node). See "ap mesh-ht-ssid-profile" on page 95. The Secure Enterprise Mesh license must be installed.	"default"
no	Negates any configured parameter.	—
regulatory-domain-profile	Configures the country code and valid channels. See "ap regulatory-domain-profile" on page 109.	"default"
rf-optimization-profile	Configures load balancing and coverage hole and interference detection. See "rf optimization-profile" on page 428.	"default"
snmp-profile	Configures SNMP-related parameters. See "ap snmp-profile (deprecated)" on page 112.	"default"

Parameter	Description	Default
`virtual-ap`	One or more profiles, each of which configures a specified WLAN. See “wlan virtual-ap” on page 1230.	“default”
`voip-cac-profile`	Configures voice over IP (VoIP) call admission control (CAC) options. See “wlan voip-cac-profile” on page 1236. This parameter requires the PEFNG license.	“default”
`wired-ap-profile`	Configures the ports for APs that are directly attached to the controller. See “ap wipe out flash” on page 121.	“default”

Usage Guidelines

Profiles that are applied to an AP group can be overridden on a per-AP name basis, and virtual APs can be added or excluded on a per-AP name basis. If a particular profile is overridden for an AP, all parameters from the overriding profile are used. There is no merging of individual parameters between the AP and the AP group to which the AP belongs.

Example

The following command excludes a virtual AP profile from a specific AP:

```
(host) (config) #ap-name 00:0b:86:c0:cf:d8
   exclude-virtual-ap corpnet
```

Related Commands

View AP settings using the command show ap-name.

Command History:

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	Support for mesh parameters was introduced.
ArubaOS 3.4.1	License requirements changed in ArubaOS 3.4.1, so the **voip-cac-profile** parameter required the PEF license instead of the Voice Services Module license required in earlier versions.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

ap-regroup

```
ap-regroup {ap-name <name>|serial-num <num>|wired-mac <macaddr>} <group>
```

Description

This command moves a specified AP into a group.

Syntax

Parameter	Description	Default
`ap-name`	Name of the AP.	—
`serial-num`	Serial number of the AP.	—
`wired-mac`	MAC address of the AP.	—
`<group>`	Name that identifies the AP group. The name must be 1-63 characters.	"default"

Usage Guidelines

All APs discovered by the controller are assigned to the "default" AP group. An AP can belong to only one AP group at a time. You can move an AP to an AP group that you created with the **ap-group** command.

Note: This command automatically reboots the AP.

Example

The following command moves an AP to the 'corpnet' group:

```
(host)(config) #ap-regroup wired-mac 00:0f:1e:11:00:00 corpnet
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

ap-rename

```
ap-rename {ap-name <name>|serial-num <num>|wired-mac <macaddr>} <new-name>
```

Description

This command changes the name of an AP to the specified new name.

Syntax

Parameter	Description
`ap-name`	Current name of the AP.
`serial-num`	Serial number of the AP.
`wired-mac`	MAC address of the AP.
`<new-name>`	New name for the AP. The name must be 1-63 characters. **NOTE:** You cannot use quotes (“) in the AP name.

Usage Guidelines

An AP name must be unique within your network.

Note: This command automatically reboots the AP.

Example

The following command renames an AP:

```
(host) (config) #ap-rename wired-mac 00:0f:1e:11:00:00 building3-lobby
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

apboot

```
apboot {all [global|local]|ap-group <group> [global|local]|ap-name <name>|ip-addr
<ipaddr>|wired-mac <macaddr>}
```

Description

This command reboots the specified APs.

Syntax

Parameter	Description	Default
`all`	Reboot all APs.	all
`global`	Reboot APs on all controllers.	global
`local`	Reboot only APs registered on this controller. This is the default.	local
`ap-group`	Reboot APs in a specified group.	ap-group
`global`	Reboot APs on all controllers.	global
`local`	Reboot only APs registered on this controller. This is the default.	local
`ap-name`	Reboot the AP with the specified name.	ap-name
`ip-addr`	Reboot the AP at the specified IP address.	ip-addr
`wired-mac`	Reboot the AP at the specified MAC address.	wired-mac

Usage Guidelines

You should not normally need to use this command as APs automatically reboot when you reprovision them. Use this command only when directed to do so by your Dell representative.

Example

The following command reboots a specific AP:

```
(host)(config)# apboot ap-name Building3-Lobby
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

apflash

```
apflash {ap-name <name>|ip-addr <ipaddr>|wired-mac <macaddr>} [backup-partition]
[server <ipaddr>]
```

Description

This command reflashes the specified AP.

Syntax

Parameter	Description
`ap-name`	Reflash the AP with the specified name.
`ip-addr`	Reflash the AP at the specified IP address.
`wired-mac`	Reflash the AP at the specified MAC address.
`server`	IP address of the FTP server.

Usage Guidelines

This command directs an AP to download its image from the controller. You should not normally need to run this command, since APs automatically download their images from a controller during bootup.

Example

The following command reflashes a specific AP:

```
(host) (config) #apflash ap-name Building3-Lobby
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config modes on master controllers

apconnect

```
apconnect {ap-name <name>|bssid <bssid>|ip-addr <ipaddr>} parent-bssid <bssid>
```

Description

This command instructs a mesh point to disconnect from its current parent and connect to a new parent.

Syntax

Parameter	Description
`ap-name <name>`	Specify the name of the mesh point to be connected to a new parent.
`bssid <bssid>`	Specific the BSSID of the mesh point to be connected to a new parent.
`ip-addr <ipaddr>`	Specific the IP address of the mesh point to be connected to a new parent.
`parent-bssid <bssid>`	BSSID of the parent to which the mesh point should connect.

Usage Guidelines

To maintain a mesh topology created using the **apconnect** command, Dell suggests setting the mesh reselection-mode to **reselect-never**, otherwise the normal mesh reselection mechanisms could break up the selected topology.

Example

The following command connects the mesh point "meshpoint1" to a new parent with the specified BSSID.

```
(host) (config) #apconnect ap-name meshpoint1 parent-bssid 00:12:6d:03:1c:f1
```

Related Commands

Command	Description	Mode
`ap mesh-radio-profile reselection-mode reselect-never`	Use this command to prevent the AP from reselecting a new parent.	Enable or Config mode

Command History

This command was introduced in ArubaOS 3.4.1

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

apdisconnect

```
apdisconnect {ap-name <name>|bssid <bssid>|ip-addr <ipaddr>}
```

Description

This command disconnects a mesh point from its parent.

Syntax

Parameter	Description
`ap-name`	Specifies the name of the parent AP.
`bssid`	Specifies the BSSID of the parent AP.
`ip-addr`	Specifies the IP address of the parent AP.

Usage Guidelines

Each mesh point learns about the mesh portal from its parent (a mesh node that is part of the path to the mesh portal). This command directs a mesh point to disassociate from its parent. The mesh point will attempt to associate with another neighboring mesh node, if available. The old parent is not eligible for re-association for 60 seconds after disconnection.

Example

The following command disconnects a specific mesh point from its parent:

```
(host) (config) #apdisconnect ap-name meshpoint1
```

Related Commands

Command	Description	Mode
`apconnect`	This command connects a mesh point to a new specified parent.	Enable or Config mode

Command History

This command was introduced in ArubaOS 3.2

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

arp

```
arp <ipaddr> <macaddr>
```

Description

This command adds a static Address Resolution Protocol (ARP) entry.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the device to be added.
`<macaddr>`	Hardware address of the device to be added, in the format xx:xx:xx:xx:xx:xx.

Usage Guidelines

If the IP address does not belong to a valid IP subnetwork, the ARP entry is not added. If the IP interface that defines the subnetwork for the static ARP entry is deleted, you will be unable to use the arp command to overwrite the entry's current values; use the no arp command to negate the entry and then enter a new arp command.

Example

The following command configures an ARP entry:

```
(host) (config) #arp 10.152.23.237 00:0B:86:01:7A:C0
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

audit-trail

```
audit-trail [all]
```

Description

This command enables an audit trail.

Syntax

Parameter	Description
`all`	Enables audit trail for all commands, including enable mode commands. The **audit-trail** command without this option enables audit trail for all commands in configuration mode.

Usage Guidelines

By default, audit trail is enabled for all commands in configuration mode. Use the **show audit-trail** command to display the content of the audit trail.

Example

The following command enables an audit trail:

```
(host) (config) #audit-trail
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

backup

```
backup {flash|pcmcia}
```

Description

This command backs up compressed critical files in flash.

Syntax

Parameter	Description
`flash`	Backs up flash directories to flashbackup.tar.gz file.
`pcmcia`	Backs up flash images to external PCMCIA flash card. This option can only be executed on controllers that have a PCMCIA slot.

Usage Guidelines

Use the **restore flash** command to untar and uncompress the flashbackup.tar.gz file.

Example

The following command backs up flash directories to the flashbackup.tar.gz file:

```
(host)(config) #backup flash
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config modes on master controllers

banner motd

```
banner motd <delimiter> <textString>
```

Description

This command defines a text banner to be displayed at the login prompt when a user accesses the controller.

Syntax

Parameter	Description	Range
`<delimiter>`	Indicates the beginning and end of the banner text.	—
`<textString>`	The text you want displayed.	up to 1023 characters

Usage Guidelines

The banner you define is displayed at the login prompt to the controller. The banner is specific to the controller on which you configure it. The WebUI displays the configured banner at its login prompt, but you cannot use the WebUI to configure the banner.

The delimiter is a single character that indicates the beginning and the end of the text string in the banner. Select a delimiter that is not used in the text string you define, because the controller ends the banner when it sees the delimiter character repeated.

There are two ways of configuring the banner message:

- Enter a space between the delimiter and the beginning of the text string. The text can include any character except a quotation mark (“). Use quotation marks to enclose your text if you are including spaces (spaces are not recognized unless your text string is enclosed in quotation marks; without quotation marks, the text is truncated at the first space). You can also use the delimiter character within quotation marks.
- Press the **Enter** key after the delimiter to be placed into a mode where you can simply enter the banner text in lines of up to 255 characters, including spaces. Quotation marks are ignored.

Example

The following example configures a banner by enclosing the text within quotation marks:

```
(host)(config) #banner motd * “Welcome to my controller. This controller is in the
production network, so please do not save configuration changes. Maintenance will be
performed at 7:30 PM, so please log off before 7:00 PM.”*
```

The following example configures a banner by pressing the **Enter** key after the delimiter:

```
(host)(config) #banner motd *
Enter TEXT message [maximum of 1023 characters].
Each line in the banner message should not exceed 255 characters.
End with the character '*'.

Welcome to my controller. This controller is in the production network, so please do not
save configuration changes. Maintenance will be performed at 7:30 PM, so please log off
before 7:00 PM.*
```

The banner display is as follows:

```
Welcome to my controller. This controller is in the production network, so please do not
save configuration changes. Maintenance will be performed at 7:30 PM, so please log off
before 7:00 PM.
```

Command History

This command was introduced in ArubaOS 1.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

boot

```
boot
   cf-test [fast | read-only | read-write]
   config-file <filename>
   system partition [0 | 1]
   verbose
```

Description

Configure the boot options for the controller.

Syntax

Parameter	Description
`cf-test`	Sets the type of compact flash test to run when booting the controller.
`fast`	Performs a fast test, which does not include media testing.
`read-only`	Performs a read-only media test.
`read-write`	Performs a read-write media test.
`config-file`	Sets the configuration file to use when booting the controller.
`<filename>`	Specifies the name of the configuration file from which to boot the controller.
`system 0 | 1`	Enter the keyword **system** followed by the partition number (0 or 1) that you want the controller to use during the next boot (login) of the controller. **NOTE:** A controller reload is required before the new boot partition takes effect.
`verbose`	Prints extra debugging information at boot.

Usage Guidelines

Use the following options to control the boot behavior of the controller:

- `cf-test`—Test the flash during boot.
- `config-file`—Set the configuration file to use during boot.
- `system`—Specify the system partition to use during the controller's next boot (login).
- `verbose`—Print extra debugging information during boot. The information is sent to the screen at boot time. Printing the extra debugging information is disabled using the `no boot verbose` command.

Example

The following command uses the configuration file january-config.cfg the next time the controller boots:

```
boot config-file january-config.cfg
```

The following command uses system partition 1 the next time the controller boots:

```
boot system partition 1
```

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

cellular profile

```
cellular profile <profile_name>
   dialer <group>
   driver acm|hso|option|sierra
   import <address>
   modeswitch {eject <params>}|rezero
   no
   priority <1-255>
   serial <sernum>
   tty <ttyport>
   user <login> password <password>
   vendor <vend_id> product <prod_id>
```

Description

Create new profiles to support new USB modems or to customize USB characteristics.

Syntax

Parameter	Description
`cellular profile <profile_name>`	Enter the keywords **cellular profile** followed by your profile name. This command changes the configuration mode and the command line prompt changes to: host (config-cellular <profile_name>)#
`dialer <group>`	Enter the keyword **dialer** followed by a group name to specify the dialing parameters for the carrier. The parameters tend to be common between service providers on the same type of network (CDMA vs. GSM) as displayed in the `show dialer group` command.
`driver acm|hso|option|sierra`	Enter the keyword **driver** followed by one of the driver options: • **acm**: Linux ACM driver. • **hso**: Option High Speed driver. • **option**: Option USB data card driver (default). • **sierra**: Sierra Wireless driver.
`import <address>`	Enter the keyword **import** followed by the USB device address as displayed in the `show usb` command. Import retrieves the vendor/product serial numbers from the USB device list and populates them into the profile.
`modeswitch {eject <params>}|rezero`	Enter the keyword **modeswitch** followed by either: • **eject** followed by the CDROM device. • **rezero**: Send SCSI CDROM rezero command. Certain cellular devices must be modeswitched before the modem switches to data mode.
`no`	Enter the keyword **no** to negate the command and revert back to the defaults.
`priority <1-255>`	Enter the keyword **priority** to override the default cellular priority (100). Range: 1 to 255. Default: 100
`serial <sernum>`	Enter the keyword **serial** followed by the USB device serial number
`tty <ttyport>`	Enter the keyword **tty** followed by the Modem TTY port (i.e. ttyUSB0, ttyACM0)
`user <login> password <password>`	Enter the keyword **user** followed by your login, and then enter the keyword **password** followed by your password to establish user name authentication.
`vendor <vend_id> product <prod_id> in hex`	Enter the keyword **vendor** followed by the vendor ID in hexadecimal (see `show usb`) and then enter the keyword **product** followed by the product ID listed in the `show usb` command.

Usage Guidelines

The cellular modems are plug-and-play and support most native USB modems. Cellular modems are activated only if it is the uplink with the highest priority (see `show uplink`). However, new profiles can be created using this command to support new data cards or to customize card characteristics.

Command History

Introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
Aruba 600 controllers	Base operating system	Config mode on master and local controllers (config-cellular <profile_name>)

cfgm

```
cfgm {mms config {enable|disable}|set config-chunk <kbytes>|set heartbeat <seconds>|set
maximum-updates <number>|snapshot-timer <minutes>|sync-command-blocks <number>|sync-
typecomplete|sync-type snapshot}
```

Description

This command configures the configuration module on the master controller.

Syntax

Parameter	Description	Range	Default
`set config-chunk`	Maximum packet size, in Kilobytes, that is sent every second to the local controller whenever the master controller sends a configuration to the local. If the connection between the master and local is slow or uneven, you can lower the size to reduce the amount of data that needs to be retransmitted. If the connection is very fast and stable, you can increase the size to make the transmission more efficient.	1-100	10 Kbytes
`set heartbeat`	Interval, in seconds, at which heartbeats are sent. You can increase the interval to reduce traffic load.	10-300	10 seconds
`set maximum-updates`	Maximum number of local controllers that can be updated at the same time with configuration changes. You can decrease this value if you have a busy network. You can increase this value to improve configuration synchronization.	2-25	5
`snapshot-timer`	Interval, in minutes, that the local controller waits for a configuration download from the master upon bootup or startup before loading the last snapshot configuration.	5-60	5 minutes
`sync-command-blocks`	To configure the number of command-list blocks. Each block contains a list of global configuration commands for each write-mem operation.	1-3	3
`sync-type complete`	To revert to the old master/local configuration synchronization behavior in case there are issues encountered using the new behavior.	—	—
`sync-type snapshot`	To revert to configuration snapshot behavior, in which only the incremental updates are sent to the local.	—	Enable

Usage Guidelines

By default, Mobility Manager configuration updates on the controller are disabled to prevent any alterations to the controller configuration. You need to explicitly enable Mobility Manager configuration updates for the controller to accept configuration changes from Mobility Manager. When Mobility Manager configuration updates are enabled, global configuration changes can only be done from Mobility Manager and are not available on the master controller. You can use the **cfgm mms config disable** command if the controller loses connectivity to the Mobility Manager and you must enter a configuration change on the master controller.

Example

The following command allows configuration updates from the Mobility Manager:

```
(host)(config) #cfgm mms config enable
```

Command History

This command was introduced in ArubaOS 3.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

clear

```
clear
   aaa
   acl
   ap
   arp
   counters
   crypto
   datapath
   dot1x
   fault
   gab-db
   ip
   ipc
   ipv6
   loginsession
   master-local-entry
   master-local-session
   port
   provisioning-ap-list
   provisioning-params
   rap-wml
   update-counter
   voice
   vpdn
   wms
clock
```

Description

This command clears various user-configured values from your running configuration.

Syntax

Parameter	Description
aaa	Clear all values associated with authentication profile
authentication-server	Provide authentication server details to clear values specific to an authentication server or all authentication server. Parameters: • all—to clear all server statistics. • internal—to clear Internal server statistics. • radius—to clear RADIUS server statistics. • tacacs—to clear TACACS server statistics.
state	Clear internal status of authentication modules. Parameters: • configuration—clear all configured objects. • debug-statistics—clear debug statistics. • messages—clear authentication messages that were sent and received.
acl	Clear ACL statistics.
hits	Clear ACL hit statistics
ap	Clear all AP related information.
arm	Clear information on AP.
mesh	Clear all mesh commands.
port	Toggle the link on the specified port.
remote	Clear all information related to remote configuration.
arp	Clear all ARP table information. You can either clear all information or enter the IP address of the ARP entry to clear a specific value.
counters	Clear all interface configuration values.
fastethernet	Clears configuration related to fastethernet ports.
gigabitethernet	Clears configuration related to fastethernet ports.
tunnel	Clears all tunnel configuration values on interface ports.
vrrp	Clears all VRRP configuration values on interface ports.

Parameter	Description
`datapath`	Clears all configuration values and statistics for the following datapath modules. • `application` • `bridge` • `bwm` • `crypto` • `dma` • `frame` • `hardware` • `ip-reassembly` • `maintenance` • `message-queue` • `route` • `route-cache` • `session` • `station` • `tunnel` • `user` • `wifi-reassembly` • `wmm`
`dot1x`	Clears all 802.1x specific counters and supplicant statistics. Use the following parameters: • `counters` • `supplicant-info`
`fault`	Clears all SNMP fault configuration.
`gap-db`	Clears global AP database. This command is often used to clear all stale AP records. Use the following parameters: • ap-name • lms • wired-mac
`ip`	Clears all IP information from DHCP bindings, IGMP groups and IP mobility configuration. Use the following parameters: • `dhcp` • `igmp` • `mobile`
`ipc`	Clears all inter process communication statistics.
`ipv6`	Clears all IPv6 session and user statistics. Use the following parameters: • `datapath session counters` • `datapath user counters`
`loginsession`	Clears loginsession information for a specific login session, as identified by the session id.
`master-local-entry`	Clears local controller information from the master controller LMS list. Specify the IP address of the local controller to be removed from master controller active LMS list.
`master-local-session`	Clear and reset master local TCP connection. Specify the IP address of either the master or local controller.
`port`	Clear all port statistics that includes link-event counters or all counters. Use the following parameters: • `link-event` • `stats`
`provisioning-ap-list`	Clear AP entries from the provisioning list.
`provisioning-params`	Clear provisioning parameters and reset them to the default configuration values.
`rap-wml`	Clear wired MAC lookup cache for a DB server.

Parameter	Description
`update-counter`	Clear all update counter statistics.

`voice`	Clear all voice state information. Use the following parameters:
	• `call-counters`
	• `call-status`
	• statistics
	  ▪ `cac`
	  ▪ `tspec-enforcement`

`vpdn`	Clear all VPDN configuration for L2TP and PPTP tunnel. Use the following parameters: • `tunnel l2tp id <l2tp-tunnel-id>` • tunnel pptp id <pptp-tunnel-id>

`wms`	Clear all WLAN management commands. Use the following parameters:
	• `ap`—clear all AP related commands. Specify the BSSID of the AP.
	• `client`—clear all wired client related commands. Specify the MAC address of the client.
	• `probe`—clear all probe information. Specify the BSSID of the probe.
	• `wired-mac`—clear all wired MAC information. You can specify MAC of APs, or name of an AP.
	  ▪ `wired-mac <mac-address>`
	  ▪ `wired-mac ap-name <name of the AP>`

Usage Guidelines

The clear command will clear the specified parameters of their current values.

Example

The following command clears all aaa counters for all authentication servers:

```
(host) (config) #clear aaa authentication-server all
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

clock set

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

Description

This command sets the date and time.

Syntax

Parameter	Description	Range
`year`	Sets the year. Requires all 4 digits.	Numeric
`month`	Sets the month. Requires the first three letters of the month.	Alphabetic
`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. You must configure all four parameters.

Specify the time using a 24-hour clock. You must specify the seconds.

Example

The following example configures the clock to January 1st of 2007, at 1:03:52 AM.

```
(host)(config) #clock set 2007 jan 1 1 3 52
```

Command History

This command was introduced in ArubaOS 1.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

clock summer-time recurring

```
clock summer-time <WORD> [recurring]
   <1-4> <start day> <start month> <hh:mm>
   first <start day> <start month> <hh:mm>
   last <start day> <start month> <hh:mm>
   <1-4> <end day> <end month> <hh:mm>
   first <end day> <end month> <hh:mm>
   last <end day> <end month> <hh:mm>
   [<-23 - 23>]
```

Description

Set the software clock to begin and end daylight savings time on a recurring basis.

Syntax

Parameter	Description	Range
WORD	Enter the abbreviation for your time zone. For example, PDT for Pacific Daylight Time.	3-5 characters
1-4	Enter the week number to start/end daylight savings time. For example, enter 2 to start daylight savings time on the second week of the month.	1-4
first	Enter the keyword **first** to have the time change begin or end on the first week of the month.	—
last	Enter the keyword **last** to have the time change begin or end on the last week of the month.	—
start day	Enter the weekday when the time change begins or ends.	Sunday-Saturday
start month	Enter the month when the time change begins or ends.	January-December
hh:mm	Enter the time, in hours and minutes, that the time change begins or ends.	24 hours
-23 - 23	Hours offset from the Universal Time Clock (UTC).	-23 - 23

Usage Guidelines

This command subtracts exactly 1 hour from the configured time.

The WORD can be any alphanumeric string, but cannot start with a colon (:). A WORD longer than five characters is not accepted. If you enter a WORD containing punctuation, the command is accepted, but the timezone is set to UTC.

You can configure the time to change on a recurring basis. To do so, set the week, day, month, and time when the change takes effect (daylight savings time starts). You must also set the week, day, month, and time when the time changes back (daylight savings time ends).

The `start day` requires the first three letters of the day. The `start month` requires the first three letters of the month.

You also have the option to set the number of hours by which to offset the clock from UTC. This has the same effect as the clock timezone command.

Example

The following example sets daylight savings time to occur starting at 2:00 AM on Sunday in the second week of March, and ending at 2:00 AM on Sunday in the first week of November. The example also sets the name of the time zone to PST with an offset of UTC - 8 hours.

```
clock summer-time PST recurring 2 Sun Mar 2:00 first Sun Nov 3:00 -8
```

Command History

This command was introduced in ArubaOS 1.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

clock timezone

`clock timezone <name> <-23 to 23>`

Description

This command sets the timezone on the controller.

Syntax

Parameter	Description	Range
`<name>`	Name of the time zone.	3-5 characters
`-23 to 23`	Hours offset from UTC.	-23 to 23

Usage Guidelines

The **name** parameter can be any alphanumeric string, but cannot start with a colon (:). A time zone name longer than five characters is not accepted. If you enter a time zone name containing punctuation, the command is accepted, but the timezone is set to UTC.

Example

The following example configures the timezone to PST with an offset of UTC - 8 hours.

```
clock timezone PST -8
```

Command History

This command was introduced in ArubaOS 1.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

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:

```
(host) (config) #
To return to enable mode, enter Ctrl-Z or exit.
```

Example

The following command allows you to enter configuration commands:

```
(host) # configure terminal
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

controller-ip

```
controller-ip [loopback|vlan <VLAN ID>]
   no ...
```

Description

This command sets the controller IP to the loopback interface address or a specific VLAN interface address.

Syntax

Parameter	Description	Default
`loopback`	Sets the controller IP to the loopback interface.	disabled
`vlan`	Set the controller IP to a VLAN interface.	—
`VLAN ID`	Specifies the VLAN interface ID.	—

Usage Guidelines

This command allows you to set the controller IP to the loopback interface address or a specific VLAN interface address. If the controller IP command is not configured then the controller IP defaults to the loopback interface address. If the loopback interface address is not configured then the first configured VLAN interface address is selected. Generally, VLAN 1 is the factory default setting and thus becomes the controller IP address.

Example

The following command sets the controller IP address to VLAN interface 6.

```
(host) (config) #controller-ip vlan 6
```

Related Commands

```
(host) (config) #show controller-ip
```

Command History

This command was introduced in ArubaOS 3.4

Command Information

Platform	License	Command Mode
Available on all platforms	Base operating system	Config mode on master controllers

control-plane-security

```
control-plane-security
   auto-cert-allowed-addrs <ipaddress-start> <ipaddress-end>
   auto-cert-allow-all
   auto-cert-prov
   cpsec-enable
   no ...
```

Description

Configure the control plane security profile by identifying APs to receive security certificates.

Syntax

Parameter	Description
`auto-cert-allowed-addrs <ipaddress-start> <ipaddress-end>`	Use this command to define a specific range of AP IP addresses. The controller will send certificates to the APs in this IP range when auto certificate provisioning is enabled. Identify a range by entering the starting IP address and the ending IP address in the range, separated by a single space. You can repeat this command as many times as necessary to define multiple IP ranges.
`auto-cert-allow-all`	When you issue the **control-plane-security auto-cert-allow-all** command, the controller will send a certificate to all associated APs when auto certificate provisioning is enabled. When disabled, the controller sends certificates only to APs whose IP addresses are in the ranges specified by **auto-cert-allowed-addrs**.
`auto-cert-prov`	Issue this command to enable automatic certificate provisioning. When this feature is enabled, the controller will attempt to send certificates to associated APs. To disable this feature, use the command **no auto-cert-prov**. Automatic certificate provisioning is disabled by default
`cpsec-enable`	Issue this command to enable control plane security. To disable this feature, use the command **no cpsec-enable**. Control plane security is enabled by default.

Usage Guidelines

Controllers enabled with control plane security will only send certificates to APs that you have identified as valid APs on the network. If you are confident that all campus APs currently on your network are valid APs, you can configure automatic certificate provisioning to send certificates from the controller to each campus AP, or to all campus APs within a specific range of IP addresses. If you want closer control over each AP that gets certified, you can manually add individual campus APs to the secure network by adding each AP's information to a campus AP whitelist.

Example

The following command defines a range of IP addresses that should receive certificates from the controller, and enables the control plane security feature:

```
(host)(config) # control-plane-security
   auto-cert-allowed-addrs 10.21.18.10 10.21.10.90
   cpsec-enable
```

Related Commands

Command	Description	Mode
`show control-plane-security`	Show the current configuration of the control plane security profile.	Config mode

Command History

This command was introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on master or local controllers

copy

```
copy
flash: <srcfilename> {flash: <destfilename> | scp: <scphost> <username>
<destfilename> |
   tftp: <tftphost> <destfilename>} |
ftp: <ftphost> <user> <filename> system: partition {0|1} |
running-config {flash: <filename> | ftp: <ftphost> <user> <password> <filename>
   [<remote-dir>] | startup-config | tftp: <tftphost> <filename>} |
scp: <scphost> <username> <filename> {flash: <destfilename>| system: partition [0|1]}|
startup-config {flash: <filename> | tftp: <tftphost> <filename>} |
system: partition {<srcpartition> 0|1} [<destpartition> 0 | 1] |
tftp: <tftphost> <filename> {flash: <destfilename> | system: partition [0|1]}
```

Description

This command copies files to and from the controller.

Syntax

Parameter	Description
`flash:`	Copy the contents of the controller's flash file system, the system image, to a specified destination.
`srcfilename`	Full name of the flash file to be copied.
`flash:`	Copy the file to the flash file system.
`destfilename`	Specify the new name of the copied file.
`tftp:`	Copy the file to a TFTP server.
`tftphost`	Specify the IP address or hostname of the TFTP server.
`ftp:`	Copy a file from the FTP server.
`ftphost`	Specify the IP address or hostname of the FTP server.
`user`	User account name required to access the FTP server.
`filename`	Full name of the file to be copied.
`0 | 1`	Specify the system partition to save the file.
`running-config`	Copy the active, running configuration to a specified destination.
`flash:`	Copy the configuration to the flash file system.
`filename`	Specify the new name of the copied configuration file.
`ftp:`	Using FTP, copy the configuration to an FTP server.
`ftphost`	Specify the IP address of the FTP server.
`user`	User account name required to access the FTP server.
`password`	Password required to access the FTP server.
`remote-dir`	Specify a remote directory, if needed.
`startup-config`	Copy the active, running configuration to the start-up configuration.
`tftp:`	Using TFTP, copy the configuration to a TFTP server
`tftphost`	Specify the IP address or hostname of the TFTP server.
`scp:`	Copy an ArubaOS image file or file from the flash file system using the Secure Copy protocol. The SCP server or remote host must support SSH version 2 protocol.
`scphost`	Specify the IP address of the SCP server or remote host.
`username`	User account name required to access the SCP server or remote host.
`filename`	Specify the absolute path of the filename to be copied.
`flash:`	Copy the file to the flash file system.
`destfilename`	Specify the new name of the copied file.
`system:`	Copy the file to the system partition.
`startup-config`	Copy the startup configuration to a specified flash file or to a TFTP server.
`flash:`	Copy the file to the flash file system.
`filename`	Specify the new name of the copied startup configuration file.
`tftp:`	Using TFTP, copy the startup configuration to a TFTP server

Parameter	Description
`tftphost`	Specify the IP address or hostname of the TFTP server.
`system:`	Copy the specified system partition
`srcpartition`	Disk partition from which to copy the system data, as either 0 or 1.
`destpartition`	Disk partition to copy the system data to, as either 0 or 1.
`tftp:`	Copy a file from the specified TFTP server to either the controller or another destination. This command is typically used when performing a system restoration, or to pull a specified file name into the wms database.
`tftphost`	Specify the IP address or hostname of the TFTP server.
`filename`	Full name of the file to be copied.
`flash:`	Copy the file to the flash file system
`destfilename`	Specify the new name of the copied file.
`system`	Copy the file to the system partition.

Usage Guidelines

Use this command to save back-up copies of the configuration file to an FTP or TFTP server, or to load a saved file from an FTP or TFTP server.

Three partitions reside on the file system flash. Totalling 256MB, the three partitions provide space to hold the system image files (in partitions 1 and 2 which are 45MB each) and user files (in partition 3, which is 165MB). System software runs on the system partitions; the database, DHCP, startup configuration, and logs are positioned on the user partition.

To restore a database, copy the database from the network server and import the database.

To restore a configuration file, copy the file from network server to the controller's flash system then copy the file from the flash system to the system configuration. This ensures that you do not accidentally overwrite your system startup configuration file.

Example

The following commands copy the configuration file named engineering from the TFTP server to the controller's flash file system and then uses that file as the startup configuration. This example assumes the startup configuration file is named default.cfg:

```
(host) (config) #copy tftp: 192.0.2.0 engineering flash: default.bak
copy flash: default.bak flash: default.cfg
```

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config modes on master controllers

cp-bandwidth-contract

```
cp-bandwidth-contract <name> {mbits <1..2000>}|{kbits <256..2000000>}
```

Description

This command configures a bandwidth contract traffic rate which can then be associated with a whitelist session ACL.

Syntax

Parameter	Description
`<name>`	Name of a bandwidth contract.
`mbits <1..2000>`	Set a bandwidth rate inn mbits/seconds.
`kbits <256..2000000>`	Set a bandwidth rate in kbits/seconds.

Example

The following example configures a bandwidth contract named “cp-rate” with a rate of 10,000Kbps.

```
(host)(config) #cp-bandwidth-contract cp-rate kbits 10000
```

Related Commands

Command	Description	Mode
`show cp-bwcontracts`	Display a list of Control Processor (CP) bandwidth contracts for whitelist ACLs.	Enable or Config modes
`firewall cp`	This command creates a new whitelist ACL and can associate a bandwidth contract with that ACL.	Enable or Config modes

Command History

This command was introduced in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license.	Config mode on master controllers

crypto dynamic-map

```
crypto dynamic-map <name> <priority>
   no ...
   set puffs {group1|group2}
   set security-association lifetime seconds <seconds>
   set transform-set <name1> [<name2>] [<name3>] [<name4>]
```

Description

This command configures a new or existing dynamic map.

Syntax

Parameter	Description	Range	Default
<name>	Name of the map.	—	—
<priority>	Priority of the map.	1-10000	10000
no	Negates a configured parameter.	—	—
pfs	Enables Perfect Forward Secrecy (PFS) mode. Use one of the following: group1: 768-bit Diffie Hellman prime modulus group group2: 1024-bit Diffie Hellman prime modulus group	group1/ group2	disabled
seconds	Configures the lifetime, in seconds, for the security association (SA).	300-86400	no limit
transform-set	Name of the transform set for this dynamic map. You can specify up to four transform sets. You configure transform sets with the crypto ipsec transform-set command.	—	default-transform

Usage Guidelines

Dynamic maps enable IPsec SA negotiations from dynamically addressed IPsec peers. Once you have defined a dynamic map, you can associate that map with the default global map using the command crypto map global-map.

Example

The following command configures a dynamic map:

```
(host) (config)# crypto dynamic-map dmap1 100
set pfs group2
set security-association lifetime seconds 300
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base OS	Config mode on master controllers

crypto ipsec

```
crypto ipsec {mtu <max-mtu>}|{transform-set <transform-set-mtu> esp-3des|esp-
aes128|esp-aes192|esp-aes256|esp-des  esp-md5-hmac|esp-sha-hmac}
```

Description

This command configures IPsec parameters.

Syntax

Parameter	Description	Range	Default
`mtu`	Configure IPsec Maximum Transmission Unit (MTU) parameters.	—	—
`<max-mtu>`	Configure IPsec MTU.	1024-1500	1500
`transform-set`	Create or modify a transform set.	—	—
`<transform-set-mtu>`	Name of the transform set to create or modify.	—	—
`esp-3des`	Use ESP with 168-bit 3DES encryption.	—	—
`esp-aes128`	Use ESP with 128-bit AES encryption.	—	—
`esp-aes192`	Use ESP with 192-bit AES encryption.	—	—
`esp-aes256`	Use ESP with 256-bit AES encryption.	—	—
`esp-des`	Use ESP with 56-bit DES encryption.	—	—
`esp-md5-hmac`	Use ESP with the MD5 (HMAC variant) authentication algorithm		
`esp-sha-hmac`	Use ESP with the SHA (HMAC variant) authentication algorithm		

Usage Guidelines

Define the Maximum Transmission Unit (MTU) size allowed for network transmissions using IPsec security, and create or edit transform sets that define a specific encryption and authentication type.

Example

The following command configures 3DES encryption and MD5 authentication for a transform set named set1:

```
(host) (config)# crypto ipsec transform-set set1 esp-3des esp-md5-hmac
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

crypto isakmp

```
crypto isakmp
   {address <peer-address> netmask <mask>}|enable|disable|{groupname <name>} |
   {key <keystring> address <peer-address> netmask <mask>}|
   {udpencap-behind-natdevice enable|disable}|
   packet-dump
```

Description

This command configures Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Syntax

Parameter	Description
`address`	Configure the IP address for the global group key.
`<peer-address>`	IP address for the group key, in dotted-decimal format.
`netmask`	Configure the IP netmask for the group key.
`<mask>`	Subnet mask for the group key.
`enable`	Enable IKE processing.
`disable`	Disable IKE processing.
`groupname`	Configure the IKE Aggressive group name. Aggressive-mode IKE is a 3-packet IKE exchange that does not provide identity-protection, but is faster, because fewer messages are exchanged.
`<name>`	Name of the IKE aggressive group.
`key`	Configure the IKE preshared key.
`<keystring>`	Configure the value of the IKE PRE-SHARED key. The key must be between 6-64 characters long.
`address`	Configure the IP address for the group key.
`<peer-address>`	An IP for the group key, in dotted-decimal format.
`netmask`	Configure the netmask for the group key IP address.
`<mask>`	A subnet mask, in dotted-decimal format
`udpencap-behind-natdevice`	Configure NAT-T if controller is behind NAT device. Only for Windows VPN Dialer
`enable`	Enable Nat-T. (This is the recommended setting if the controller is behind a NAT device.)
`disable`	Disable Nat-T.
`packet-dump`	Enable the packet dump feature to troubleshoot an IPsec tunnel establishment by looking at the packet exchanges between the controller and the remote AP or the other IPsec peer. The packet dump output is saved to a file named ike.pcap. **NOTE:** This is a testing feature only, and should not be enabled on a production network. To disable this feature, use the command **no crypto isakmp packet-dump.**

Usage Guidelines

Preshared key (PSK)-refresh allows you to refresh the IKE PSK used by remote APs. By default, PSK-refresh is disabled. With PSK-refresh enabled, the controller accepts connections from remote APs using the previously configured PSK for the specified interval. After the interval elapses, that PSK expires and the controller uses the

new PSK to authenticate remote APs. If you enable and then disable PSK-refresh, the remote AP attempts to authenticate with the currently configured global PSK only.

To enable PSK-refresh, you must:

1. Configure the amount of time in days or hours (known as the interval), to remember the previously configured PSK used in your remote AP deployment.

   NOTE: Best practices is to configure a large interval to prevent remote APs from being unable to authenticate and connect to the network. Consider your existing PSK interval when configuring this feature.

2. Configure the global PSK using the command **crypto isakmp key**. The IP address must be 0.0.0.0, and the netmask must be 0.0.0.0.

Example

The following command configures an ISAKMP peer IP address and subnet mask. After configuring an ISAKMP address and netmask, you will be prompted to enter the IKE preshared key.

```
(host)(config) #crypto isakmp address 10.3.14.21 netmask 255.255.255.0
Key:*******
Re-Type Key:*******
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

crypto isakmp policy

```
crypto isakmp policy
   authentication pre-share|rsa-sig
   encryption 3DES|AES128|AES192|AES256|DES
   group 1|2
   hash md5|sha
   lifetime <seconds>
```

Description

This command configures Internet Key Exchange (IKE) policy parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Syntax

Parameter	Description
`policy`	Configure an IKE policy
`<priority>`	Specify a number from 1 to 10,000 to define a priority level for the policy. The higher the number, the higher the priority level.
`authentication`	Configure the IKE authentication method.
`pre-share`	Use Pre Shared Keys for IKE authentication. This is the default authentication type.
`rsa-sig`	Use RSA Signatures for IKE authentication.
`encryption`	Configure the IKE encryption algorithm.
`3DES`	Use 168-bit 3DES-CBC encryption algorithm. This is the default encryption value.
`AES128`	Use 128-bit AES-CBC encryption algorithm.
`AES192`	Use 192-bit AES-CBC encryption algorithm.
`AES256`	Use 256-bit AES-CBC encryption algorithm.
`DES`	Use 56-bit DES-CBC encryption algorithm.
`group`	Configure the IKE Diffie Hellman group.
`1`	Use the 768-bit Diffie Hellman prime modulus group.
`2`	Use the 1024-bit Diffie Hellman prime modulus group. This is the default group setting.
`hash`	Configure the IKE hash algorithm
`md5`	Use MD5 (HMAC variant) as the hash algorithm.
`sha`	Use SHA-1 (HMAC variant) as the hash algorithm. This is the default policy algorithm.
`lifetime <seconds>`	Specify the lifetime of the IKE security association (SA), from 300 - 86400 seconds.

Usage Guidelines

To define settings for a ISAKMP policy, issue the command **crypto isakmp policy <priority>** then press **Enter**. The CLI will enter config-isakmp mode, which allows you to configure the policy **authentication**, **encryption**, **group**, **hash algorithm** and **lifetime** values.

Example

The following command configures an ISAKMP peer IP address and subnet mask. After configuring an ISAKMP address and netmask, you will be prompted to enter the IKE preshared key.

```
(host)(config) #crypto isakmp policy1
(host)(config-isakmp) #auth rsa-sig
                      lifetime 86400
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

crypto map global-map

```
crypto map global-map <map-number> ipsec-isakmp {dynamic <dynamic-map-name>}|{ipsec
<ipsec-map-name>}
```

Description

This command configures the default global map.

Syntax

Parameter	Description
<map-number>	Priority of the map.
dynamic	Use a dynamic map.
<dynamic-map-name>}	Name of the dynamic map.
ipsec	Use a IPsec map.
<ipsec-map-name>	Name of an IPsec map.

Usage Guidelines

This command identifies the dynamic or ipsec map used as the default global map. If you have not yet defined a dynamic or ipsec map, issue the command crypto map global-map or crypto-local ipsec-map to define map parameters.

Example

The following command configures the global map with the dynamic map named *dynamic_map_2*.

```
(host)(config) #crypto map global-map 2 ipsec-isakmp dynamic dynamic_map_2
```

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

crypto pki

```
crypto pki csr key <key_val> common_name <common_val> country <country_val>
state_or_province <state> city <city_val> organization <organization_val> unit
<unit_val> email <email_val>
```

Description

Generate a certificate signing request (CSR) for the captive portal feature.

Syntax

Parameter	Description
`key <key_val>`	Specify the CSR key length:**1024**, **2048**, or **4096.**
`common_name <common_val>`	Specify a common name, e.g., www.yourcompany.com.
`country <country_val>`	Specify a country name, e.g., US or CA.
`state_or_province <state>`	Specify the name of a state or province.
`city <city_val>`	Specify the name of a city.
`organization <organization_val>`	Specify the name of an organization unit, e.g., sales.
`unit <unit_val>`	Specify a unit value, e.g. EMEA.
`email <email_val>`	Specify an email address, in the format name@mycompany.com.

Usage Guidelines

Use this command to generate a CSR for the Captive Portal feature. Display the CSR output by entering the command **show crypto pki csr**. Note that this command will only generate CSR on a controller running ArubaOS 3.x or later. Earlier versions require that you generate the certificate externally.

Example

The following command configures a CSR for a user with the email address *jdoe@example.com*.

```
(host)(config) #crypto pki csr key 1024 common_name www.example.lcom country US state_or_province ca cit
organization engineering unit pubs email jdoe@example.com
```

Command History

This command was introduced in ArubaOS 3.1

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

crypto pki-import

```
crypto pki-import {der|pem|pfx|pkcs12|pkcs7} {PublicCert|ServerCert|TrustedCA} <name>
```

Description

Import certificates for the captive portal feature.

Syntax

Parameter	Description
`der`	Import a certificate in DER format.
`pem`	Import a certificate in x509 PEM format.
`pfx`	Import a certificate in PFX format.
`pkcs12`	Import a certificate in PKCS12 format.
`pkcs7`	Import a certificate in PKCS7 format.
`PublicCert`	Import a public certificate.
`ServerCert`	Import a server certificate.
`TrustedCA`	Import a trusted CA certificate.
`<name>`	Name of a certificate.

Usage Guidelines

Use this command to install a CSR for the Captive Portal feature.

Example

The following command installs a server certificate in DER format.

```
(host)(config) #crypto pki-import der ServerCert cert_20
```

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

crypto-local ipsec-map

```
crypto-local
crypto-local ipsec-map <map> <priority>
   dst-net <ipaddr> <mask>
   force-natt
   no ...
   local-fqdn <local_id_fqdn>
   peer-ip <ipaddr>
   pre-connect {disable|enable}
   set ca-certificate <cacert-name>
   set pfs {group1|group2}
   set security-association lifetime seconds <seconds>
   set server-certificate <cert-name>
   set transform-set <name1> [<name2>] [<name3>] [<name4>]
   src-net <ipaddr> <mask>
   trusted {disable|enable}
   vlan <vlan>
```

Description

This command configures IPsec mapping for site-to-site VPN.

Syntax

Parameter	Description	Range	Default
`<map>`	Name of the IPsec map.	—	—
`<priority>`	Priority of the entry.	1-9998	—
`dst-net`	IP address and netmask for the destination network.	—	—
`force-natt`	Include this parameter to always enforce UDP 4500 for IKE and IPSEC. This option is disabled by default.	—	—
`no`	Negates a configured parameter.	—	—
`local-fqdn <local_id_fqdn>`	If the local controller has a dynamic IP address, you must specify the fully qualified domain name (FQDN) of the controller to configure it as a initiator of IKE aggressive-mode.		
`peer-ip <ipaddr>`	IP address of the peer gateway. **NOTE:** If you are configuring an IPsec map for a static-ip controller with a dynamically addressed remote peer, you must leave the peer gateway set to its default value of 0.0.0.0.	—	—
`pre-connect`	Enables or disables pre-connection.	enable/ disable	disabled
`set ca-certificate <cacert-name>`	User-defined name of a trusted CA certificate installed in the controller. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the controller.	—	—
`set pfs`	If you enable Perfect Forward Secrecy (PFS) mode, new session keys are not derived from previously used session keys. Therefore, if a key is compromised, that compromised key will not affect any previous session keys. To enable this feature, specify one of the following Perfect Forward Secrecy modes: • **group1**: 768-bit Diffie Hellman prime modulus group • **group2**: 1024-bit Diffie Hellman prime modulus group	group1/ group2	disabled
`set security-association lifetime seconds <seconds>`	Configures the lifetime, in seconds, for the security association (SA).	300-86400	7200 seconds
`set server-certificate <cert-name>`	User-defined name of a server certificate installed in the controller. Use the **show crypto-local pki ServerCert** command to display the server certificates that have been imported into the controller.	—	—
`set transform-set <name1>`	Name of the transform set for this IPsec map. One transform set name is required, but you can specify up to four transform sets. Configure transform sets with the **crypto ipsec transform-set** command.	—	default-transform
`src-net <ipaddr> <mask>`	IP address and netmask for the source network.	—	—
`trusted`	Enables or disables a trusted tunnel.	enable/ disable	disabled
`vlan <vlan>`	VLAN ID. Enter 0 for the loopback.	1-4094	—

Usage Guidelines

You can use controllers instead of VPN concentrators to connect sites at different physical locations.

You can configure separate CA and server certificates for each site-to-site VPN. You can also configure the same CA and server certificates for site-to-site VPN and client VPN. Use the **show crypto-local ipsec-map** command to display the certificates associated with all configured site-to-site VPN maps; use the **tag <map>** option to display certificates associated with a specific site-to-site VPN map.

ArubaOS supports site-to-site VPNs with two statically addressed controllers, or with one static and one dynamically addressed controller. By default, site-to-site VPN uses IKE Main-mode with Pre-Shared-Keys to authenticate the IKE SA. This method uses the IP address of the peer, and therefore will not work for dynamically addressed peers.

To support site-site VPN with dynamically addressed devices, you must enable IKE Aggressive-Mode with Authentication based on a Pre-Shared-Key. A controller with a dynamic IP address must be configured to be the initiator of IKE Aggressive-mode for Site-Site VPN, while the controller with a static IP address must be configured as the responder of IKE Aggressive-mode.

Examples

The following commands configures site-to-site VPN between two controllers:

```
(host) (config) #crypto-local ipsec-map sf-chi-vpn 100
   src-net 101.1.1.0 255.255.255.0
   dst-net 100.1.1.0 255.255.255.0
   peer-ip 172.16.0.254
   vlan 1
   trusted

(host) (config) #crypto-local ipsec-map chi-sf-vpn 100
   src-net 100.1.1.0 255.255.255.0
   dst-net 101.1.1.0 255.255.255.0
   peer-ip 172.16.100.254
   vlan 1
   trusted
```

For a dynamically addressed controller that initiates IKE Aggressive-mode for Site-Site VPN:

```
(host) (config)crypto-local ipsec-map <name> <priority>
   src-net <ipaddr> <mask>
   dst-net <ipaddr> <mask>
   peer-ip <ipaddr>
   local-fqdn <local_id_fqdn>
   vlan <id>
   pre-connect enable|disable
   trusted enable
```

For the Pre-shared-key:

```
crypto-local isakmp key <key> address <ipaddr> netmask <mask>
```

```
For a static IP controller that responds to IKE Aggressive-mode for Site-Site VPN:
```

```
(host) (config)crypto-local ipsec-map <name2> <priority>
   src-net <ipaddr> <mask>
   dst-net <ipaddr> <mask>
   peer-ip 0.0.0.0
   peer-fqdn fqdn-id <peer_id_fqdn>
   vlan <id>
   trusted enable
```

For the Pre-shared-key:

```
crypto-local isakmp key <key> fqdn <fqdn-id>
```

For a static IP controller that responds to IKE Aggressive-mode for Site-Site VPN with One PSK for All FQDNs:

```
(host) (config)crypto-local ipsec-map <name2> <priority>
   src-net <ipaddr> <mask>
   peer-ip 0.0.0.0
   peer-fqdn any-fqdn
   vlan <id>
   trusted enable
```

For the Pre-shared-key for All FQDNs:

```
   crypto-local isakmp key <key> fqdn-any
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

crypto-local isakmp ca-certificate

```
crypto-local isakmp ca-certificate <cacert-name>
```

Description

This command assigns the Certificate Authority (CA) certificate used to authenticate VPN clients.

Syntax

Parameter	Description
`ca-certificate`	User-defined name of a trusted CA certificate installed in the controller. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the controller.

Usage Guidelines

You can assign multiple CA certificates. Use the **show crypto-local isakmp ca-certificate** command to view the CA certificates associated with VPN clients.

Example

This command configures a CA certificate:

```
crypto-local isakmp ca-certificate TrustedCA1
```

Command History

This command was introduced in ArubaOS 3.2.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

crypto-local isakmp dpd

```
crypto-local isakmp dpd idle-timeout <seconds> retry-timeout <seconds>  retry-attempts
<number>
```

Description

This command configures IKE Dead Peer Detection (DPD) on the local controller.

Syntax

Parameter	Description	Range	Default
`idle-timeout`	Idle timeout, in seconds.	10-3600	22 seconds
`retry-timeout`	Retry interval, in seconds.	2-60	2 seconds
`retry-attempts`	Number of retry attempts.	3-10	3

Usage Guidelines

DPD is enabled by default on the controller for site-to-site VPN.

Example

This command configures DPD parameters:

```
crypto-local isakmp dpd idle-timeout 60 retry-timeout 3 retry-attempts 5
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master and local controllers

crypto-local isakmp key

```
crypto-local isakmp key <key> {address <peer-ipaddr> netmask <mask>}|{fqdn <ike-id-fqdn>}|fqdn-any
```

Description

This command configures the IKE preshared key on the local controller for site-to-site VPN.

Syntax

Parameter	Description
`key <key>`	IKE preshared key value, between 6-64 characters.
`address <peer-ipaddr>`	IP address for the preshared key.
`netmask <mask>`	Netmask for the preshared key.
`fqdn <ike-id-fqdn>`	Configure the PSK for the specified FQDN
`fqdn-any`	Configure the PSK for any FQDN

Usage Guidelines

This command configures the IKE preshared key.

Example

The following command configures an IKE preshared key for site-to-site VPN:

```
crypto-local isakmp key R8nD0mK3y address 172.16.100.1 netmask 255.255.255.255
```

Command History

Version	Modification
ArubaOS 3.0	Command introduced.
ArubaOS 3.4	The **fqdn** and **fqdn-any** parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master and local controllers

crypto-local isakmp permit-invalid-cert

```
crypto-local isakmp permit-invalid-cert
```

Description

This command allows invalid or expired certificates to be used for site-to-site VPN.

Syntax

No parameters.

Usage Guidelines

This command allows invalid or expired certificates to be used for site-to-site VPN.

Command History

This command was introduced in ArubaOS 3.2.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master and local controllers

crypto-local isakmp server-certificate

```
crypto-local isakmp server-certificate <cert-name>
```

Description

This command assigns the server certificate used to authenticate the controller for VPN clients.

Syntax

Parameter	Description
`server-certificate`	User-defined name of a server certificate installed in the controller. Use the **show crypto-local pki ServerCert** command to display the server certificates that have been imported into the controller.

Usage Guidelines

This certificate is only for VPN clients and not for site-to-site VPN clients. You can assign only one server certificate for use with VPN clients. Use the **show crypto-local isakmp server-certificate** command to view the server certificate associated with VPN clients. You must import and configure server certificates separately on master and local controllers.

Note: There is a default server certificate installed in the controller, however this certificate does not guarantee security for production networks. Best practices is to replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. You can use the WebUI to generate a Certificate Signing Request (CSR) to submit to a CA and then import the signed certificate received from the CA into the controller. For more information, see "Managing Certificates" in the ArubaOS User Guide.

Example

This command configures a server certificate:

```
crypto-local isakmp server-certificate ServerCert1
```

Command History

This command was introduced in ArubaOS 3.2.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master and local controllers

crypto-local isakmp xauth

```
crypto-local isakmp xauth
```

Description

This command enables IKE XAuth for VPN clients.

Syntax

No parameters.

Usage Guidelines

The **no crypto-local isakmp xauth** command disables IKE XAuth for VPN clients. This command only applies to VPN clients that use certificates for IKE authentication. If you disable XAuth, then a VPN client that uses certificates will not be authenticated using username/password. You must disable XAuth for Cisco VPN clients using CAC Smart Cards.

Example

This command disables IKE XAuth for Cisco VPN clients using CAC Smart Cards:

```
no crypto-local isakmp xauth
```

Command History

This command was introduced in ArubaOS 3.2.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master and local controllers

crypto-local pki

```
crypto-local pki {PublicCert|ServerCert|TrustedCA} <name> <filename>
```

Description

This command is saved in the configuration file when you import a certificate.

Syntax

Parameter	Description
`PublicCert`	Public key of a certificate. This allows an application to identify an exact certificate.
`ServerCert`	Server certificate. This certificate must contain both a public and a private key (the public and private keys must match). You can import a server certificate in either PKCS12 or x509 PEM format; the certificate is stored in x509 PEM DES encrypted format on the controller.
`TrustedCA`	Trusted CA certificate. This can be either a root CA or intermediate CA. Dell encourages (but does not require) an intermediate CA's signing CA to be the controller itself.
`<name>`	Name of the certificate.
`<filename>`	Internal directory structure in the controller in which the imported certificate is stored.

Usage Guidelines

This command in the configuration file verifies the presence of the certificate in the controller's internal directory structure.

Command History

This command was introduced in ArubaOS 3.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	This command appears in the configuration file after you import a certificate

database synchronize

```
database synchronize {[period <minutes>][rf-plan-data]}
```

Description

This command manually synchronizes the database between a pair of redundant master controllers and includes RF Plan data when synchronizing with standby.

Syntax

Parameter	Description
`period`	Configures the interval for automatic database synchronization.
`<minutes>`	Interval in minutes. Range is 1 — 25200 minutes.
`rf-plan-data`	Includes the RF Plan data when synchronizing with standby mode.

Usage Guidelines

This command takes effect immediately. If a peer is not configured, the controller displays an error message.

Use the **database synchronize period** command in config mode to configure the interval for automatic database synchronization. Use the **database synchronize rf-plan-data** command to include RF plan data when synchronizing in standby mode.

Example

The following commands cause the database on the active master controller to synchronize with the standby in 25 minute intervals. The synchronization includes RF plan data.

```
(host) (config) #database synchronize period 25
(host) (config) #database synchronize rf-plan-data
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config modes on master controllers

delete

```
delete {filename <filename>|ssh-host-addr <ipaddr>|ssh-known-hosts}
```

Description

This command deletes a file or RSA signature entry from flash.

Syntax

Parameter	Description
`filename`	Name of the file to be deleted.
`ssh-host-addr`	Deletes the entry stored in flash for the RSA host signature created when you run the **copy scp** command.
`ssh-known -hosts`	Deletes all entries stored in flash for the RSA host signatures created when you run the **copy scp** command.

Usage Guidelines

To prevent running out of flash file space, you should delete files that you no longer need.

The **copy scp** command creates RSA signatures whenever it connects to a new host. These host signatures are stored in the flash file system.

Example

The following command deletes a file:

```
(host) #delete filename december-config-backup.cfg
```

The following command deletes an RSA signature entry from flash:

```
(host) #delete ssh-host-addr 10.100.102.101
```

The following command deletes all RSA signature entries from flash:

```
(host) #delete ssh-known-hosts
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

destination

```
destination <STRING> <A.B.C.D> [invert]
```

Description

This command configures the destination name and address.

Syntax

Parameter	Description	Range
`STRING`	Destination name.	Alphanumeric
`A.B.C.D`	Destination IP address or subnet.	—
`invert`	Specifies all destinations except this one.	—

Usage Guidelines

You can configure the name and IP address of the destination. You can optionally configure the subnet, or invert the selection.

Example

The following example configures a destination called “Home” with an IP address of 10.10.10.10.

```
(host) (config) #destination Home 10.10.10.10
```

Command History

Release	Modification
ArubaOS 1.0	Command introduced
ArubaOS 3.0	Replaced with **netdestination** command.

Command Information

Availability	License	Command Mode
Can be used only on the master controller.	Requires the PEF NG license	Config mode on master controllers

dir

```
dir
```

Description

This command displays a list of files stored in the flash file system.

Syntax

No parameters.

Usage Guidelines

Use this command to view the system files associated with the controller.

Output from this command includes the following:

- The first column contains ten place holders that display the file permissions.
  - First place holder: Displays `-` for a file or `d` for directory.
  - Next three place holders: Display file owner permissions: `r` for read access, `w` for write access permissions, `x` for executable.
  - Following three place holders: Display member permissions: `r` for read access or `x` for executable.
  - Last three place holders: Display non-member permissions: `r` for read access or `x` for executable.
- The second column displays the number of links the file has to other files or directories.
- The third column displays the file owner.
- The fourth column displays group/member information.
- The remaining columns display the file size, date and time the file was either created or last modified, and the file name.

Example

The following command displays the files currently residing on the system flash:

```
(host) #dir
```

The following is sample output from this command:

```
-rw-r--r--    1 root     root         9338 Nov 20 10:33 class_ap.csv
-rw-r--r--    1 root     root         1457 Nov 20 10:33 class_sta.csv
-rw-r--r--    1 root     root        16182 Nov 14 09:39 config-backup.cfg
-rw-r--r--    1 root     root        14174 Nov  9  2005 default-backup-11-8-05.cfg
-rw-r--r--    1 root     root        16283 Nov  9 12:25 default.cfg
-rw-r--r--    1 root     root        22927 Oct 25 12:21 default.cfg.2006-10-25_20-21-38
-rw-r--r--    2 root     root        19869 Nov  9 12:20 default.cfg.2006-11-09_12-20-22
```

Command History

Introduced in ArubaOS 1.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable and Config modes on local or master controllers

dynamic-ip

```
dynamic-ip restart
```

Description

This command restarts the PPPoE or DHCP process.

Syntax

No parameters.

Usage Guidelines

This command can be used to renegotiate DHCP or PPPoE parameters. This can cause new addresses to be assigned on a VLAN where the DHCP or PPPoE client is configured.

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on master controllers

enable

```
enable
```

Description

This user mode command switches the controller into enable mode. The enable mode allows you to access privileged commands.

Usage Guidelines

To enter enable mode, you are prompted for the password configured during the controller's initial setup. Passwords display as asterisks (*) when you enter them.

To change the password, use the config mode "enable secret" command. If you lose or forget the enable mode password, resetting the default admin user password also resets the enable mode password to "enable". See the *ArubaOS User Guide* for more information about resetting the admin and enable mode passwords.

When you are in enable mode, the CLI prompt ends with the hash (#) character.

Example

The following example allows you to enter enable mode on the controller.

```
(host) >enable
Password: ******
(host) #
```

Command History

Command introduced in ArubaOS 1.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	User mode on master or local controllers

enable secret

`enable secret`

Description

This config mode command allows you to change the password for enable mode.

Usage Guidelines

Use this command to change the password for enable mode. To reset the password to the factory default of "enable", use the `no enable` command.

Note: The password must not contain the space and '?' special characters.

Example

The following example allows you to change the password for enable mode.

```
(host) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(host) (config) #enable secret
Password:******
Re-Type password: ******
(host) (config) #
```

Command History

Version	Modification
ArubaOS1.0	Command introduced
ArubaOS 3.3.2	Updated with restriction of the secret phase

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master or local controllers

enable bypass

```
enable bypass
   no enable bypass
```

Description

This config mode command allows you to bypass the enable password prompt and go directly to the privileged command mode.

Usage Guidelines

Use this command when you want to access the privileged mode directly after logging in to the controller and not be prompted to enter an enable mode password.

To restore the enable mode password prompt, use the config mode command. `no enable bypass`.

Example

The following example allows bypass the enable mode password prompt.

```
(host) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(host) (config) #enable bypass
(host) (config) #
```

Command History

Version	Modification
ArubaOS 6.0	Command introduced

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master or local controllers

encrypt

```
encrypt {disable|enable}
```

Description

This command allows passwords and keys to be displayed in plain text or encrypted.

Syntax

Parameter	Description	Default
disable	Passwords and keys are displayed in plain text	—
enable	Passwords and keys are displayed encrypted	enabled

Usage Guidelines

Certain commands, such as **`show crypto isakmp key`**, display configured key information. Use the **`encrypt`** command to display the key information in plain text or encrypted.

Example

The following command allows passwords and keys to be displayed in plain text:

```
(host) #encrypt disable
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on master or local controllers

esi group

```
esi group <name>
esi
   [no] |
   [ping <attributes>] |
   [server <server>]
```

Description

This command configures an ESI group.

Syntax

Parameter	Description
`no`	Negates any configured parameter.
`ping`	Specify the name of a set of ping checking attributes defined via the command **`esi ping`**. Only one set is allowed.
`server`	Specify the name of a server to be added or removed from the ESI group. You define ESI servers via the command **`esi server`**.

Usage Guidelines

Use the `show esi group` command to show ESI group information.

Example

The following command sets up the ESI group named “fortinet.”

```
(host) (config) #esi group fortinet
   ping default
   server forti_1
```

Command History

Introduced in ArubaOS 2.5

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config mode on master or local controllers

esi parser domain

```
esi parser domain <name>
   [no] |
   [peer <peer-ip>] |
   [server <ipaddr>]
```

Description

This command configures an ESI syslog parser domain.

Syntax

Parameter	Description
no	Negates any configured parameter
peer	(Optional.) Specify the IP address of an another controller in this domain. These controllers are notified when the user cannot be found locally. This command is needed only when multiple controllers share a single ESI server
server	Specify the IP address of the ESI server to which the controller listens.

Usage Guidelines

The ESI parser is a generic syslog parser on the controller that accepts syslog messages from external third-party appliances such as anti-virus gateways, content filters, and intrusion detection systems. It processes syslog messages according to user-defined rules and takes configurable actions on the corresponding system users.

ESI servers (see “esi server” on page 21) are configured into domains to which ESI syslog parser rules (see “esi parser rule” on page 15) are applied.

Use the **`show esi parser domains`** command to show ESI parser domain information.

Example

The following commands configure a virus syslog parser domain named “fortinet” which contains the ESI server “forti_1” with the trusted IP address configured using the command “esi server” on page 21.

```
(host) (config) #esi parser domain fortinet
server 10.168.172.3
```

Command History

Introduced in ArubaOS 3.1.

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config mode on master or local controllers

esi parser rule

```
esi parser rule <rule_name>
   [condition <expression>] |
   [domain <name>] |
   [enable]
   [match {ipaddr <expression> | mac <expression> | user <expression> }] |
   [no] |
   [position <position>] |
   [set {blacklist | role <role>} |
   [test {msg <msg> | file <filename>}]
```

Description

This command creates or changes an ESI syslog parser rule.

Syntax

Parameter	Description	Range	Default
`condition`	Specifies the REGEX (regular expression) pattern that uniquely identifies the syslog.	—	—
`domain`	(Optional.) Specify the ESI syslog parser domain to which this rule applies. If not specified, the rule matches with all configured ESI servers.	—	—
`enables`	Enables this rule. **Note**: The condition, user match, and set action parameters must be configured before the rule can be enabled.	—	Not enabled
`match`	Specifies the user identifier to match, where ipaddr, mac, and user take a REGEX pattern that uniquely identifies the user.	—	—
`no`	Negates any configured parameter.	—	—
`position`	Specifies the rule's priority position.	1–32; 1 highest	—
`set`	Specifies the action to take: blacklist the user or change the user role. **Note**: The role entity should be configured before it is accepted by the ESI rule.	—	—
`test`	Test the regular expression output configured in the esi parser rules command. You can test the expressions against a specified syslog message, or test the expression against a sequence of syslog messages contained in a file.	—	—

Usage Guidelines

The user creates an ESI rule by using characters and special operators to specify a pattern that uniquely identifies a syslog message. This "condition" defines the type of message and the ESI domain to which this message pertains. The rule contains three major fields:

- Condition: The pattern that uniquely identifies the syslog message type.
- User: The username identifier. It can be in the form of a name, MAC address, or IP address.
- Action: The action to take when a rule match occurs.

Once a condition match occurs, no further rule-matching will be made. For the matching rule, only one action can be defined.

For more details on the character-matching operators, repetition operators, and expression anchors used to defined the search or match target, see the External Services Interface chapter in the *ArubaOS User Guide*.

Use the **`show esi parser rules`** command to show ESI parser rule information. Use the **`show esi parser stats`** command to show ESI parser rule statistical information

Examples

The following command sets up the Fortigate virus rule named “forti_rule.” This rule parses the virus detection syslog scanning for a condition match on the log_id value (log_id=) and a match on the IP address (src=).

```
(host) (config) #esi parser rule forti_rule
   condition “log_id=[0-9]{10}[ ]”
   match ipaddr “src=(.*)[ ]”
   set blacklist
   domain fortinet
   enable
```

In this example, the corresponding ESI expression is:

```
< Sep 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
```

The following example of the test command tests a rule against a specified single syslog message.

```
test msg "26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4"

< 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
=====
Condition:     Matched with rule "forti_rule"
User:          ipaddr = 1.2.3.4
=====
```

The following example of the test command tests a rule against a file named test.log, which contains several syslog messages.

```
test file test.log

 < Sep 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
==========
Condition:      Matched with rule "forti_rule"
User:           ipaddr = 1.2.3.4
==========

 < Oct 18 10:43:40  cli[627]: PAPI_Send: To: 7f000001:8372 Type:0x4 Timed out. >
==========
Condition:      No matching rule condition found
==========

 < Oct 18 10:05:32  mobileip[499]: <500300> <DBUG> |mobileip|  Station 00:40:96:a6:a1:
a4,
10.0.100.103: DHCP FSM received event: RECEIVE_BOOTP_REPLY current: PROXY_DHCP_NO_PROX
Y, next: PROXY_DHCP_NO_PROXY >
==========
Condition:      No matching rule condition found
==========
```

Command History

Introduced in ArubaOS 3.1

Command Information

Platform	License	Command Mode
Available on all platforms.	Requires the PEFNG license	Config mode on master and local controllers

esi parser rule-test

```
esi parser rule-test
   [file <filename>] |
   [msg <msg>]
```

Description

This command allows you to test all of the enabled parser rules.

Syntax

Parameter	Description
`file`	Tests against a specified file containing more than one syslog message.
`msg`	Tests against a syslog message, where <msg> is the message text.

Usage Guidelines

You can test the enabled parser rules against a syslog message input, or run the expression through a file system composed of syslog messages. The command shows the match result as well as the user name parsed for each message.

Example

The following command tests against a specified single syslog message.

```
(host) (config) #esi parser rule-test msg
"26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4"

< 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
=====
Condition:     Matched with rule "forti_rule"
User:          ipaddr = 1.2.3.4
=====
```

The following command tests against a file named test.log, which contains several syslog messages.

```
esi parser rule-test file test.log

 < Sep 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
==========
Condition:      Matched with rule "forti_rule"
User:           ipaddr = 1.2.3.4
==========

 < Oct 18 10:43:40  cli[627]: PAPI_Send: To: 7f000001:8372 Type:0x4 Timed out. >
==========
Condition:      No matching rule condition found
==========

 < Oct 18 10:05:32  mobileip[499]: <500300> <DBUG> |mobileip|  Station 00:40:96:a6:a1:
a4,
10.0.100.103: DHCP FSM received event: RECEIVE_BOOTP_REPLY current: PROXY_DHCP_NO_PROX
Y, next: PROXY_DHCP_NO_PROXY >
==========
Condition:      No matching rule condition found
==========
```

Command History

Introduced in ArubaOS 3.1

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config mode on master and local controllers

esi ping

```
esi ping <ping-name>
   [frequency <seconds>] |
   [no] |
   [retry-count <count>] |
   [timeout <seconds>] |
```

Description

This command specifies the ESI ping health check configuration.

Syntax

Parameter	Description	Range	Default
`frequency`	Specifies the ping frequency in seconds.	1–65536	
`no`	Negates any configured parameter	—	—
`retry-count`	Specifies the ping retry count	1–65536	2
`timeout`	Specifies the ping timeout in seconds.	1–65536	2

Usage Guidelines

Use the `show esi ping` command to show ESI ping information.

Example

The following command specifies the ping health check attributes.

```
(host) (config) #esi ping default
   frequency 5
   retry-count 2
   timeout 2
```

Command History

Introduced in ArubaOS 2.5

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config mode on master and local controllers

esi server

```
esi server <name>
   [dport <tcp-udp-port>] |
   [mode {bridge | nat | route}] |
   [no] |
   [trusted-ip-addr <ip-addr> [health-check]] |
   [trusted-port <slot/port>] |
   [untrusted-ip-port <ip-addr> [health-check]] |
   [untrusted-port <slot/port>]
```

Description

This command configures an ESI server.

Syntax

Parameter	Description
`dport`	Specifies the NAT destination TCP/UDP port.
`mode`	Specifies the ESI server mode of operation: bridge, nat, or route
`no`	Negates any configured parameter.
`trusted-ip-addr`	Specifies the server IP address on the trusted network. As an option, you can also enable a health check on the specified address
`trusted-port`	Specifies the port connected to the trusted side of the ESI server; slot/port format.
`untrusted-ip-addr`	Specifies the server IP address on the untrusted network. As an option, you can also enable a health check on the specified address
`untrusted-port`	Specifies the port connected to the untrusted side of the ESI server.

Usage Guidelines

Use the **`show esi server`** command to show ESI server information.

Example

The following command specifies the ESI server attributes.

```
(host) (config) #esi server forti_1
   mode route
   trusted-ip-addr 10.168.172.3
   untrusted-ip-addr 10.168.171.3
```

Command History

Introduced in ArubaOS 2.5.

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config mode on master and local controllers

exit

`exit`

Description

This command exits the current CLI mode.

Syntax

No parameters.

Usage Guidelines

Upon entering this command in a configuration sub-mode, you are returned to the configuration mode. Upon entering this command in configuration mode, you are returned to the enable mode. Upon entering this command in enable mode, you are returned to the user mode. Upon entering this command in user mode, you are returned to the user login.

Example

The following sequence of **`exit`** commands return the user from the interface configuration sub-mode to the user login:

```
(host) (config-if) #exit
(host) (config) #exit
(host) #exit
(host) >exit
User:
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Available in the following command modes: • User • Enable • Config • Config sub-modes

export

```
export gap-db <filename>
```

Description

This command exports the global AP database to the specified file.

Syntax

Parameter	Description
`<filename>`	Name of the file to which the global AP database is exported.

Usage Guidelines

This command is intended for system troubleshooting. You should run this command only when directed to do so by an Dell support representative.

The global AP database resides on a master controller and contains information about known APs on all controllers in the system. You can view the contents of the global AP database with the **`show ap database`** command.

Example

The following command exports the global AP database to a file:

```
(host) #export gap-db global-ap-db
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on master controllers.

firewall

```
firewall
   {allow-tri-session |attack-rate {cp <rate>|ping <number>|session
   <number>}|broadcast-filter-arp |cp|bwcontracts-subnet-broadcast|cp-bandwidth-
   contract|tcp-syn <number>|bwcontracts-subnet-broadcast |deny-inter-user-bridging
   |deny-inter-user-traffic|disable-ftp-server |disable-ftp-server| disable-stateful-
   h323| disable-stateful-sccp-processing|disable-stateful-sip-processing |disable-
   stateful-ua-processing|disable-stateful-vocera-processing|drop-ip-fragments
   |enable-per-packet-logging |enforce-tcp-handshake |gre-call-id-processing
   |local-valid-users|log-icmp-error|prohibit-arp-spoofing|prohibit-ip-spoofing
   |prohibit-rst-replay
   |session-idle-timeout <seconds> |session-mirror-destination {ip-address <ipaddr>
   |port <slot>/<port>} |shape-mcastfirew |voip-wmm-content-enforcement}
```

Description

This command configures firewall options on the controller.

Syntax

Parameter	Description	Range	Default
`allow-tri-session`	Allows three-way session when performing destination NAT. This option should be enabled when the controller is not the default gateway for wireless clients and the default gateway is behind the controller. This option is typically used for captive portal configuration.	—	disabled
`attack-rate`	Sets rates which, if exceeded, can indicate a denial of service attack.	—	—
`broadcast-filter-arp`	If enabled, all broadcast ARP requests are converted to unicast and sent directly to the client. You can check the status of this option using the **show ap active** and the **show datapath tunnel** command. If enabled, the output will display the letter a in the flags column.	—	disabled
`bwcontracts-subnet-broadcast`	Applies bw contracts to local subnet broadcast traffic	—	—
`cp`	See "firewall cp" on page 201		
`cp-bandwidth-contract`	See "firewall cp-bandwidth-contract" on page 203		
`deny-inter-user-bridging`	Prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic. This option can be used to prevent traffic, such as Appletalk or IPX, from being forwarded.	—	disabled
`deny-inter-user-traffic`	Denies traffic between untrusted users by disallowing layer2 and layer3 traffic. This parameter does not depend on the deny-inter-user-bridging parameter being enabled or disabled.	—	disabled
`disable-ftp-server`	Disables the FTP server on the controller. Enabling this option prevents FTP transfers. Enabling this option could cause APs to not boot up. You should not enable this option unless instructed to do so by an Dell representative.	—	disabled
`disable-stateful-h323-processing`	Disables stateful H.323 processing.	—	disabled
`disable-stateful-sccp-processing`	Disables SCCP processing.	—	disabled
`disable-stateful-sip-processing`	Disables monitoring of exchanges between a voice over IP or voice over WLAN device and a SIP server. This option should be enabled only when thee is no VoIP or VoWLAN traffic on the network.	—	disabled
`disable-stateful-ua-processing`	Disables stateful UA processing.	—	disabled
`disable-stateful-vocera-processing`	Disables stateful VOCERA processing.	—	disabled
`drop-ip-fragments`	When enabled, all IP fragments are dropped. You should not enable this option unless instructed to do so by an Dell representative.	—	disabled

Parameter	Description	Range	Default
enable-per-packet-logging	Enables logging of every packet if logging is enabled for the corresponding session rule. Normally, one event is logged per session. If you enable this option, each packet in the session is logged. You should not enable this option unless instructed to do so by an Dell representative, as doing so may create unnecessary overhead on the controller.	—	disabled
enforce-tcp-handshake	Prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network.	—	disabled
gre-call-id-processing	Creates a unique state for each PPTP tunnel. You should not enable this option unless instructed to do so by an Dell representative.	—	disabled
local-valid-users	Adds only IP addresses, which belong to a local subnet, to the user-table.	—	disabled
log-icmp-error	Logs received ICMP errors. You should not enable this option unless instructed to do so by an Dell representative.	—	disabled
prohibit-arp-spoofing	Detects and prohibits arp spoofing. When this option is enabled, possible arp spoofing attacks are logged and an SNMP trap is sent.	—	disabled
prohibit-ip-spoofing	Detects IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.	—	disabled
prohibit-rst-replay	Closes a TCP connection in both directions if a TCP RST is received from either direction. You should not enable this option unless instructed to do so by an Dell representative.	—	disabled
session-idle-timeout	Time, in seconds, that a non-TCP session can be idle before it is removed from the session table. You should not modify this option unless instructed to do so by an Dell representative.	16-259	15 seconds
session-mirror-destination	Destination to which mirrored packets are sent. This option is used only for troubleshooting or debugging. Packets can be mirrored in multiple ACLs, so only a single copy is mirrored if there is a match within more than one ACL. You can configure the following: Ethertype to be mirrored with the Ethertype ACL mirror option. See “ip access-list eth” on page 255. IP flows to be mirrored with the session ACL mirror option. See “ip access-list session” on page 262. MAC flows to be mirrored with the MAC ACL mirror option. See “ip access-list mac” on page 260. If you configure both an IP address and a port to receive mirrored packets, the IP address takes precedence.	—	—
session-mirror-ipsec	Configures session mirroring of all frames that are processed by IPsec. Frames are sent to IP address specified by the session-mirror-destination option.This option is used only for troubleshooting or debugging.	—	disabled
session-voip-timeout	Idle session timeout, in seconds, for sessions that are marked as voice sessions. If no voice packet exchange occurs over a voice session for the specified time, the voice session is removed.	16-300	300 seconds

Parameter	Description	Range	Default
`shape-mcast`	Enables multicast optimization and provides excellent streaming quality regardless of the amount of VLANs or IP IGMP groups that are used.	—	disabled
`voip-wmm-voip-content-enforcement`	If traffic to or from the user is inconsistent with the associated QoS policy for voice, the traffic is reclassified to best effort and data path counters incremented. This parameter requires the PEFNG license.	—	disabled

Usage Guidelines

This command configures global firewall options on the controller.

Example

The following command disallows forwarding of non-IP frames between users:

```
firewall deny-inter-user-bridging
```

Related Commands

```
(host) (config) #show firewall
```

Command History

Version	Modification
ArubaOS 3.0	Command introduced.
ArubaOS 3.2	The **wmm-voip-content-enforcement** parameter was introduced.
ArubaOS 3.3	The **session-mirror-destination** parameter was modified.
ArubaOS 3.3.2	The **local-valid-users** parameter was added.
ArubaOS 3.4	The v**oip-proxy-arp** parameter was renamed to broadcast-filter-arp and it does not require a Voice license. The p**rohibit-arp-spoofing** parameter was added. The **deny-inter-user-traffic** parameter was added.
ArubaOS 6.0	The **shape-mcast** parameter was added.

Command Information

Platform	License	Command Mode
Available on all platforms	This command requires the PEFNG license	Config mode on master controllers

firewall cp

```
firewall cp {deny|permit} proto <IP protocol number> ports <start port number>
<last port number> [bandwidth-contract <name>]
   no ...
```

Description

This command creates whitelist session ACLs. Whitelist ACLs consist of rules that explicitly permit or deny session traffic from being forwarded or not to the controller. This prohibits traffic from being automatically forwarded to the controller if it was not specifically denied in a blacklist.The maximum number of entries allowed in the whitelist is 64.

Syntax

Parameter	Description	Range	Default
deny	Specifies the entry to reject on the session ACL whitelist	—	disabled
proto	Indicates the protocol.	—	—
IP protocol number	Specifies the IP protocol number that is rejected.	1-255	—
ports	Port that the session traffic is using	—	
start port	Specifies the start port	1-65535	
last port	Specifies the last port	1-65535	
permit	Specifies an entry that is allowed on the session ACL whitelist	—	
proto	Protocol that the session traffic is using	—	—
IP protocol number	Specifies the IP protocol number that is allowed	1-255	—
ports	Indicates the port on which session traffic is running	—	
start port	Specifies the starting port, in the port range, on which session traffic is running.	1-65535	
last port	Specifies the last port, in the port range, on which session traffic is running.	1-65535	
bandwidth-contract <name>	Specify the name of a bandwidth contract defined via the cp-bandwidth-contract command.	—	

Usage Guidelines

This command turns the session ACL from a blacklist to a whitelist. A rule must exist that explicitly permits the session before it is forwarded to the controller and the last rule in the list denies everything else.

Example

The following command creates a whitelist ACL that allows traffic using protocol 6 on ports 5000 through 6000 to be forwarded to the controller.

```
(host) (config-fw-cp) #firewall cp permit proto 6 ports 5000 6000
```

The following command creates a a whitelist ACL entry that denies traffic using protocol 2 on port 5000 from being forwarded to the controller:

```
(host) (config-fw-cp) #firewall cp deny proto 2 ports 5000 5000
```

Related Commands

Command	Description	Mode
`show firewall-cp`	Show Control Processor (CP) whitelist ACL info.	Enable or Config modes
`cp-bandwidth-contract`	This command configures a bandwidth contract traffic rate which can then be associated with a whitelist session ACL.	Enable or Config modes

Command History

Introduced in ArubaOS 3.4

Command Information

Platform	License	Command Mode
Available on all platforms	This command requires the PEFNG license	Config mode on master controllers

firewall cp-bandwidth-contract

```
firewall cp-bandwidth-contract {auth|route|sessmirr|trusted-mcast|trusted-ucast
|untrusted-mcast|untrusted-ucast} <Rate>
```

Description

This command configures bandwidth contract traffic rate limits to prevent denial of service attacks.

Syntax

Parameter	Description	Range	Default
`auth`	Specifies the traffic rate limit that is forwarded to the authentication process.	1-200 Mbps	1
`route`	Specifies the traffic rate limit that needs ARP requests.	1-200 Mbps	1
`sessmirr`	Specifies the session mirrored traffic forwarded to the controller.	1-200 Mbps	1
`trusted-mcast`	Specifies the trusted multicast traffic rate limit.	1-200 Mbps	2
`trusted-ucast`	Specifies the trusted unicast traffic rate limit.	1-200 Mbps	80
`untrusted-mcast`	Specifies the untrusted multicast traffic rate limit.	1-200 Mbps	2
`untrusted-ucast`	Specifies the untrusted unicast traffic rate limit.	1-200 Mbps	10

Usage Guidelines

This command configures firewall bandwidth contract options on the controller.

Example

The following command disallows forwarding of non-IP frames between users:

```
(host) (config) #firewall deny-inter-user-bridging
```

Related Commands

```
(host) (config) #show firewall
```

Command History

Introduced in ArubaOS 3.4

Command Information

Platform	License	Command Mode
`Available on all platforms`	This command requires the PEFNG license	Config mode on master controllers

gateway health-check disable

```
gateway health-check disable
```

Description

Disable the gateway health check.

Usage Guidelines

The gateway health check feature can only be enabled by Dell Technical Support. This command disables the gateway health check, and should only be issued under the guidance of the support staff.

Related Commands

Command	Description	Mode
`show gateway health-check`	Display the current status of the gateway health-check feature	This command is available in Config and Enable mode on master and local controllers

```
(host) (config) #show gateway health-check
```

History

Introduced in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master or local controllers.

guest-access-email

```
guest-access-email
   smtp-port
   smtp-server
   no...
```

Description

This command configures the SMTP server which is used to send guest email. Guest email is generated when a guest user account is created or when the Guest Provisioning user sends guest user account email a later time.

Syntax

Parameter	Description	Range	Default
`smtp-port`	Identifies the SMTP port through which the guest-access email is sent.	—	—
`<Port number>`	The SMTP port number.	1–65535	25
`smtp-server`	The SMTP server to which the controller sends the guest-access email.	—	—
`<IP-Address>`	The SMTP server's IP address.	—	—
`no`	Deletes the command configuration	—	—

Usage Guidelines

As part of the guest provisioning feature, the **guest-access-email** command allows you to set up the SMTP port and server that process guest provisioning email. This email process sends email to either the guest or the sponsor whenever a guest user account is created or when the Guest Provisioning user manually sends email from the Guest Provisioning page.

Example

The following command creates a guest-access email profile and sends guest user email through SMTP server IP address 1.1.1.1 on port 25.

```
(host) (config) #guest-access-email
(host) (Guest-access Email Profile) #
(host) (Guest-access Email Profile) #smtp-port 25
(host) (Guest-access Email Profile) #smtp-server 1.1.1.1
```

Related Commands

```
(host) #show guest-access-email
(host) #local-userdb-guest add
(host) #local-userdb-guest modify
(host) #show local-userdb-guest
```

Command History

Version	Modification
ArubaOS 3.4	Introduced for the first time.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on master controllers.

halt

```
halt
```

Description

This command halts all processes on the controller.

Syntax

No parameters.

Usage Guidelines

This command gracefully stops all processes on the controller. You should issue this command before rebooting or shutting down to avoid interrupting processes.

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Enable mode on master and local controllers.

help

`help`

Description

This command displays help for the CLI.

Syntax

No parameters.

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 command displays help:

```
(host) #help
```

Command History

Available in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Available in the following command modes: • User • Enable • Config

hostname

```
hostname <hostname>
```

Description

This command changes the hostname of the controller.

Syntax

Parameter	Description	Range	Default
hostname	The hostname of the controller	1-63	See below

Usage Guidelines

The hostname is used as the default prompt. You can use any alphanumeric character, punctuation, or symbol character. To use spaces, plus symbols (+), question marks (?), or asterisks (*), enclose the text in quotes.

The default names for the following controllers are:

- W-3200Multi-Service Controller: Dell3200
- W-3400 Multi-Service Controller: Dell3400
- W-3600 Multi-Service Controller: Dell3600

Example

The following example configures the controller hostname to “Controller 1”.

```
hostname “Controller 1”
```

Command History

Introduced in ArubaOS 1.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master and local controllers

ids ap-classification-rule

```
id-classification-rule <rule-name>
   check-min-discovered-aps
   classify-to-type [neighbor | suspected-rogue]
   clone
   conf-level-incr
   discovered-ap-cnt <discovered-ap-cnt>
   match-ssids
   no
   snr-max <value>
   snr-min <value>
   ssid <ssid>
```

Description

Configure the AP classification rule profile.

Syntax

Parameter	Description	Range	Default
`<rule-name>`	Enter the AP classification rule profile name.	—	—
`check-min-discovered-aps`	Have the rule check for the minimum number of APs	true false	true
`classify-to-type [neighbor | suspected-rogue]`	Specify if the type the AP will be classified, neighbor or suspected-rogue, if the rule is matched.	—	suspected-rogue
`clone`	Copy data from another AP classification rule profile	—	—
`conf-level-incr`	Increase the confidence level (in percentage) when the rule matches	0-100	5
`discovered-ap-cnt <discovered-ap-cnt>`	Enter the keyword discovered-ap-cnt followed by the number of APs to be discovered.	0-100	0
`match-ssids`	Match SSIDs; match or do not match	true false	false
`no`	Negates any configured parameter	—	—
`snr-max <value>`	Use the maximum SNR value	0-100	0
`snr-min <value>`	Use the minimum SNR value	0-100	0
`ssid <ssid>`	Enter the keyword **ssid** followed by the SSID string to be matched or excluded	—	—

Usage Guidelines

Paragraph describing command usage

Example

The following example configures the AP Configuration Rule Profile named “rule1”:

```
(host) (config) #ids ap-classification-rule rule1
(host) (IDS AP Classification Rule Profile "rule1") #check-min-discovered-aps
(host) (IDS AP Classification Rule Profile "rule1") #classify-to-type neighbor
```

Command History

Release	Modification
ArubaOS 6.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on master controllers

ids ap-rule-matching

```
no
rule-name
```

Description

Configure the IDS active AP rules profile

Syntax

Parameter	Description
`no`	Negates any configured parameter
`rule-name`	Enter the name of the AP to activate

Usage Guidelines

This command activates an active AP rule. You must create the rule before you can activate it.

Example

```
(host) (IDS Active AP Rules Profile) #rule-name rule2
```

Command History

Release	Modification
ArubaOS 60	Command introduced

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on master controllers

ids dos-profile

```
ids
ids dos-profile <profile>
   ap-flood-inc-time <seconds>
   ap-flood-quiet-time <seconds>
   ap-flood-threshold <number>
   assoc-rate-thresholds <number>
   auth-rate-thresholds <number>
   block-ack-dos-quiet-time
   chopchop-quiet-time
   client-ht-40mhz-intol-quiet-time <seconds>
   client-flood-inc-time
   client-flood-quiet-time
   client-flood-threshold
   client-ht-40mhz-intolerance
   clone <profile>
   cts-rate-quiet-time
   cts-rate-threshold
   cts-rate-time-interval
   deauth-rate-thresholds <number>
   detect-ap-flood
   detect-block-ack-dos
   detect-chopchop-attack
   detect-client-flood
   detect-cts-rate-anomaly
   detect-disconnect-station
   detect-eap-rate-anomaly
   detect-fata-jack-attack
   detect-ht-40mhz-intolerance
   detect-invalid-address
   detect-malformed-association-request
   detect-malformed-auth-frame
   detect-malformed-htie
   detect-malformed-large-duration
   detect-omerta-attack
   detect-overflow-eapol-key
   detect-overflow-ie
   detect-rate-anomalies
   detect-rts-rate-anomaly
   detect-tkip-replay-attack
   disassoc-rate-thresholds <number>
   disconnect-deauth-disassoc-threshold
   disconnect-sta-assoc-resp-threshold
   disconnect-sta-quiet-time <seconds>
   eap-rate-quiet-time <seconds>
   eap-rate-threshold <number>
   eap-rate-time-interval <seconds>
   fata-jack-quiet-time
   invalid-address-combination-quiet-time
   malformed-association-request-quiet-time
   malformed-auth-frame-quiet-time
   malformed-htie-quiet-time
   malformed-large-duration-quiet-time
   no ...
   omerta-quiet-time
   omerta-threshold
   overflow-eapol-key-quiet-time
```

```
overflow-ie-quiet-time
probe-request-rate-thresholds <number>
probe-response-rate-thresholds <number>
rts-rate-threshold
rts-rate-time-interval
spoofed-deauth-blacklist
tkip-replay-quiet-time
```

Description

This command configures traffic anomalies for denial of service (DoS) attacks.

Syntax

Parameter	Description	Range	Default
<profile>	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
ap-flood-inc-time	Time, in seconds, during which a configured number of fake AP beacons must be received to trigger an alarm.	0-36000	3600 seconds
ap-flood-quiet-time	After an alarm has been triggered by a fake AP flood, the time, in seconds, that must elapse before an identical alarm may be triggered.	60-360000	900 seconds
ap-flood-threshold	Number of fake AP beacons that must be received within the flood increase time to trigger an alarm.	0-100,000	50
assoc-rate-thresholds	Rate threshold for associate request frames.	—	—
auth-rate-thresholds	Rate threshold for authenticate frames.	—	—
block-ack-dos-quiet-time	Time to wait, in seconds, after detecting an attempt to reset the receive window using a forged block ACK add.	60-360000 seconds	900 seconds
chopchop-quiet-time	Time to wait, in seconds, after detecting a ChopChop attack after which the check can be resumed.	60-360000 seconds	900 seconds
client-ht-40mhz-intol-quiet-time <seconds>	Controls the quiet time (when to stop reporting intolerant STAs if they have not been detected), in seconds, for detection of 802.11n 40 MHz intolerance setting.	60-360000 seconds	900 seconds
client-flood-inc-time	Number of consecutive seconds over which the client count is more than the threshold.	0-36000 seconds	3 seconds
client-flood-quiet-time	Time to wait, in seconds, after detecting a client flood before continuing the check.	60-360000 seconds	900 seconds
client-flood-threshold	Threshold for the number of spurious clients in the system.	0-100000	150
clone	Copy data from another IDS Denial Of Service Profile.	—	—
cts-rate-quiet-time	Time to wait, in seconds, after detecting a CTS rate anomaly after which the check can be resumed.	60-360000 seconds	900 seconds
cts-rate-threshold	Number of CTS control packets over the time interval that constitutes an anomaly.	0-100000	5000
cts-rate-time-interval	Time interval, in seconds, over which the packet count should be checked.	1-120 seconds	5 seconds
deauth-rate-thresholds	Rate threshold for deauthenticate frames.	—	—
detect-ap-flood	Enables detection of flooding with fake AP beacons to confuse legitimate users and to increase the amount of processing needed on client operating systems.	true false	false
detect-block-ack-dos	Enable/disable detection of attempts to reset traffic receive windows using forged Block ACK Add messages.	true false	true
detect-chopchop-attack	Enable/disable detection of ChopChop attack.	true false	false

Parameter	Description	Range	Default
detect-client-flood	Enable/disable detection of client flood attack.	true false	disable
detect-cts-rate-anomaly	Enable/disable detection of CTS rate anomaly.	true false	disable
detect-disconnect-station	In a station disconnection attack, an attacker spoofs the MAC address of either an active client or an active AP. The attacker then sends deauthenticate frames to the target device, causing it to lose its active association. Use this command to enable the detection of disconnect station attack.	true false	enable
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.	true false	false
detect-fata-jack-attack	Enable/disable detection of FATA-Jack attack	true false	enable
detect-ht-40mhz-intolerance	Enables or disables detection of 802.11n 40 MHz intolerance setting, which controls whether stations and APs advertising 40 MHz intolerance will be reported.	true false	false
detect-invalid-address	Enable/disable detection of invalid address combinations	true false	false
detect-malformed-association-request	Enable/disable detection of malformed association requests.	true false	disable
detect-malformed-auth-frame	Enable/disable detection of malformed authentication frames	true false	disable
detect-malformed-htie	Enable/disable detection of malformed HT IE	true false	false
detect-malformed-large-duration	Enable/disable detection of unusually large durations in frames	true false	true
detect-omerta-attack	Enable/disable detection of Omerta attack	true false	enable
detect-overflow-eapol-key	Enable/disable detection of overflow EAPOL key requests	true false	disable
detect-overflow-ie	Enable/disable detection of overflow Information Elements (IE)	true false	disable
detect-rate-anomalies	Enable/disable detection of rate anomalies	true false	disable
detect-rts-rate-anomaly	Enable/disable detection of RTS rate anomaly	true false	disable
detect-tkip-replay-attack	Enable/disable detection of TKIP replay attack	true false	disable
disassoc-rate-thresholds	Rate threshold for disassociate frames.	—	—
disconnect-deauth-disassoc-threshold	Rate thresholds for Disassociate frames	1-50	8

Parameter	Description	Range	Default
disconnect-sta-assoc-resp-threshold	The number of successful Association Response or Reassociation response frames seen in an interval of 10 seconds that should trigger this event.	1-30	5
disconnect-sta-quiet-time	After a station disconnection attack is detected, the time, in seconds, that must elapse before another identical alarm can be generated.	60-360000seconds	900 seconds
eap-rate-quiet-time	After an EAP rate anomaly alarm has been triggered, the time, in seconds, that must elapse before another identical alarm may be triggered.	60-360000	900 seconds
eap-rate-threshold	Number of EAP handshakes that must be received within the EAP rate time interval to trigger an alarm.	0-100000	60
eap-rate-time-interval	Time, in seconds, during which the configured number of EAP handshakes must be received to trigger an alarm.	1-120 seconds	3 seconds
fata-jack-quiet-time	Time to wait, in seconds, after detecting a FATA-Jack attack after which the check can be resumed.	60-360000 seconds	900 seconds
invalid-address-combination-quiet-time	Time to wait, in seconds, after detecting an invalid address combination after which the check can be resumed.	60-360000 seconds	900 seconds
malformed-association-request-quiet-time	Time to wait, in seconds, after detecting a malformed association request after which the check can be resumed.	60-360000 seconds	900 seconds
malformed-auth-frame-quiet-time	Time to wait, in seconds, after detecting a malformed authentication frame after which the check can be resumed.	60-360000 seconds	900 seconds
malformed-htie-quiet-time	Time to wait, in seconds, after detecting a malformed HT IE after which the check can be resumed.	60-360000 seconds	900 seconds
malformed-large-duration-quiet-time	Time to wait, in seconds, after detecting a large duration for a frame after which the check can be resumed.	60-360000 seconds	900 seconds
no	Negates any configured parameter.	—	—
omerta-quiet-time	Time to wait, in seconds, after detecting an Omerta attack after which the check can be resumed.	60-360000 seconds	900 seconds
omerta-threshold	The Disassociation packets received by a station as a percentage of the number of data packets sent, in an interval of 10 seconds.	1-100	10%
overflow-eapol-key-quiet-time	Time to wait, in seconds, after detecting a overflow EAPOL key request after which the check can be resumed.	60-360000 seconds	900 seconds
overflow-ie-quiet-time	Time to wait, in seconds, after detecting a overflow IE after which the check can be resumed.	60-360000 seconds	900 seconds
probe-request-rate-thresholds	Rate threshold for probe request frames.	—	—
probe-response-rate-thresholds	Rate threshold for probe response frames.	—	—
rts-rate-quiet-time	Time to wait, in seconds, after detecting an RTS rate anomaly after which the check can be resumed.	60-360000 seconds	900 seconds

Parameter	Description	Range	Default
rts-rate-threshold	Number of RTS control packets over the time interval that constitutes an anomaly.	0-100000	5000
rts-rate-time-interval	Time interval, in seconds, over which the packet count should be checked.	1-120 seconds	5 seconds
spoofed-deauth-blacklist	Enables detection of a deauth attack initiated against a client associated to an AP. When such an attack is detected, the client is quarantined from the network to prevent a man-in-the-middle attack from being successful.	true false	false
tkip-replay-quiet-time	Time to wait, in seconds, after detecting a TKIP replay attack after which the check can be resumed.	60-360000 seconds	900 seconds

Usage Guidelines

DoS attacks are designed to prevent or inhibit legitimate clients from accessing the network. This includes blocking network access completely, degrading network service, and increasing processing load on clients and network equipment.

Example

The following command enables a detection in the DoS profile named “floor2”:

```
(host) (config) #ids dos-profile floor2
(host) (IDS Denial Of Service Profile "floor2") detect-ap-flood
```

Command History

Release	Modification
ArubaOS 3.0	Command Introduced.
ArubaOS 3.3	Updated with support for high-throughput IEEE 802.11n standard.
ArubaOS 3.4	detect-disconnect-sta and disconnect-sta-quiet-time parameters deprecated.
ArubaOS 6.0	Deprecated predefined profiles and added numerous DoS profile options

Deprecated Predefined Profiles

Deprecated DOS profile:

- ids-dos-disabled
- ids-dos-low-setting
- ids-dos-medium-setting
- ids-dos-high-setting

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on master controllers

ids general-profile

```
ids general-profile <profile-name>
   adhoc-ap-inactivity-timeout
   adhoc-ap-max-unseen-timeout
   ap-inactivity-timeout <seconds>
   ap-max-unseen-timeout
   clone <profile>
   ids-events [logs-and-traps | logs-only | none | traps-only]
   min-pot-ap-beacon-rate <percent>
   min-pot-ap-monitor-time <seconds>
   mobility-manager-rtls
   no ...
   signature-quiet-time <seconds>
   sta-inactivity-timeout <seconds>
   stats-update-interval <seconds>
   wired-containment
   wireless-containment [deauth-only | none | tarpit-all-sta | tarpit-non-valid-sta]
   wireless-containment-debug
```

Description

Configure an IDS general profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`adhoc-ap-inactivity-timeout`	Ad hoc (IBSS) AP inactivity timeout in number of scans.	5-36000 seconds	5 seconds
`adhoc-ap-max-unseen-timeout`	Ageout time in seconds since ad hoc (IBSS) AP was last seen.	5-36000 seconds	5 seconds
`ap-inactivity-timeout`	Time, in seconds, after which an AP is aged out.	5-36000 seconds	5 seconds
`ap-max-unseen-timeout`	Ageout time, in seconds, since AP was last seen.	5-36000 seconds	600 seconds
`clone`	Name of an existing IDS general profile from which parameter values are copied.	—	—
`ids-events [logs-and-traps | logs-only | none | traps-only]`	Enable or disable IDS event generation from the AP. Event generation from the AP can be enabled for syslogs, traps, or both. This does not affect generation of IDS correlated events on the switch.	—	logs-and-traps
`min-pot-ap-beacon-rate`	Minimum beacon rate acceptable from a potential AP, in percentage of the advertised beacon interval.	0-100	25%
`min-pot-ap-monitor-time`	Minimum time, in seconds, a potential AP has to be up before it is classified as a real AP.	2-36000	2 seconds
`mobility-manager-rtls`	Enable/disable RTLS communication with the configured mobility-manager	enabled disabled	disabled
`mon-stats-update-interval`	Time interval, in seconds, for AP to update the switch with stats for monitored devices. Minimum is 60.	60-360000 seconds	60 seconds
`no`	Negates any configured parameter.	—	—
`send-adhoc-info-to-controller`	Enable or disable sending Adhoc information to the controller from the AP.	enable disable	disable
`signature-quiet-time`	After a signature match is detected, the time to wait, in seconds, to resume checking.	60-360000 seconds	900 seconds
`sta-inactivity-timeout`	Time, in seconds, after which a station is aged out.	30-360000 seconds	60 seconds
`sta-max-unseen-timeout`	Ageout time, in seconds, since station was last seen. Minimum is 5.	5-36000 seconds	5 seconds
`stats-update-interval`	Interval, in seconds, for the AP to update the controller with statistics. This setting takes effect only if the Mobility Manager is configured. Otherwise, statistics update to the controller is disabled.	60-360000 seconds	60 seconds
`wired-containment`	Enable containment from the wired side.	true false	false
`wired-containment-ap-adj-mac`	Enable/disable wired containment of MACs offset by one from APs BSSID.	true false	false

Parameter	Description	Range	Default
`wireless-containment [deauth-only | none | tarpit-all-sta | tarpit-non-valid-sta]`	Enable wireless containment including Tarpit Shielding. Tarpit shielding works by steering a client to a tarpit so that the client associates with it instead of the AP that is being contained. **deauth-only**—Containment using deauthentication only **none**—Disable wireless containment **tarpit-all-sta**—Wireless containment by tarpit of all stations **tarpit-non-valid-sta**—Wireless containment by tarpit of non-valid clients	—	deauth-only
`wireless-containment-debug`	Enable/disable debug of containment from the wireless side. **Note**: Enabling this debug option will cause containment to *not* function properly.	true false	false

Usage Guidelines

This command configures general IDS profile attributes.

Example

The following command enables containments in the general IDS profile:

```
(host) (config) #ids general-profile floor7
(host) (IDS General Profile "floor7") #wired-containment
(host) (IDS General Profile "floor7") #wireless-containment tarpit-all-sta
(host) (IDS General Profile "floor7") #wireless-containment-debug
```

Command History

Version	Description
ArubaOS 3.0	Command Introduced
ArubaOS 5.0	mobility-manager-rtls parameter introduced
ArubaOS 6.0	Deprecated predefined profiles and added numerous General profile options

Deprecated Predefined Profiles

Deprecate General profiles:

- ids-general-disabled
- ids-general-high-setting

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the RFprotect license.	Config mode on master controllers

ids impersonation-profile

```
ids impersonation-profile <name>
   beacon-diff-threshold <percent>
   beacon-inc-wait-time <seconds>
   beacon-wrong-channel-quiet-time
   clone <profile>
   detect-ap-impersonation
   detect-ap-spoofing
   detect-beacon-wrong-channel
   detect-hotspotter
   hotspotter-quiet-time
   no ...
   protect-ap-impersonation
```

Description

This command configures anomalies for impersonation attacks.

Syntax

Parameter	Description	Range	Default
<profile>	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
beacon-diff-threshold	Percentage increase in beacon rates that triggers an AP impersonation event.	0-100	50%
beacon-inc-wait-time	Time, in seconds, after the beacon difference threshold is crossed before an AP impersonation event is generated.	—	3 seconds
beacon-wrong-channel-quiet-time	Time to wait, in seconds, after detecting a beacon with the wrong channel after which the check can be resumed.	60-360000 seconds	900 seconds
clone	Name of an existing IDS impersonation profile from which parameter values are copied.	—	—
detect-ap-impersonation	Enables detection of AP impersonation. In AP impersonation attacks, the attacker sets up an AP that assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for man-in-the-middle attacks, a rogue AP attempting to bypass detection, or a honeypot attack.	—	true
detect-ap-spoofing	Enable/disable AP Spoofing detection	—	enable
detect-beacon-wrong-channel	Enable/disable detection of beacons advertising the incorrect channel	—	disable
detect-hotspotter	Enable/disable detection of the Hotspotter attack to lure away valid clients.	—	disable
hotspotter-quiet-time	Time to wait in seconds after detecting an attempt to Use the Hotspotter tool against clients.	60-360000 seconds	900 seconds
no	Negates any configured parameter.	—	—
protect-ap-impersonation	When AP impersonation is detected, both the legitimate and impersonating AP are disabled using a denial of service attack.	—	false

Usage Guidelines

A successful man-in-the-middle attack will insert an attacker into the data path between the client and the AP. In such a position, the attacker can delete, add, or modify data, provided he has access to the encryption keys. Such an attack also enables other attacks that can learn a client's authentication credentials. Man-in-the-middle attacks often rely on a number of different vulnerabilities.

Example

The following command enables detections in the impersonation profile:

```
(host) (config) #ids impersonation-profile floor1
(host) (IDS Impersonation Profile "floor1") #detect-beacon-wrong-channel
(host) (IDS Impersonation Profile "floor1") #detect-ap-impersonation
```

Command History

Version	Modification
ArubaOS 3.0	Command Introduced
ArubaOS 3.4	detect-sequence-anomaly, sequence-diff, sequence-quiet-time, sequence-time-tolerance parameters deprecated.
ArubaOS 6.0	Deprecated predefined profiles and added numerous Impersonation profile options

Deprecated Predefined Profiles

IDS Impersonation profile:

- ids-impersonation-disabled
- ids-impersonation-high-setting

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on master controllers

ids management-profile

```
event-correlation
   [logs-and-traps | logs-only | none | traps-only]
event-correlation-quiet-time <value>
```

Description

Mange the event correlation.

Syntax

Parameter	Description	Range	Default

`event-correlation`
`logs-and-traps`
`logs-only`
`none`
`traps-only`
	Correlation mode for IDS event traps and syslogs (logs). Event correlation can be enabled with generation of correlated logs, traps, or both. To disable correlation, enter the keyword **none**.		logs-and-traps

`event-correlation-quiet-time` `<value>`	Time to wait, in seconds, after generating a correlated event after which the event could be raised again. This only applies to events that are repeatedly raised by an AP.	30-360000 seconds	900 seconds

Usage Guidelines

Manage the events correlation for IDS event traps and syslogs (logs).

Example

```
(host) (config) #ids management-profile
(host) (IDS Management Profile) #event-correlation-quiet-time 30
(host) (IDS Management Profile) #event-correlation logs-and-traps
```

Command History

Release	Modification
ArubaOS 6.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on master controllers

ids profile

```
ids profile <name>
   clone <profile>
   dos-profile <profile>
   general-profile <profile>
   impersonation-profile <profile>
   no ...
   signature-matching-profile <profile>
   unauthorized-device-profile <profile>
```

Description

This command defines a set of IDS profiles.

Syntax

Parameter	Description	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	"default"
`clone`	Name of an existing IDS profile from which parameter values are copied.	—
`dos-profile`	Name of a IDS denial of service profile to be applied to the AP group/name. See "ids dos-profile" on page 16.	"default"
`general-profile`	Name of an IDS general profile to be applied to the AP group/name. See "ids general-profile" on page 22.	"default"
`impersonation-profile`	Name of an IDS impersonation profile to be applied to the AP group/name. See "ids impersonation-profile" on page 25.	"default"
`no`	Negates any configured parameter.	—
`signature-matching-profile`	Name of an IDS signature matching profile to be applied to the AP group/name. See "ids signature-matching-profile" on page 33	"default"
`unauthorized-device-profile`	Name of an IDS unauthorized device profile to be applied to the AP group/name. See "ids unauthorized-device-profile" on page 37.	"default"

Usage Guidelines

This command defines a set of IDS profiles that you can then apply to an AP group (with the **ap-group** command) or to a specific AP (with the **ap-name** command).

Example

The following command defines a set of IDS profiles:

```
(host) (config) #ids profile floor2
(host) (IDS Profile "floor2") #dos-profile dos1
   general-profile general1
   impersonation-profile mitm1
   signature-matching-profile sig1
   unauthorized-device-profile unauth1
```

Command History

Version	Modification
ArubaOS 3.0	Command Introduced
ArubaOS 6.0	Deprecated predefined profiles

Deprecated Predefined Profile

Deprecated Profile for levels: disabled, high, medium, and low

- ids-disabled
- ids-high-setting
- ids-medium-setting
- ids-high-setting

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on master controllers.

ids rate-thresholds-profile

```
ids rate-thresholds-profile <name>
   channel-inc-time <seconds>
   channel-quiet-time <seconds>
   channel-threshold
   clone <profile>
   no ...
   node-quiet-time <seconds>
   node-threshold <number>
   node-time-interval <seconds>
```

Description

This command configures thresholds that are assigned to the different frame types for rate anomaly checking.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`channel-inc-time`	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.	0 - 360000 seconds	15 seconds
`channel-quiet-time`	After a channel rate anomaly alarm has been triggered, the time that must elapse before another identical alarm may be triggered. This option prevents excessive messages in the log file.	60-360000	900 seconds
`channel-threshold`	Number of a specific type of frame that must be exceeded within a specific interval in an entire channel to trigger an alarm.	any	300
`clone`	Name of an existing IDS rate thresholds profile from which parameter values are copied.	—	—
`no`	Negates any configured parameter.	—	—
`node-quiet-time`	After a node rate anomaly alarm has been triggered, the time, in seconds, that must elapse before another identical alarm may be triggered. This option prevents excessive messages in the log file.	60-360000	900 seconds
`node-threshold`	Number of a specific type of frame that must be exceeded within a specific interval for a particular client MAC address to trigger an alarm.	0 -100000 frames	200
`node-time-interval`	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.	1-120	15 seconds

Usage Guidelines

A profile of this type is attached to each of the following 802.11 frame types in the IDS denial of service profile:

- Association frames
- Disassociation frames
- Deauthentication frames
- Probe Request frames
- Probe Response frames
- Authentication frames

Example

The following command configures frame thresholds:

```
(host) (config) #ids rate-thresholds-profile Lobby
(host) (IDS Rate Thresholds Profile "Lobby") #channel-threshold 250
```

Command History

Version	Modification
ArubaOS 3.0	Command Introduced
ArubaOS 6.0	Deprecated predefined profiles

Deprecated Predefined Profiles

Deprecated the predefined profile with probe-request-response-threshold.

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on master controllers

ids signature-matching-profile

```
ids signature-matching-profile <name>
   clone <profile>
   no ...
   signature <profile>
```

Description

This command contains defined signature profiles.

Syntax

Parameter	Description	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	"default"
`clone`	Name of an existing IDS signature matching profile from which parameter values are copied.	—
`no`	Negates any configured parameter.	—
`signature`	Name of a signature profile. See "ids signature-profile" on page 34.	—

Usage Guidelines

You can include one or more predefined signature profiles or a user-defined signature profile in a signature matching profile.

Example

The following command configures a signature matching profile:

```
(host) (config) IDS signature matching LobbyEast
(host) (IDS Signature Matching Profile "LobbyEast") #signature Null-Probe-Response
```

Command History

Version	Modification
ArubaOS 3.0	Command Introduced
ArubaOS 6.0	Deprecated predefined profiles

Deprecated Predefined Profiles

Deprecated Signature Matching profile:

- factory-default-signatures

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on master controllers

ids signature-profile

```
ids signature-profile <name>
   bssid <macaddr>
   clone <profile>
   dst-mac <macaddr>
   frame-type {assoc|auth|beacon|control|data|deauth|disassoc|mgmt|probe-request|
   no ...
   payload <pattern> [offset <number>]
   seq-num <number>
   src-mac <macaddr>
```

Description

This command configures signatures for wireless intrusion detection.

Syntax

Parameter	Description	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	"default"
`bssid`	BSSID field in the 802.11 frame header.	—
`clone`	Name of an existing IDS signature profile from which parameter values are copied.	—
`dst-mac`	Destination MAC address in the 802.11 frame header.	—
`frame-type`	Type of 802.11 frame. For each type of frame, further parameters can be specified to filter and detect only the required frames.	—
`assoc`	Association frame type	
`auth`	Authentication frame type	
`beacon`	Beacon frame type	
`control`	All control frames	
`data`	All data frames	
`deauth`	Deauthentication frame type	
`disassoc`	Disassociation frame type	
`mgmt`	Management frame type	
`ssid`	For beacon, probe-request, and probe-response frame types, specify the SSID as either a string or hex pattern.	—
`ssid-length`	For beacon, probe-request, and probe-response frame types, specify the length, in bytes, of the SSID. Maximum length is 32 bytes.	—
`no`	Negates any configured parameter.	—
`payload <pattern>`	Pattern at a fixed offset in the payload of an 802.11 frame. Specify the pattern to be matched as a string or hex pattern. Maximum length is 32 bytes.	—
`offset`	When a payload pattern is configured, specify the offset in the payload where the pattern is expected to be found in the frame.	—
`seq-num`	Sequence number of the frame.	—
`src-mac`	Source MAC address in the 802.11 frame header.	—

Example

The following command configures a signature profile:

```
(host) (config) #ids signature-profile floor4
(host) (IDS Signature Profile "floor4") #frame-type assoc
(host) (IDS Signature Profile "floor4") #src-mac 00:00:00:00:00:00
```

Usage Guidelines

The following describes the configuration for the predefined signature profiles:

Signature Profile	Parameter	Value
AirJack	frame-type	beacon ssid = AirJack

Signature Profile	Parameter	Value
ASLEAP	frame-type	beacon ssid = asleap
Deauth-Broadcast	frame-type	deauth
	dst-mac	ff:ff:ff:ff:ff:ff
Netstumbler Generic	payload	offset=3 pattern=0x00601d
	payload	offset=6 pattern=0x0001
Netstumbler Version 3.3.0x	payload	offset=3 pattern=0x00601d
	payload	offset=12 pattern=0x000102
Null-Probe-Response	frame-type	probe-response ssid length = 0

Command History

Version	Modification
ArubaOS 3.0	Command Introduced

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on master controllers

ids unauthorized-device-profile

```
ids unauthorized-device-profile <name>
   adhoc-using-valid-ssid-quiet-time <seconds>
   allow-well-known-mac [hsrp|iana|local-mac|vmware|vmware1|vmware2|vmware3]
   cfg-valid-11a-channel <channel>
   cfg-valid-11g-channel <channel>
   classification
   clone <profile>
   detect-adhoc-network
   detect-adhoc-using-valid-ssid
   detect-bad-wep
   detect-ht-greenfield
   detect-invalid-mac-oui
   detect-misconfigured-ap
   detect-unencrypted-valid-client
   detect-valid-client-misassociation
   detect-windows-bridge
   detect-wireless-bridge
   mac-oui-quiet-time <seconds>
   no ...
   oui-classification
   overlay-classification
   privacy
   prop-wm-classification
   protect-adhoc-network
   protect-high-throughput
   protect-ht-40mhz
   protect-misconfigured-ap
   protect-ssid
   protect-valid-sta
   protect-windows-bridge
   require-wpa
   rogue-containment
   suspect-rogue-conf-level <level>
   suspect-rogue-containment
   unencrypted-valid-client-quiet-time
   valid-and-protected-ssid <ssid>
   valid-oui <oui>
   valid-wired-mac <macaddr>
   wireless-bridge-quiet-time <seconds>
```

Description

This command configures detection of unauthorized devices, as well as rogue AP detection and containment.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	"default"
`adhoc-quiet-time`	DEPRECATED		
`adhoc-using-valid-ssid-quiet-time`	Time to wait, in seconds, after detecting an adhoc network using a valid SSID, after which the check can be resumed.	60-360000	900 seconds

`allow-well-known-mac`	Allows devices with known MAC addresses to classify rogues APs.
	Depending on your network, configure one or more of the following options for classifying rogue APs:
	hsrp—Routers configured for HSRP, a Cisco-proprietary redundancy protocol, with the HSRP MAC OUI 00:00:0c.
	iana—Routers using the IANA MAC OUI 00:00:5e.
	local-mac—Devices with locally administered MAC addresses starting with 02.
	vmware—Devices with any of the following VMWare OUIs: 00:0c:29, 00:05:69, or 00:50:56
	vmware1—Devices with VMWare OUI 00:0c:29.
	vmware2—Devices with VMWare OUI 00:05:69.
	vmware3—Devices with VMWare OUI 00:50:56.
	If you modify an existing configuration, the new configuration overrides the original configuration. For example, if you configure `allow-well-known-mac hsrp` and then configure `allow-well-known-mac iana`, the original configuration is lost. To add more options to the original configuration, include all of the required options, for example: `allow-well-known-mac hsrp iana`.
	Use caution when configuring this command. If the neighboring network uses similar routers, those APs might be classified as rogues. If containment is enabled, clients attempting to associate to an AP classified as a rogue are disconnected through a denial of service attack.
	To clear the well known MACs in the system, use the following commands on all controllers:
	`clear wms wired-mac`
	This clears all of the learned wired MAC information on the controller.
	`reload`
	This reboots the controller.
		—	—

`cfg-valid-11a-channel`	List of valid 802.11a channels that third-party APs are allowed to use.	34-165	N/A
`cfg-valid-11g-channel`	List of valid 802.11b/g channels that third-party APs are allowed to use.	1-14	N/A
`classification`	Enable/disable rogue AP classification. A rogue AP is one that is unauthorized and plugged into the wired side of the network. Any other AP seen in the RF environment that is not part of the valid enterprise network is considered to be interfering — it has the potential to cause RF interference but it is not connected to the wired network and thus does not represent a direct threat.	—	true

Parameter	Description	Range	Default
clone	Name of an existing IDS rate thresholds profile from which parameter values are copied.	—	—
detect-adhoc-network	Enable detection of adhoc networks.	—	false
detect-adhoc-using-valid-ssid	Enable/disable detection of adhoc networks using valid/protected SSIDs	—	enable
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.	—	false
detect-ht-greenfield	Enables or disables detection of high-throughput devices advertising greenfield preamble capability.	—	false
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.	—	false
detect-misconfigured-ap	Enables detection of misconfigured APs. An AP is classified as misconfigured if it is classified as valid and does not meet any of the following configurable parameters: - valid channels - encryption type - list of valid AP MAC OUIs - valid SSID list	—	false
detect-unencrypted-valid-client	Enable/disable detection of unencrypted valid clients	—	enable
detect-valid-client-misassociation	Enable/disable detection of misassociation between a valid client and an unsafe AP	—	enable
detect-windows-bridge	Enables detection of Windows station bridging.	—	true
detect-wireless-bridge	Enables detection of wireless bridging.	—	false
mac-oui-quiet-time	Time, in seconds, that must elapse after an invalid MAC OUI alarm has been triggered before another identical alarm may be triggered.	60-360000 seconds	900 seconds
no	Negates any configured parameter.	—	—
oui-classification	Enable/disable OUI based rogue AP classification	—	enable
overlay-classification	Enable/disable overlay rogue AP classification	—	enable
privacy	Enables encryption as a valid AP configuration.	—	false
prop-wm-classification	Enable/disable rogue AP classification through propagated wired MACs	—	true
protect-adhoc-network	Enables protection from adhoc networks. When adhoc networks are detected, they are disabled using a denial of service attack.	—	false
protect-high-throughput	Enables or disables protection of high-throughput (802.11n) devices.	—	false

Parameter	Description	Range	Default
protect-ht-40mhz	Enables or disables protection of high-throughput (802.11n) devices operating in 40 MHz mode.	—	false
protect-misconfigured-ap	Enables protection of misconfigured APs.	—	false
protect-ssid	Enables use of SSID by valid APs only.	—	false
protect-valid-sta	When enabled (true), does not allow valid stations to connect to a non-valid AP.	—	false
protect-windows-bridge	Enable/disable protection of a windows station bridging	—	disabled
require-wpa	When enabled (true), any valid AP that is not using WPA encryption is flagged as misconfigured.	—	false
rogue-containment	Rogue APs can be detected (see classification) but are not automatically disabled. This option automatically shuts down rogue APs. When this option is enabled (true), clients attempting to associate to an AP classified as a rogue are disconnected through a denial of service attack.	—	false
suspect-rogue-conf-level	Confidence level of suspected Rogue AP to trigger containment. When an AP is classified as a suspected rogue AP, it is assigned a 50% confidence level. If multiple APs trigger the same events that classify the AP as a suspected rogue, the confidence level increases by 5% up to 95%. In combination with suspected rogue containment, this option configures the threshold by which containment should occur. Suspected rogue containment occurs only when the configured confidence level is met.	50-100	60%
suspect-rogue-containment	Suspected rogue APs are treated as interfering APs, thereby the controller attempts to reclassify them as rogue APs. Suspected rogue APs are not automatically contained. In combination with the configured confidence level (see suspect-rogue-conf-level), this option contains the suspected rogue APs.	—	false
unencrypted-valid-client-quiet-time	Time to wait, in seconds, after detecting an unencrypted valid client after which the check can be resumed.	60-360000 seconds	900 seconds
valid-and-protected-ssid	List of valid and protected SSIDs.	—	—
valid-oui	List of valid MAC OUIs.	—	—
valid-wired-mac	List of MAC addresses of wired devices in the network, typically gateways or servers.	—	—
wireless-bridge-quiet-time	Time, in seconds, that must elapse after a wireless bridge alarm has been triggered before another identical alarm may be triggered.	60-360000	900 seconds

Usage Guidelines

Unauthorized device detection includes the ability to detect and disable rogue APs and other devices that can potentially disrupt network operations.

Example

The following command copies the settings from the ids-unauthorized-device-disabled profile and then enables detection and protection from adhoc networks:

```
(host) (config) #ids unauthorized-device-profile floor7
(host) (IDS Unauthorized Device Profile "floor7") #unauth1
(host) (IDS Unauthorized Device Profile "floor7") #clone ids-unauthorized-device-
disable
(host) (IDS Unauthorized Device Profile "floor7") #detect-adhoc-network
(host) (IDS Unauthorized Device Profile "floor7") #protect-adhoc-network
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3	Update with support for the high-throughput IEEE 802.11n standard. Also, introduced allow-well-known-mac, suspect-rogue-conf-level, and suspect-rogue-containment parameters.
ArubaOS 6.0	Deprecated predefined profiles

Deprecated Predefined Profiles

IDS Unauthorized Device profile:

- ids-unauthorized-device-disabled
- ids-unauthorized-device-medium-setting
- ids-unauthorized-device-high-setting

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on master controllers

interface fastethernet | gigabitethernet

```
interface
interface {fastethernet|gigabitethernet} <slot>/<port>
   description <string>
   duplex {auto|full|half}
   ip access-group <acl> {in|out|session {vlan <vlanId>}}
   no ...
   poe [cisco]
   port monitor {fastethernet|gigabitethernet} <slot>/<port>
   priority-map <name>
   shutdown
   spanning-tree [cost <value>] [port-priority <value>] [portfast]
   speed {10|100|auto}
   switchport {access vlan <vlan>|mode {access|trunk}|
    trunk {allowed vlan {<vlans>|add <vlans>|all|except <vlans>|remove <vlans>}|
    native vlan <vlan>}}
   trusted {vlan <word>}
   xsec {point-to-point <macaddr> <key> allowed vlan <vlans> [<mtu>]|vlan <vlan>}
```

Description

This command configures a FastEthernet or GigabitEthernet interface on the controller.

Syntax

Parameter	Description	Range	Default
<slot>	<slot> is always 1.	—	—
<port>	Number assigned to the network interface embedded in the controller. Port numbers start at 0 from the left-most position.	—	—
description	String that describes this interface.	—	—
duplex	Transmission mode on the interface: full or half-duplex or auto to automatically adjust transmission.	auto/full/half	auto
ip access-group	Applies the specified access control list (ACL) to the interface. Use the **ip access-list** command to configure an ACL. **NOTE**: This parameter requires the PEFNG license.	—	—
in	Applies ACL to interface's inbound traffic.	—	—
out	Applies ACL to interface's outbound traffic.	—	—
session	Applies session ACL to interface and optionally to a selected VLAN associated with this port.	—	—
no	Negates any configured parameter.	—	—
poe	Enables Power-over-Ethernet (PoE) on the interface.	—	enabled
cisco	Enables Cisco-style PoE on the interface.	—	disabled
port monitor	Monitors another interface on the controller.	—	—
priority-map	Applies a priority map to the interface. Use the **priority-map** command to configure a priority map which allows you to map ToS and CoS values into high priority traffic queues.	—	—
shutdown	Causes a hard shutdown of the interface.	—	—
spanning-tree	Enables Rapid spanning tree or Per-VLAN spanning tree	—	enabled
cost	Administrative cost associated with the spanning tree.	1-65535	19 (Fast Ethernet) 4 (Gigabit Ethernet)
port-priority	Spanning tree priority of the interface. A lower setting brings the port closer to root port position (favorable for forwarding traffic) than does a higher setting. This is useful if ports may contend for root position if they are connected to an identical bridge.	0-255	128
portfast	Enables forwarding of traffic from the interface.	—	disabled
speed	Sets the interface speed: 10 Mbps, 100 Mbps, or auto configuration.	10|100|auto	auto
switchport	Sets switching mode parameters for the interface.	—	—
access vlan	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.	—	1
mode	Sets the mode of the interface to access or trunk mode only.	access|trunk	access
trunk	Sets the interface as a trunk port for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the controller, or add or remove specified VLANs. Specify **native** to identify the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.	—	—

Parameter	Description	Range	Default
`trusted`	Set this interface and range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted. Trusted ports and VLANs are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When Dell APs are attached directly to the controller, set the port to be trusted.	—	enabled
`vlan <word>`	Sets the supplied range of VLANs as trusted. All remaining become untrusted automatically. For example, If you set a VLAN range as: vlan 1-10, 100-300, 301, 305-400, 501-4094 Then all VLANs in this range are trusted and all others become untrusted by default. You can also use the **no trusted vlan** command to explicitly make an individual VLAN untrusted. The no trusted vlan command is additive and adds given vlans to the existing untrusted vlan set. However, if you execute the **trusted vlan** <**word**> command, it overrides any earlier untrusted VLANs or a range of untrusted VLANs and creates a new set of trusted VLANs. **NOTE:** A port supports a user VLAN range from 1-4094. If you want to set all VLANs (1-4094) on a port as untrusted then mark the port itself as untrusted. By default the port and all its associated VLANs are trusted.	1-4094	—
`xsec`	Enables and configures the Extreme Security (xSec) protocol. **NOTE**: You must purchase and install the xSec software module license in the controller.	—	—
`point-to-point`	MAC address of the controller that is the xSec tunnel termination point, and the 16-byte shared key used to authenticate the controllers to each other. The key must be the same on both controllers.	—	—
`allowed vlan`	VLANs that are allowed on the xSec tunnel.	—	—
`mtu`	(Optional) MTU size for the xSec tunnel.	—	—
`vlan`	xSec VLAN ID. For controller-to-controller communications, both controllers must belong to the same VLAN.	1-4094	—

Usage Guidelines

Use the **show port status** command to obtain information about the interfaces available on the controller.

Example

The following commands configure an interface as a trunk port for a set of VLANs:

```
(host) (config) # interface fastethernet 1/2
(host) (config-range)# switchport mode trunk
(host) (config-range)# switchport trunk native vlan 10
(host) (config-range)# switchport trunk allowed vlan 1,10,100
```

The following commands configure trunk port 1/2 with test-acl session for VLAN 2.

```
(host) (config) # interface range fastethernet 1/2
(host) (config-range)# switchport mode trunk
(host) (config-range)# ip access-group
(host) (config-range) # ip access-group test session vlan 2
```

Related Commands

(host) #show interface {fastethernet|gigabitethernet} <slot>/<port>

(host) #show datapath port vlan-table <slot>/<port>

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4	The **trusted VLAN** and i**p access-group session vlan** parameters were introduced.
ArubaOS 3.4.1	The **trusted vlan <word>** parameter was added.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command is available in the base operating system. The **ip access-group** parameter requires the PEFNG license. The **xsec** parameter requires the xSec license.	Config mode on master and local controllers

interface loopback

```
interface loopback
   ip address <ipaddr>
   no ...
```

Description

This command configures the loopback address on the controller.

Syntax

Parameter	Description
`ip address`	Host IP address in dotted-decimal format. This address should be routable from all external networks.
`no`	Negates any configured parameter.

Usage Guidelines

If configured, the loopback address is used as the controller's IP address. If you do not configure a loopback address for the controller, the IP address assigned to VLAN 1 is used as the controller's IP address. After you configure or modify a loopback address, you need to reboot the controller.

Example

The following command configures a loopback address:

```
(host) (config) #interface loopback
   ip address 10.2.22.220
```

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	This command is available in the base operating system	Config mode on master and local controllers

interface port-channel

```
interface port-channel <id>
   add {fastethernet|gigabitethernet} <slot>/<port>
   del {fastethernet|gigabitethernet} <slot>/<port>
   ip access-group <acl> {in|out|session {vlan <vlanId>}}
   no ...
   shutdown
   spanning-tree [portfast]
   switchport {access vlan <vlan>|mode {access|trunk}|
    trunk {allowed vlan {<vlans>|add <vlans>|all|except <vlans>|remove <vlans>|
    native vlan <vlan>}
   trusted {vlan <word>}
   xsec {point-to-point <macaddr> <key> allowed vlan <vlans> [<mtu>]|vlan
<vlan>}
```

Description

This command configures an Ethernet port channel.

Syntax

Parameter	Description	Range	Default
`port-channel`	ID number for this port channel.	0-7	—
`add`	Adds the specified FastEthernet or GigabitEthernet interface to the port channel. You cannot specify both FastEthernet and GigabitEthernet interfaces for the same port channel.	—	—
`del`	Deletes the specified Fastethernet or Gigabitethernet interface to the port channel.	—	—
`ip access-group`	Applies the specified access control list (ACL) to the interface. Use the **ip access-list** command to configure an ACL. **NOTE:** This command requires the PEFNG license.	—	—
`in`	Applies ACL to interface's inbound traffic.	—	—
`out`	Applies ACL to interface's outbound traffic.	—	—
`session`	Applies session ACL to interface and optionally to a selected VLAN associated with this port.	—	—
`no`	Negates any configured parameter.	—	—
`shutdown`	Causes a hard shutdown of the interface.	—	—
`spanning-tree`	Enables spanning tree.	—	—
`portfast`	Enables forwarding of traffic from the interface.	—	—
`switchport`	Sets switching mode parameters for the interface.	—	—
`access vlan`	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.	—	—
`mode`	Sets the mode of the interface to access or trunk mode only.	—	—
`trunk`	Sets the interface as a trunk port for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the controller, or add or remove specified VLANs.	—	—
`native`	Specifies the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.	—	—
`trusted`	Set this interface and range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted. Trusted ports and VLANs are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When Dell APs are attached directly to the controller, set the port to be trusted.	—	disabled

Parameter	Description	Range	Default
`vlan <word>`	Sets the supplied range of VLANs as trusted. All remaining become untrusted automatically. For example, if you set a VLAN range as: vlan 1-10, 100-300, 301, 305-400, 501-4094 Then all VLANs in this range are trusted and all others become untrusted by default. You can also use the **no trusted vlan** command to explicitly make an individual VLAN untrusted. The no trusted vlan command is additive and adds given vlans to the existing untrusted vlan set. However, if you execute the **trusted vlan** <**word**> command, it overrides any earlier untrusted VLANs or a range of untrusted VLANs and creates a new set of trusted VLANs. **NOTE:** A port supports a user VLAN range from 1-4094. If you want to set all VLANs (1-4094) on a port as untrusted then mark the port itself as untrusted. By default the port and all its associated VLANs are trusted.	1-4094	—
`xsec`	Enables and configures the Extreme Security (xSec) protocol. **NOTE**: You must purchase and install the xSec software module license in the controller.	—	—
`point-to-point`	MAC address of the controller that is the xSec tunnel termination point, and the 16-byte shared key used to authenticate the controllers to each other. The key must be the same on both controllers.	—	—
`allowed vlan`	VLANs that are allowed on the xSec tunnel.	—	—
`mtu`	(Optional) MTU size for the xSec tunnel.	—	—
`vlan`	xSec VLAN ID. For controller-to-controller communications, both controllers must belong to the same VLAN.	1-4094	—

Usage Guidelines

A port channel allows you to aggregate ports on a controller. You can configure a maximum of 8 port channels per supported controller with a maximum of 8 interfaces per port channel.

Note the following when setting up a port channel between a controller and a Cisco switch (such as a Catalyst 6500 Series Switch):

- There must be no negotiation of the link parameters.
- The port-channel mode on the Cisco switch must be “on”.

Example

The following command configures a port channel:

```
(host) (config) #interface port channel 7
  add fastethernet 1/1
  add fastethernet 1/2
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4	The **trusted VLAN** and i**p access-group session vlan** parameters were introduced.
ArubaOS 3.4.1	The **trusted vlan <word>** parameter was added.

Command Information

Platforms	Licensing	Command Mode
W-3000 Controller Series Multi-Service Controller	This command is available in the base operating system. The **ip access-group** parameter requires the PEFNG license. The **xsec** parameter requires the xSec license.	Config mode on master and local controllers

interface range

```
interface range {fastethernet|gigabitethernet} <slot>/<port>-<port>
   duplex {auto|full|half}
   ip access-group <acl> {in|out|session {vlan <vlanId>}}
   no ...
   poe [cisco]
   shutdown
   spanning-tree [cost <value>] [port-priority <value>] [portfast]
   speed {10|100|auto}
   switchport {access vlan <vlan>|mode {access|trunk}|
    trunk {allowed vlan {<vlans>|add <vlans>|all|except <vlans>|remove
<vlans>}|
    native vlan <vlan>}}
   trusted {vlan <word>}
```

Description

This command configures a range of FastEthernet or GigabitEthernet interfaces on the controller.

Syntax

Parameter	Description	Range	Default
`range`	Range of Ethernet ports in the format <slot>/<port>-<port>.	—	—
`duplex`	Transmission mode on the interface: full- or half-duplex or auto to automatically adjust transmission.	auto/full/ half	auto
`ip access-group`	Applies the specified access control list (ACL) to the interface. Use the ip access-list command to configure an ACL.	—	—
`in`	Applies ACL to interface's inbound traffic.	—	—
`out`	Applies ACL to interface's outbound traffic.	—	—
`session`	Applies session ACL to interface and optionally to a selected VLAN associated with this port.	—	—
`no`	Negates any configured parameter.	—	—
`poe`	Enables Power-over-Ethernet (PoE) on the interface.	—	—
`cisco`	Enables Cisco-style PoE on the interface.	—	—
`shutdown`	Causes a hard shutdown of the interface.	—	—
`spanning-tree`	Enables spanning tree.	—	—
`cost`	Administrative cost associated with the spanning tree.	1-65535	—
`port-priority`	Spanning tree priority of the interface. A lower setting brings the port closer to root port position (favorable for forwarding traffic) than does a higher setting. This is useful if ports may contend for root position if they are connected to an identical bridge.	0-255	
`portfast`	Enables forwarding of traffic from the interface.	—	—
`speed`	Sets the interface speed: 10 Mbps, 100 Mbps, or auto configuration.	10|100|auto	auto
`switchport`	Sets switching mode parameters for the interface.	—	—
`access vlan`	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.	—	—
`mode`	Sets the mode of the interface to access or trunk mode only.	—	—
`trunk`	Sets the interface as a trunk port for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the controller, or add or remove specified VLANs. Specify **native** to identify the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.	—	—
`trusted`	Set this interface and range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted. Trusted ports and VLANs are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When Dell APs are attached directly to the controller, set the port to be trusted.	—	enabled

Parameter	Description	Range	Default
`vlan <word>`	Sets the supplied range of VLANs as trusted. All remaining become untrusted automatically. For example, If you set a VLAN range as: vlan 1-10, 100-300, 301, 305-400, 501-4094 Then all VLANs in this range are trusted and all others become untrusted by default. You can also use the **no trusted vlan** command to explicitly make an individual VLAN untrusted. The no trusted vlan command is additive and adds given vlans to the existing untrusted vlan set. However, if you execute the **trusted vlan <word>** command, it overrides any earlier untrusted VLANs or a range of untrusted VLANs and creates a new set of trusted VLANs. **NOTE:** A port supports a user VLAN range from 1-4094. If you want to set all VLANs (1-4094) on a port as untrusted then mark the port itself as untrusted. By default the port and all its associated VLANs are trusted.	1-4094	—

Usage Guidelines

Use the show port status command to obtain information about the interfaces available on the controller.

Example

The following command configures a range of interface as a trunk port for a set of VLANs:

```
interface range fastethernet 1/12-15
   switchport mode trunk
   switchport trunk native vlan 10
   switchport trunk allowed vlan 1,10,100
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4	The **trusted VLAN** and i**p access-group session vlan** parameters were introduced.
ArubaOS 3.4.1	The **trusted vlan <word>** parameter was added.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master and local controllers

interface tunnel

```
interface tunnel <number>
   description <string>
   inter-tunnel-flooding
   ip address <ipaddr> <netmask>
   mtu <mtu>
   no ...
   shutdown
   trusted
   tunnel checksum|destination <ipaddr>|keepalive [<interval> <retries>]|key
<key>|mode gre {<protocol>|ip}|source {<ipaddr>|loopback|vlan <vlan>}|vlan
<vlans>
```

Description

This command configures a tunnel interface.

Syntax

Parameter	Description	Range	Default
`tunnel`	Identification number for the tunnel.	1-2147483647	—
`description`	String that describes this interface.	—	Tunnel Interface
`inter-tunnel-flooding`	Enables inter-tunnel flooding.	—	enabled
`ip address`	IP address of the tunnel. This represents the entrance to the tunnel.	—	—
`mtu`	MTU size for the interface.	—	1500
`no`	Negates any configured parameter.	—	—
`shutdown`	Causes a hard shutdown of the interface.	—	—
`trusted`	Set this interface and range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted. Trusted ports and VLANs are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When Dell APs are attached directly to the controller, set the port to be trusted.	—	disabled
`tunnel`	Configures tunneling.	—	mode gre ip
`checksum`	Enables end-to-end checksum of packets that pass through the tunnel.	—	disabled
`destination`	Destination IP address for the tunnel endpoint.	—	—
`keepalive`	Enables sending of periodic keepalive frames on the tunnel to determine the tunnel status (up or down). You can optionally set the interval at which keepalive frames are sent, and the number of times the frames are resent before a tunnel is considered to be down.	—	disabled
`<interval>`	(Optional) Number of seconds at which keepalive frames are sent.	1-86400	10 seconds
`<retries>`	(Optional) Number of consecutive times that the keepalives fail before the tunnel is considered to be down.	0-1024	3
`key`	Key used to authenticate packets on the tunnel.	0-4294967295	—
`mode gre`	Specifies generic route encapsulation (GRE) type. You configure either a 16-bit protocol number (for Layer-2 tunnels) or **ip** (for a Layer-3 tunnel). The 16-bit protocol number uniquely identifies a Layer-2 tunnel. The controllers at both endpoints of the tunnel must be configured with the same protocol number.	—	—
`source`	The local endpoint of the tunnel on the controller. This can be one of the following: • specified IP address • the loopback interface configured on the controller • specified VLAN	—	—
`vlan`	VLANs to be included in this tunnel.	—	—

Usage Guidelines

You can configure a GRE tunnel between an Dell controller and another GRE-capable device. Layer-3 GRE

tunnel type is the default (**tunnel mode gre ip**). You can direct traffic into the tunnel using a static route (specify the tunnel as the next hop for a static route) or a session-based access control list (ACL).

Example

The following command configures a tunnel interface:

```
(host) (config) #interface tunnel 200
   ip address 10.1.1.1 255.255.2550
   tunnel source loopback
   tunnel destination 20.1.1.242
   tunnel mode gre ip
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	The **keepalive** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master and local controllers

interface vlan

```
interface vlan <vlan>
   bandwidth-contract <name>
   bcmc-optimization
   description <string>
   ip address {<ipaddr> <netmask>|dhcp-client|pppoe}|helper-address
   <ipaddr>|igmp|local-proxy-arp|nat inside|{ospf area <id>}routing}
   ipv6 mld [snooping]
   mtu
   no ...
   operstate up
   shutdown
```

Description

This command configures a VLAN interface.

Syntax

Parameter	Description	Range	Default
`vlan`	VLAN ID number.	1-4094	—
`bandwidth-contract`	Name of the bandwidth contract to be applied to this VLAN interface. When applied to a VLAN, the contract only limits multicast traffic and does not affect other data. Use the aaa bandwidth-contract command to configure a bandwidth contract.	—	—
`bcmc-optimization`	Enables broadcast and multicast traffic optimization to prevent flooding of broadcast and multicast traffic on VLANs.	—	—
`description`	String that describes this interface.	—	802.1Q VLAN
`ip`	Configures IPv4 for this interface.		
`address`	Configures the IP address for this interface, which can be one of the following: <ipaddr> <netmask> dhcp-client: use DHCP to obtain the IP address pppoe: use PPPoE to obtain the IP address	—	—
`helper-address`	IP address of the DHCP server for relaying DHCP requests for this interface. If the DHCP server is on the same subnetwork as this VLAN interface, you do not need to configure this parameter.	—	—
`igmp`	Enables IGMP and/or IGMP snooping on this interface.	—	—
`local-proxy-arp`	Enables local proxy ARP.	—	—
`nat inside`	Enables source network address translation (NAT) for all traffic routed from this VLAN.	—	—
`ospf`	Define an OSPF area. See `ip ospf` for complete details on this command.	—	—
`pppoe-max-segment-site`	Configures the TCP maximum segment size in bytes.	128	—
`pppoe-password`	Configures the PAP password on the PPPoE Access Concentrator for the switch.	1–80	—
`pppoe-service-name`	Configures the PPPoE service name.	1–80	—
`pppoe-username`	Configures the PAP username on the PPPoE Access Concentrator for the switch.	1–80	—
`routing`	Enables layer-3 forwarding on the VLAN interface. To disable layer-3 forwarding, you must configure the IP address for the interface and specify **no ip routing**.	—	(enabled)
`ipv6`	Configures IPv6 for this interface.		
`mld`	Enables Multicast Listener Discovery (MLD) on this interface.	—	—
`snooping`	Enables MLD snooping on this interface.	—	—
`no`	Negates any configured parameter.	—	—
`mtu`	MTU setting for the VLAN.	1024-1500	—
`operstate up`	Set the state of the interface to be up.	—	—
`shutdown`	Causes a hard shutdown of the interface.	—	—

Usage Guidelines

All ports on the controller are assigned to VLAN 1 by default. Use the interface fastethernet|gigabitethernet command to assign a port to a configured VLAN.

Example

The following command configures a VLAN interface:

```
(host) (config) #interface vlan 16
   ip address 10.26.1.1 255.255.255.0
   ip helper-address 10.4.1.22
```

Command History

This command was introduced in ArubaOS 3.0

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3	The **ipv6** parameters were introduced.
ArubaOS 3.4	The **igmp snooping** parameter was deprecated. For information on configuring IGMP snooping in ArubaOS 3.4 or later, see "interface vlan ip igmp proxy" on page 31.
ArubaOS 6.0	The **pppoe-max-segment-site**, **pppoe-password**, **pppoe-service-name** and **pppoe-password** parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master and local controllers

interface vlan ip igmp proxy

```
interface vlan <vlan>
   ip igmp snooping|{proxy fastethernet|gigabitethernet <slot>/<port>}
```

Description

This command enables IGMP and/or IGMP snooping on this interface, or configures a VLAN interface for uninterrupted streaming of multicast traffic.

Syntax

Parameter	Description
`snooping`	Enable IGMP snooping. The IGMP protocol enables an router to discover the presence of multicast listeners on directly-attached links. Enable IGMP snooping to limit the sending of multicast frames to only those nodes that need to receive them.
`proxy`	Enable IGMP on this interface.
`fastethernet`	Enable IGMP proxy on the FastEthernet (IEEE 802.3) interface.
`gigabitethernet`	Enable IGMP proxy on the GigabitEthernet (IEEE 802.3) interface.
`<slot>/<port>`	Any command that references a Fast Ethernet or Gigabit Ethernet interface requires that you specify the corresponding port on the controller in the format <slot>/<port>. The **<slot>** parameter is always 1. The **<port>** parameter refers to the network interfaces that are embedded in the front panel of the W-3000 Controller Series Multi-Service Controller. Port numbers start at 0, from the left-most position.

Usage Guidelines

The newer IGMP proxy feature and the older IGMP snooping feature cannot be enabled at the same time, as both features add membership information to multicast group table. For most multicast deployments, you should enable the IGMP Proxy feature on all VLAN interfaces to manage all the multicast membership requirements on the controller. If IGMP snooping is configured on some of the interfaces, there is a greater chance that multicast information transfers may be interrupted.

Example

The following example configures IGMP proxy for vlan 2. IGMP reports from the controller would be sent to the upstream router on fastethernet port 1/3.

```
(host) (conf)# interface vlan 2
   (conf-subif)# ip igmp proxy fastethernet 1/3
```

Related Commands

This release of ArubaOS supports version 1 of the Multicast Listener Discovery (MLD) protocol (MLDv1). MLDv1, defined in RFC 2710, is derived from version 2 of the IPv4 Internet Group Management Protocol (IGMPv2)

Issue the command **interface vlan <vlan> ipv6 mld** to enable the MLD protocol and allow an IPv6 router to discover the presence of multicast listeners on directly-attached links. Use the CLI command **interface vlan <vlan> ipv6 mld snooping**, and the IPv6 router will send multicast frames to only those nodes that need to receive them.

Command History

This command was introduced in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

ip access-list eth

```
ip
ip access-list eth {<number>|<name>}
   deny {<ethtype> [<bits>]|any} [mirror]
   no ...
   permit {<ethtype> [<bits>]|any} [mirror]
```

Description

This command configures an Ethertype access control list (ACL).

Syntax

Parameter	Description	Range
`eth`	Enter a name, or a number in the specified range.	200-299
`deny`	Reject the specified packets, which can be one of the following: Ethertype in decimal or hexadecimal (0-65535) and optional wildcard (0-65535) any: match any Ethertype Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.	—
`no`	Negates any configured parameter.	—
`permit`	Allow the specified packets, which can be one of the following: Ethertype in decimal or hexadecimal (0-65535) and optional wildcard (0-65535) any: match any Ethertype Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.	—

Usage Guidelines

The Ethertype field in an Ethernet frame indicates the protocol being transported in the frame. This type of ACL filters on the Ethertype field in the Ethernet frame header, and is useful when filtering non-IP traffic on a physical port. This ACL can be used to permit IP frames while blocking other non-IP protocols such as IPX or Appletalk.

If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see “firewall” on page 197.

Example

The following command configures an Ethertype ACL:

```
(host) (config) #ip access-list eth 200
   deny 809b
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3	The **mirror** parameter was introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license.	Config mode on master controllers

ip access-list extended

```
ip access-list extended {<number>|<name>}
   deny <protocol> <source> <dest>
   ipv6
   no ...
   permit <protocol> <source> <dest>
```

Description

This command configures an extended access control list (ACL). To configure IPv6 specific rules, use the `ipv6` keyword for each rule.

Syntax

Parameter	Description	Range
`extended`	Enter a name, or a number in the specified range.	100-199, 2000-2699
`ipv6`	Use the ipv6 keyword to add IPv6 specific rules.	
`deny`	Reject the specified packets.	
`<protocol>`	Protocol, which can be one of the following: • Protocol number between 0-255 • any: any protocol • icmp: Internet Control Message Protocol • igmp: Internet Gateway Message Protocol • tcp: Transmission Control Protocol • udp: User Datagram Protocol	—
`<source>`	Source, which can be one of the following: • Source address (IPv4 or IPv6) and wildcard • any: any source • host: specify a single host IP address	—
`<dest>`	Destination, which can be one of the following: • Destination address (IPv4 or IPv6) and wildcard • any: any destination • host: specify a single host IP address	—
`no`	Negates any configured parameter.	—
`permit`	Allow the specified packets.	
`<protocol>`	Protocol, which can be one of the following: • Protocol number between 0-255 • any: any protocol • icmp: Internet Control Message Protocol • igmp: Internet Gateway Message Protocol • tcp: Transmission Control Protocol • udp: User Datagram Protocol	—
`<source>`	Source, which can be one of the following: Source address (IPv4 or IPv6) and wildcard any: any source host: specify a single host IP address	—
`<dest>`	Destination, which can be one of the following: Destination address (IPv4 or IPv6) and wildcard any: any destination host: specify a single host IP address	—

Usage Guidelines

Extended ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source or destination IP address or IP protocol.

Example

The following command configures an extended ACL:

```
(host) (config) #ip access-list extended 100
   deny any host 1.1.21.245 any
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config mode on master controllers

ip access-list mac

```
ip access-list mac {<number>|<name>}
   deny {<macaddr>[<wildcard>]|any|host <macaddr>} [mirror]
   no ...
   permit {<macaddr>[<wildcard>]|any|host <macaddr>} [mirror]
```

Description

This command configures a MAC access control list (ACL).

Syntax

Parameter	Description	Range
mac	Configures a MAC access list. Enter a name, or a number in the specified range.	700-799, 1200-1299
deny	Reject the specified packets, which can be the following: MAC address and optional wildcard any: any packets host: specify a MAC address Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.	—
no	Negates any configured parameter.	—
permit	Allow the specified packets, which can be the following: MAC address and optional wildcard any: any packets host: specify a MAC address Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.	—

Usage Guidelines

MAC ACLs allow filtering of non-IP traffic. This ACL filters on a specific source MAC address or range of MAC addresses.

If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see “firewall” on page 197.

Example

The following command configures a MAC ACL:

```
(host) (config) #ip access-list mac 700
   deny 11:11:11:00:00:00
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3	The **mirror** parameter was introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config

ip access-list session

```
ip access-list session <accname>
   <source> <dest> <service> <action> [<extended action>]
   ipv6 [alias | any | host | network | user]
   no ...
```

Description

This command configures an access control list (ACL) session. To create IPv6 specific rules, use the `ipv6` keyword.

Syntax

Parameter	Description
<accname>	Enter a name for this ACL
ipv6	Use the ipv6 keyword to create IPv6 specific rules.
<source>	The traffic source, which can be one of the following: **alias**: specify the network resource (use the **netdestination** command to configure aliases; use the **show netdestination** command to see configured aliases) **any**: match any traffic **host**: specify a single host IP address **localip**: specify the local IP address to match traffic **network**: specify the IP address and netmask **user**: represents the IP address of the user
<dest>	The traffic destination, which can be one of the following: **alias**: specify the network resource (use the **netdestination** command to configure aliases; use the **show netdestination** command to see configured aliases) **any**: match any traffic **host**: specify a single host IP address **localip**: specify the local IP address to match traffic **network**: specify the IP address and netmask **user**: represents the IP address of the user
<service>	Network service, which can be one of the following: IP protocol number (0-255) name of a network service (use the show netservice command to see configured services) **any**: match any traffic **tcp**: specify the TCP port number (0-65535) **udp**: specify the UDP port number (0-65535)
<action>	Action if rule is applied, which can be one of the following: **deny**: reject packets **dst-nat**: perform destination NAT on packets **dual-nat**: perform both source and destination NAT on packets **permit:** forward packets **redirect**: specify the location to which packets are redirected, which can be one of the following: • datapath destination ID (**0-65535**) • **esi-group**: specify the ESI server group configured with the esi group command • **opcode**: specify the datapath destination ID (0x33, 0x34, or 0x82). Do not use this parameter without proper guidance from Dell PowerConnect **tunnel:** specify the ID of the tunnel configured with the interface tunnel command **src-nat**: perform source NAT on packets
<extended action>	Optional action if rule is applied, which can be one of the following: **blacklist**: blacklist user **disable-scanning**: pause ARM scanning while traffic is present. Note that you must enable “Voice Aware Scanning” in the ARM profile for this feature to work. **dot1p-priority**: specify 802.1p priority (0-7) **log**: generate a log message **mirror**: mirror all session packets to datapath or remote destination If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see “firewall” on page 197. **position**: specify the position of the rule (1 is first, default is last) **queue**: assign flow to priority queue (high/low) **send-deny-response**: if <action> is deny, send an ICMP notification to the source **time-range**: specify time range for this rule (configured with time-range command) **tos**: specify ToS value (0-63)

Parameter	Description
no	Negates any configured parameter.

Usage Guidelines

Session ACLs define traffic and firewall policies on the controller. You can configure multiple rules for each policy, with rules evaluated from top (1 is first) to bottom. The first match terminates further evaluation. Generally, you should order more specific rules at the top of the list and place less specific rules at the bottom of the list. The ACL ends with an implicit deny all. To configure IPv6 rules, use the `ipv6` keyword followed by the regular ACL keywords.

Example

The following command configures a session ACL that drops any traffic from 10.0.0.0 subnetwork:

```
ip access-list session drop-from10
   network 10.0.0.0 255.0.0.0 any any
```

The following command configures a session ACL with IPv4 and IPv6 address:

```
(host) (config)#ip access-list session common
(host) (config-sess-common)#host 10.12.13.14 any any permit
(host) (config-sess-common)#ipv6 host 11:12:11:11::2 any any permit
(host) (config-sess-common)#show ip access-list common
ip access-list session common

common
-------
Priority  Source          Destination  Service  Action  ...  Queue  TOS  8021P  ...  ClassifyMedia  IPv4/6
--------  ------          -----------  -------  ------  ...  -----  ---  -----  ...  -------------  ------
1         1.2.3.4         any          any      permit  ...  Low               ...                 4
2         11:12:11:11::2  any          any      permit  ...  Low               ...                 6
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config mode on master controllers

ip access-list standard

```
ip access-list standard {<number>|<name>}
   deny {<ipaddr> <wildcard>|any|host <ipaddr>}
   no ...
   permit {<ipaddr> <wildcard>|any|host <ipaddr>}
```

Description

This command configures a standard access control list (ACL).

Syntax

Parameter	Description	Range
`standard`	Enter a name, or a number in the specified range.	1-99, 1300-1399
`ipv6`	Use the ipv6 keyword to create IPv6 specific standard rules.	
`deny`	Reject the specified packets, which can be the following: IP address and optional wildcard any: any packets host: specify a host IP address	—
`no`	Negates any configured parameter.	—
`permit`	Allow the specified packets, which can be the following: IP address and optional wildcard any: any packets host: specify a host IP address	—

Usage Guidelines

Standard ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source address of the packet.

Example

The following command configures a standard ACL:

```
(host) (config) #ip access-list standard 1
   permit host 10.1.1.244
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config mode on master controllers

ip cp-redirect-address

```
ip cp-redirect-address <ipaddr> | disable
```

Description

This command configures a redirect address for captive portal.

Syntax

Parameter	Description
`<ipaddr>`	Host address with a 32-bit netmask. This address should be routable from all external networks.
`disable`	Disables automatic DNS resolution for captive portal.

Usage Guidelines

This command redirects wireless clients that are on different VLANs (from the controller's IP address) to the captive portal on the controller.

If you have the Next Generation Policy Enforcement Firewall (PEFNG) license installed in the controller, modify the captive portal session ACL to permit HTTP/S traffic to the destination **cp-redirect-address <ipaddr>** instead of **mswitch**. If you do not have the PEFNG license installed in the controller, the implicit captive-portal-profile ACL is automatically modified when you issue this command.

Example

The following command configures a captive portal redirect address:

```
(host) (config) #ip cp-redirect-address
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip default-gateway

```
ip default-gateway <ipaddr>|{import cell|dhcp|pppoe}|{ipsec <name>} <cost>
```

Description

This command configures the default gateway for the controller.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the default gateway.
`import`	Use a gateway IP address obtained through the cell interface, DHCP or PPPoE. The default gateway is imported into the routing table and removed when the uplink is no longer active.
`cell`	Use Cell interface when available to obtain default gateway.
`dhcp`	Use DHCP when available to obtain default gateway.
`pppoe`	Use PPPOE when available to obtain default gateway.
`ipsec <name>`	Define a static route using an ipsec map.
`<cost>`	Distance metric for this route.

Usage Guidelines

You can use this command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect the controller. If you define more than one dynamic gateway type, you must also define a cost for the route to each gateway. The controller will first attempt to obtain a gateway IP address using the option with the lowest cost. If the controller is unable to obtain a gateway IP address, it will then attempt to obtain a gateway IP address using the option with the next-lowest path cost.

Example

The following command configures the default gateway for the controller:

```
(host) (config) #ip default-gateway 10.1.1.1
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip dhcp excluded-address

```
ip dhcp excluded-address <low-ipaddr> [<high-ipaddr>]
```

Description

This command configures an excluded address range for the DHCP server on the controller.

Syntax

Parameter	Description
`<low-ipaddr>`	Low end of range of IP addresses. For example, you can enter the IP address of the controller so that this address is not assigned.
`<high-ipaddr>`	High end of the range of IP addresses.

Usage Guidelines

Use this command to specifically exclude certain addresses from being assigned by the DHCP server. It is good practice to exclude any statically assigned addresses.

Example

The following command configures an excluded address range:

```
ip dhcp excluded-address 192.168.1.1 192.168.1.255
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in base operating system	Config mode on master controllers

ip dhcp pool

```
ip dhcp pool <name>
   default-router <ipaddr> ...
   dns-server {<ipaddr> ... |import}
   domain-name <name>
   lease <days> <hours> <minutes>
   netbios-name-server {<ipaddr> ... |import}
   network <ipaddr> {<netmask>|<prefix>}
   no ...
   option <code> ip <ipaddr>
```

Description

This command configures a DHCP pool on the controller.

Syntax

Parameter	Description
`default-router`	IP address of the default router for the DHCP client. The client should be on the same subnetwork as the default router. You can specify up to eight IP addresses.
`dns-server`	IP address of the DNS server, which can be one of the following:
`<address>`	IP address of the DNS server. You can specify up to eight IP addresses.
`import`	Use the DNS server address obtained through PPPoE or DHCP.
`domain-name`	Domain name to which the client belongs.
`lease`	The amount of time that the assigned IP address is valid for the client. Specify the lease in <days> <hours> <minutes>.
`netbios-name-server`	IP address of the NetBIOS Windows Internet Naming Service (WINS) server, which can be one of the following:
`<address>`	IP address of the WINS server. You can specify up to eight IP addresses.
`import`	Use the NetBIOS name server address obtained through PPPoE or DHCP.
`network`	Range of addresses that the DHCP server may assign to clients, in the form of <ipaddr> and <netmask> or <ipaddr> and <prefix> (/n).
`no`	Negates any configured parameter.
`option`	Client-specific option code and IP address. See RFC 2132, "DHCP Options and BOOTP Vendor Extensions".

Usage Guidelines

A DHCP pool should be created for each IP subnetwork for which DHCP services should be provided. DHCP pools are not specifically tied to VLANs, as the DHCP server exists on every VLAN. When the controller receives a DHCP request from a client, it examines the origin of the request to determine if it should respond. If the IP address of the VLAN matches a configured DHCP pool, the controller answers the request.

Example

The following command configures a DHCP pool:

```
(host) (config) #ip dhcp pool floor1
   default-router 10.26.1.1
   dns-server 192.168.1.10
   domain-name floor1.test.com
```

```
lease 0 8 0
network 10.26.1.0 255.255.255.0
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip domain lookup

```
ip domain lookup
```

Description

This command enables Domain Name System (DNS) hostname to address translation.

Syntax

There are no parameters for this command.

Usage Guidelines

This command is enabled by default. Use the **no** form of this command to disable.

Example

The following command enables DNS hostname translation:

```
(host)(config) #ip domain lookup
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip domain-name

```
ip domain-name <name>
```

Description

This command configures the default domain name.

Syntax

Parameter	Description
`domain-name`	Name used to complete unqualified host names. Do not specify the leading dot (.).

Usage Guidelines

The controller uses the default domain name to complete hostnames that do not contain domain names. You must have at least one domain name server configured on the controller (see “ip name-server” on page 286).

Example

The following command configures the default domain name:

```
(host) (config) #ip domain-name yourdomain.com
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip igmp

```
ip igmp
   last-member-query-count <number>
   last-member-query-interval <seconds>
   query-interval <seconds>
   query-response-interval <.1 seconds>
   robustness-variable <2-10>
   startup-query-count <number>
   startup-query-interval <seconds>
   version-1-router-present-timeout <seconds>
```

Description

This command configures Internet Group Management Protocol (IGMP) timers and counters.

Syntax

Parameter	Description	Range	Default
`last-member-query-count`	Number of group-specific queries that the controller sends before assuming that there are no local group members.	—	2
`last-member-query-interval`	Maximum time, in seconds, that can elapse between group-specific query messages.	—	10 seconds
`query-interval`	Interval, in seconds, at which the controller sends host-query messages to the multicast group address 224.0.0.1 to solicit group membership information.	1-1024	125 seconds
`query-response-interval`	Maximum time, in .1 seconds, that can elapse between when the controller sends a host-query message and when it receives a response. This must be less than the query-interval.	1-1024	100 (10 seconds)
`robustness-variable`	Increase this value to allow for expected packet loss on a subnetwork.	2-10	2
`startup-query-count`	Number of queries that the controller sends out on startup, separated by startup-query-interval. The default is the robustness-variable value.	—	2
`startup-query-interval`	Interval, in seconds, at which the controller sends general queries on startup. The default is 1/4 of the query-interval.	—	31 seconds
`version-1-router-present-timeout`	Timeout, in seconds, if a version 1 IGM router is detected.	—	400 seconds

Usage Guidelines

IGMP is used to establish and manage IP multicast group membership. See RFC 3376, “Internet Group Management Protocol, version 3” for more information.

Example

The following command configures IGMP:

```
(host) (config) #ip igmp
   query-interval 130
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip local

```
ip local pool <name> <start-ipaddr> [<end-ipaddr>]
```

Description

This command configures a local IP pool for Layer-2 Tunnel Protocol (L2TP).

Syntax

Parameter	Description
`pool`	Name for the address pool.
`<start-ipaddr>`	Starting IP address for the pool.
`<end-ipaddr>`	(Optional) Ending IP address for the pool.

Usage Guidelines

VPN clients can be assigned IP addresses from the L2TP pool.

Example

The following command configures an L2TP pool:

```
(host) (config) #ip local pool 10.1.1.1 10.1.1.99
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip mobile active-domain

```
ip mobile
ip mobile active-domain <name>
```

Description

This command configures the mobility domain that is active on the controller.

Syntax

Parameter	Description
`active-domain`	Name of the mobility domain.

Usage Guidelines

All controllers are initially part of the “default” mobility domain. If you use the “default” mobility domain, you do not need to specify this domain as the active domain on the controller. However, once you assign a controller to a user-defined domain, the “default” mobility domain is no longer an active domain on the controller.

Example

The following command assigns the controller to a user-defined mobility domain:

```
(host) (config) #ip mobile active-domain campus1
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip mobile domain

```
ip mobile domain <name>
   hat <subnetwork> <mask> <vlan> <ha-ipaddr> <desc>
   no ...
```

Description

This command configures the mobility domain on the controller.

Syntax

Parameter	Description	Range
`domain`	Name of the mobility domain.	—
`hat`	Configures a home agent table (HAT) entry.	—
`<subnetwork>`	Subnet that requires mobility service.	—
`<mask>`	Netmask for the IP address.	—
`<vlan>`	VLAN ID. The VLAN ID must be the VLAN number on the home agent controller.	1-4094
`<ha-ipaddr>`	IP address of the home agent.	—
`<desc>`	Description of a HAT entry. The description can be a maximum of 30 characters (including spaces).	
`no`	Negates any configured parameter.	—

Usage Guidelines

You configure the HAT on a master controller; the mobility domain information is pushed to all local controllers that are managed by the same master.

HAT entries map subnetworks or VLANs and the home agents. The home agent is typically the controller's IP address. The home agent's IP address must be routable; that is, all controllers that belong to the same mobility domain must be able to reach the home agent's IP address.

The controller looks up information in the HAT to obtain the IP address of the home agent for a mobile client. Because there can be multiple home agents on a subnetwork, the HAT can contain more than one entry for the same subnetwork.

Example

The following command configures HAT entries:

```
(host) (mobility-domain) #ip mobile domain east_building
(host) (mobility-domain) #hat 10.11.1.0 255.255.255.0 120 10.11.1.200 description "East
building entries"
(host) (mobility-domain) #show ip mobile domain east_building
Mobility Domains:, 1 domain(s)
------------------------------

Domain name east_building
   Home Agent Table, 1 subnet(s)
   subnet          mask            VlanId Home Agent      Description
   --------------- --------------- ------ --------------- -------------------------
   10.11.1.0       255.255.255.0   120    10.11.1.200     East building entries
```

Command History

Release	Modification
ArubaOS 3.0	Command available.
ArubaOS 6.0	A new parameter, **description** is added for providing more information about a HAT entry.
ArubaOS 3.4.1	**vlan range** parameter introduced.
ArubaOS 6.0	**wired aaa-profile** parameter introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip mobile foreign-agent

```
ip mobile foreign-agent {lifetime <seconds> | max-visitors <number> |
registrations {interval <msecs> | retransmits <number>}}
```

Description

This command configures the foreign agent for IP mobility.

Syntax

Parameter	Description	Range	Default
`lifetime`	Requested lifetime, in seconds, as per RFC 3344, "IP Mobility Support for IPv4".	10-65534	180 seconds
`max-visitors`	Maximum number of active visitors.	0-5000	5000
`registrations`	Frequency at which re-registration messages are sent to the home agent:		
`interval`	Retransmission interval, in milliseconds	100-10000	1000 milliseconds
`retransmits`	Maximum number of times the foreign agent attempts mobile IP registration message exchanges before giving up.	0-5	3

Usage Guidelines

A foreign agent is the controller which handles all mobile IP communication with a home agent on behalf of a roaming client.

Example

The following command configures the foreign agent:

```
(host) (config) #ip mobile foreign-agent registration interval 10000
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip mobile home-agent

```
ip mobile home-agent {max-bindings <number>|replay <seconds>}
```

Description

This command configures the home agent for IP mobility.

Syntax

Parameter	Description	Range	Default
`max-bindings`	Maximum number of mobile IP bindings. This option is an additional limitation to control the maximum number of roaming users. When the limit is reached, registration requests from the foreign agent fail which causes a mobile client to set a new session on the visited controller, which will become its home controller.	0-5000	5000
`replay`	Time difference, in seconds, for timestamp-based replay protection, as described by RFC 3344, “IP Mobility Support for IPv4”. 0 disables replay.	0-300	7 seconds

Usage Guidelines

A home agent for a mobile client is the controller where the client first appears when it joins the mobility domain. The home agent is the single point of contact for the client when it roams.

Example

The following command configures the home agent:

```
(host) (config) #ip mobile home-agent replay 100
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ip mobile proxy

```
ip mobile proxy auth-sta-roam-only | block-dhcp-release | dhcp {max-requests <number>|
transaction-hold <seconds>|transaction-timeout <seconds>}| event-threshold <number> |
log-trail | no-service-timeout <seconds> | on-association |re-home |
stale-timeout <seconds> | stand-alone-AP | trail-length <number> |trail-timeout
<seconds>
```

Description

This command configures the proxy mobile IP module in a mobility-enabled controller.

Syntax

Parameter	Description	Range	Default
auth-sta-roam-only	Allows a client to roam only if has been authenticated. If a client has not been authenticated, no mobility service is offered if it roams to a different VLAN or controller.	—	enabled
block-dhcp-release	Determines whether DHCP release packets generated from the client should be dropped or forwarded to the DHCP server. Blocking the packets prevents the DHCP server from assigning the same IP address to another client until the lease has expired.		disabled
dhcp	Configures proxy DHCP		
aggressive-transaction	Terminate Proxy DHCP on aggressive Transaction ID change. **NOTE:** Best practices is to keep this parameter at the default setting	0-65534	25
max-requests	Maximum number of BOOTP packets that are allowed to be handled during one DHCP session.	0-65534	25
transaction-hold	Hold time, in seconds, on proxy DHCP state after completion of DHCP transaction (DHCP ACK) was forwarded to the client. This option ensures that late BOOTP replies reach the station and that a retransmitted BOOTP request does not trigger a new proxy DHCP session.	1-600	5 seconds
transaction-timeout	Maximum time allowed for a proxy DHCP session to complete.	10-600	60 seconds
event-threshold	Maximum number of mobility events (events that can trigger mobility) handled per second. Mobility events above this threshold are ignored. This helps to control frequent mobility state changes when the client bounces back and forth on APs before settling down.	1-65535	25
log-trail	Enables logging at the notification level for mobile client moves.	—	enabled
no-service-timeout	Time, in seconds, after which mobility service expires. If nothing has changed from the previous state, the client is given another bridge entry but it will have limited connectivity.	30-60000	180 seconds
on-association	Mobility move detection is performed when the client associates with the controller instead of when the client sends packets. Enabled by default. Mobility on association can speed up roaming and improve connectivity for devices that do not send many uplink packets out that can trigger mobility. Downside is security; an association is all it takes to trigger mobility. This is irrelevant unless layer-2 security is enforced.	—	enabled
re-home	Allows on-hook phones to be assigned a new home agent. This is to load balance voice client home agents across controllers in a mobility domain. This parameter requires that you install the PEFNG license in the controller.	—	disabled
stale-timeout	Number of seconds the mobility state is retained after the loss of connectivity. This allows authentication state and mobility information to be preserved on the home agent controller. The default is 60 seconds but can be safely increased. Note that in many case a station state is deleted without waiting for the stale timeout; user delete from management, foreign agent to foreign agent handoff, etc. (This is different from the no-service-timeout; no-service-timeout occurs up front while the stale-timeout begins when mobility service is provided but the connection is disrupted for some reason.)	30-3600	60 seconds

`stand-alone-AP`	Enables support for third party or standalone APs. When this is enabled, broadcast packets are not used to trigger mobility and packets from untrusted interfaces are accepted. If mobility is enabled, you must also enable standalone AP for the client to connect to the controller's untrusted port. If the controller learns wired users via the following methods, enable standalone AP: • Third party AP connected to the controller through the untrusted port. • Clients connected to ENET1 on APs with two ethernet ports. • Wired user connected directly to the controller's untrusted port.	—	disabled
`trail-length`	Specifies the maximum number of entries (client moves) stored in the user mobility trail.	1-100	30
`trail-timeout`	Specifies the maximum interval, in seconds, an inactive mobility trail is held.	120-86400	3600 seconds

Usage Guidelines

The *proxy mobile IP module* in a mobility-enabled controller detects when a mobile client has moved to a foreign network and determines the home agent for a roaming client. The proxy mobile IP module performs the following functions:

- Derives the address of the home agent for a mobile client from the HAT using the mobile client's IP address. If there is more than one possible home agent for a mobile client in the HAT, the proxy mobile IP module uses a discovery mechanism to find the current home agent for the client.
- Detects when a mobile client has moved. Client moves are detected based on ingress port and VLAN changes and mobility is triggered accordingly. For faster roaming convergence between AP(s) on the same controller, it is recommended that you keep the "on-association" option enabled. This helps trigger mobility as soon as 802.11 association packets are received from the mobile client.

Example

The following command enables re-home for voice clients:

```
(host) (config) #ip mobile proxy re-home
```

Note: The re-home parameter requires the PEFNG license.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system. The re-home parameter requires the PEFNG license.	Config mode on master controllers

ip mobile revocation

```
ip mobile revocation {interval <msec>|retransmits <number>
```

Description

This command configures the frequency at which registration revocation messages are sent.

Syntax

Parameter	Description	Range	Default
`interval`	Retransmission interval, in milliseconds.	100-10000 ms	1000 ms
`retransmits`	Maximum number of times the home agent or foreign agent attempts mobile IP registration/revocation message exchanges before giving up.	0-5	3

Usage Guidelines

A home agent or foreign agent can send a registration revocation message, which revokes registration service for the mobile client. For example, when a mobile client roams from one foreign agent to another, the home agent can send a registration revocation message to the first foreign agent so that the foreign agent can free any resources held for the client.

Example

The following command configures registration revocation messages:

```
(host) (config) #ip mobile revocation interval 2000
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on master controllers

ip mobile trail

```
ip mobile trail {host IP address | host MAC address}
```

Description

This command configures the capture of association trail for all devices.

Syntax

Parameter	Description	Default
`Host IP address`	The IP address of the client for which the association trail is captured.	disabled
`Host MAC address`	The MAC address of the client for which the association trail is captured.	disabled

Usage Guidelines

A device can move from one home agent to another or between home agents. When the client makes an association, the agent can store information about the client and registration time. The association trail can be captured for devices even when mobility is disabled.

Example

The following command configures trail capture for a client using its IP address:

```
(host) (config) #ip mobile trail 1.2.3.4
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on master controllers

ip name-server

```
ip name-server <ipaddr>
```

Description

This command configures servers for name and address resolution.

Syntax

Parameter	Description
<ip-addr>	IP address of the server.

Usage Guidelines

You can configure up to six servers using separate commands. Specify one or more servers when you configure a default domain name (see “ip domain-name” on page 272).

Example

The following command configures a name server:

```
ip name-server 10.1.1.245
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on master controllers

ip nat

```
ip nat pool <name> <start-ipaddr> <end-ipaddr> [<dest-ipaddr>]
```

Description

This command configures a pool of IP addresses for network address translation (NAT).

Syntax

Parameter	Description
`pool`	Name of the NAT pool.
`<start-ipaddr>`	IP address that defines the beginning of the range of source NAT addresses in the pool.
`<end-ipaddr>`	IP address that defines the end of the range of source NAT addresses in the pool.
`<dest-ipaddr>`	Destination NAT IP address.

Usage Guidelines

This command configures a NAT pool which you can reference in a session ACL rule (see "ip access-list session" on page 262).

Example

The following command configures a NAT pool:

```
(host) (config) #ip nat pool 2net 2.1.1.1 2.1.1.125
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	This command requires the PEFNG license.	Config mode on master and local controllers

ip ospf

```
ip ospf area|{authentication message-digest | cost <cost> | dead-interval <seconds> |
hello-interval <seconds> | message-digest-key <keyid> <passwd> | priority <number> |
retransmit-interval <seconds> |transmit-delay <seconds>
```

Description

Configure OSPF on the VLAN interface.

Syntax

Parameter	Description	Range	Default
`area`	Enable OSPF on a specific interface by entering the IP address of the router that will use OSPF.		
`authentication message-digest`	Set the OSPF authentication mode to message digest.		disabled
`cost <cost>`	Set the cost associated with the OSPF traffic on an interface.	1 to 65535	1
`dead-interval <seconds>`	Set the elapse interval (seconds) since the last hello-packet was received from the router. After the interval elapses, the neighboring routers declare the router dead.	1 to 65535 seconds	40
`hello-interval <seconds>`	Set the elapse interval (seconds) between hello packets sent on the interface.	1 to 65535 seconds	10
`message-digest-key <keyid> <passwd>`	Enable OSPF MD5 authentication and set the key identification and a character string password.	<keyid> = 1 to 256	No default
`priority <number>`	Set the priority number of the interface to determine the DR.	0 to 255	1
`retransmit-interval <seconds>`	Set the retransmission time between link state advertisements for adjacencies belonging to the interface. **NOTE:** Set the time interval long enough to prevent unnecessary retransmissions.	1 to 65535 seconds	5
`transmit-delay <seconds>`	Set the elapse time before retransmitting link state update packets on the interface.	1 to 65535 seconds	1

Usage Guidelines

When configuring OSPF over multiple vendors, use this **ip ospf cost** command to ensure that all routers use the same cost. Otherwise, OSPF may route improperly.

Related Commands

Command	Description
show ip ospf	View the OSPF configuration

Command History

Release	Modification
ArubaOS 3.4	Command introduced

Command Information

Platforms	Licensing	Command Mode
All Platforms	Base operating system	Configuration Interface Mode (config-subif)

ip pppoe-max-segment-size

```
ip pppoe-max-segment-size <mss>
```

Description

This command configures the maximum TCP segment size (mss), in bytes, for Point-to-Point Protocol over Ethernet (PPPoE) data.

Syntax

Parameter	Description	Range	Default
<mss>	Enter the keywords **pppoe-max-segment-size** followed by the TCP max segment size (mss) in bytes.	128-1452	1452

Usage Guidelines

The maximum segment size for PPPoE is smaller than the normal Ethernet encapsulation size because of the PPPoE overhead.

Example

The following command configures the PPPoE maximum TCP segment size:

```
(host) (config) #ip pppoe-max-segment-size 1412
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode (config) on master and local controllers

ip pppoe-password

```
ip pppoe-password <password>
```

Description

This command configures the PPP over Ethernet (PPPoE) password.

Syntax

Parameter	Description
<password>	Enter the keyword **ip-pppoe-password** followed by the PAP password configured on the PPPoE Access Concentrator for the controller.

Usage Guidelines

Note the following about enabling the PPPoE client on the controller:

- You cannot enable both the DHCP and PPPoE client on the controller at the same time.
- You can enable the PPPoE client on only one VLAN on the controller (the VLAN cannot be VLAN 1).
- You can connect only one port in the VLAN to the uplink switch.
- At least one interface in the VLAN must be in the up state before the PPPoE client requests an IP address from the server.

Example

The following commands configure the PPPoE client on the controller:

```
(host) (config) #ip pppoe-service-name ppp2056
ip pppoe-username rudolph123
ip pppoe-password 1234567890
vlan 22
interface vlan 22
   ip address pppoe
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode (config) on master or local controllers

ip pppoe-service-name

```
ip pppoe-service-name <service_name>
```

Description

This command configures the PPP over Ethernet (PPPoE) service name.

Syntax

Parameter	Description
<service_name>	Enter the keyword **ip-pppoe-service-name** followed by the PPPoE service name.

Usage Guidelines

Note the following about enabling the PPPoE client on the controller:

- You cannot enable both the DHCP and PPPoE client on the controller at the same time.
- You can enable the PPPoE client on only one VLAN on the controller (the VLAN cannot be VLAN 1).
- You can connect only one port in the VLAN to the uplink switch.
- At least one interface in the VLAN must be in the up state before the PPPoE client requests an IP address from the server.

Example

The following commands configure the PPPoE client on the controller:

```
(host) (config) #ip pppoe-service-name ppp2056
ip pppoe-username rudolph123
ip pppoe-password 1234567890
vlan 22
interface vlan 22
   ip address pppoe
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode (config) on master and local controllers

ip pppoe-username

```
ip pppoe-username <username>
```

Description

This command configures the PPP over Ethernet (PPPoE) username.

Syntax

Parameter	Description
`<username>`	Enter the keywords **ip pppoe-username** followed by the PAP user name configured on the PPPoE Access Concentrator for the controller.

Usage Guidelines

Note the following about enabling the PPPoE client on the controller:

- You cannot enable both the DHCP and PPPoE client on the controller at the same time.
- You can enable the PPPoE client on only one VLAN on the controller (the VLAN cannot be VLAN 1).
- You can connect only one port in the VLAN to the uplink switch.
- At least one interface in the VLAN must be in the up state before the PPPoE client requests an IP address from the server.

Example

The following commands configure the PPPoE client on the controller:

```
(host) (config) #ip pppoe-service-name ppp2056
ip pppoe-username rudolph123
ip pppoe-password 1234567890
vlan 22
interface vlan 22
   ip address pppoe
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode (config) on master and local controllers

ip radius

```
ip radius {nas-ip <ipaddr>|rfc-3576-server udp-port <port>|source-interface
{loopback|vlan <vlan>}
```

Description

This command configures global parameters for configured RADIUS servers.

Syntax

Parameter	Description	Range	Default
`nas-ip`	NAS IP address to send in RADIUS packets. A server-specific NAS IP configured with the **`aaa authentication-server radius`** command supersedes this configuration.	—	—
`rfc-3576-server`	Configures the UDP port to receive requests from a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576, "Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)". See the **aaa rfc-3576-server** command to configure the server. **NOTE:** This parameter can only be used on the master controller.		
`udp-port`	UDP port to receive server requests.	0-65535	3799
`source-interface`	Interface for all outgoing RADIUS packets. The IP address of the specified interface is included in the IP header of RADIUS packets. The interface can be one of the following:		
`loopback`	The loopback interface.	—	—
`vlan`	The specified VLAN.	—	—

Usage Guidelines

This command configures global RADIUS server parameters. If the **aaa authentication-server radius** command configures a server-specific NAS IP, the server-specific IP address is used instead.

Example

The following command configures a global NAS IP address sent in RADIUS packets:

```
(host) (config) #ip radius nas-ip 192.168.1.245
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	The **ip radius rfc-3576-server udp-port** command requires the PEFNG license. Other commands are available in the base operating system.	Config mode on master and local controllers

ip route

```
ip route <destip> <destmask> {<nexthop> [<cost>]|ipsec <name>|null 0}
```

Description

This command configures a static route on the controller.

Syntax

Parameter	Description
`<destip>`	Enter the destination prefix address in dotted decimal format (A.B.C.D).
`<destmask>`	Enter the destination prefix mask address in dotted decimal format (A.B.C.D).
`<nexthop> [<cost>]`	Enter the forwarding router address in dotted decimal format (A.B.C.D). Optionally, enter the distance metric (cost) for this route. The cost prioritizes routing to the destination. The lower the cost, the higher the priority.
`ipsec <name>`	Enter the keyword **ipsec** followed by the ipsec map name to use a static ipsec route map.
`null 0`	Enter the key word **null 0** to designate a null interface.

Usage Guidelines

This command configures a static route on the controller other than the default gateway. Use the **ip default-gateway** command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect the controller.

Example

The following command configures a static route:

```
(host) (config) #ip route 172.16.0.0 255.255.0.0 10.1.1.1
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master and local controllers

ipv6 enable

```
ipv6 enable
```

Description

This command enables IPv6 packet processing globally. This option is disabled by default.

Syntax

No parameters.

Usage Guidelines

This command enables IPv6 packet processing globally.

Command History

This command was introduced in ArubaOS 6.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

ipv6 firewall

```
ipv6 firewall
   attack-rate {ping <number>|session <number>|tcp-syn <number>}
   deny-inter-user-bridging |
   drop-ip-fragments |
   enable |
   enable-per-packet-logging |
   enforce-tcp-handshake |
   prohibit-ip-spoofing |
   prohibit-rst-replay |
   session-idle-timeout <seconds> |
   session-mirror-destination {ip-address <ipaddr>}|{port <slot/<port>}
```

Description

This command configures firewall options on the controller for IPv6 traffic.

Syntax

Parameter	Description	Range	Default
attack-rate	Sets rates which, if exceeded, can indicate a denial of service attack.		
ping	Number of ICMP pings per second, which if exceeded, can indicate a denial of service attack. Recommended value is 4	1-255	—
session	Number of TCP or UDP connection requests per second, which if exceeded, can indicate a denial of service attack. Recommended value is 32.	1-255	—
tcp-syn	Number of TCP SYN messages per second, which if exceeded, can indicate a denial of service attack. Recommended value is 32.	1-255	—
deny-inter-user-bridging	Prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic. This option can be used to prevent Appletalk or IPX traffic from being forwarded.	—	disabled
drop-ip-fragments	When enabled, all IP fragments are dropped. You should not enable this option unless instructed to do so by an Dell representative.	—	disabled
enable	This command enables firewall functions for IPv6 packet forwarding. If IPv6 firewall is not enabled the IPv6 packets are forwarded without session management.	—	disabled
enable-per-packet-logging	Enables logging of every packet if logging is enabled for the corresponding session rule. Normally, one event is logged per session. If you enable this option, each packet in the session is logged. You should not enable this option unless instructed to do so by an Dell representative, as doing so may create unnecessary overhead on the controller.	—	disabled
enforce-tcp-handshake	Prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network.	—	disabled
prohibit-ip-spoofing	Detects IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.	—	disabled
prohibit-rst-replay	Closes a TCP connection in both directions if a TCP RST is received from either direction. You should not enable this option unless instructed to do so by an Dell representative.	—	disabled
session-idle-timeout	Time, in seconds, that a non-TCP session can be idle before it is removed from the session table. You should not modify this option unless instructed to do so by an Dell representative.	16-259	15 seconds
session-mirror-destination	Destination to which mirrored session packets are sent. The destination can be either an IPv4 address or a controller port. You configure IPv6 flows to be mirrored with the **mirror** option of the **ipv6 access-list session** command. Use this option only for troubleshooting or debugging.	—	—
ip-address <ipaddr>	Send mirrored session packets to the specified IP address		
port <slot>/<port>	Send mirrored session packets to the specified controller port.		

Usage Guidelines

This command configures global firewall options on the controller for IPv6 traffic.

Example

The following command disallows forwarding of non-IP frames between IPv6 clients:

```
(host) (config) #ipv6 firewall deny-inter-user-bridging
```

Command History

Introduced in ArubaOS 3.3

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system, except for noted parameters	Config mode on master controllers

lacp group

```
lacp group <group_number> mode {active | passive}
lacp
```

Description

Enable Link Aggregation Control Protocol (LACP) and configure LACP on the interface.

Syntax

Parameter	Description
`<group_number>`	Enter the link aggregation group (LAG) number. Range: 0-7
`mode {active | passive}`	Enter the keyword **mode** followed by either the keyword **active** or **passive**. • Active mode—the interface is in active negotiating state. LACP runs on any link that is configured to be in the active state. The port in an active mode also automatically initiates negotiations with other ports by initiating LACP packets. • Passive mode—the interface is *not* in an active negotiating state. LACP runs on any link that is configured in a passive state. The port in a passive mode responds to negotiations requests from other ports that are in an active state. Ports in passive state respond to LACP packets.

Usage Guidelines

LACP is disabled by default; this command enables LACP. If the group number assigned contains static port members, the command is rejected.

Related Command

Command	Description
`show lacp`	View the LACP configuration status
`show lacp sys-id`	View the LACP system ID information
`show interface port-channel`	View information on a specified port channel interface

Command History

Release	Modification
ArubaOS 3.4.1	Command introduced

Command Information

Platform	Licensing	Command Mode
All Platforms	Base operating system	Configuration Interface Mode (config-if) for Master and Local controllers

lacp port-priority

```
lacp port-priority <priority_value>
```

Description

Configure the LACP port priority.

Syntax

Parameter	Description
`<priority_value>`	Enter the port-priority value. The higher the value number the lower the priority. Range: 1 to 65535 Default: 255

Usage Guidelines

Set the port priority for LACP.

Related Command

Command	Description
`lacp group`	Enable LACP and configure on the interface
`lacp system-priority`	Set the LACP system priority
`show lacp`	View the LACP configuration status
`show lacp sys-id`	View the LACP system ID information
`show interface port-channel`	View information on a specified port channel interface

Command History

Release	Modification
ArubaOS 3.4.1	Command introduced

Command Information

Platform	Licensing	Command Mode
All Platforms	Base operating system	Configuration Interface Mode (config-if) for Master and Local controllers

lacp system-priority

```
lacp system-priority <priority_value>
```

Description

Configure the LACP system priority.

Syntax

Parameter	Description
<priority_value>	Enter the system priority value. The higher the value number the lower the priority. Range: 1 to 65535 Default: 32768

Usage Guidelines

Set the LACP system priority.

Related Command

Command	Description
lacp group	Enable LACP and configure on the interface
lacp port-priority	Set the LACP port priority
show lacp	View the LACP configuration status
show lacp sys-id	View the LACP system ID information
show interface port-channel	View information on a specified port channel interface

Command History

Release	Modification
ArubaOS 3.4.1	Command introduced

Command Information

Platforms	Licensing	Command Mode
All Platforms	Base operating system	Configuration Mode (config) for Master and Local controllers

lacp timeout

```
lacp timeout {long | short}
```

Description

Configure the timeout period for the LACP session.

Syntax

Parameter	Description
`long`	Enter the keyword **long** to set the LACP session to 90 seconds. This is the default.
`short`	Enter the keyword **short** to set the LACP session to 3 seconds.

Usage Guidelines

The timeout value is the amount of time that a port-channel interface waits for a LACPDU (Link Aggregation Control Protocol data unit) from the remote system before terminating the LACP session. The default time out value is 90 seconds (long).

Related Command

Command	Description
`lacp group`	Enable LACP and configure on the interface
`show lacp`	View the LACP configuration status
`show lacp sys-id`	View the LACP system ID information
`show interface port-channel`	View information on a specified port channel interface

Command History

Release	Modification
ArubaOS 3.4.1	Command introduced

Command Information

Platforms	Licensing	Command Mode
All Platforms	Base operating system	Configuration Interface Mode (config-if) for Master and Local controllers

license

```
license {add <key>|del <key>|export <filename>|import <filename>|report <filename>}
```

Description

This command allows you to install, delete, and manage software licenses on the controller.

Syntax

Parameter	Description
`add`	Installs the software license key in the controller. The key is normally sent to you via email.
`del`	Removes the software license key from the controller. The key is normally sent to you via email.
`export`	Exports the license database on the controller to the specified file in flash.
`import`	Replaces the license database on the controller with the specified file in flash. The system serial numbers referenced in the imported file must match the numbers on the controller.
`report`	Saves a license report to the specified file in flash.

Usage Guidelines

Obtain an Dell software license certificate from your Dell sales representative or authorized reseller. Use the certificate ID and the system serial number to obtain a software license key which you install in the controller.

Note: Users that are not very familiar with this procedure may wish to use the License Management page in the WebUI to install and manage licenses on the controller.

Example

The following command adds a license key on the controller:

```
license add 890BobXs-cVPCb3aJ-7FbCijhZ-BuQPtuI4-RjLJW6Pl-n5K
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on master and local controllers

localip

```
localip <ipaddr> ipsec <key>
```

Description

This command configures the IP address and preshared key for the local controller on a master controller.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the local controller. Use the 0.0.0.0 address to configure a global preshared key for all inter-controller communications.
`ipsec`	Preshared key, which must be between 6-64 characters.

Usage Guidelines

Use this command on a master controller to configure the IP address and preshared key for communication with a local controller. On the local controller, use the **masterip** command to configure the IP address and preshared key for the master controller.

Example

The following command configures the local controller on a master controller:

```
(host) (config) #localip 0.0.0.0 ipsec gw1234xyz
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

local-userdb add

```
localuserdb
local-userdb add {generate-username|username <name>} {generate-password|password
<passwd>} [comment <g_comments>][email <email>] [expiry {duration <minutes>|time <hh/
mm/yyy> <hh:mm>}] [guest-company <g_company>][guest-fullname <g_fullname>][guest-phone
<g-phone>][mode disable][opt-field-1 <opt1>][opt-field-2 <opt2>][opt-field-3
<opt3>][opt-field-4 <opt4>][role <role>][sponsor-dept <sp_dept>][sponsor-mail
<sp_email>][sponsor-fullname <sp_fullname>][sponsor-name <sp_name>]
[start-time <mm/dd/yyyy> <hh.mm>]
```

Description

This command creates a user account entry in the controller's internal database.

Syntax

Parameter	Description	Range	Default
`generate-username`	Automatically generate and add a username.	—	—
`username`	Add the specified username.	1 – 64 characters	—
`generate-password`	Automatically generate a password for the username.	—	—
`password`	Add the specified password for the username.	6 – 128 characters	—
`comments`	Comments added to the user account.	—	—
`email`	Email address for the user account.	—	—
`expiry`	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
`duration`	Duration, in minutes, for the user account.	1-2147483647	—
`time`	Date and time, in mm/dd/yyy and hh:mm format, that the user account expires.	—	—
`guest-company`	Name of the guest's company. **NOTE:** A guest is the person who needs guest access to the company's Dell wireless network.		
`guest-fullname`	The guest's full name.		
`guest-phone`	The guest's phone number.		
`mode`	Enables or disables the user account,	—	Disable
`opt-field-1`	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.	—	—
`opt-field-2`	Same as `opt-field-1`.	—	—
`opt-field-3`	Same as `opt-field-1`.	—	—
`opt-field-4`	Same as `opt-field-1`.	—	—
`role`	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.	—	guest
`sponsor-dept`	The guest sponsor's department name **NOTE:** A sponsor is the guest's primary contact for the visit.	—	—
`sponsor-email`	The sponsor's email address.	—	—
`sponsor-fullname`	The sponsor's full name.	—	—
`sponsor-name`	The sponsor's name.	—	—
`start-time`	Date and time, in mm/dd/yyy and hh:mm format, the guest account begins.	—	—

Usage Guidelines

When you specify the internal database as an authentication server, client information is checked against the user

accounts in the internal database. You can modify an existing user account in the internal database with the **local-userdb modify** command, or delete an account with the **local-userdb del** command.

By default, the internal database in the master controller is used for authentication. Issue the **aaa authentication-server internal use-local-switch** command to use the internal database in a local controller; you then need to add user accounts to the internal database in the local controller.

Example

The following command adds a user account in the internal database with an automatically-generated username and password:

```
(host) #local-userdb add generate-username generate-password expiry duration 480
```

The following information is displayed when you enter the command:

```
GuestConnect
Username: guest4157
Password: cDFD1675
Expiration: 480 minutes
```

Related Commands

Command	Description	Mode
show local-userdb	Use **this command** to show the parameters displayed in the output of this command.	Enable and Config modes
show local-userdb-guest	Use **this command** to show the parameters displayed in the output of the **local-userdb-guest add command.**	Enable and Config modes
mgmt-user	Use the **webui-cacert <certificate name>** command if you want an external authentication server to derive the management user role. This is helpful if there are a large number of users who need to be authenticated. Use the **mgmt-user webui-cacert <certificate_name> serial <number> <username> <role>** command if you want the authentication process to use previously configured certificate name and serial number to derive the user role.	Config mode

Command History

Version	Modification
ArubaOS 3.0	Introduced for the first time.
ArubaOS 3.4	The **guest, sponsor and optional field** parameters were added.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system. The **role** parameter requires the PEFNG license.	Enable mode on master controllers.

local-userdb del

```
local-userdb {del username <name>|del-all}
```

Description

This command deletes entries in the controller's internal database.

Syntax

Parameter	Description
`del username`	Deletes the user account for the specified username.
`del-all`	Deletes all entries in the internal database.

Usage Guidelines

User account entries created with expirations are automatically deleted from the internal database at the specified expiration. Use this command to delete an entry before its expiration or to delete an entry that was created without an expiration.

Example

The following command deletes a specific user account entry:

```
(host)#local-userdb del username guest4157
```

Command History

Introduced in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on master controllers.

local-userdb export

```
local-userdb export <filename>
```

Description

This command exports the internal database to a file.

Caution: Use this command with caution. It replaces the existing users with user entries from the imported file.

Syntax

Parameter	Description
`export`	Saves the internal database to the specified file in flash.

Usage Guidelines

After using this command, you can use the **copy** command to transfer the file from flash to another location.

Example

The following command saves the internal database to a file:

```
(host)#local-userdb export jan-userdb
```

Command History

Introduced in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on master controllers.

local-userdb fix-database

```
local-userdb fix-database
```

Description

This command deletes and reinitializes the internal database.

Syntax

No parameters.

Usage Guidelines

Before using this command, you can save the internal database with the **local-userdb export** command.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on master controllers.

local-userdb import

```
local-userdb import <filename>
```

Description

This command replaces the internal database with the specified file from flash.

Syntax

Parameter	Description
`import`	Replaces the internal database with the specified file.

Usage Guidelines

This command replaces the contents of the internal database with the contents in the specified file. The file must be a valid internal database file saved with the **`local-userdb export`** command.

Example

The following command imports the specified file into the internal database:

```
(host)#local-userdb import jan-userdb
```

Command History

Introduced in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on master controllers.

local-userdb maximum-expiration

```
local-userdb maximum-expiration <minutes>
```

Description

This command configures the maximum time, in minutes, that a guest account in the internal database can remain valid.

Syntax

Parameter	Description	Range
`maximum-expiration`	Maximum time, in minutes, that a guest account in the internal database can remain valid.	1-2147483647

Usage Guidelines

The user in the guest-provisioning role cannot create guest accounts that expire beyond the configured maximum time. This command is not available to the user in the guest-provisioning role.

Example

The following command sets the maximum time for guest accounts in the internal database to 8 hours (480 minutes):

```
(host)#local-userdb maximum-expiration 480
```

Command History

Introduced in ArubaOS 3.0.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Configuration mode on master controllers.

local-userdb modify

```
local-userdb modify username <name> [comments <g_comments>][email <email>] [expiry
{duration <minutes>|time <hh/mm/yyy> <hh:mm>}] [guest-company <g_company>][guest-
fullname <g_fullname>][guest-phone <g-phone>][mode disable][opt-field-1 <opt1>][opt-
field-2 <opt2>][opt-field-3 <opt3>][opt-field-4 <opt4>][role <role>][sponsor-dept
<sp_dept>][sponsor-mail <sp_email>][sponsor-fullname <sp_fullname>][sponsor-name
<sp_name>][start-time <mm/dd/yyyy> <hh.mm>]
```

Description

This command modifies an existing user account entry in the controller's internal database.

Syntax

Parameter	Description	Range	Default
`username`	Name of the existing user account entry.	1 – 64 characters	—
`comments`	Comments added to the user account.	—	—
`email`	Email address for the use account.	—	—
`expiry`	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
`duration`	Duration, in minutes, for the user account.	1-2147483647	—
`time`	Date and time, in mm/dd/yyy and hh:mm format, that the user account expires.	—	—
`guest-company`	Name of the guest's company. **NOTE:** A guest is the person who needs guest access to the company's Dell wireless network.		
`guest-fullname`	The guest's full name.		
`guest-phone`	The guest's phone number.		
`mode`	Enables or disables the user account,	—	Disable
`opt-field-1`	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.	—	—
`opt-field-2`	Same as `opt-field-1`.	—	—
`opt-field-3`	Same as `opt-field-1`.	—	—
`opt-field-4`	Same as `opt-field-1`.	—	—
`role`	Role for the user. This parameter requires the PEFNG license.	—	guest
`sponsor-dept`	The guest sponsor's department name **NOTE:** A sponsor is the guest's primary contact for the visit.	—	—
`sponsor-email`	The sponsor's email address.	—	—
`sponsor-fullname`	The sponsor's full name.	—	—
`sponsor-name`	The sponsor's name.	—	—
`start-time`	Date and time, in mm/dd/yyy and hh:mm format, the guest account begins.	—	—

Usage Guidelines

Use the **show local-userdb** command to view the current user account entries in the internal database.

Example

The following command disables an existing user account in the internal database:

```
(host)# local-userdb modify username guest4157 mode disable
```

Command History

Version	Modification
ArubaOS 3.0	Introduced for the first time.
ArubaOS 3.4	The guest, sponsor and optional parameters were added.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on master controllers.

local-userdb send-to-guest

```
local-userdb send-to-guest
```

Description

This command automatically sends email to the guest when the guest user is created.

Syntax

No parameters.

Usage Guidelines

A guest is the person who needs guest access to the company's Dell wireless network. Email is sent directly to the guest after the guest user is created. When configuring the guest provisioning feature, the guest user is generally created by Guest Provisioning user. This is the person who is responsible for signing in guests at your company.

Example

```
(host)(config) #local-userdb send-to-guest
```

Command History

Introduced in ArubaOS 3.4.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Configuration mode on master controllers.

local-userdb send-to-sponsor

```
local-userdb send-to-sponsor
```

Description

This command automatically sends email to the guest's sponsor when the guest user is created.

Syntax

No parameters.

Usage Guidelines

The sponsor is the guest's primary contact. Email is sent directly to the guest's sponsor after the guest user is created. When configuring the guest provisioning feature, the sponsor is generally created by the Guest Provisioning user. This is the person who responsible for signing in guests at your company.

Example

```
(host)(config)#local-userdb send-to-sponsor
```

Command History

Introduced in ArubaOS 3.4.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Configuration mode on master controllers.

local-userdb-guest add

```
local-userdb-guest
local-userdb-guest add {generate-username|username <name>} {generate-password|password
<passwd>} [comment <g_comments>][email <email>] [expiry {duration <minutes>|time <hh/
mm/yyy> <hh:mm>}] [guest-company <g_company>][guest-fullname <g_fullname>][guest-phone
<g-phone>][mode disable][opt-field-1 <opt1>][opt-field-2 <opt2>][opt-field-3
<opt3>][opt-field-4 <opt4>][sponsor-dept <sp_dept>][sponsor-mail <sp_email>][sponsor-
fullname <sp_fullname>][sponsor-name <sp_name>]
[start-time <mm/dd/yyyy> <hh.mm>]
```

Description

This command creates a guest user in a local user database.

Syntax

Parameter	Description	Range	Default
`generate-username`	Automatically generate and add a guest username.	—	—
`username`	Add the specified guest username.	1 – 64 characters	—
`generate-password`	Automatically generate a password for the username.	—	—
`password`	Add the specified password for the username.	6 – 128 characters	—
`comments`	Comments added to the guest user account.	—	—
`email`	Email address for the guest user account.	—	—
`expiry`	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
`duration`	Duration, in minutes, for the user account.	1-2147483647	—
`time`	Date and time, in mm/dd/yyy and hh:mm format, that the user account expires.	—	—
`guest-company`	Name of the guest's company. **NOTE:** A guest is the person who needs guest access to the company's Dell wireless network.		
`guest-fullname`	The guest's full name.		
`guest-phone`	The guest's phone number.		
`mode`	Enables or disables the user account,	—	Disable
`opt-field-1`	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.	—	—
`opt-field-2`	Same as `opt-field-1`.	—	—
`opt-field-3`	Same as `opt-field-1`.	—	—
`opt-field-4`	Same as `opt-field-1`.	—	—
`sponsor-dept`	The guest sponsor's department name. **NOTE:** A sponsor is the guest's primary contact for the visit.	—	—
`sponsor-email`	The sponsor's email address.	—	—
`sponsor-fullname`	The sponsor's full name.	—	—
`sponsor-name`	The sponsor's name.	—	—
`start-time`	Date and time, in mm/dd/yyy and hh:mm format, the guest account begins.	—	—

Usage Guidelines

When you specify the internal database as an authentication server, client information is checked against the user accounts in the internal database. You can modify an existing user account in the internal database with the **local-userdb-guest modify** command, or delete an account with the **local-userdb-guest del** command.

By default, the internal database in the master controller is used for authentication. Issue the **aaa authentication-server internal use-local-switch** command to use the internal database in a local controller; you then need to add user accounts to the internal database in the local controller.

Example

The following command adds a guest user in the internal database with an automatically-generated username and password:

```
(host) #local-userdb-guest add generate-username generate-password expiry none
```

The following information is displayed when you enter the command:

```
GuestConnect
Username: guest-5433352
Password: mBgJ6764
Expiration: none
```

Related Commands

Command	Description	Mode
`show local-userdb-guest`	Use **`this command`** to show the parameters displayed in the output of this **`command.`**	Enable and Config modes
`show local-userdb`	Use **`this command`** to show the parameters displayed in the **`local-userdb`** command.	Enable and Config modes

Command History

Introduced in ArubaOS 3.4.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system. The **`role`** parameter requires the PEFNG license.	Enable and config modes on master controllers.

local-userdb-guest del

```
local-userdb-guest {del username <name>|del-all}
```

Description

This command deletes entries in the controller's internal database.

Syntax

Parameter	Description
`del username`	Deletes the user account for the specified username.
`del-all`	Deletes all entries in the internal database.

Usage Guidelines

User account entries created with expirations are automatically deleted from the internal database at the specified expiration. Use this command to delete an entry before its expiration or to delete an entry that was created without an expiration.

Example

The following command deletes a specific user account entry:

```
(host) #local-userdb-guest del username guest4157
```

Command History

Introduced in ArubaOS 3.4.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable and config modes on master controllers.

local-userdb-guest modify

```
local-userd-guest modify username <name> [comments <g_comments>][email <email>] [expiry
{duration <minutes>|time <hh/mm/yyy> <hh:mm>}] [guest-company <g_company>][guest-
fullname <g_fullname>][guest-phone <g-phone>][mode disable][opt-field-1 <opt1>][opt-
field-2 <opt2>][opt-field-3 <opt3>][opt-field-4 <opt4>][password <passwd][sponsor-dept
<sp_dept>][sponsor-mail <sp_email>][sponsor-fullname <sp_fullname>][sponsor-name
<sp_name>][start-time <mm/dd/yyyy> <hh.mm>]
```

Description

This command modifies an existing guest user entry in the controller's internal database.

Syntax

Parameter	Description	Range	Default
`username`	Name of the existing user account entry.	1 – 64 characters	—
`comments`	Comments added to the user account.	—	—
`email`	Email address for the use account.	—	—
`expiry`	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
`duration`	Duration, in minutes, for the user account.	1-2147483647	—
`time`	Date and time, in mm/dd/yyy and hh:mm format, that the user account expires.	—	—
`guest-company`	Name of the guest's company. **NOTE:** A guest is the person who needs guest access to the company's Dell wireless network.		
`guest-fullname`	The guest's full name.		
`guest-phone`	The guest's phone number.		
`mode`	Enables or disables the user account,	—	Disable
`opt-field-1`	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.	—	—
`opt-field-2`	Same as `opt-field-1`.	—	—
`opt-field-3`	Same as `opt-field-1`.	—	—
`opt-field-4`	Same as `opt-field-1`.	—	—
`password`	User's password	1– 6 characters	—
`sponsor-dept`	The guest sponsor's department name **NOTE:** A sponsor is the guest's primary contact for the visit.	—	—
`sponsor-email`	The sponsor's email address.	—	—
`sponsor-fullname`	The sponsor's full name.	—	—
`sponsor-name`	The sponsor's name.	—	—
`start-time`	Date and time, in mm/dd/yyy and hh:mm format, the guest account begins.	—	—

Usage Guidelines

Use the **show local-userdb-guest** command to view the current user account entries in the internal database.

Example

The following command disables an guest user account in the internal database:

```
(host)local-userdb-guest modify username guest4157 mode disable
```

Command History

Introduced in ArubaOS 3.4.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable and config modes on master controllers.

local-userdb-guest send-email

```
local-userdb-guest send-email <username> [to-guest][to-sponsor]
```

Description

This command causes the controller to send email to the guest and/or sponsor any time a guest user is created.

Syntax

Parameter	Description	Range	Default
`<username>`	Name of the guest	1 – 64 characters	—
`to-guest`	Allows you to send email to the guest user's address.	—	—
`to-sponsor`	Allows you to send email to the sponsor's email address.	—	—

Usage Guidelines

This command allows the guest provisioning user or network administrator to causes the controller to send email to the guest and/or sponsor any time a guest user is created.

Example

The following command causes the controller to send an email to the sponsor alerting them that the guest user "Laura" was just created.

```
(host)# local-userdb-guest send-email Laura to-sponsor
```

Command History

Introduced in ArubaOS 3.4.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on master controllers

local-userdb-remote-node

```
localuserdb
local-userdb-remote-node add mac-address <mac-address> remote-node-profile
<remote-node-profile>
   del mac-address <mac-address>
```

Description

This command adds a Remote Node to the Remote Node whitelist. You can also delete the whitelist entry using this command.

Syntax

Parameter	Description	Range	Default
`mac-address <mac-address>`	MAC address of the Remote Node in colon-separated six-octet format.	—	—
`remote-node-profile <remote-node-profile>`	The Remote Node configuration profile to be assigned to that Remote Node.	1 – 64 characters	—

Usage Guidelines

A Remote Node-master can only assign a configuration profile to a Remote Node in its Remote Node whitelist. To assign a different configuration to an unprovisioned Remote Node, you must delete the whitelist entry and create a new Remote Node whitelist entry with the correct Remote Node configuration profile. A remote-node profile has to be validated before it is configured and pushed to a Remote Node.

Example

This example adds the Remote Node profile named Location-1 to the Remote Node whitelist.

```
(remote-node-master) #local-userdb-remote-node add mac-address 00:16:CF:AF:3E:E1
remote-node-profile Location_1
```

This example removes a Remote Node from the Remote Node whitelist.

(remote-node-master)(config) #local-userdb-remote-node del mac-address 00:16:CF:AF:3E:E1

Related Commands

Command	Description	Mode
remote-node-localip	Configures security for all Remote Node and Remote Controller control traffic	Config modes
remote-node-masterip	Configures security for the Remote Node master IP address.	Config mode
remote-node-profile	The remote-node-profile command lets you create a Remote Node profile.	Config mode
show remote-node	Shows Remote Node configuration, dhcp instance, license usage and running configuration information.	Enable and Config mode
show remote-node-dhcp-pool	Shows Remote Node dhcp pool configuration information.	Enable and Config mode
show remote-node-profile	Shows Remote Node profile status information.	Enable and Config mode
show local-userdb-remote-node	The output of this command lists the MAC address and assigned Remote Node-profile for of each Remote Node associated with that Remote Node master.	Enable and Config mode

Command History

Version	Modification
ArubaOS 6.0	Introduced for the first time.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Enable mode on master controllers.

location

```
location <string>
```

Description

This command configures the location of the controller.

Syntax

Parameter	Description
`location`	A text string that specifies the system location.

Usage Guidelines

Use this command to indicate the location of the controller. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the text string.

To change the existing name, enter the command with a different string. To unconfigure the location, enter `“”` at the prompt.

Example

The following command configures the location:

```
(host) (config) #location “Building 10, second floor, room 21E”
```

Command History

Introduced in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

logging

```
logging <ipaddr>
   [facility] |
   [severity] |
   [type>]
```

Description

Use this command to specify the IP address of the remote logging server, facility, severity, and the type.

Syntax

Parameter	Description	Range	Default
`facility`	To set the remote logging server facility.	local 0 to local7	—
`severity`	To set the remote logging server severity.	—	—
`type`	To set the remote logging server message type.	—	—

Usage Guidelines

The local use facilities (local0, local1, local2, local3, local4, local5, local6, and local7) are not reserved for specific message-generating sources, and can be used for sending syslog messages. Use the `show logging` command to verify that the device sends logging messages.

Example

The following command adds the remote logging server with the IP address 10.1.2.3 with a user log type using local4.

```
(host) (config) #logging 1.1.1.1 user facility local4
```

Command History

Introduced in ArubaOS 6.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

logging facility

```
logging facility <facility>
```

Description

Use this command to set the facility to use when logging to the remote syslog server.

Syntax

Parameter	Description	Range
`<facility>`	The facility to use when logging to a remote syslog server.	local0 to local7

Usage Guidelines

The local use facilities (local0, local1, local2, local3, local4, local5, local6, and local7) are not reserved for specific message-generating sources, and can be used for sending syslog messages.

Example

The following command sets the facility to `local4`.

```
(host) (config) #logging facility local4
```

Command History

Introduced in ArubaOS 2.5

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

logging level

```
logging level <level> <category> [process <process>] [subcat <subcategory>]
```

Description

Use this command to set the categories or subcategories and the severity levels of messages that are logged.

Syntax

Parameter	Description
<level>	The message severity level, which can be one of the following (in order of severity level):
emergencies	(0) Panic conditions that occur when the system becomes unstable.
alerts	(1) Any condition requiring immediate attention and correction.
critical	(2) Any critical conditions, such as hard drive errors.
errors	(3) Error conditions.
warnings	(4) Warning messages.
notifications	(5) Significant events of a non-critical and normal nature.
informational	(6) Messages of general interest to system users.
debugging	(7) Messages containing information for debugging purposes.
<category>	Message category, which can be one of the following:
ap-debug	AP troubleshooting messages. You must specify a debug value.
network	Network messages.
security	Security messages.
system	System messages.
user	User messages.
user-debug	User troubleshooting messages. You must specify a MAC address.
wireless	Wireless messages.
process	Controller process, which can be one of the following:
aaa	AAA logging
ads	Anomaly detection
approc	AP processes
authmgr	User authentication
cfgm	Configuration Manager
crypto	VPN (IKE/IPsec)
cts	Transport service
dbsync	Database synchronization
dhcpd	DHCP packets
esi	External Services Interface
fpapps	Layer 2 and 3 control
httpd	Apache
l2tp	L2TP
licensemgr	License manager
localdb	Local database
mobileip	Mobile IP

Parameter	Description
packetfilter	Packet filtering of messaging and control frames
pim	Protocol Independent Multicast
pppoed	PPPoE
pptp	PPTP
processes	Run-time processes
profmgr	Profile Manager
publisher	Publish subscribe service
rfm	RF Troubleshooting Manager
snmp	SNMP
stm	Station management
syslogdwrap	Syslogd wrap
traffic	Traffic
vrrpd	VRRP
wms	Wireless management (master controller only)
subcat	Message subcategory, which depends upon the message category specified. The following lists the subcategories available for each message category: • ap-debug: all • network: all, dhcp, mobility, packet-dump • security: aaa, all, dot1x, firewall, ike, mobility, packet-trace, vpn, webserver • system: all, configuration, messages, snmp, webserver • user: all, captive-portal, dot1x, radius, vpn • user-debug: all, configuration • wireless: all

Usage Guidelines

There are eight logging severity levels, each with its associated types of messages. Each level also includes the levels below it. For example, if you set the logging level to informational (6), all messages from level 0 through level 5 (from emergencies through notifications) are also logged. The warnings severity level is set by default for all message categories and subcategories.

Example

The following command logs critical system messages.

```
logging level critical system
```

Command History

Introduced in ArubaOS 2.5

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master and local controllers

loginsession

```
loginsession timeout <minutes>
```

Description

This command configures the time management session (via Telnet or SSH) remains active without 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	15 minutes

Usage Guidelines

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

Note: The TCP session timeout for wireless and wired user sessions through the controller is 15 minutes; this timeout for user sessions is not configurable.

Example

The following command configures management sessions on the controller to not time out:

```
(host) (config) #loginsession timeout 0
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config mode on master controllers

logout

```
logout
```

Description

This command exits the current CLI session.

Syntax

No parameters.

Usage Guidelines

Use this command to leave the current CLI session and return to the user login.

Example

The following command exits the CLI session:

```
(host) >logout
User:
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	User mode on local or master controllers

mac-address-table

```
mac-address-table static <macaddr> {fastethernet|gigabitethernet} <slot>/<port> vlan
<vlan>
```

Description

This command adds a static entry to the MAC address table.

Syntax

Parameter	Description	Range
<macaddr>	Media Access Control (MAC) address, in the format xx:xx:xx:xx:xx:xx.	—
<slot>	<slot> is always 1.	—
<port>	Number assigned to the network interface embedded in the controller. Port numbers start at 0 from the left-most position.	
vlan	ID number of the VLAN.	1-4094

Usage Guidelines

The MAC address table is used to forward traffic between ports on the controller. The table includes addresses learned by the controller. This command allows you to manually enter static addresses that are bound to specific ports and VLANs.

Example

The following command configures a MAC address table entry:

```
(host) (config) #mac-address-table static 00:0b:86:f0:05:60 fastethernet 1/12 vlan 22
```

Command History

Available in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master and local controllers

masterip

```
masterip <ipaddr> ipsec <key> [fqdn <fqdn>][uplink][vlan <id>]
```

Description

This command configures the IP address and preshared key for the master controller on a local controller.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the master controller.
`ipsec <key>`	Preshared key, which must be between 6-64 characters.
`fqdn <fqdn>`	The local controller's Fully Qualified Domain Name (FQDN) used in IKE.
`uplink`	Use the current active uplink to initiate IKE.
`vlan <id>`	VLAN interface to initiate IKE. The controller IP address will be used if the VLAN is not specified.

Usage Guidelines

Use this command on a local controller to configure the IP address and preshared key for communication with the master controller. On the master controller, use the **localip** command to configure the IP address and preshared key for a local controller.

Note: Changing the IP address of the master on a local controller requires a reboot of the local controller

Example

The following command configures the master controller on a local controller:

```
(host) (config) #masterip 10.1.1.250 ipsec gw1234567
```

Command History

Available in ArubaOS 3.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Available in Config mode on master and local controllers

master-redundancy

```
master-redundancy
   master-vrrp <id>
   no ...
   peer-ip-address <ipaddr> ipsec <key>
```

Description

This command associates a VRRP instance with master controller redundancy.

Syntax

Parameter	Description	Range
`master-vrrp`	The virtual router ID for the VRRP instance configured with the **vrrp** command.	1-255
`no`	Negates any configured parameter.	—
`peer-ip-address`	IP address of the peer controller for master redundancy.	—
`ipsec`	Preshared key used to secure communications between the master controllers. Specify a key of up to 64 bytes in length.	—

Usage Guidelines

To maintain a highly redundant network, you can use a controller as a standby for the master controller. The underlying protocol used is VRRP which you configure using the **vrrp** command.

Example

The following command configures VRRP for the initially preferred master controller:

```
(host) (config) #vrrp 22
   vlan 22
   ip address 10.200.22.254
   priority 110
   preempt
   description Preferred-Master
   tracking master-up-time 30 add 20
   no shutdown
master-redundancy
   master-vrrp 22
   peer-ip-address 192.168.2.1 ipsec qwerTY012
```

The following shows the corresponding VRRP configuration for the peer controller.

```
(host) (config) #vrrp 22
   vlan 22
   ip address 10.200.22.254
   priority 100
   preempt
   description Backup-Master
   tracking master-up-time 30 add 20
   no shutdown
master-redundancy
   master-vrrp 22
peer-ip-address 192.168.22.1 ipsec qwerTY012
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

mgmt-server

```
wlan
mgmt-server type {amp|other} primary-server <ip-addr> secondary-server <ip-addr>
```

Description

Register a management server with the controller by specifying the IP address of an AirWave Management Server or any other server that should receive messages from the controller using the Application Monitoring (AMON) protocol.

Syntax

Parameter	Description
`amp`	Define an AirWave Management Server.
`other`	Define any other type of management server.
`primary-server <ip-addr>`	IP address of the primary management server.
`secondary-server <ip-addr>`	IP address of the secondary management server.

Example

The following command defines a primary and secondary Airwave Management server.

```
(host) (config) #mgmt-server type amp primary-server 192.168.6.2 secondary-server 192.168.14.38
```

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on master controllers

mgmt-user

```
mgmt-user <username> <role> <password>
mgmt-user localauth-disable
mgmt-user ssh-pubkey client-cert <certificate> <username> <role>
mgmt-user webui-cacert <certificate_name> serial <number> <username> <role>
```

Description

This command configures an administrative user.

Syntax

Parameter	Description	Default
<username>	Name of the user. You can create a maximum of 10 management users. **NOTE:** If you configure a root management user, you can use special characters except for double-byte characters.	—
<role>	Role assigned to the user. Predefined roles include: • guest-provisioning: Allows the user to create guest accounts on a special WebUI page. • location-api-mgmt: Permits access to location API information. You can log into the CLI; however, you cannot use any CLI commands. • network-operations: Permits access to Monitoring, Reports, and Events pages in the WebUI. You can log into the CLI; however, you can only use a subset of CLI commands to monitor the controller. • read-only: Permits access to CLI show commands or WebUI monitoring pages only. • root: Permits access to all management functions on the controller.	—
<password>	**NOTE:** You are prompted for the <password> for this user after you type in <role> and press Enter. The password must have a minimum of six characters. You can use special characters in the management user password. The restrictions are as follows: • You cannot use double-byte characters • You cannot use the question mark (?) • You cannot use white space <space >	—
localauth-disable	Disables authentication of management users based on the results returned by the authentication server. To cancel this setting, use the no form of the command: **no mgmt-user localauth-disable** To verify if authentication of local management user accounts is enabled or disabled, use the following command: show mgmt-user local-authentication-mode	Enabled
ssh-pubkey	Configures certificate authentication of administrative users using the CLI through SSH.	—
client-cert	Name of the X.509 client certificate for authenticating administrative users using SSH.	—
<username>	Name of the user.	—
<role>	Role assigned to the authenticated user.	—
webui-cacert	The client certificate for authenticating administrative users using the WebUI.	—
<certificate_name>	The CA certificate. If configured, certificate authentication and authorization are automatically completed using an authentication server.	—
serial	Serial number of the client certificate.	—
<username>	Name of the user.	—
<role>	Role assigned to the authenticated user.	—

Usage Guidelines

You can configure client certificate authentication of WebUI or SSH management users (by default, only username/password is used). To configure certificate authentication for the WebUI or SSH, use the web-server mgmt-auth certificate or ssh mgmt-auth public-key commands, respectively.

Use **webui-cacert <certificate name>** command if you want an external authentication server to derive the management user role. This is helpful if there are a large number of users who need to be authenticated.

Or, use the if the **mgmt-user webui-cacert <certificate_name> serial <number> <username> <role>** if you want the authentication process to use previously configured certificate name and serial number to derive the user role.

Example

See the web-server and ssh command descriptions for examples of certificate and public key authentication. The following command configures a management user and role:

```
(host) (config) #mgmt-user kgreen root
Password: *****
Re-Type password: *****
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.1	The **ssh-pubkey** and **webui-cacert** parameters were introduced.
ArubaOS 3.2	The **network-operations** role was introduced.
ArubaOS 3.3	The **location-api-mgmt** role and **localauth-disable** parameters were introduced.
ArubaOS 3.4	The **webui-cacert <certificate name>** parameter had additional functionality introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

mobility-manager

```
mobility-manager <ipaddr> user <username> <password> [interval <secs>]
[retrycount <number>] [udp-port <port>] [rtls <rtls-udp-port>] trap-version {1|2c|3}
```

Description

This command allows the controller to communicate with an Mobility Manager server.

Syntax

Parameter	Description	Range	Default
`<ipaddr>`	IP address of the Mobility Manager server.	—	—
`user`	Name and SNMP password for the Mobility Manager server user.	—	—
`interval`	Round-trip time, in seconds, to trap server.	1-65535	60 seconds
`retrycount`	Number of retries to the Mobility Manager server before giving up.	1-65535	3
`udp-port`	UDP port number for trap server.	0-65535	162
`rtls`	UDP port number on which RSSI location data should be received from APs.	0-65535	8000
`trap-version`	Allows the you to specify the SNMP trap version by the remote trap receiver.	1, 2c, or 3	3

Usage Guidelines

This command needs to be configured before the controller can communicate with the Mobility Manager server. This command performs three tasks:

- Configures the IP address of the Mobility Manager server. In previous ArubaOS releases, this was done with the mobility-server command.
- Creates an SNMP version 3 user profile with the configured <username> and <password>. This allows SNMP SETs from the Mobility Manager server to be received by the controller. The authentication protocol is Secure Hash Algorithm (SHA) and Data Encryption Standard (DES) is used for encryption. If <username> and <password> match an existing SNMP v3 user profile, the existing one is used. Otherwise, a new profile is created.

  This username and password must be used when adding this controller to the Mobility Manager server in the Mobility Manager Dashboard.
- Allows SNMP traps and notifications to be sent to the Mobility Manager server IP address, by adding this Mobility Manager server as a trap receiver.
- Optionally enables the Mobility Manager server to function as a Real Time Location System (RTLS) server to receive location information via APs from RTLS tags or other devices.

Use the **show mobility-manager** command to check the current status of the configured Mobility Manager servers.

Example

The following command configures the IP address and SNMP user profile for the Mobility Manager server:

```
(host) (config)# mobility-manager 10.2.1.245 user mms-user my-password.
```

Command History

This command was introduced in ArubaOS 3.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

netdestination

```
netdestination <name>
   host <ipaddr> [position <number>]
   invert
   network <ipaddr> <netmask> [position <number>]
   no ...
   range <start-ipaddr> <end-ipaddr> [position <number>]
```

Description

This command configures an alias for a network host, subnetwork, or range of addresses.

Syntax

Parameter	Description	Default
<name>	Name for this alias.	—
host	Configure a single host	—
invert	Specifies that the inverse of the network addresses configured are used. For example, if a network of 172.16.0.0 255.255.0.0 is configured, this parameter specifies that the alias matches everything except this subnetwork.	—
network	An IP subnetwork consisting of an IP address and netmask.	—
no	Negates any configured parameter.	—
position	Specifies the position of this network specification relative to other specifications (1 is first, default is the last position). To view current position settings for network destinations, use the command **show netdestination network**.	(last)
range	A range of IP addresses consisting of sequential addresses between a lower and an upper value. The maximum number of addresses in the range is 16. If larger ranges are needed, convert the range into a subnetwork and use the **network** parameter.	—

Usage Guidelines

Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the traffic source and/or destination. Once you configure an alias, you can use it in multiple session ACLs.

When using the **invert** option, use caution when defining multiple aliases, as entries are processed one at a time. As an example, consider a netdestination configured with the following two network hosts:

```
netdestination dest1 invert
network 1.0.0.0 255.0.0.0
network 2.0.0.0 255.0.0.0
```

A frame from http://1.0.0.1 would match the first alias entry, (which allows everything except for 1.0.0.0/8) so the frame would be rejected. However, it would then be compared against the second alias, which allows everything except for 2.0.0.0/8, and the frame would be permitted.

Example

The following command configures an alias for an internal network:

```
(host) (config) #netdestination Internal
   network 10.1.0.0 255.255.0.0
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Requires the Policy Enforcement Firewall license.	Config mode on master controllers

netservice

```
netservice <name> <protocol>|tcp|udp {list <port>,<port>}|{<port> [<port>]}
[ALG <service>]
```

Description

This command configures an alias for network protocols.

Syntax

Parameter	Description	Range
`netservice`	Name for this alias.	—
`<protocol>`	IP protocol number.	0-255
`tcp`	Configure an alias for a TCP protocol	
`udp`	Configure an alias for a UDP protocol	
`list <port>,<port>`	Specify a list of non-contiguous port numbers, by entering up to six port numbers, separated by commas.	0-65535
`<port> [<port>]`	TCP or UDP port number. You can specify a single port number, or define a port range by specifying both the lower and upper port numbers.	0-65535
`ALG`	Application-level gateway (ALG) for this alias.	—
`<service>`	Specify one of the following service types: • **dhcp**: Service is DHCP • **dns**: Service is DNS • **ftp**: Service is FTP • **h323**: Service is H323 • **noe**: Service is Alcatel NOE • **rtsp**: Service is RTSP • **sccp**: Service is SCCP • **sip**: Service is SIP • **sips**: Service is Secure SIP • **svp**: Service is SVP • **tftp**: Service is TFTP • **vocera**: Service is VOCERA	

Usage Guidelines

Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the network service. Once you configure an alias, you can use it in multiple session ACLs.

Example

The following command configures an alias for a network service:

```
(host) (config) #netservice HTTP tcp 80
```

Command History

Version	Modification
ArubaOS 3.0	Command introduced.
ArubaOS 6.0	The **list** parameter for defining non-contiguous ports was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

network-printer

```
network-printer [max-clients <2-20> |
   max-clients-per-host <1-20> |
   max-jobs <1-1000>]
```

Description

This command allows you to configure client and print job for the USB printer connected to a Aruba 600 series controller.

Syntax

Parameter	Description
`max-clients`	Specify the maximum number of clients that can use the printer. Currently, the Aruba 600 series supports a maximum of 20 concurrent clients.
`max-clients-per-host`	Specify the maximum number of concurrent clients for a single host. Currently, the Aruba 600 series supports a maximum of 20 concurrent clients.
`max-jobs`	Specify the maximum number of jobs that can be saved in the memory Currently, the Aruba 600 series controller will support a storage of 1000 jobs.

Usage Guidelines

Use this command in the config mode.

In the enable mode, you can use the `network-printer delete <printer-name> job <job-id>` command to delete print jobs in specific printer.

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
Aruba 600 series	Base operating system	Config or enable mode.

network-storage

```
network-storage [share <share-name>]
   share [usb: disk <disk-name> <filesystem-path> mode {read-only | read-write}
   no share
```

Description

This command allows you to perform the following operation on a network share:

- Configure a file system path for the share–This allows users to access the share from their computer.
- Remove the share access using the `no share` command.

Syntax

Parameter	Description
`share`	Enter a name for the share on the controller. After you enter this command, the CLI mode will shift to operations on that share.

Usage Guidelines

To access the share, you must create a filesystem path to the share. enter:

```
(host) (config-network-storage share)# share usb: disk <disk name> <filesystem path>
mode
```

Where,

disk name is the name of the disk. You can also specify the disk alias instead of the disk name.

filesystem path is the path to access the share. This path contains the partition name and the shared folder name.

mode is the permission settings. You can either specify `read-only` or `read-write` modes.

Example

The following command associates a share to a file system path and configures the access mode.

```
(host) (config-network-storage share)#share usb: disk Maxtor1TB Maxtor-Basics_Desktop-2HBADMJ4_p1/
documents mode read-write
(host) (config-network-storage share)#show network-storage shares
NAS Shares
----------
Disk Name  Partition Name  Folder Name  Share Name  Share Path
```

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
W-600 Series Controller	Base operating system	Enable mode.

ntp server

```
ntp server <ipaddr> [iburst]
```

Description

This command configures a Network Time Protocol (NTP) server.

Syntax

Parameter	Description	Default
`<ipaddr>`	IP address of the NTP server, in dotted-decimal format.	—
`iburst`	(Optional) This parameter causes the controller to send up to ten queries within the first minute to the NTP server. This option is considered "aggressive" by some public NTP servers.	disabled

Usage Guidelines

You can configure the controller to set its system clock using NTP by specifying one or more NTP servers.

Example

The following command configures an NTP server:

```
(host) (config) #ntp server 10.1.1.245
```

Command History

Release	Modification
ArubaOS 1.0	Command introduced
ArubaOS 3.0	The **iburst** parameter was introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

packet-capture

```
packet-capture [other {disable | enable}] [sysmsg {all | disable | <opcodes>]
[tcp {all | disable | <ports>}] [udp {all | disable | <ports>]]
```

Description

Use this command to enable or disable packet capturing and set packet capturing options for a single packet capture session.

Syntax

Parameter	Description	Default
`other`	Enable or disable all other types of packets. Specify up to ten comma-separated opcodes to capture; use `all` to sniff all opcodes; use `disable` to bypass the all setting. All CLI ports are always skipped.	Enabled
`sysmsg`	Enable or disable internal messaging packets.	Disabled
`tcp ports`	Enable or disable TCP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all TCP ports; use `disable` to bypass the `all` setting. All CLI ports are always skipped.	Disabled
`udp ports`	Enable or disable UDP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all UDP ports; use `disable` to bypass the `all` setting. All CLI ports are always skipped.	Disabled

Usage Guidelines

This command applies to control path packets; not datapath packets. Packets can be retrieved through the **tar log** command; look for the filter.pcap file. This command activates packet capture options on the current switch. They are not saved and applied across switches.

If you do want to enable a packet capture session without setting values that can be saved and used for another session, use the command packet-capture. The related command packet-capture-defaults lets you define a set of packet capture options that will run every time you enable the packet capture feature.

Example

The following command enables packet capturing for debugging a wireless WEP station doing VPN. This example uses the following parameters and values:

- Station up/down: sysmsg opcode 30
- WEP key plumbing: sysmsg opcode 29
- DHCP: sysmsg opcode 90
- IKE: UDP port 500 and 4500
- Layer 2 Tunneling Protocol (L2TP): UDP port 1701

```
(host) #packet-capture sysmsg 30,29,90 udp 500,4500,1701,1812,1645
```

Command History

This command was introduced in ArubaOS 2.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

packet-capture-defaults

```
packet-capture-defaults [other {disable | enable}]
[sysmsg {all | disable | <opcodes>] [tcp {all | disable | <ports>}]
[udp {all | disable | <ports>]]
```

Description

Use this command to enable or disable packet capturing and define a set of default packet capturing options on the control path for debugging purposes.

Syntax

Parameter	Description	Default
`other`	Enable or disable all other types of packets. Specify up to ten comma-separated opcodes to capture; use `all` to sniff all opcodes; use `disable` to bypass the all setting. All CLI ports are always skipped.	Enabled
`sysmsg`	Enable or disable internal messaging packets.	Disabled
`tcp ports`	Enable or disable TCP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all TCP ports; use `disable` to bypass the `all` setting. All CLI ports are always skipped.	Disabled
`udp ports`	Enable or disable UDP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all UDP ports; use `disable` to bypass the `all` setting. All CLI ports are always skipped.	Disabled

Usage Guidelines

This command applies to control path packets; not datapath packets. Packets can be retrieved through the **tar log** command; look for the filter.pcap file. This command activates packet capture options on the current switch. They are not saved and applied across switches.

Example

The following command sets the default packet capture values to debug a wireless WEP station doing VPN. Once these default settings are defined, you can use the packet-capture command to enable packet capturing with these values. This example uses the following parameters and values:

- Station up/down: sysmsg opcode 30
- WEP key plumbing: sysmsg opcode 29
- DHCP: sysmsg opcode 90
- IKE: UDP port 500 and 4500
- Layer 2 Tunneling Protocol (L2TP): UDP port 1701

```
packet-capture-defaults sysmsg 30,29,90 udp 500,4500,1701,1812,1645
```

Use the `show packet-capture` command to show the current action and the default values.

```
(host) show packet-capture

Current Active Packet Capture Actions(current switch)
=====================================================
Packet filtering TCP with 2 port(s) enabled:
  2
  1
Packet filtering UDP with 1 port(s) enabled:
  1
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.


Packet Capture Defaults(across switches and reboots if saved)
=============================================================
Packet filtering TCP with 2 port(s) enabled:
  2
  1
Packet filtering UDP with 1 port(s) enabled:
  1
```

Command History

This command was introduced in ArubaOS 2.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

page

```
page <length>
```

Description

This command sets the number of lines of text the terminal will display when paging is enabled.

Syntax

Parameter	Description	Range
`length`	Specifies the number of lines of text displayed.	24 - 100

Usage Guidelines

Use this command in conjunction with the **paging** command to specify the number of lines of text to display. For more information on the pause mechanism that stops the command output from printing continuously to the terminal, refer to the command "paging" on page 370.

If you need to adjust the screen size, use your terminal application to do so.

Example

The following command sets 80 as the number of lines of text displayed:

```
(host) (config) #page 80
```

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config and Enable mode on master controllers

paging

`paging`

Description

This command stops the command output from printing continuously to the terminal.

Syntax

No parameters

Usage Guidelines

By default, paging is enabled.

With paging enabled, there is a pause mechanism that stops the command output from printing continuously to the terminal. If paging is disabled, the output prints continuously to the terminal. To disable paging, use the **no paging** command. You must be in enable mode to disable paging.

The paging setting is active on a per-user session. For example, if you disable paging from the CLI, it only affects that session. For new or existing sessions, paging is enabled by default.

You can also configure the number of lines of text displayed when paging is enabled. For more information, refer to the command "page" on page 369.

If you need to adjust the screen size, use your terminal application to do so.

Example

The following command enables paging:

```
(host) (config) #paging
```

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config and Enable mode on master controllers

panic

```
panic {clear | info {file <filename> <symbolfile>|nvram <symbolfile>} | list {file
<filename>|nvram} | save <filename>}
```

Description

This command manages information created during a system crash.

Syntax

Parameter	Description
`clear`	Removes panic information from non-volatile random access memory (NVRAM).
`info`	Displays the content of specified panic files.
`list`	Lists panic information in the specified file in flash or in NVRAM.
`save`	Saves panic information from NVRAM into the specified file in flash.

Usage Guidelines

To troubleshoot system crashes, use the **panic save** command to save information from NVRAM into the specified file, then use the **panic clear** command to clear the information from NVRAM.

Example

The following command lists panic information in NVRAM:

```
(host) #panic list nvram
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

papi-security

```
papi-security
   key <key>
   [enhanced-security]
   no...
```

Description

The papi-security command enforces advanced security options and provides an enhanced level of security.

Caution: The best practice is to refrain from modifying these settings unless advised to do so by Dell technical support.

Syntax

Parameter	Description	Default
`key`	The key authenticates the messages between systems.	—
`key`	The key string.	Range: 10–64 characters
`enhanced-security`	Allows you to use the enhanced security mode. This mode causes the system to reject messages when an incorrect key is used.	disabled
`no key`	Reverts to the default key.	—

Usage Guidelines

This command allows you to use advanced options which regulate the controller and AP communication. One way PAPI messages are authenticated is through a shared secret key. The papi-security command lets you configure a key on the master controller which then distributes it to other controllers and APs, thus allowing each site to have a unique key. If no key is configured, then the controller uses the default key.

When enhanced-security mode is disabled, any AP can obtain the current shared secret key.

When enhanced-security mode is enabled, an AP is not updated with the new shared secret key unless the AP knows the previous key and the AP is updated with the new key within one hour of the key creation.

Note: Make sure that the enhanced-security mode is disabled before installing new APs.

If an AP cannot be authenticated because it has the wrong key, the show ap database command displays a “Bad key” status.

Example

This example sets a unique shared secret key called “testkey123” on the master controller.

```
(host) (config) #papi-security
(host) (PAPI Security Profile) #
(host) (PAPI Security Profile) #key testkey123
(host) (PAPI Security Profile) #exit
```

Related Commands

```
(host)(config) #show papi-security
(host)(config) #show ap database
```

Command History

This command was introduced in ArubaOS 3.4

Command Information

Platform	License	Command Mode
Available on all platforms	Base operating system	Config mode on master controllers

pcap

```
pcap {raw-start <ipaddr> <target-ipaddr> <target-port> <format> [bssid <bssid>]
[channel <number>] [maxlen <maxlen>]}|{interactive <am-ip> <filter> <target-ipaddr>
<target-port> [bssid <bssid>][channel <number>]}|{clear|pause|resume|stop <am-ip> <id>
[bssid <bssid>]}
```

Description

These commands manage packet capture (PCAP) on Dell air monitors.

Syntax

Parameter	Description
`raw-start`	Stream raw packets to an external viewer.
`<ipaddr>`	IP address of the air monitor collecting packets.
`<target-ipaddr>`	IP address of the client station running Wildpacket's AiroPeek monitoring application.
`<target-port>`	UDP port number on the client station where the captured packets are sent.
`<format>`	Specify a number to indicate one of the following formats for captured packets: • **0** : pcap • **1** : peek • **2** : airmagnet • **3** : pcap+radio header • **4** : ppi
`bssid`	(Optional) BSSID of the Air Monitor interface for the PCAP session.
`<bssid>`	BSSID of the Air Monitor Interface, which is usually its MAC address.
`channel`	(Optional) Number of a radio channel to tune into to capture packets
`maxlen`	(Optional) Limit the length of 802.11 frames to include in the capture to a specified maximum.
`<maxlen>`	(Optional) Maximum number of packets to be captured.
`interactive`	Start an interactive packet capture session.
`<am-ip>`	IP address of the air monitor collecting packets.
`<filter-spec>`	Packet Capture filter specification.
`<target-ipaddr>`	IP Address of host to which the frames should be sent
`<target-port>`	UDP Port Number to which the frames should be sent
`bssid`	(Optional) Specify the BSSID of the Air Monitor interface for the PCAP session.
`<bssid>`	BSSID of the Air Monitor Interface, which is usually its MAC address.
`channel`	(Optional) Number of a radio channel to tune into to capture packets
`clear`	Clears the packet capture session.
`pause`	Pause a packet capture session.
`resume`	Resume a packet capture session.
`start`	Start a new packet capture session.
`stop`	Stop a packet capture session.
`<am-ip>`	IP address of the air monitor collecting packets.
`<id>`	ID of the PCAP session.
`bssid`	(Optional) Specify the BSSID of the Air Monitor interface for the PCAP session.
`<bssid>`	BSSID of the Air Monitor Interface, which is usually its MAC address.

Usage Guidelines

These commands direct an Dell air monitor to send packet captures to the Wildpacket's AiroPeek monitoring application on a remote client. The AiroPeek application listens for packets sent by the air monitor.

The following pcap commands are available:

Command	Description
`clear`	Clears the packet capture session.
`pause`	Pause a packet capture session.
`resume`	Resume a packet capture session.
`start`	Start a new packet capture session.
`stop`	Stop a packet capture session.

Before using these commands, you need to start the AiroPeek application on the client and open a capture window for the air monitor. The AiroPeek application cannot be used to control the flow or type of packets sent from Dell air monitors.

The AiroPeek application processes all packets, however, you can apply display filters on the capture window to control the number and type of packets being displayed. In the capture window, the time stamp displayed corresponds to the time that the packet is received by the client and is not synchronized with the time on the Dell air monitor.

Example

The following command starts a raw packet capture session for the air monitor at 10.100.100.1 and sends the packets to the client at 192.168.22.44 on port 604 with pcap format:

```
(host) (config) #pcap raw-start 10.100.100.1 192.168.22.44 604 0
```

Command History

Version	Change
ArubaOS3.0	Command Introduced
ArubaOS3.4	The **maxlen** parameter was introduced, and the **pcap start** command deprecated.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

phonehome

```
phonehome
   auto-report
   disable
   enable
   now
   smtp <a.b.c.d> <from_addy> [port <port_num>] {size <max_size>] [user <username> pass
   <password>]
```

Description

This command configures the PhoneHome auto reporting feature.

Syntax

Parameter	Description	Range
`auto-report`	The controller will periodically contact Dell support once a week to report any errors or changes to the controller configuration or inventory. If the controller has not reported any errors and its configuration file has not changed, no report will be sent. **NOTE:** Before you enable auto-reporting, you must first enable the PhoneHome feature using the command **phonehome enable**.	
`disable`	This parameter disables the phonehome feature. Phonehome automatic reporting is disabled by default.	
`enable`	This parameter enables the phonehome feature.	
`now`	Issue the **phonehome now** command in enable mode to immediately create and send a report from the controller to Dell support. **NOTE:** Before you use the **phonehome now** command to create and send a report, you must first access the command-line interface in config mode and issue the command **phonehome enable** to enable this feature.	
`smtp`	Configure the SMTP server that will send email messages from the controller to Dell support.	
`<a.b.c.d>`	IP address of the SMPT server	
`<from_addy>`	Local email address from which the auto reporting messages will be sent. For example, *admin@mycorp.com*.	
`port <port_num>`	(Optional) Port number from which the SMTP server will send auto reporting emails. The default port is port 25.	25
`size <max_size>`	(Optional) If your SMTP server has a restriction on the size of the emails it can send, use this parameter to specify the maximum size limit. Any reports larger than this limit will be divided into multiple smaller emails.	1-10 MB
`user <username>` `pass <password>`	(Optional) If your SMTP server requires user authentication before it can send an email message, enter the username and password for a valid user on your network.	

Usage Guidelines

The automatic reporting feature, also known as *PhoneHome*, allows a controller to securely contact Dell support servers over the Internet to report events such as hardware failures, software malfunctions, and other critical events. When the PhoneHome automatic reporting feature is enabled, the controller sends Dell support weekly reports about the controller's configuration, licenses, software and hardware status, and any software malfunctions via a secure email.

This feature requires that your network has a local SMTP server capable of relaying email. When the controller generates the report email with the phonehome data file attachment, it forwards the email to the SMTP server

configured on your local network, which then delivers the message to Dell. If your email server requires the sender to be authenticated before message delivery, the controller can connect to the SMTP by supplying the sender's user name and password.

Each PhoneHome report attachment is encrypted before it is transmitted to the SMTP server, and is decrypted by Dell support when it is received. If the PhoneHome status report email is larger than the maximum email size supported by your SMTP server, the controller will divide the PhoneHome attachment into multiple smaller attachments and send the report to Dell in multiple emails.

In the event that you need to contact Dell support with a question about your controller, you can use the **phonehome now** command in enable mode to generate and immediately send a status report, so that Dell support can diagnose the issue with the most current controller data.

Example

The following command turns on the PhoneHome feature, enables weekly auto-reports, and identifies the SMTP server to be used by this feature:

```
(host) (config) #phonehome enable auto-report smtp 172.21.18.170 admin@mycorp.com
```

Command History

This command was introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	The **phonehome now** command must be issued in enable mode. All other phonehome commands require config mode.

ping

```
ping <ipaddress>
```

Description

This command sends five ICMP echo packets to the specified ip address.

Syntax<

Parameter	Description
<ipaddress>	Destination IP Address

Usage Guidelines

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

Example

The following example pings 10.10.10.5.

```
(host) >ping 10.10.10.5
```

The sample controller output is:

```
Press 'q' to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.5, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.408/0.5434/1.073 ms
```

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	User, Enable, and Config modes on master controllers

pkt-trace

```
pkt-trace acl <acl-name> {enable|disable} [trace {cptrace|pktrace} [trace-mask
<tmask>]]]
```

Description

Enable packet tracing in the datapath. Use this feature only under the supervision of Dell technical support.

Syntax

Parameter	Description
`<acl-name>`	Enable packet tracing for the specified access-control list.
`enable`	Enable packet tracing for the ACL.
`disable`	Disable packet tracing for the ACL.
`cptrace`	Send packet trace data into the Control Processor.
`pktrace`	Write packet trace data in the packet.
`tracemask <tmask>`	Specify the trace mask. This value will be provided by Dell technical support.

Example

The following example enables packet tracing for the traffic matching the acl **stateful-dot1x**.

```
(host) #pkt-trace acl stateful-dot1x enable trace cptrace trace-mask <val>
```

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

pkt-trace-global

```
pkt-trace-global {enable|disable} [trace-mask <tmask>]
```

Description

Enable global packet tracing in the datapath. Use this feature only under the supervision of Dell technical support.

Syntax

Parameter	Description
`<acl-name>`	Enable packet tracing for the specified access-control list.
`enable`	Enable global packet tracing for the ACL.
`disable`	Disable global packet tracing for the ACL.
`tracemask <tmask>`	Specify a trace mask. Use this feature only under the supervision of Dell technical support.

Example

The following command enables the global packet tracing for all traffic.

```
(host) (config) #pkt-trace-global enable
```

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

pptp ip local pool

```
pptp ip local pool <pool> <ipaddr> [<end-ipaddr>]
```

Description

This command configures an IP address pool for VPN users using Point-to-Point Tunneling Protocol (PPTP).

Syntax

Parameter	Description
`<pool>`	User-defined name for the address pool.
`<ipaddr>`	Starting IP address for the pool.
`<end-ipaddr>`	Ending IP address for the pool.

Usage Guidelines

If VPN is used as an access method, you specify the pool from which the user's IP address is assigned when the user negotiates a PPTP session. Use the **show vpdn pptp local** command to see the used and free addresses in the pool.

PPTP is an alternative to IPsec that is supported by various hardware platforms. PPTP is considered to be less secure than IPsec but also requires less configuration. You configure PPTP with the **vpdn** command.

Example

The following command configures an IP address pool for PPTP VPN users:

```
(host) (config) #pptp ip local pool pptp-pool1 172.16.18.1 172.16.18.24
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

priority-map

```
priority-map <name>
   dot1p <priority> high
   dscp <priority> high
   no ...
```

Description

This command configures the Type of Service (ToS) and Class of Service (CoS) values used to map traffic into high priority queues.

Syntax

Parameter	Description	Range
<name>	User-defined name of the priority map.	—
dot1p	IEEE 802.1p priority value, or a range of values separated by a dash (-).	0-7
dscp	Differentiated Services Code Point (DSCP) priority value, or a range of values separated by a dash (-).	0-63
no	Negates any configured parameter.	—

Usage Guidelines

This command allows you to prioritize inbound traffic that is already tagged with 802.1p and/or IP ToS in hardware queues. You apply configured priority maps to ports on the controller (using the **interface fastethernet** or **interface gigbitethernet** command). This causes the controller to inspect inbound traffic on the port; when a matching QoS tag is found, the packet or flow is mapped to the specified queue.

Example

The following commands configure a priority map and apply it to a port:

```
(host) (config) #priority-map pri1
   dscp 4-20 high
   dscp 60 high
   dot1p 4-7 high
interface gigabitethernet 1/24
   priority-map pri1
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

process monitor

```
process monitor log|restart|
```

Description

The process monitor validates the integrity of processes every 120 seconds. If a process does not respond during three consecutive 120-second timeout intervals, that process is flagged as nonresponsive and the process monitor will create a log message, restart the process or reboot the controller

Syntax

Parameter	Description
`log`	The process monitor creates a log message when a process fails to responding properly. This is the default behavior for the process monitor
`restart`	This parameter enables strict behavior for runtime processes. When you enable this option, the process monitor will restart processes that fail to responding properly.

Usage Guidelines

The CLI command **process monitor log** enables logging for process monitoring. By default, whenever a process does not update a required file or send a heartbeat pulse within the required time limit, the process monitor records a critical log message, but does not restart any process. If you want the configure watchdog to restart a process once it fails to respond, use the CLI **command process monitor restart**.

Example

The following changes the default process monitor behavior, so the process monitor restarts nonresponsive processes.

```
(host) #process monitor restart
```

Related Commands

The show **process monitor statistics** command displays the current status of all the processes running under the process monitor watchdog.A partial example of the output of this command is show below:

```
(host) (config) #show process monitor statistics

Process Monitor Statistics
--------------------------
Name                          State            Restarts  Timeout Value  Timeout
            Chances
----                          -----            --------  -------------  --------------
/mswitch/bin/arci-cli-helper  PROCESS_RUNNING  0         120            3
/mswitch/bin/fpcli            PROCESS_RUNNING  0         120            3
/mswitch/bin/packet_filter    PROCESS_RUNNING  0         120            3
/mswitch/bin/certmgr          PROCESS_RUNNING  0         120            3
/mswitch/bin/dbstart          PROCESS_RUNNING  0         120            3
/mswitch/bin/cryptoPOST       PROCESS_RUNNING  0         120            3
/mswitch/bin/sbConsoled       PROCESS_RUNNING  0         120            3
/mswitch/bin/pubsub           PROCESS_RUNNING  0         120            3
/mswitch/bin/cfgm             PROCESS_RUNNING  0         120            3
/mswitch/bin/syslogdwrap      PROCESS_RUNNING  0         120            3
/mswitch/bin/aaa              PROCESS_RUNNING  0         120            3
/mswitch/bin/fpapps           PROCESS_RUNNING  0         120            3
```

Command History

Release	Modification
ArubaOS 3.4	Command introduced
ArubaOS 3.4	The **process restart** command was deprecated.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

prompt

```
prompt <prompt>
```

Description

This command changes the prompt text.

Syntax.

Parameter	Description	Range	Default
`prompt`	The prompt text displayed by the controller.	1–64	<hostname>

Usage Guidelines

You can use any alphanumeric character, punctuation, or symbol character. To use spaces, plus symbols (+), question marks (?), or asterisks (*), enclose the text in quotes.

You cannot alter the parentheses that surround the prompt text, or the greater-than (>) or hash (#) symbols that indicate user or enable CLI mode.

Example

The following example changes the prompt text to “It’s a new day!”.

```
(host) (config) #prompt “It’s a new day!”
(It’s a new day!) (config) #
```

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

provision-ap

```
provision-ap
   a-ant-bearing <bearing>
   a-ant-gain <gain>
   a-ant-tilt-angle <angle>
   a-antenna {1|2|both}
   altitude <altitude>
   ap-group <group>
   ap-name <name>
   copy-provisioning-params {ap-name <name> | ip-addr <ipaddr>}
   dns-server-ip <ipaddr>
   domain-name <name>
   external-antenna
   fqln <name>
   g-ant-bearing <bearing>
   g-ant-gain <gain>
   g-ant-tilt-angle <angle>
   g-antenna {1|2|both}
   gateway <ipaddr>
   ikepsk <key>
   installation default|indoor|outdoor
   ipaddr <ipaddr>
   latitude <location>
   longitude <location>
   master {<name>|<ipaddr>}
   mesh-role {mesh-point|mesh-portal|none|remote-mesh-portal}
   mesh-sae {sae-disable|sae-enable}
   netmask <netmask>
   no ...
   pap-passwd <string>
   pap-user <name>
   pppoe-passwd <string>
   pppoe-service-name <name>
   pppoe-user <name>
   read-bootinfo {ap-name <name>|ip-addr <ipaddr>|wired-mac <macaddr>}
   reprovision {all|ap-name <name>|ip-addr <ipaddr>|serial-num <string>|
    wired-mac <macaddr>}
   reset-bootinfo {ap-name <name>|ip-addr <ipaddr>|wired-mac <macaddr>}
   server-ip <ipaddr>
   server-name <name>
   set-ikepsk-by-addr <ip-addr>
   syslocation <string>
   uplink-vlan <uplink-vlan>
   usb-dev <usb-dev>
   usb-dial <usb-dial>
   usb-init <usb-init>
   usb-passwd <usb-passwd>
   usb-tty <usb-tty>
   usb-type <usb-type>
   usb-user <usb-user>
```

Description

This command provisions or reprovisions an AP.

Syntax

Parameter	Description	Range	Default
a-ant-bearing	Determines the horizontal coverage distance of the 802.11a (5GHz) antenna from True North. From a planning perspective, the horizontal coverage pattern does not consider the elevation or vertical antenna pattern. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	0-360 Decimal Degrees	—
a-ant-gain	Antenna gain for 802.11a (5GHz) antenna.	—	—
a-ant-tilt-angle	Directs the angle of the 802.11a (5GHz) antenna for optimum coverage. Use a - (negative) value for downtilt and a + (positive) value for uptilt. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	-90 to +90 Decimal Degrees	—
a-antenna	Antenna use for 5 GHz (802.11a) frequency band. • 1: Use antenna 1 • 2: Use antenna 2 • both: Use both antennas	1, 2, both	both
altitude	Altitude, in meters, of the AP. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	—	—
ap-group	Name of the AP group to which the AP belongs.	—	"default"
ap-name	Name for this AP.	—	—
copy-provisioning-params	Initializes the provisioning-params workspace with the current provisioning parameters of the specified AP, The provisioning parameters of the AP must have previously been retrieved with the **read-bootinfo** option. **NOTE:** This parameter can only be used on the master controller.	—	—
dns-server-ip	IP address of the DNS server for the AP.	—	—
domain-name	Domain name for the AP.	—	—
external-antenna	Use an external antenna with the AP.	—	—
fqln	Fully-qualified location name (FQLN) for the AP, in the format <APname.floor.building.campus>.	—	—
g-ant-bearing	Determines the horizontal coverage distance of the 802.11g (2.4GHz) antenna from True North. From a planning perspective, the horizontal coverage pattern does not consider the elevation or vertical antenna pattern. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	0-360 decimal degrees	—
g-ant-gain	Antenna gain for 802.11g (2.4GHz) antenna.	—	—

Parameter	Description	Range	Default
g-ant-tilt-angle	Directs the angle of the 802.11g (2.4GHz) antenna for optimum coverage. Use a - (negative) value for downtilt and a + (positive) value for uptilt. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	-90 to +90 Decimal Degrees	—
g-antenna	Antenna use for 2.4 GHz (802.11g) frequency band. • 1: Use antenna 1 • 2: Use antenna 2 • both: Use both antennas	1, 2, both	both
gateway	IP address of the default gateway for the AP.	—	—
ikepsk	IKE preshared key for the AP.	—	—
installation	Specify the type of installation (indoor or outdoor). The default parameter automatically selects an installation mode based upon the AP model type.	default indoor outdoor	default
ipaddr	Static IP address for the AP.	—	—
latitude	Latitude coordinates of the AP. Use the format: Degrees, Minutes, Seconds (DMS). For example: 37 22 00 N	—	—
longitude	Longitude coordinates of the AP. Use the DMS format. For example: 122 02 00 W	—	—
master	Name or IP address of the master controller.	—	—
mesh-role	Configure the AP to operate as a mesh node. You assign one of three roles: **mesh portal**, **mesh point** or **remote mesh point**. If you select "none," the AP operates as a thin AP.	mesh-portal mesh-point remote-mesh-portal none	—
mesh-sae	Enable or disable Secure Attribute Exchange (SAE) on a mesh network. To use the SAE feature, you must enable this parameter on all mesh nodes (points and portals) in the network, to prevents mesh link connectivity issues. **NOTE:** This is a Beta feature only. This parameter should be kept "disabled" for this release.	sae-disable sae-enable	sae-disable
netmask	Netmask for the IP address.	—	—
no	Negates any configured parameter.	—	—
pap-passwd	Password Authentication Protocol (PAP) password for the AP. You can use special characters in the PAP password. Following are the restrictions: • You cannot use double-byte characters • You cannot use a tilde (~) • You cannot use a tick (') • If you use quotes (single or double), you must use the backslash (\) before and after the password	—	—
pap-user	PAP username for the AP.	—	—
pppoe-passwd	Point-to-Point Protocol over Ethernet (PPPoE) password for the AP.	—	—
pppoe-service-name	PPPoE service name for the AP.	—	—

Parameter	Description	Range	Default
`pppoe-user`	PPPoE username for the AP.	—	—
`read-bootinfo`	Retrieves current provisioning parameters of the specified AP. **NOTE:** This parameter can only be used on the master controller.	—	—
`reprovision`	Provisions one or more APs with the values in the provisioning-params workspace. To use **reprovision**, you must use **read-bootinfo** to retrieve the current values of the APs into the provisioning-ap-list. **NOTE:** This parameter can only be used on the master controller.	—	—
`reset-bootinfo`	Restores factory default provisioning parameters to the specified AP. **NOTE:** This parameter can only be used on the master controller.	—	—
`server-ip`	IP address of the controller from which the AP boots.	—	—
`server-name`	DNS name of the controller from which the AP boots.	—	—
`set-ikepsk-by-addr`	Set a IKE preshared key to correspond to a specific IP address.		
`syslocation`	User-defined description of the location of the AP.	—	—
`uplink-vlan <uplink-vlan>`	If you configure an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature. **NOTE:** If an AP is provisioned with an uplink VLAN, it *must be connected to a trunk mode port* or the AP's frames will be dropped.	0 (disabled) to 4095	0
`usb-dev`	The USB device identifier.		
`usb-dial`	The dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.		
`usb-init`	The initialization string for the USB modem. This parameter only needs to be specified if the default string is not correct.		
`usb-passwd`	A PPP password, if provided by the cellular service provider		
`usb-tty`	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.		
`usb-type`	The USB driver type.		
`usb-user`	The PPP username provided by the cellular service provider		

Usage Guidelines

You do not need to provision APs before installing and using them.

The exceptions are:

- APs configured for mesh. You must provision the AP before you install it as a mesh node in a mesh deployment.

Note: Users less familiar with this process may prefer to use the **Provisioning** page in the WebUI to provision an AP.

Provisioned or reprovisioned values do not take effect until the AP is rebooted. APs reboot automatically after they are successfully reprovisioned.

Provisioning a Single AP

To provision a single AP:

1. Use the **read-bootinfo** option to read the current information from the deployed AP you wish to reprovision.
2. Use the **show provisioning-ap-list** command to see the AP to be provisioned.
3. Use the **copy-provisioning-params** option to copy the AP's parameter values to the provisioning-params workspace.
4. Use the provision-ap options to set new values. Use the **show provisioning-params** command to display parameters and values in the provisioning-params workspace. Use the **clear provisioning-params** command to reset the workspace to default values.
5. Use the **reprovision** option to provision the AP with the values in provisioning-params workspace. The AP automatically reboots.

Provisioning Multiple APs at a Time

You can change parameter values for multiple APs at a time, however, note the following:

- You cannot provision the following AP-specific options on multiple APs:
  - ap-name
  - ipaddr
  - pap-user
  - pap-passwd
  - ikepsk

  If any of these options are already provisioned on the AP, their values are retained when the AP is reprovisioned.
- The values of the server-name, a-ant-gain, or g-ant-gain options are retained if they are not reprovisioned.
- All other values in the provisioning-params workspace are copied to the APs.

To provision multiple APs at the same time:

1. Use the **read-bootinfo** to read the current information from each deployed AP that you wish to provision.

Note: The AP parameter values are written to the provisioning-ap-list. To reprovision multiple APs, the APs must be present in the provisioning-ap-list. Use the **show provisioning-ap-list** command to see the APs that will be provisioned. Use the **clear provisioning-ap-list** command to clear the provisioning-ap-list.

2. Use the **copy-provisioning-params** option to copy an AP's parameter values to the provisioning-params workspace.
3. Use the provision-ap options to set new values. Use the **show provisioning-params** command to display parameters and values in the provisioning-params workspace. Use the **clear provisioning-params** command to reset the workspace to default values.

4. Use the **reprovision all** option to provision the APs in the provisioning-ap-list with the values in provisioning-params workspace. All APs in the provisioning-ap-list automatically reboot.

The following are useful commands when provisioning one or more APs:

- **show|clear provisioning-ap-list** displays or clears the APs that will be provisioned.
- **show|clear provisioning-params** displays or resets values in the provisioning-params workspace.
- **show ap provisioning** shows the provisioning parameters an AP is currently using.

Example

The following commands change the IP address of the master controller on the AP:

```
(host) (config) #provision-ap
   read-bootinfo ap-name lab103
   show provisioning-ap-list
   copy-provisioning-params ap-name lab103
   master 10.100.102.210
   reprovision ap-name lab103
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	Introduced support for the mesh parameters, additional antenna parameters, and AP location parameters.
ArubaOS 3.4	Introduced support for the following parameters: • installation • mesh-sae • set-ikepsk-by-addr • usb-dev • usb-dial • usb-init • usb-passwd • usb-tty • usb-type • usb-user
ArubaOS 5.0	The mesh-sae parameter no longer has the **sae-default** option. Use the **sae-disable** option to return this parameter to its default disabled setting.
ArubaOS 6.0	The **uplink-vlan** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms, except for the parameters noted in the Syntax table.	Base operating system, except for the parameters noted in the Syntax table.	Config mode on master controllers

rap-wml

```
rap-wml <server-name> [ageout <period>] [cache {disable|enable}] [db-name <name>]
[ip-addr <ipaddr>] [password <password>] [type {mssql|mysql}] [user <name>]
```

Description

Use this command to specify the name and attributes of a MySQL or an MSSQL server.

Syntax

Parameter	Description	Default
`ageout`	(Optional) Specifies the cache ageout period, in seconds.	0
`cache`	(Optional) Enables the cache, or disables the cache.	Disabled
`db-name`	(Optional) Specifies the name of the MySQL or MSSQL database.	—
`ip-addr`	(Optional) Specifies the IP address of the named MSSQL server.	0.0.0.0
`no`	Negates any configured parameter.	—
`password`	(Optional) Specifies the password required for database login.	—
`type`	(Optional) Specifies the server type.	—
`user`	(Optional) Specifies the user name required for database login.	—

Usage Guidelines

Use the **show rap-wml cache** command to show the cache of all lookups for a database server. Use the **show rap-wml servers** command to show the database server state. Use the **show rap-wml wired-mac** command to show wired MAC discovered on traffic through the AP.

Example

This example configures a MySQL server and sets up associated rap-wml table attributes.

```
(host) (config) #rap-wml mysqlserver type mysql ip-addr 10.4.11.10 db-name
automatedtestdatabase user sa password sa
rap-wml table mysqlserver mactest_undelimited mac timestamp-column time 600
rap-wml table mysqlserver mactest_delimited mac delimiter : timestamp-column time 600
```

This example configures an MSSQL server and sets up associated rap-wml table attributes.

```
(host) (config) #rap-wml mssqlserver type mssql ip-addr 10.4.11.11 db-name
automatedtestdatabase user sa password sa
rap-wml table mssqlserver mactest_undelimited mac timestamp-column time 600
rap-wml table mssqlserver mactest_delimited mac delimiter : timestamp-column time 600
```

Command History

This command was introduced in ArubaOS 2.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Requires the RF Protect license.	Config mode on master controllers

rap-wml table

```
rap-wml table <server-name> <table-name> <column-name> {[delimiter <char>] |
[timestamp-column <timestamp-column-name> <lookup-time>]}
```

Description

Use this command to specify the name and attributes of the database table to be used for lookup.

Syntax

Parameter	Description	Default
`server-name`	Specifies the database server name (created using the **rap-wml <server-name>** command.	—
`table-name`	Specifies the database table name.	—
`column-name`	Specifies the database column name with the MAC address.	—
`delimiter`	Specifies the optional delimiter character for the MAC address in the database.	No delimiter
`no`	Negates the rap-wml table for the named server.	—
`timestamp-column`	Specify the database column name with the timestamp last seen.	—
`timestamp-column-name`	Specify the database column name with the timestamp last seen.	—
`lookup-time`	Specifies how far back—in seconds—to look for the MAC address. Use 0 seconds to lookup everything.	0

Usage Guidelines

Use the **rap-wml <servername>** command to configure a MySQL or an MSSQL server, then use the **rap-wml table** command to configure the associated database table for the server.

Example

This example configures a MySQL server and sets up associated rap-wml table attributes for that server.

```
(host) (config) #rap-wml mysqlserver type mysql ip-addr 10.4.11.10 db-name
automatedtestdatabase user sa password sa
rap-wml table mysqlserver mactest_undelimited mac timestamp-column time 600
rap-wml table mysqlserver mactest_delimited mac delimiter : timestamp-column time 600
```

This example configures an MSSQL server and sets up associated rap-wml table attributes for that server.

```
(host) (config) # rap-wml mssqlserver type mssql ip-addr 10.4.11.11 db-name
automatedtestdatabase user sa password sa
rap-wml table mssqlserver mactest_undelimited mac timestamp-column time 600
rap-wml table mssqlserver mactest_delimited mac delimiter : timestamp-column time 600
```

Command History

This commands was introduced in ArubaOS 2.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Requires the RF Protect license.	Config mode on master controllers

reload

```
reload
```

Description

This command performs a reboot of the controller.

Syntax

No parameters.

Usage Guidelines

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

After you use the **reload** command, the controller prompts you for confirmation of this action. If you have not saved your configuration, the controller 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 controller.

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

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

- Enter **y** to reboot the controller.
- 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 controller:

```
(host) (config) #reload
```

The controller returns the following messages:

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

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config modes on master controllers

remote-node-localip

```
localuserdb
remote-node-localip <remote-node-switch-ip> ipsec KEY <keyword>
```

Description

This command configures the switch-IP address and preshared key for the local Remote Node on a master Remote Node.

Syntax

Parameter	Description
`<remote-node-switch-ip>`	Switch-IP address of the local remote node. Use the 0.0.0.0 address to configure a global preshared key for all inter-controller communications.
`ipsec <keyword>`	Preshared key, which must be between 6-64 characters.

Usage Guidelines

Use this command on a master remote node to configure the switch-IP address and preshared key for communication with a local remote node. On the local remote node, the pre-shared key is configured in the setup wizard during the initial boot. The pre-shared keys for both the master and local controllers must match.

On the local remote node, use the **remote-node-masterid** command to configure the switch-IP address and preshared key for the master remote node.

Example

The following command configures the local remote node on a master remote node:

```
(host) (config) remote-node-localip 172.16.0.254 ipsec rhyopevs
```

Command History

Introduced in ArubaOS 6.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on master controllers

remote-node-masterip

```
remote-node-masterip <masterip> ipsec KEY <pre-shared key>
```

Description

This command configures the IP address and preshared key for the master Remote Node on a local Remote Node.

Syntax

Parameter	Description
`<masterip>`	IP address of the master Remote Node.
`ipsec <key>`	Preshared key, which must be between 6-64 characters.

Usage Guidelines

Use this command on a local Remote Node to configure the IP address and preshared key for communication with the master Remote Node. On the master controller, use the **remote-node-localip** command to configure the IP address and preshared key for a local Remote Node.

Note: Changing the IP address of the master on a local Remote Node requires a reboot of the local Remote Controller.

Example

The following command configures the master Remote Node on a local Remote Node:

```
(host) (config) #remote-node-masterip 172.16.0.254 ipsec rhyopevs
```

Command History

Introduced in ArubaOS6.0

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Available in Config mode on master and local controllers.

remote-node-profile

```
localuserdb
remote-node-profile <remote-node-profile-name>
   aaa
   cellular
   clone
   controller-ip
   dialer
   instance
   interface
   ip
   logging
   mgmt-user
   model
   no
   priority-map
   remote-node-dhcp-pool
   router ospf {area <area-id>|redistribute vlan [<vlan-ids>|add <vlan-ids>|remove
   <vlan-ids>] |router-id <rtr-id> |subnet exclude <addr>}
   spanning-tree
   uplink
   validate
   vlan
   vrrp
```

Description

The remote-node-profile command lets you create a Remote Node profile. Once in Remote Node profile configuration mode, you can issue any of the following commands to define the values you want to assign to that profile.

Syntax

Parameter	Description
`aaa`	Configure authentication server using an internal server. For details, see "aaa authentication-server internal" on page 39
`cellular profile <name>`	Cellular interface profile associated with this Remote Node profile. For details, see "cellular profile" on page 144.
`clone <profile-name>`	Use this command to copy a Remote Node profile to this profile.
`controller-ip loopback`	Configure the controller IP. For details on using this command, see "controller-ip" on page 158.
`controller-ip vlan <id> ip address`	Select one of the following parameters for the VLAN interface **dhcp-client**: The remote node will use DHCP to obtain IP address **internal**: Then remote node IP will be derived from the remote node DHCP pool. **pppoe**: Use PPPoE to obtain IP address
`dialer group <name>`	Dialer group profile associated with this Remote Node profile.
`instance`	Configure the Remote Node MAC address to associate the Remote Node to this profile. When you create a new Remote Node profile, enter the **remote-node profile instance** command first.
`interface`	Configure the Remote Node interface • cellular—Configure the cellular Interface. • fastethernet—Configure the FastEthernet (IEEE 802.3) interface. • gigabitethernet—Configure the GigabitEthernet Interface. • loopback—Configure the Loopback Interface. • port-channel—Configure the Ethernet channel of interfaces. • tunnel—Configure the Tunnel interface. • vlan —Configure the Switch VLAN Virtual Interface. **NOTE:** The VLAN ID mapped using the "interface vlan <id> ip address" command can use the following parameters to define how the controller-ip is derived: ▪ **dhcp-client**: The remote node will use DHCP to obtain IP address ▪ **internal**: Then remote node IP will be derived from the remote node DHCP pool. ▪ **pppoe:** Use PPPoE to obtain IP address For details on using this command, see "interface fastethernet | gigabitethernet" on page 247
`ip`	Configure the Interface Internet Protocol configuration commands • default-gateway • domain • domain-name • name-server • radius • route

Parameter	Description
`logging`	Set the logging level up to which messages are logged. • alerts • critical • debugging • emergencies • errors • informational • notifications • warnings For details on using this command, see "logging" on page 340
`mgmt-user`	Configure a management user. For details on using this command, see "mgmt-user" on page 353.
`model`	Controller model associated to the Remote Node profile, where <model-type> is one of the following controller model types: • M3 • 3200 • 3400 • 3600 • 620 • 650 • 651
`no`	Delete a remote node profile.
`priority-map`	Priority Map specification, used to prioritize the incoming packets on an interface. For details on using this command, see "priority-map" on page 381.
`remote-node-dhcp-pool`	Define a remote node address pool.
`router ospf`	Enables and configures OSPF. Configure an OSP area, control distribution of default information, redistribute the route, configure the Router ID and specific the subnet.
`spanning-tree`	Create a Spanning Tree Subsystem. For details on using this command, see "spanning-tree (Global Configuration)" on page 1148.
`uplink`	Define an uplink manager configuration. For details on using this command, see "uplink" on page 1169.
`validate`	After you have defined configuration settings for a Remote Node profile, you must activate that profile by issuing the command **remote-node-profile <profile-name> validate** to validate that the configuration has a correctly defined uplink, model type, and an interface type supported by the Remote Node model. You cannot assign a Remote Node configuration profile to a Remote Node until that profile has been activated.
`vlan`	Create a Remote Node VLAN Virtual Interface vlan. For details on using this command, see "vlan" on page 1176.
`vrrp`	Define a Virtual Router Redundancy Protocol (VRRP) configuration. For details on using this command, see "vrrp" on page 1194.

Usage Guidelines

Use the **remote-node-profile** command to create a Remote Node profile. You define configuration settings for each Remote Node through a Remote Node profile on the Remote Node-master, which can be either a local controller or a master controller.

Related Commands

Command	Description	Mode
`remote-node-localip`	Configures security for all Remote Node and Remote Controller control traffic	Enable and Config mode
`remote-node-masterip`	Configures security for the Remote Node master IP address.	Enable and Config mode
`local-userdb-remote-node`	This command adds a Remote Node to the Remote Node whitelist. You can also delete the whitelist entry using this command.	Enable and Config mode
`show remote-node`	Shows Remote Node configuration, dhcp instance, license usage and running configuration information.	Enable and Config mode
`show remote-node-dhcp-pool`	Shows Remote Node dhcp pool configuration information.	Enable and Config mode
`show remote-node-profile`	Shows Remote Node profile status information.	Enable and Config mode
`show local-userdb-remote-node`e	The output of this command lists the MAC address and assigned remote-node-profile for each Remote Controller associated with that Remote Controller master.	Enable and Config mode

Command History

Version	Modification
ArubaOS 6.0	Introduced for the first time.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Enable and Config modes on master controllers.

rename

```
rename <filename> <newfilename>
```

Description

This command renames an existing system file.

Syntax

Parameter	Description
`filename`	An alphanumeric string that specifies the current name of the file on the system.
`newfilename`	An alphanumeric string that specifies the new name of the file on the system.

Usage Guidelines

Use this command to rename an existing system file on the controller. You can use a combination of numbers, letters, and punctuation (periods, underscores, and dashes) to rename a file. The new name takes affect immediately.

Make sure the renamed file uses the same file extension as the original file. If you change the file extension, the file may be unrecognized by the system. For example, if you have an existing file named `upgrade.log`, the new file must include the `.log` file extension.

You cannot rename the active configuration currently selected to boot the controller. If you attempt to rename the active configuration file, the controller returns the following message:

```
Cannot rename active configuration file
```

To view a list of system files, and for more information about the directory contents, see "dir" on page 188.

Example

The following command changes the file named **test_configuration** to **deployed_configuration**:

```
(host) (config) #rename test_configuration deployed_configuration
```

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Eanble and Config modes on master controllers

restore

```
restore flash
```

Description

This command restores flash directories backed up to the flashbackup.tar.gz file.

Syntax

Parameter	Description
`flash`	Restores flash directories from the flashbackup.tar.gz file.

Usage Guidelines

Use the **backup flash** command to tar and compress flash directories to the flashbackup.tar.gz file.

Example

The following command restores flash directories from the flashbackup.tar.gz file:

```
(host) #restore flash
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

rf am-scan-profile

```
<profile-name>
   clone <profile>
   dwell-time-active-channel
   dwell-time-other-reg-domain-channel
   dwell-time-other-reg-domain-channel
   no
   scan-mode
```

Description

Configure an Air Monitor (AM) scanning profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this instance of the profile.	1-63 characters	—
`clone <profile>`	Copy data from another AM scanning profile	—	—
`dwell-time-active-channel`	Dwell time (in ms) for channels where there is wireless activity.	100-32768 ms	500 ms
`dwell-time-other-reg-domain-channel`	Dwell time (in ms) for channels not in the APs regulatory domain.	100-32768 ms	250 ms
`dwell-time-rare-reg-domain-channel`	Dwell time (in ms) for rare channels.	100-32768 ms	100 ms
`dwell-time-reg-domain-channel`	Dwell time (in ms) for AP's Regulatory domain channels	100-32768 ms	250 ms
`no`	Delete the command	—	—
`scan-mode`	Set the scanning mode for the radio.	—	—
`all-reg-domain`	Scan channels in all regulatory domain	—	—
`rare`	Scan *all* channels (all regulatory domains and rare channels)	—	—
`reg-domain`	Scan channels in the APs regulatory domain	—	—

Command History

Release	Modification
ArubaOS 6.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All Platforms	RFProtect	Configuration Mode (config)

rf arm-profile

```
rf arm-profile <profile>
   40MHz-allowed-bands {All|None|a-only|g-only}
   acceptable-coverage-index <number>
   active-scan (not intended for use)
   assignment {disable|maintain|multi-band|single-band}
   backoff-time <seconds>
   client-aware
   clone <profile>
   error-rate-threshold <percent>
   error-rate-wait-time <seconds>
   free-channel-index <number>
   ideal-coverage-index <number>
   load-aware-scan-threshold
   max-tx-power <dBm>
   min-scan-time <# of scans>
   min-tx-power <dBm>
   mode-aware
   multi-band-scan
   no ...
   noise-threshold <number>
   noise-wait-time <seconds>
   ps-aware-scan
   rogue-ap-aware
   scan-interval <seconds>
   scan mode all-reg-domain|reg-domain
   scan-time <milliseconds>
   scanning
   video-aware-scan
   voip-aware-scan
```

Description

This command configures the Adaptive Radio Management (ARM) profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`40MHz-allowed- bands`	The specified setting allows ARM to determine if 40 MHz mode of operation is allowed on the 5 GHz or 2.4 GHz frequency band only, on both frequency bands, or on neither frequency band.	All/None/ a-only/g-only	a-only
`All`	Allows 40 MHz channels on both the 5 GHZ (802.11a) and 2.4 GHZ (802.11b/g) frequency bands.		
`None`	Disallows use of 40 MHz channels.		
`a-only`	Allows use of 40 MHz channels on the 5 GHZ (802.11a) frequency band only.		
`g-only`	Allows use of 40 MHz channels on the 2.4 GHZ (802.11b/g) frequency band only.		
`acceptable-cov erage-index`	The minimal coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. This setting applies to multi-band implementations only.	1-6	4
`active-scan`	When the **Active Scan** checkbox is selected, an AP initiates active scanning via probe request. This option elicits more information from nearby APs, but also creates additional management traffic on the network. **Active Scan** is disabled by default, and should *not be enabled* except under the direct supervision of Dell Support. Default: disabled		disabled
`assignment`	Activates one of four ARM channel/power assignment modes.	—	single-band (new installations only)
`disable`	Disables ARM channel/power assignments.		
`maintain`	Maintains existing channel assignments.		
`multi-band`	Computes ARM assignments for both 5 GHZ (802.11a) and 2.4 GHZ (802.11b/g) frequency bands.		
`single-band`	Computes ARM assignments for a single band.		
`backoff-time`	Time, in seconds, an AP backs off after requesting a new channel or power.	120-3600	240 seconds
`client-aware`	If the Client Aware option is enabled, the AP does not change channels if there is active client traffic on that AP. If Client Aware is disabled, the AP may change to a more optimal channel, but this change may also disrupt current client traffic.	—	enabled
`clone`	Name of an existing ARM profile from which parameter values are copied.	—	—
`error-rate- threshold`	The percentage of errors in the channel that triggers a channel change. Recommended value is 50%.	0-100	50%
`error-rate-wait -time`	Time, in seconds, that the error rate has to be at least the error rate threshold to trigger a channel change.	1-2,147,483,647 Recommended Values: 1-100	30 seconds

Parameter	Description	Range	Default
`free-channel-index`	The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel. Recommended value is 25.	10-40	25
`ideal-coverage-index`	The coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. Recommended value is 10.	2-20	10
`load-aware-scan-threshold`	Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high. The Load Aware Scan Threshold is the traffic throughput level an AP must reach before it stops scanning. The supported range for this setting is 0-20000000 bytes/second. (Specify 0 to disable this feature.)		1250000 bytes/ second
`max-tx-power`	Maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links. This value takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 127	127 dBm
`min-scan-time`	Minimum number of times a channel must be scanned before it is considered for assignment. The supported range for this setting is 0-2,147,483,647 scans. Best practices are to configure a Minimum Scan Time between 1-20 scans. Default: 8 scans	1-2,147,483,647 Recommended Values: 1-20	8 scans
`min-tx-power`	Minimum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory minimum.This value takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 127	9 dBm
`mode-aware`	If enabled, ARM will turn APs into Air Monitors (AMs) if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (e.g. less than 60 feet apart).	—	disabled
`multi-band-scan`	When enabled, single-radio APs try to scan across bands for rogue AP detection.	—	enabled
`no`	Negates any configured parameter.	—	—
`noise-threshold`	Maximum level of noise in a channel that triggers a channel change (-dBm).	0-2,147,483,647 Recommended Values: 0-80 -dBm	75 -dBm
`noise-wait-time`	Minimum time in seconds the noise level has to exceed the Noise Threshold before it triggers a channel change.	1-3600	120 seconds
`ps-aware-scan`	When enabled, the AP will not scan if Power Save is active.	—	enabled
`rogue-ap-aware`	When enabled, the AP will try to contain off-channel rogue APs.	—	disabled

Parameter	Description	Range	Default
scan-interval	If Scanning is enabled, the Scan Interval defines how often the AP will leave its current channel to scan other channels in the band. Off-channel scanning can impact client performance. Typically, the shorter the scan interval, the higher the impact on performance. If you are deploying a large number of new APs on the network, you may want to lower the Scan Interval to help those APs find their optimal settings more quickly. Raise the Scan Interval back to its default setting after the APs are functioning as desired.	0-2,147,483,647 Recommended Values: 0-30	10 seconds
scan-mode	Select the scan mode for the AP. • **all-reg-domain**: The AP scans channels within all regulatory domains. This is the default setting. • **reg-domain**:Limit the AP scans to just the regulatory domain for that AP.		all-reg-domain
scan-time	The amount of time, in milliseconds, an AP will drift out of the current channel to scan another channel.	50-2,147, 483,647 Recommended Values: 50-200	110 milliseconds
scanning	The Scanning checkbox enables or disables AP scanning across multiple channels. Disabling this option also disables the following scanning features: • Multi Band Scan • Rogue AP Aware • Voip Aware Scan • Power Save Scan Do not disable Scanning unless you want to disable ARM and manually configure AP channel and transmission power.	—	enabled
video-aware-scan	As long as there is at least one video frame every 100 mSec the AP will reject an ARM scanning request. Note that for each radio interface, video frames must be defined in one of two ways: • Classify the frame as video traffic via a session ACL. • Enable WMM on the WLAN's SSID profile and define a specific DSCP value as a video stream. Next, create a session ACL to tag the video traffic with the that DSCP value.	—	enabled
voip-aware-scan	Dell's VoIP Call Admission Control (CAC) prevents any single AP from becoming congested with voice calls. When you enable CAC, you should also enable **voip-aware-scan** parameter in the ARM profile, so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that **scanning** is also enabled.	—	disabled

Usage Guidelines

Adaptive Radio Management (ARM) is a radio frequency (RF) resource allocation algorithm that allows each AP to determine the optimum channel selection and transmit power setting to minimize interference and maximize coverage and throughput. This command configures an ARM profile that you apply to a radio profile for the 5 GHz or 2.4 GHz frequency band (see “rf dot11a-radio-profile” on page 397 or “rf dot11g-radio-profile” on page 403).

If you were running an earlier version of ArubaOS with ARM disabled, ARM remains disabled when you upgrade to the current release.

Note: AP configuration settings related to the IEEE 802.11n standard are configurable for Dell's W-AP120 series access points, which are IEEE 802.11n standard compliant devices.

Using Adaptive Radio Management (ARM) in a Remote Network

Starting in ArubaOS 3.4.1.x-rn 4.0, the ARM feature can be used by remote APs in bridge mode. Earlier versions of ArubaOS supported ARM on campus APs only.

Using Adaptive Radio Management (ARM) in a Mesh Network

When a mesh portal operates on a mesh network, the mesh portal determines the channel used by the mesh feature. When a mesh point locates an upstream mesh portal, it will scan the regulatory domain channels list to determine the channel assigned to it, for a mesh point always uses the channel selected by its mesh portal. However, if a mesh portal uses an ARM profile enabled with a single-band or multi-band channel/power assignment and the scanning feature, the mesh portal will scan the configured channel lists and the ARM algorithm will assign the proper channel to the mesh portal.

If you are using ARM in your network, is important to note that mesh points, unlike mesh portals, do not scan channels. This means that once a mesh point has selected a mesh portal or an upstream mesh point, it will tune to this channel, form the link, and will not scan again unless the mesh link gets broken. This provides good mesh link stability, but may adversely affect system throughput in networks with mesh portals and mesh points. When ARM assigns optimal channels to mesh portals, those portals use different channels, and once the mesh network has formed and all the mesh points have selected a portal (or upstream mesh point), those mesh points will not be able to detect other portals on other channels that could offer better throughput. This type of suboptimal mesh network may form if, for example, two or three mesh points select the same mesh portal after booting, form the mesh network, and leave a nearby mesh portal without any mesh points. Again, this will not affect mesh functionality, but may affect total system throughput.

Example

The following command configures VoIP-aware scanning for the arm-profile named "voice-arm:"

```
(config) (host) #rf arm-profile voice-arm
   voip-aware-scan
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3.	Support for the high-throughput IEEE 802.11n standard was introduced
ArubaOS 3.3.2	Support for the **wait-time** parameter was removed.
ArubaOS 3.4.1	The **voip-aware-scan** parameter no longer requires a license, and is available in the base OS.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

rf dot11a-radio-profile

```
rf dot11a-radio-profile <profile>
   am-scan-profile <profile-name>
   arm-profile <profile>
   beacon-period <milliseconds>
   beacon-regulate
   cap-reg-eirp <cap-reg-eirp>
   channel <num|num+|num->
   channel-reuse {static|dynamic|disable}
   channel-reuse-threshold
   clone <profile>
   csa
   csa-count <number>
   disable-arm-wids-function
   dot11h
   high-throughput-enable
   ht-radio-profile <profile>
   maximum-distance <maximum-distance>
   mgmt-frame-throttle-interval <seconds>
   mgmt-frame-throttle-limit <number>
   mode {ap-mode|am-mode|spectrum-mode}
   no ...
   radio-enable
   slb-mode channel|radio
   slb-update-interval <secs>
   spectrum-load-bal-domain
   spectrum-load-balancing
   tpc-power <tpc-power>
   tx-power <dBm>
```

Description

This command configures AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`am-scan-profile <name>`	Configure an Air Monitor (AM) scanning profile	—	"default"
`arm-profile`	Configures Adaptive Radio Management (ARM) feature. See "rf arm-profile" on page 391.	—	"default"
`beacon-period`	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.	60 (minimum)	100 milliseconds
`beacon-regulate`	Enabling this setting introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air.	—	disabled
`cap-reg-eirp <cap-reg-eirp>`	Work around a known issue on Cisco 7921G telephones by specfying a cap for an radio's maximum equivalent isotropic radiated power (EIRP). When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise onlythis capped maximum EIRP in its radio beacons.	1–31 dBm.	
`channel`	Channel number for the AP 802.11a/802.11n physical layer. The available channels depend on the regulatory domain (country). Channel number configuration options for 20 MHz and 40 MHz modes: • **num**: Entering a channel number disables 40 MHz mode and activates 20 MHz mode for the entered channel. • **num+**: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 157+ represents 157 as the primary channel and 161 as the secondary channel. • **num-**: Entering a channel number with a minus (-) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 157- represents 157 as the primary channel and 153 as the secondary channel. **NOTE:** 20 MHz clients are allowed to associate when a primary and secondary channel are configured; however, the client will only use the primary channel.	Depends on regulatory domain	—

Parameter	Description	Range	Default
`channel-reuse`	When you enable the channel reuse feature, it can operate in either of the following three modes; static, dynamic or disable. (This feature is disabled by default.) • **Static mode**: This mode of operation is a coverage-based adaptation of the Clear Channel Assessment (CCA) thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. • **Dynamic mode**: In this mode, the Clear Channel Assessment (CCA) thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. • **Disable mode**: This mode does not support the tuning of the CCA Detect Threshold.	enabled disabled	enabled
`channel-reuse-threshold`	RX Sensitivity Tuning Based Channel Reuse Threshold, in - dBm. If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (in -dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. If the value is set to zero, the feature will automatically determine an appropriate threshold.	Depends on regulatory domain	—
`clone`	Name of an existing radio profile from which parameter values are copied.	—	—
`csa`	Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. Clients must support CSA in order to track the channel change without experiencing disruption.	—	disabled
`csa-count`	Number of CSA announcements that are sent before the AP begins transmitting on the new channel.	1-16	4
`disable-arm-wids-function`	Disables Adaptive Radio Management (ARM) and Wireless IDS functions. These can be disabled if a small increase in packet processing performance is desired. If a radio is configured to operate in Air Monitor mode, then these functions are always enabled irrespective of this option. CAUTION: Use carefully, since this effectively disables ARM and WIDS	1-16	4
`dot11h`	Enable advertisement of 802.11d (Country Information) and 802.11h (TPC or Transmit Power Control) capabilities This parameter is enabled by default.	—	enabled
`high-throughput-enable`	Enables high-throughput (802.11n) features on a radio using the 5 GHz frequency band.	—	enabled
`ht-radio-profile`	Name of high-throughput radio profile to use for configuring high-throughput support on the 5 GHz frequency band. See "rf ht-radio-profile" on page 412.	—	"default-a"

Parameter	Description	Range	Default
`maximum-distance`	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km. The upper limit for this parameter varies, depending on the 20/40 MHz mode for a 5 GHz frequency band radio: • 20MHz mode: 58km • 40MHz mode: 27km Note that if you configure a value above the supported maximum, the maximum supported value will be used instead. Values below 600m will use default settings.	0-57km (40MHz mode) 0-27km (20MHz mode)	0 meters
`mgmt-frame-throttle-interval`	Averaging interval for rate limiting management frames in seconds. Zero disables rate limiting. Note: This parameter only applies to AUTH and ASSOC/ RE-ASSOC management frames.	0-60	1 second interval
`mgmt-frame-throttle-limit`	Maximum number of management frames allowed in each throttle interval. **NOTE:** This parameter only applies to AUTH and ASSOC/ RE-ASSOC management frames.	0-999999	20 frames per interval
`mode`	One of the operating modes for the AP.		ap-mode
`ap-mode`	Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN.		
`am-mode`	Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.		
`spectrum-mode`	Device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.		
`no`	Negates any configured parameter.	—	—
`radio-enable`	Enables or disables radio configuration.	—	enabled
`slb-mode channel|radio`	SLB Mode allows control over how to balance clients. Slect one of the following optoins • **channel**: Channel-based load-balancing balances clients across channels. This is the default load-balancing mode • **radio**: Radio-based load-balancing balances clients across APs		channel
`slb-update-interval <secs>`	Specify how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.	1-2147483647 seconds	30 seconds

Parameter	Description	Range	Default
`spectrum-load-bal-domain`	Define a spectrum load balancing domain to manually create RF neighborhoods. Use this option to create RF neighborhood information for networks that have disabled Adaptive Radio Management (ARM) scanning and channel assignment. • If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is *not* defined, ArubaOS uses the ARM feature to calculate RF neighborhoods. • If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain *is also* defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by the ARM feature.	—	—
`spectrum-load-balancing`	The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests. If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Dell AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default. **NOTE:** The spectrum load balancing feature available in ArubaOS 3.4.x and later releases completely replaces the AP load balancing feature available in earlier versions of ArubaOS. When you upgrade to ArubaOS 3.4.x or later, you must manually configure the spectrum load balancing settings, as the AP load balancing feature can no longer be used, and any previous AP load balancing settings will not be preserved.	—	disabled
`tpc-power`	The transmit power advertised in the TPC IE of beacons and probe responses. Range: 0-51 dBm	0-51 dBm	15 dBm
`tx-power`	Sets the initial transmit power (dBm) on which the AP operates, unless a better choice is available through either calibration or from RF Plan. This parameter can be set from 0 to 51 in .5 dBm increments, or set to the regulatory maximum value of 127 dBm. Transmission power may be further limited by regulatory domain constraints and AP capabilities.	0-51 dBm, 127 dBm	14 dBm

Usage Guidelines

This command configures radios that operate in the 5 GHz frequency band, which includes radios utilizing the IEEE 802.11a or IEEE 802.11n standard. Channels must be valid for the country configured in the AP regulatory domain profile (see "ap regulatory-domain-profile" on page 108).

To view the supported channels, use the **show ap allowed-channels** command.

Examples

The following command configures APs to operate in AM mode for the selected dot11a-radio-profile named "samplea:"

```
(host) (config) #rf dot11a-radio-profile samplea mode am-mode
```

The following command configures APs to operate in high-throughput (802.11n) mode on the 5 Ghz frequency band for the selected dot11a-radio profile named “samplea” and assigns a high-throughout radio profile named “default-a:”

```
(host) (config) #rf dot11a-radio-profile samplea
   high-throughput-enable
   ht-radio-profile default-a
```

The following command configures a primary channel number of 157 and a secondary channel number of 161 for 40 MHz mode of operation for the selected dot11a-radio profile named “samplea:”

```
(host) (config) #rf dot11a-radio-profile samplea
   channel <157+>
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3.2	Introduced support for the high-throughput IEEE 802.11n standard.
ArubaOS 3.4	Support for the following parameters: • Spectrum load balancing • Spectrum load balancing domain • RX Sensitivity Tuning Based Channel Reuse • RX Sensitivity Threshold • ARM/WIDS Override
ArubaOS 3.4.1	The **maximum-distance** parameter was introduced.
ArubaOS 3.4.2	The **beacon-regulate** parameter was introduced.
ArubaOS 6.0	Added support to configure an Air Monitor (AM) scanning profile (am-scan-profile)

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

rf dot11g-radio-profile

```
rf dot11g-radio-profile <profile>
   am-scan-profile <profile-name>
   arm-profile <profile>
   beacon-period <milliseconds>
   beacon-regulate
   cap-reg-eirp <cap-reg-eirp>
   channel <num|num+|num->
   channel-reuse {static|dynamic|disable}
   channel-reuse-threshold
   clone <profile>
   csa
   csa-count <number>
   disable-arm-wids-function
   dot11b-protection
   dot11h
   high-throughput-enable
   ht-radio-profile <profile>
   interference-immunity
   maximum-distance <maximum-distance>
   mgmt-frame-throttle-interval <seconds>
   mgmt-frame-throttle-limit <number>
   mode {ap-mode|am-mode|spectrum-mode}
   no ...
   radio-enable
   slb-mode channel|radio
   slb-update-interval <secs>
   spectrum-load-bal-domain
   spectrum-load-balancing
   tpc-power <tpc-power>
   tx-power <dBm>
```

Description

This command configures AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`am-scan-profile <profile-name>`	Configure an Air Monitor (AM) scanning profile.	—	—
`arm-profile`	Configures Adaptive Radio Management (ARM) feature. See "rf arm-profile" on page 391.	—	"default"
`beacon-period`	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.	60 (minimum)	100 milliseconds
`beacon-regulate`	Enabling this setting introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air.	—	disabled
`cap-reg-eirp <cap-reg-eirp>`	Work around a known issue on Cisco 7921G telephones by specfying a cap for an radio's maximum equivalent isotropic radiated power (EIRP). When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise onlythis capped maximum EIRP in its radio beacons.	1–31 dBm.	
`clone`	Name of an existing radio profile from which parameter values are copied.	—	—
`csa`	Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. Clients must support CSA in order to track the channel change without experiencing disruption.	—	disabled
`csa-count`	Number of CSA announcements that are sent before the AP begins transmitting on the new channel.	1-16	4
`channel`	Channel number for the AP 802.11a/802.11n physical layer. The available channels depend on the regulatory domain (country). Channel number configuration options for 20 MHz and 40 MHz modes: • **num**: Entering a channel number disables 40 MHz mode and activates 20 MHz mode for the entered channel. • **num+**: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 157+ represents 157 as the primary channel and 161 as the secondary channel. • **num-**: Entering a channel number with a minus (-) sign selects a primary and secondary channel for 40 MHz mode. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 157- represents 157 as the primary channel and 153 as the secondary channel. **NOTE:** 20 MHz clients are allowed to associate when a primary and secondary channel are configured; however, the client will only use the primary channel.	Depends on regulatory domain	—

Parameter	Description	Range	Default
channel-reuse	When you enable the channel reuse feature, it can operate in either of the following three modes; static, dynamic or disable. (This feature is disabled by default.) • **Static mode**: This mode of operation is a coverage-based adaptation of the Clear Channel Assessment (CCA) thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. • **Dynamic mode**: In this mode, the Clear Channel Assessment (CCA) thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. • **Disable mode**: This mode does not support the tuning of the CCA Detect Threshold.	enabled disabled	enabled
channel-reuse-threshold	RX Sensitivity Tuning Based Channel Reuse Threshold, in -dBm. If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (in -dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. If the value is set to zero, the feature will automatically determine an appropriate threshold.	Depends on regulatory domain	—
disable-arm-wids-function	Disables Adaptive Radio Management (ARM) and Wireless IDS functions. These can be disabled if a small increase in packet processing performance is desired. If a radio is configured to operate in Air Monitor mode, then these functions are always enabled irrespective of this option. CAUTION: Use carefully, since this effectively disables ARM and WIDS	1-16	4
dot11b-protection	Enable or disable protection for 802.11b clients. This parameter is enabled by default. Disabling this feature may improve performance if there are no 802.11b clients on the WLAN. WARNING: Disabling protection violates the 802.11 standard and may cause interoperability issues. If this feature is disabled on a WLAN with 802.11b clients, the 802.11b clients will not detect an 802.11g client talking and can potentially transmit at the same time, thus garbling both frames.	—	enabled
dot11h	Enable advertisement of 802.11d (Country Information) and 802.11h (TPC or Transmit Power Control) capabilities This parameter is enabled by default.	—	enabled
high-throughput-enable	Enables high-throughput (802.11n) features on a radio using the 2.4 GHz frequency band.	—	enabled
ht-radio-profile	Name of high-throughput radio profile to use for configuring high-throughput support on the 5 GHz frequency band. See "rf ht-radio-profile" on page 412.	—	"default-a"

Parameter	Description	Range	Default
`interference-immunity`	Set a value for 802.11 Interference Immunity. This parameter sets the interference immunity on the 2.4 Ghz band. The default setting for this parameter is level 2. When performance drops due to interference from non-802.11 interferers (such as DECT or Bluetooth devices), the level can be increased up to level 5 for improved performance. However, increasing the level makes the AP slightly "deaf" to its surroundings, causing the AP to lose a small amount of range. The levels for this parameter are: • Level-0: no ANI adaptation. • Level-1: noise immunity only. • Level-2: noise and spur immunity. This is the default setting • Level-3: level 2 and weak OFDM immunity. • Level-4: level 3 and FIR immunity. • Level-5: disable PHY reporting. **NOTE:** Do not raise the noise immunity feature's default setting if the channel-reuse-threshold feature is also enabled. A level-3 to level-5 Noise Immunity setting is not compatible with the Channel Reuse feature.	Level-0 - Level-5	Level-2
`maximum-distance`	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km. The upper limit for this parameter varies, depending on the 20/40 MHz mode for a 2.4GHz frequency band radio: • 20MHz mode: 54km • 40MHz mode: 24km Note that if you configure a value above the supported maximum, the maximum supported value will be used instead. Values below 600m will use default settings.	0-24km (40MHz mode) 0-54km (20MHz mode)	0 meters
`mgmt-frame-throttle-interval`	Averaging interval for rate limiting management frames in seconds. Zero disables rate limiting. Note: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.	0-60	1 second interval
`mgmt-frame-throttle-limit`	Maximum number of management frames allowed in each throttle interval. **NOTE:** This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.	0-999999	20 frames per interval
`mode`	One of the operating modes for the AP.		ap-mode
`ap-mode`	Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN.		
`am-mode`	Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.		
`spectrum-mode`	Device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.		
`no`	Negates any configured parameter.	—	—
`radio-enable`	Enables or disables radio configuration.	—	enabled

Parameter	Description	Range	Default
`slb-mode channel|radio`	SLB Mode allows control over how to balance clients. Slect one of the following optoins • **channel**: Channel-based load-balancing balances clients across channels. This is the default load-balancing mode • **radio**: Radio-based load-balancing balances clients across APs		channel
`slb-update-interval <secs>`	Specify how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.	1-2147483647 seconds	30 seconds
`spectrum-load-bal-domain`	Define a spectrum load balancing domain to manually create RF neighborhoods. Use this option to create RF neighborhood information for networks that have disabled Adaptive Radio Management (ARM) scanning and channel assignment. • If spectrum load balancing is enabled in a 802.11g radio profile but the spectrum load balancing domain is *not* defined, ArubaOS uses the ARM feature to calculate RF neighborhoods. • If spectrum load balancing is enabled in a 802.11g radio profile and a spectrum load balancing domain *is also* defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by the ARM feature.	—	—
`spectrum-load-balancing`	The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests. If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Dell AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default. **NOTE:** The spectrum load balancing feature available in ArubaOS 3.4.x and later releases completely replaces the AP load balancing feature available in earlier versions of ArubaOS. When you upgrade to ArubaOS 3.4.x or later, you must manually configure the spectrum load balancing settings, as the AP load balancing feature can no longer be used, and any previous AP load balancing settings will not be preserved.	—	disabled
`tpc-power`	The transmit power advertised in the TPC IE of beacons and probe responses. Range: 0-51 dBm	0-51 dBm	15 dBm
`tx-power`	Sets the initial transmit power (dBm) on which the AP operates, unless a better choice is available through either calibration or from RF Plan. This parameter can be set from 0 to 51 in .5 dBm increments, or set to the regulatory maximum value of 127 dBm. Transmission power may be further limited by regulatory domain constraints and AP capabilities.	0-51 dBm, 127 dBm	14 dBm

Usage Guidelines

This command configures radios that operate in the 2.4 GHz frequency band, which includes radios utilizing the IEEE 802.11b/g or IEEE 802.11n standard. Channels must be valid for the country configured in the AP regulatory domain profile (see “ap regulatory-domain-profile” on page 108).

To view the supported channels, use the **show ap allowed-channels** command.

Examples

The following command configures APs to operate in AM mode for the selected dot11g-radio-profile named “sampleg:”

```
rf dot11g-radio-profile sampleg
   mode am-mode
```

The following command configures APs to operate in high-throughput (802.11n) mode on the 2.4 Ghz frequency band for the selected dot11g-radio profile named “sampleg” and assigns a high-throughout radio profile named “default-g:”

```
rf dot11g-radio-profile sampleg
   high-throughput-enable
   ht-radio-profile default-g
```

The following command configures a primary channel number of 1 and a secondary channel number of 5 for 40 MHz mode of operation for the selected dot11g-radio profile named “sampleg:”

```
rf dot11g-radio-profile sampleg
   channel <1+>
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3.2	Introduced protection for 802.11b clients and support for the high-throughput IEEE 802.11n standard.
ArubaOS 3.4	Support for the following parameters: • Spectrum load balancing • Spectrum load balancing domain • RX Sensitivity Tuning Based Channel Reuse • RX Sensitivity Threshold • ARM/WIDS Override
ArubaOS 3.4.1	The **maximum-distance** parameter was introduced.
ArubaOS 3.4.2	The **beacon-regulate** parameter was introduced.
ArubaOS 6.0	Configure an Air Monitor (AM) scanning profile (am-scan-profile)

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

rf event-thresholds-profile

```
rf event-thresholds-profile <profile>
   bwr-high-wm <percent>
   bwr-low-wm <percent>
   clone <profile>
   detect-frame-rate-anomalies
   fer-high-wm <percent>
   fer-low-wm <percent>
   ffr-high-wm <percent>
   ffr-low-wm <percent>
   flsr-high-wm <percent>
   flsr-low-wm <percent>
   fnur-high-wm <percent>
   fnur-low-wm <percent>
   frer-high-wm <percent>
   frer-low-wm <percent>
   frr-high-wm <percent>
   frr-low-wm <percent>
   no ...
```

Description

This command configures the event thresholds profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`bwr-high-wm`	If bandwidth in an AP exceeds this value, a bandwidth exceeded condition exists. The value represents the percentage of maximum for a given radio. (For 802.11b, the maximum bandwidth is 7 Mbps. For 802.11 a and g, the maximum is 30 Mbps.) The recommended value is 85%.	0-100	0%
`bwr-low-wm`	After a bandwidth exceeded condition exists, the condition persists until bandwidth drops below this value. The recommended value is 70%.	0-100	0%
`clone`	Name of an existing radio profile from which parameter values are copied.	—	—
`detect-frame-rate-anomalies`	Enable or disables detection of frame rate anomalies.	—	disabled
`fer-high-wm`	If the frame error rate (as a percentage of total frames in an AP) exceeds this value, a frame error rate exceeded condition exists. The recommended value is 16%.	0-100	0%
`fer-low-wm`	After a frame error rate exceeded condition exists, the condition persists until the frame error rate drops below this value. The recommended value is 8%.	0-100	0%
`ffr-high-wm`	If the frame fragmentation rate (as a percentage of total frames in an AP) exceeds this value, a frame fragmentation rate exceeded condition exists. The recommended value is 16%.	0-100	16%
`ffr-low-wm`	After a frame fragmentation rate exceeded condition exists, the condition persists until the frame fragmentation rate drops below this value. The recommended value is 8%.	0-100	8%
`flsr-high-wm`	If the rate of low-speed frames (as a percentage of total frames in an AP) exceeds this value, a low-speed rate exceeded condition exists. This could indicate a coverage hole. The recommended value is 16%.	0-100	16%
`flsr-low-wm`	After a low-speed rate exceeded condition exists, the condition persists until the percentage of low-speed frames drops below this value. The recommended value is 8%.	0-100	8%
`fnur-high-wm`	If the non-unicast rate (as a percentage of total frames in an AP) exceeds this value, a non-unicast rate exceeded condition exists. This value depends upon the applications used on the network.	0-100	0%
`fnur-low-wm`	After a non-unicast rate exceeded condition exists, the condition persists until the non-unicast rate drops below this value.	0-100	0%
`frer-high-wm`	If the frame receive error rate (as a percentage of total frames in an AP) exceeds this value, a frame receive error rate exceeded condition exists. The recommended value is 16%.	0-100	16%
`frer-low-wm`	After a frame receive error rate exceeded condition exists, the condition persists until the frame receive error rate drops below this value. The recommended value is 8%.	0-100	8%

Parameter	Description	Range	Default
`frr-high-wm`	If the frame retry rate (as a percentage of total frames in an AP) exceeds this value, a frame retry rate exceeded condition exists. The recommended value is 16%.	0-100	16%
`frr-low-wm`	After a frame retry rate exceeded condition exists, the condition persists until the frame retry rate drops below this value. The recommended value is 8%.	0-100	8%
no	Negates any configured parameter.	—	—

Usage Guidelines

The event threshold profile configures Received Signal Strength Indication (RSSI) metrics. When certain RF parameters are exceeded, these events can signal excessive load on the network, excessive interference, or faulty equipment. This profile and many of the detection parameters are disabled (value is 0) by default.

Example

The following command configures an event threshold profile:

```
(host) (config) #rf event-thresholds-profile et1
   detect-frame-rate-anomalies
```

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

rf ht-radio-profile

```
rf ht-radio-profile <profile>
   40MHz-intolerance
   clone <profile>
   honor-40MHz-intolerance
   no
   single-chain-legacy
```

Description

This command configures high-throughput AP radio settings. High-throughput features use the IEEE 802.11n standard.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters. Default Options: • "Default-a" is generally used in association with high-throughput devices running on the 5 GHz frequency band, see "rf dot11a-radio-profile" on page 397. • "Default-g" is generally used in association with high-throughput devices running on the 2.4 GHz frequency band, see "rf dot11g-radio-profile" on page 403. • "Default" is generally used when the same ht-radio-profile is desired for use with both frequency bands.	—	default-a default-g default
`40MHz-intolerance`	Controls whether or not APs using this radio profile will advertise intolerance of 40 MHz operation. By default, 40 MHz operation is allowed.	—	disabled
`clone`	Name of an existing high-throughput radio profile from which parameter values are copied.	—	—
`honor-40MHz-intolerance`	When enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.	—	enabled
`no`	Negates any configured parameter.	—	—
`single-chain-legacy`	Interoperability for misbehaving legacy stations (keep disabled unless necessary)		disabled

Usage Guidelines

The ht-radio-profile configures high-throughput settings for networks utilizing the IEEE 802.11n standard, which supports 40 MHZ channels and operates in both the 2.4 GHZ and 5 GHZ frequency bands.

The ht-radio-profile you wish to use must be assigned to a dot11a and/or dot11g-radio-profile. You can assign the same profile or different profiles to the 2.4 GHZ and 5 GHZ frequency bands. See "rf dot11a-radio-profile" on page 397 and "rf dot11g-radio-profile" on page 403.

Example

The following command configures an ht-radio-profile named "default-g" and enables 40MHz-intolerance:

```
(host) (config) #rf ht-radio-profile default-g
   40MHz-intolerance
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3.2	Support for the dsss-cck-40mhz parameter removed
ArubaOS 3.4	Introduced the **single-chain-legacy** parameter.

Command Information

Platforms	Licensing	Command Mode
All platforms, but operates with IEEE 802.11n compliant devices only	Base operating system	Config mode on master controllers

rf optimization-profile

```
rf optimization-profile <profile-name>
   clone <profile>
   handoff-assist
   low-rssi-threshold <number>
   no ...
   rssi-check-frequency <number>
   rssi-falloff-wait-time <seconds>
```

Description

This command configures the RF optimization profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing optimization profile from which parameter values are copied.	—	—
`handoff-assist`	Allows the controller to force a client off an AP when the RSSI drops below a defined minimum threshold.	—	disabled
`low-rssi-threshold`	Minimum RSSI, above which deauth should never be sent.	1-255	0
`no`	Negates any configured parameter.	—	—
`rssi-check-frequency`	Interval, in seconds, to sample RSSI.	9-255	0 seconds
`rssi-falloff-wait-time <seconds>`	Time, in seconds, to wait with decreasing RSSI before deauth is sent to the client. The maximum value is 8 seconds.	0-8	0 seconds

Example

The following command configures an RF optimization profile:

```
(host) (config) #rf optimization-profile Helen1
(host) (RF Optimization Profile "Helen1") #rssi-falloff-wait-time 3
(host) (RF Optimization Profile "Helen1") #rssi-check-frequency 2
```

Command History

Version	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4	The following parameters were deprecated: • ap-lb-max-retries <number> • ap-lb-user-high-wm <percent> • ap-lb-user-low-wm <percent> • ap-lb-util-high-wm <percent> • ap-lb-util-low-wm <percent> • ap-lb-util-wait-time <seconds • ap-load-balancing Use the command rf dot11a-radio-profile spectrum-load-balancing and rf dot11g-radio-profile spectrum-load-balancing to enable the spectrum load balanncing feature.
ArubaOS 5.0	The following parameters were deprecated: • coverage-hole-detection hole-detection-interval • hole-good-rssi-threshold • hole-good-sta-ageout • hole-idle-sta-ageout • hole-poor-rssi-threshold
ArubaOS 6,0	• detect-association-failure • detect-interference • hole-detection-interval • hole-good-rssi-threshold • hole-good-sta-ageout • hole-idle-sta-ageout • hole-poor-rssi-threshold • interference-baseline • interference-exceed-time • interference-threshold

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

rf spectrum-profile

```
rf spectrum-profile <profile-name>
   age-out audio|bluetooth|cordless-ff-phone|cordless-fh-base|cordless-fh-
   network|generic-ff|generic-fh|microwave|microwave-inverter|unknown|video|wifi|xbox
   clone <source>
   no
   spectrum-band 2ghz|5ghz-lower|5ghz-middle|5ghz-upper
```

Description

Define the spectrum band and device ageout times used by a spectrum monitor radio.

Syntax

Parameter	Description	Range	Default
age-out	Use the **age-out** parameter to define the number of seconds for which a specific device type must stop sending a signal before the spectrum monitor considers that device no longer active on the network.		
audio	Audio devices.	5-65535 seconds	10 sec
bluetooth	Bluetooth devices. Note that this setting is applicable to 2.4GHz spectrum monitor radios only.	5-65535 seconds	25 sec
cordless-ff-phone	Cordless phone fixed frequency devices.	5-65535 seconds	10 sec
cordless-fh-base	Cordless base frequency hopper devices.	5-65535 seconds	25 sec
cordless-fh-network	Cordless network frequency hopper devices.	5-65535 seconds	25 sec
generic-ff	Generic fixed frequency devices.	5-65535 seconds	10 sec
generic-fh	Generic frequency hopper devices.	5-65535 seconds	25 sec
generic-interferer	Unknown device type.	5-65535 seconds	25 sec
microwave	Microwaves. Note that this setting is applicable to 2.4GHz spectrum monitor radios only.	5-65535 seconds	15 sec
microwave-inverter	Inverter-type microwaves. Note that this setting is applicable to 2.4GHz spectrum monitor radios only.	5-65535 seconds	15 sec
video	Video devices.	5-65535 seconds	10 sec
wifi	WIFI devices.	5-65535 seconds	
xbox	Xbox consoles. Note that this setting is applicable to 2.4GHz spectrum monitor radios only.	5-65535 seconds	600 sec
clone <source>	Make a copy of an existing spectrum profile.		600 sec
no	Remove a spectrum profile or negate a configured parameter.		
spectrum-band	Define one of the following spectrum bands for the spectrum profile. If you do not select a spectrum band, the profile will use a default setting of 2Ghz. • **2ghz**: Scan 2GHz channels • **5ghz-lower**: Scan 5GHz channels 36-64 • **5ghz-middle**: Scan 5GHz channels 100-140 • **5ghz-upper**: Scan 5GHz channels 149-165	• 2ghz • 5ghz-lower • 5ghz-middle • 5ghz-upper	

Usage Guidelines

The Spectrum Analysis software module provides visibility into RF coverage, allowing you to troubleshoot RF interference and identify the 802.11 devices on the network. APs that gather spectrum data are called Spectrum Monitors, or *SMs*, and reference a spectrum profile that determines the band monitored by that SM radio. Note that you can only convert a radio on an AP model W-AP105, W-AP120 Series, or W-AP90 Series to a spectrum monitor. The spectrum analysis feature is not supported by any other AP model.

Example

The following command creates the spectrum profile **spectrum5**, and configures it to use the upper portion of the 5 Ghz radio band

```
(host) (config) #rf spectrum-profile spectrum5
   5ghz-upper
```

Related Commands

`show rf spectrum-profile`

Command History

Introduced in ArubaOS 6.0

Command Information

Platforms	Licensing	Command Mode
All platforms	RF Protect license	Config mode on master and local controllers

rft

```
rft test profile antenna-connectivity ap-name <name> [dest-mac <macaddr> [phy {a|g}|
radio {0|1}]]

rft test profile link-quality {ap-name <name> dest-mac <macaddr> [phy {a|g}|
 radio {0|1}] | bssid <bssid> dest-mac <macaddr> | ip-addr <ipaddr>
 dest-mac <macaddr> [phy {a|g}|radio {0|1}]}

rft test profile raw {ap-name <name> dest-mac <macaddr> [phy {a|g}|radio {0|1}] | bssid
<bssid> dest-mac <macaddr> | ip-addr <ipaddr> dest-mac <macaddr> [phy {a|g}|radio
{0|1}]}
```

Description

This command is used for RF troubleshooting.

Syntax

Parameter	Description	Range
`ap-name`	Name of the AP that performs the test.	—
`dest-mac`	MAC address of the client to be tested.	—
`phy`	802.11 type, either a or g.	a | g
`radio`	Radio ID, either 0 or 1.	0 | 1
`bssid`	BSSID of the AP that performs the test.	—
`ip-addr`	IP address of the AP that performs the test.	

Usage Guidelines

This command can run predefined test profiles for antenna connectivity, link quality, or raw testing. You should only run these commands when directed to do so by an Dell support representative.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

router mobile

```
router mobile
```

Description

This command enables Layer-3 (IP) mobility.

Syntax

No parameters.

Usage Guidelines

IP mobility is disabled by default on the controller. You need to use this command to enable IP mobility. This command must be executed on all controllers (master and local) that need to provide support for layer-3 roaming in a mobility domain.

You can disable IP mobility in a virtual AP profile with the **wlan virtual-ap** command (IP mobility is enabled by default in a virtual AP profile).

Example

This command enables IP mobility:

(host) (config) #router mobile

Command History

Release	Modification
ArubaOS 3.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

router ospf

```
router ospf
   area <area-id>
      default-cost <cost>
      nssa [default-information no-redistribution | no-summary]
      stub [no-summary]
   default-information originate always
   redistribute vlan [<vlan-ids> | add <vlan-ids> | remove <vlan-ids>]
   router-id <rtr-id>
   subnet exclude <addr> <mask>
```

Description

Global OSPF configuration for the upstream router.

Syntax

Parameter	Description
`area <area-id>`	Enter the keyword area followed by the area identification, in dotted decimal format, to configure an OSPF area.
`default-cost <cost>`	Set the summary cost of a NSSA/stub area (in route metric) Range: 0 to 16777215
`nssa`	Set an area as a NSSA
`default-information-originate`	Originate Type 7 default into the NSSA area
`no-redistribution`	Set the NSSA area for no distribution into this NSSA area
`no-summary`	Do not send summary LSA into this NSSA area
`stub [no-summary]`	Set an area as a Total Stub Area and optionally do not send summary LSA into this area
`default-information originate always`	Control distribution of default information by distributing a default route.
`redistribute vlan <vlan-ids>`	Redistribute the vlan user subnet.
`add <vlan-ids>`	Add the user VLANs to the list
`remove <vlan-ids>`	Remove user VLANs to the list.
`router-id <rtr-id>`	Enter the router ID in IP address format.
`subnet exclude <addr> <mask>`	Specify the subnet that OSPF will *not* advertise. Enter the subnet and mask address in dotted decimal format (A.B.C.D).

Usage Guidelines

OSPFv2 is a dynamic Interior Gateway routing Protocol (IGP) based on IETF RFC 2328. The ArubaOS implementation of OSPF allows controllers to deploy effectively in a Layer 3 topology. For more detailed information, refer to the OSPF Chapter in the ArubaOS User Guide.

Example

By default OSPF will advertise all the user VLAN subnet addresses in the router LSA (Link-State Advertisement). To control the OSPF advertisement, execute the following command:

```
(host) (config) # router ospf subnet exclude 75.1.1.0 255.255.0.0
```

With the above command, any user VLAN subnet matching 75.1/16 will not be advertised in the router LSA. To return to the default advertisement, execute the command:

```
(host) (config) # no router ospf subnet exclude 75.1.1.0 255.255.0.0
```

Related Commands

Command	Description
show ip ospf	View OSPF configuration

Command History

Release	Modification
ArubaOS 3.4	Command introduced
ArubaOS 6.0	Added the options: area, default-cost, nssa, and default-information originate always

Command Information

Platforms	Licensing	Command Mode
All Platforms	Base operating system	Configuration Mode (config)

service

```
service [dhcp] [network-storage] [print-server]
```

Description

This command enables the DHCP server on the controller.

Syntax

Parameter	Description	Default
dhcp	Enables the DHCP server	disabled
network-storage	Enables the NAS service	disabled
print-server	Enables the printer service	disabled

Usage Guidelines

You can enable and configure DHCP, network-storage or print server in the controller to provide the following:

- DHCP: IP addresses to wireless clients if an external DHCP server is not available.
- Network-storage: To provide access to the storage devices attached to the controller.
- Printer-server: To provide access to printers attached to the controller.

Example

The following command enables the DHCP server in the controller:

```
(host) (config) #service dhcp
```

The following command enables the NAS services in the controller:

(host) (config) #service network-storage

The following command enables the printer services in the controller:

(host) (config) #service print-server

Command History

The DHCP command was introduced in ArubaOS 3.0.

The network-storage and print-server options was introduced in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show aaa authentication all

```
show
show aaa authentication all
```

Description

Show authentication statistics for your controller, including authentication methods, successes and failures.

Usage Guidelines

This command displays a general overview of authentication statistics. To view authentication information for specific profiles such as a captive-portal, MAC or 801.x authentication profile, issue the commands specific to those features.

Example

The output of this command displays an authentication overview for your controller, including the authentication methods used, and the numbers of successes or failures for each method. This example shows the numbers of authentication successes and failures for a controller using TACACS+ and RADIUS authentication methods.

```
(host) #show aaa authentication all

Auth Method Statistics
----------------------
Method  Success  Failures
------  -------  --------
tacacs    12       2
Radius    9        1
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show aaa authentication captive-portal

```
show aaa authentication captive-portal [<profile-name>]
```

Description

This command shows configuration information for captive portal authentication profiles.

Syntax

Parameter	Description
<profile-name>	The name of an existing captive portal authentication profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire Captive Portal Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

If you do not yet have any captive portal authentication profiles defined, use the command aaa authentication captive-portal to configure your captive portal profiles.

Examples

This first example shows that there are three configured captive portal profiles in the Captive Profile Authentication Profile List. The **References** column lists the number of other profiles with references to a captive portal authentication profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication captive-portal

Captive Portal Authentication Profile List
------------------------------------------
Name            References  Profile Status
----            ----------  --------------
c-portal        2
remoteuser      1
portal1         1

Total: 4
```

Include a captive portal profile name to display a complete list of configuration settings for that profile. The example below shows settings for the captive portal profile *portal1*.

```
Captive Portal Authentication Profile "portal1"
-----------------------------------------------
Parameter                                 Value
---------                                 -----
Default Role                              guest
Server Group                              default
Redirect Pause                            10 sec
User Login                                Enabled
Guest Login                               Disabled
Logout popup window                       Enabled
Use HTTP for authentication               Disabled
Logon wait minimum wait                   5 sec
Logon wait maximum wait                   10 sec
logon wait CPU utilization threshold      60%
Max Authentication failures               0
Show FQDN                                 Disabled
Use CHAP (non-standard)                   Disabled
Sygate-on-demand-agent                    Disabled
Login page                                /auth/index.html
Welcome page                              /auth/welcome.html
Show Welcome Page                         Yes
Adding switch ip address in redirection URL  Disabled
Allow only one active user session        Disabled
```

The output of this command includes the following parameters:

Parameter	Description
`Default Role`	Role assigned to the captive portal user upon login.
`Server Group`	Name of the group of servers used to authenticate captive portal users.
`Redirect Pause`	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link.
`User Login`	Shows whether the profile has enabled or disabled captive portal with authentication of user credentials.
`Guest Login`	Shows whether the profile has enabled or disabled captive portal guest login without authentication.
`Logout popup window`	Shows whether the profile has enabled or disabled a pop-up window that allows a user to log out. If this is disabled, the user remains logged in until the user timeout period has elapsed or the station resets.
`Use HTTP for authentication`	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.
`Login wait minimum time`	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high.
`logon wait CPU utilization threshold`	CPU utilization percentage above which the logon wait interval is applied when directing a captive portal user with the logon page.
`Max Authentication failures`	Maximum number of authentication failures before the user is blacklisted.
`Show FQDN`	If enabled, the user can see and select the fully-qualified domain name (FQDN) on the captive portal login page.
`Use CHAP (non-standard)`	If enabled, the captive portal profile can use the CHAP protocol.

Parameter	Description
`Sygate-on-demand-agent`	Shows whether the controller has enabled or disabled client remediation with Sygate-on-demand-agent.
`Login page`	URL of the page that appears for the user logon.
`Welcome page`	URL of the page that appears after logon and before the user is redirected to the web URL.

Related Commands

Command	Description	Mode
`aaa authentication captive-portal`	Use **`aaa authentication captive-portal`** to configure the parameters displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication captive-portal customization

```
show aaa authentication captive-portal customization <profile-name>
```

Description

Display customization settings for a captive portal profile

Syntax

Parameter	Description
`<profile-name>`	The name of an existing captive portal authentication profile.

Usage Guidelines

The this command shows how a captive portal profile has been customized with non-default configuration settings. If you do not yet have any captive portal authentication profiles defined, use the command `aaa authentication captive-portal` to configure your captive portal profiles

Example

The output of the following command shows how the captive portal profile *c-portal* has been customized. If an individual parameter has not been changed from its default settings, its value entry will be blank.

```
(host) #show aaa authentication captive-portal customization c-portal

Captive-Portal Customization
----------------------------
Parameter Value
--------- -----
Login page design theme 3
Login page logo image
Login page text URL/flash/upload/custom/ssu-guest-cp/logintext.html
Login policy text URL/upload/custom/ssu-guest-cp/acceptableusepolicy.html
Custom page background color
Custom page background image    /upload/custom/default/auth-slider-1.gif
```

The output of this command includes the following parameters:

Parameters	Description
`Login page design theme`	Indicates whether the controller is using one of the two predefined login page designs (**1** or **2**) or has a custom background (**3**).
`Login page logo image`	Path and filename for a custom captive portal logo. This option is only available if the controller has a predefined login design.
`Login page text`	Path and filename of the page that appears for the user logon.
`Login policy text`	Path and filename of the page that displays user policy text.
`Custom page background color`	Hexadecimal value for a custom background color. This option is only available if the controller has a custom login page design theme.
`Custom page background image`	Path and filename for a custom JPEG captive portal background image. This option is only available if the controller has a custom login page design theme.

Related Commands

Command	Description	Mode
`aaa authentication captive-portal`	If you do not yet have any captive portal profiles defined, use the command **`aaa authentication captive-portal`** to configure your captive portal profiles.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication dot1x

```
show aaa authentication dot1x [<profile-name>|countermeasures]
```

Description

This command shows information for 802.1x authentication profiles.

Syntax

Parameter	Description
`<profile-name>`	The name of an existing 802.1x authentication profile.
`countermeasures`	Reports if WPA/WPA2 Countermeasures have been enabled for 802.1x profiles. If enabled, the AP scans for message integrity code (MIC) failures in traffic received from clients.

Usage Guidelines

Issue this command without the **<profile-name>** or **countermeasures** options to display the entire 802.1x Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed dot1x authentication configuration information for that profile. The **countermeasures** option indicates whether the 802.1x profiles have been configured for WPA/WPS2 countermeasures. If countermeasures have not been configured, the output for this command will be blank.

Examples

The following example lists all dot1x authentication profiles. The **References** column lists the number of other profiles with references to a 802.1x authentication profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined 802.1x profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication dot1x

802.1X Authentication Profile List
----------------------------------
Name         References  Profile Status
----         ----------  --------------
default      2
default-psk  1           Predefined (editable)
dot1x        5
dot1xtest 0

Total:4
```

To display a complete list of parameters for an individual profile, include the <profile> parameter. The example below displays some of the profile details for the authentication profile **pDotix**.

```
(host) #show aaa authentication dot1x pDot1x

802.1X Authentication Profile "pDot1x"
--------------------------------------
Parameter                                                Value
---------                                                -----
Max authentication failures                              0
Enforce Machine Authentication                           Disabled
Machine Authentication: Default Machine Role             guest
Machine Authentication Cache Timeout                     24 hrs
Blacklist on Machine Authentication Failure              Disabled
Machine Authentication: Default User Role                guest
Interval between Identity Requests                       30 sec
Quiet Period after Failed Authentication                 30 sec
Reauthentication Interval                                86400 sec
Use Server provided Reauthentication Interval            Disabled
Multicast Key Rotation Time Interval                     1800 sec
Unicast Key Rotation Time Interval                       900 sec
...
```

The output of the **show aaa authentication dot1x** command includes the following parameters:

Parameter	Value
Max authentication failures	Number of times a user can try to login with wrong credentials after which the user is blacklisted as a security threat. Blacklisting is disabled if this parameter is set to 0.
Enforce Machine Authentication	Shows if machine authentication is enabled or disabled for Windows environments. If enabled, If enabled, either the machine-default-role or the user-default-role is assigned to the user, depending on which authentication is successful.
Machine Authentication: Default Machine Role	Default role assigned to the user after completing only machine authentication.
Machine Authentication Cache Timeout	The timeout period, in hours, for machine authentication. After this period passes, the use will have to re-authenticate.
Blacklist on Machine Authentication Failure	If enabled, the client is blacklisted if machine authentication fails.
Machine Authentication: Default User Role	Default role assigned to the user after 802.1x authentication.
Interval between Identity Requests	Interval, in seconds, between identity request retries
Quiet Period after Failed Authentication	Interval, in seconds, following failed authentication.
Reauthentication Interval	Interval, in seconds, between reauthentication attempts.
Use Server provided Reauthentication Interval	If enabled, 802.1x authentication will use the server-provided reauthentication period.
Multicast Key Rotation Time Interval	Interval, in seconds, between multicast key rotations.
Unicast Key Rotation Time Interval	Interval, in seconds, between unicast key rotations.
Authentication Server Retry Interval	Server group retry interval, in seconds.
Authentication Server Retry Count	The number of server group retries.
Framed MTU	Shows the framed MTU attribute sent to the authentication server.

Parameter	Value
Number of times ID-Requests are retried	Maximum number of times ID requests are sent to the client.
Maximum Number of Reauthentication Attempts	Maximum number of reauthentication attempts.
Maximum number of times Held State can be bypassed	Number of consecutive authentication failures which, when reached, causes the controller to not respond to authentication requests from a client while the controller is in a held state after the authentication failure.
Dynamic WEP Key Message Retry Count	Number of times unicast/multicast EAPOL key messages are sent to the client.
Dynamic WEP Key Size	Dynamic WEP key size, either 40 or 128 bits.
Interval between WPA/WPA2 Key Messages	Interval, in milliseconds, between each WPA key exchange.
Delay between WPA/WPA2 Unicast Key and Group Key Exchange	Interval, in milliseconds, between unicast and multicast key exchanges.
WPA/WPA2 Key Message Retry Count	Number of times WPA/WPA2 key messages are retried.
Multicast Key Rotation	Shows if multicast key rotation is enabled or disabled.
Unicast Key Rotation	Shows if unicast key rotation is enabled or disabled.
Reauthentication	If enabled, this option forces the client to do a 802.1x reauthentication after the expiration of the default timer for reauthentication. (The default value of the timer is 24 hours.)
Opportunistic Key Caching	If enabled, a cached pairwise master key (PMK) is derived with a client and an associated AP and used when the client roams to a new AP.
Validate PMKID	Shows if the **Validate PMKID** feature is enabled or disabled. When this option is enabled, the client must send a PMKID in the associate or reassociate frame to indicate that it supports OKC; otherwise, full 802.1x authentication takes place. (This feature is optional, since most clients that support OKC do not send the PMKID in their association request.)
Use Session Key	If enabled, the controller will use a RADIUS session key as the unicast WEP key.
Use Static Key	If enabled, the controller will use a static key as the unicast/multicast WEP key.
xSec MTU	Shows the size of the MTU for xSec.
Termination	Shows if 802.1x termination is enabled or disabled on the controller.
Termination EAP-Type	Shows the current Extensible Authentication Protocol (EAP) method, either EAP-PEAP or EAP-TLS.
Termination Inner EAP-Type	When EAP-PEAP is the EAP method, this parameter displays the inner EAP type.
Token Caching	If this feature enabled (and EAP-GTC is configured as the inner EAP method), token caching allows the controller to cache the username and password of each authenticated user.
Token Caching Period	Timeout period, in hours, for the cached information.
CA-Certificate	Name of the CA certificate for client authentication loaded in the controller.
Server-Certificate	Name of the Server certificate used by the controller to authenticate itself to the client.

Parameter	Value
TLS Guest Access	Shows if guest access for valid EAP-TLS users is enabled or disabled.
TLS Guest Role	User role assigned to EAP-TLS guest.
Ignore EAPOL-START after authentication	If enabled, the controller ignores EAPOL-START messages after authentication.
Handle EAPOL-Logoff	Shows if handling of EAPOL-LOGOFF messages is enabled or disabled.
Ignore EAP ID during negotiation	If enabled, the controller will Ignore EAP IDs during negotiation.
WPA-Fast-Handover	Shows if WPA-fast-handover is enabled or disabled. This feature is only applicable for phones that support WPA.
Disable rekey and reauthentication for clients on call	Shows if the rekey and reauthentication features for voice-over-WLAN clients has been enabled or disabled.

Related Commands

Command	Description	Mode
aaa authentication dot1x	If you do not yet have any 802.1x authentication profiles defined, use the command **aaa authentication dot1x** to configure your 802.1x profiles.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication mac

show aaa authentication mac [<profile-name>]

Description

This command shows information for MAC authentication profiles. Issue this command without the **<profile-name>** option to display the entire MAC Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed MAC authentication configuration information for that profile.

Parameter	Description
<profile-name>	The name of an existing MAC authentication profile.

Examples

The output of the example below shows two MAC authentication profiles, **default** and **macProfile1**, which are referenced three times by other profiles. the **Profile Status** columns are blank, indicating that these profiles are both user-defined. (If a profile is predefined, the value **Predefined** appears in the Profile Status column.)

```
(host) #show aaa authentication mac

MAC Authentication Profile List
-------------------------------
Name         References  Profile Status
----         ----------  --------------
default      3
MacProfile1  3

Total:2
```

The following example displays configuration details for the MAC authentication profile “MacProfile1,” including the delimiter and case used in the authentication request, and the maximum number of times a client can fail to authenticate before it is blacklisted.

```
(host) #show aaa authentication mac MacProfile1

MAC Authentication Profile "MacProfile1"
----------------------------------------
Parameter                   Value
---------                   -----
Delimiter                   colon
Case                        upper
Max Authentication failures  3
```

Related Commands

Command	Description	Mode
aaa authentication mac	Configure MAC authentication values on your controller.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication mgmt

```
show aaa authentication mgmt
```

Description

This command displays administrative user authentication information, including management authentication roles and servers.

Usage Guidelines

Issue this command to identify the default management role assigned to authenticated administrative users, and the name of the group of servers used to authenticate these users.

Example

The output of the following example displays management authentication information for your controller.

```
(host) #show aaa authentication mgmt

Management Authentication Profile
---------------------------------
Parameter     Value
---------     -----
Default Role  root
Server Group  ServerGroup1
Mode          Enabled
```

The output of the **show aaa authentication mgmt** command includes the following parameters:

Parameter	Description
`Default Role`	This parameter shows which of the following roles the controller uses for authentication management. • **root**, the super user role (default). • **guest-provisioning**, guest provisioning role. • n**etwork-operations**, network operator role. • **read-only**, read only role. • **location-api-mgmt**, location API management role. • **no-access**, no commands are accessible.
`Server Group`	The name of a server group.
`Mode`	The **Mode** parameter indicates whether or not this feature is enabled or disabled.

Related Commands

Command	Description	Mode
`aaa authentication mgmt`	Configure management authentication settings.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication stateful-dot1x

```
show aaa authentication stateful-dot1x [config-entries]
```

Description

This command displays configuration settings for 802.1x authentication for clients on non-Dell APs.

Syntax

Parameter	Description
`config-entries`	Display details for the AP Server configuration list.

Usage Guidelines

Issue this command to identify the default role assigned to the 802.1x user group, name of the group of RADIUS servers used to authenticate the 802.1x users, and the 802.1x authentication timeout period, in seconds.

Example

The output of the following example displays 802.1x authentication information for your controller.

```
(host) #show aaa authentication stateful-dot1x

Stateful 802.1X Authentication Profile
--------------------------------------
Parameter     Value
---------     -----
Default Role  guest
Server Group  newgroup2
Timeout       10 sec
Mode          Enabled
```

The output of this command includes the following parameters:

Parameter	Description
`Default Role`	This parameter shows which role the controller uses for 802.1x authentication management.
`Server Group`	The name of a server group.
`Timeout`	Timeout period for an authentication request, in seconds.
`Mode`	The **Mode** parameter indicates whether or not this feature is enabled or disabled.

When you include the **config-entries** parameter, the output shows the AP - Server Configuration List.

```
(host) #show aaa authentication stateful-dot1x config-entries

AP-Server Configuration List
----------------------------
Cfg-Name  AP-IP      Server    Shared-Secret
--------  -----      ------    -------------
cfg22      10.3.14.6  RADIUS1   secret-pwd
```

The output of this command includes the following parameters:

Parameter	Description
`Cfg-Name`	is a auto-generated name
`AP-IP`	IP address of the AP.
`Server`	Name of the authentication server.
`Shared-Secret`	Shared authentication secret.

Related Commands

Command	Description	Mode
`aaa authentication stateful-dot1x`	Use the command `aaa authentication stateful-dot1x` to configure the settings displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication stateful-ntlm

```
show aaa authentication stateful-ntlm
```

Description

This command displays configuration settings for the Stateful NTLM Authentication profile. Issue this command without the **<profile-name>** option to display the entire Stateful NTLM Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed Stateful NTLM authentication configuration information for that profile.

Syntax

Parameter	Description
<profile-name>	The name of an existing Stateful NTLM authentication profile.

Usage Guidelines

Issue this command to identify the default role assigned to users who have successfully authenticated the using NT Lan Manager (NTLM) authentication protocol, the name of the group of windows servers used to authenticate these users, and the NTLM authentication timeout period, in seconds.

Examples

The output of the example below shows two stateful NTLM authentication profiles, **default** and **NTLMprofile1**, which are each referenced one time by other profiles. the **Profile Status** columns are blank, indicating that these profiles are both user-defined. (If a profile is predefined, the value **Predefined** appears in the Profile Status column.)

```
(host) #show aaa authentication stateful-ntlm

Stateful NTLM Authentication Profile List
-----------------------------------------
Name               References  Profile Status
----               ----------  --------------
default            1
NTLMprofile1       1

Total:2
```

The following example displays configuration details for the stateful NTLM authentication profile “default”.

```
(host) #show aaa authentication stateful-ntlm default


Stateful NTLM Authentication Profile "default"
----------------------------------------------
Parameter     Value
---------     -----
Default Role  guest
Server Group  default
Mode          Disabled
Timeout       10 sec
```

The output of this command includes the following parameters:

Parameter	Description
`Default Role`	This parameter shows the role assigned to NTLM authenticated users.
`Server Group`	The name of a windows server group.
`Mode`	The **Mode** parameter indicates whether or not this authentication profile is enabled or disabled.
`Timeout`	Timeout period for an authentication request, in seconds.

Related Commands

Command	Description
`aaa authentication stateful-ntlm`	Use the command `aaa authentication stateful-ntlm` to configure the settings displayed in the output of this show command.

Command History

This command was introduced in ArubaOS 3.4.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication via auth-profile

```
show aaa authentication via auth-profile [<profile-name>]
```

Description

This command displays configuration settings for the VIA Authentication profile. Issue this command without the **<profile-name>** option to display the entire VIA Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed VIA authentication configuration information for that profile.

Syntax

Parameter	Description
<profile-name>	The name of an existing VIA authentication profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire VIA Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

If you do not yet have any VIA authentication profiles defined, use the command aaa authentication via auth-profile to configure your VIA authentication profiles.

Examples

This first example shows that there are three configured captive portal profiles in the Captive Profile Authentication Profile List. The **References** column lists the number of other profiles with references to a VIA authentication profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication via auth-profile

VIA Authentication Profile List
-------------------------------
Name     References  Profile Status
----     ----------  --------------
default  0
via1     2
via2     1

Total:3
```

Include a VIA authentication profile name to display a complete list of configuration settings for that profile. The example below shows settings for the VIA authentication profile *via1*.

```
VIA Authentication Profile "via1"
---------------------------------
Parameter                   Value
---------                   -----
Default Role                default-via-role
Server Group                internal
Max Authentication failures  2
Description                 VIA config for the MV office
```

The output of this command includes the following parameters:

Parameter	Description
`Default Role`	Role assigned to the captive portal user upon login.
`Server Group`	Name of the group of servers used to authenticate captive portal users.
`Max Authentication failures`	Maximum number of authentication failures before the user is blacklisted.
`Description`	Description of the VIA authentication profile.

Related Commands

Command	Description	Mode
`aaa authentication via auth-profile`	Use **`aaa authentication via auth-profile`** to configure the parameters displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication via connection-profile

```
show aaa authentication via connection-profile [<profile-name>]
```

Description

This command displays configuration settings for the VIA connection profile. Issue this command without the **<profile-name>** option to display the entire VIA Connection profile list, including profile status and the number of references to each profile. Include a profile name to display detailed VIA connection configuration information for that profile.

Syntax

Parameter	Description
<profile-name>	The name of an existing VIA connection profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire VIA connection profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

If you do not yet have any VIA connection profiles defined, use the command aaa authentication via connection-profile to configure your VIA connection profiles.

Examples

This first example shows that there are three configured connection profiles in the Captive Profile Authentication Profile List. The **References** column lists the number of other profiles with references to a VIA connection profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication via connection-profile

VIA Connection Profile List
---------------------------
Name          References  Profile Status
----          ----------  --------------
connection_1  3
connection_2  1
default       0

Total:3
```

Include a connection profile name to display a complete list of configuration settings for that profile. The example below shows settings for the captive portal profile *connection_1*.

```
(host)# show aaa authentication via connection-profile connection_1

VIA Connection Profile "connection_1"
-------------------------------------
Parameter                                Value
---------                                -----
VIA controllers                          N/A
Client Auto-Login                        Enabled
VIA Authentication Profiles to provision N/A
Allow client to auto-upgrade             Enabled
VIA tunneled networks                    N/A
Enable split tunneling                   Disabled
VIA Client WLAN profiles                 N/A
Allow client side logging                Enabled
VIA IKE Policy                           Default
Use Windows Credentials                  Enabled
VIA IPSec Crypto Map                     default-dynamicmap/10000
Allow user to save passwords             Enabled
VIA Client Network Mask                  255.255.255.255
Validate Server Certificate              Enabled
VIA Client DNS Suffix List               N/A
VIA max session timeout                  1440 min
VIA Support E-Mail Address               N/A
Maximum reconnection attempts            3
VIA external download URL                N/A
Allow user to disconnect VIA             Enabled
```

The output of this command includes the following parameters:

Configuration Option	Description
VIA Controller	Displays the following information about the VIA controller: • *Controller Hostname/IP Address*: This is the public IP address or the DNS hostname of the VIA controller. Users will connect to remote server using this IP address or the hostname. • Controller Internal IP Address: This is the IP address of any of the VLAN interface IP addresses belongs to this controller. • Controller Description: This is a human-readable description of the controller.
Client Auto-Login	Enable or disable VIA client to auto login and establish a secure connection to the controller. Default: Enabled
VIA Authentication Profiles to provision	This is the list of VIA authentication profiles that will be displayed to users in the VIA client.
Allow client to auto-upgrade	Enable or disable VIA client to automatically upgrade when an updated version of the client is available on the controller. Default: Enabled
VIA tunneled networks	A list of network destination (IP address and netmask) that the VIA client will tunnel through the controller. All other network destinations will be reachable directly by the VIA client.
Enable split-tunneling	Enable or disable split tunneling. • If enabled, all traffic to the VIA tunneled networks will go through the controller and the rest is just bridged directly on the client. • If disabled, all traffic will flow through the controller. Default: off
Allow client-side logging	Enable or disable client side logging. If enabled, VIA client will collect logs that can be sent to the support email-address for troubleshooting. Default: Enabled
VIA Client WLAN profiles	A list of VIA client WLAN profiles that needs to be pushed to the client machines that use Windows Zero Config (WZC) to configure or manage their wireless networks.

Configuration Option	Description
VIA IKE Policy	List of IKE policies that the VIA Client has to use to connect to the controller.
Use Windows Credentials	Enable or disable the use of the Windows credentials to login to VIA. If enabled, the SSO (Single Sign-on) feature can be utilized by remote users to connect to internal resources. Default: Enabled
VIA IPSec Crypto Map	List of IPSec Crypto Map that the VIA client uses to connect to the controller. These IPSec Crypto Maps are configured in CLI using the `crypto-local ipsec-map <ipsec-map-name>` command.
Allow user to save passwords	Enable or disable users to save passwords entered in VIA. Default: Enabled
VIA Client Network Mask	The network mask that has to be set on the client after the VPN connection is established. Default: 255.255.255.255
Validate Server Certificate	Enable or disable VIA from validating the server certificate presented by the controller. Default: Enabled
VIA Client DNS Suffix List	The DNS suffix list (comma separated) that has be set on the client once the VPN connection is established. Default: None.
VIA max session timeout	The maximum time (minutes) allowed before the VIA session is disconnected. Default: 1440 min
VIA Support E-mail Address	The support e-mail address to which VIA users will send client logs. Default: None.
Maximum reconnection attempts	The maximum number of re-connection attempts by the VIA client due to authentication failures. Default: 3
VIA external download URL	End users will use this URL to download VIA on their computers.
Allow user to disconnect VIA	Enable or disable users to disconnect their VIA sessions. Default: on

Related Commands

Command	Description	Mode
`aaa authentication via connection-profile`	Use **`aaa authentication via connection-profile`** to configure the parameters displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication via web-auth

```
show aaa authentication via web-auth [default]
```

Description

A VIA web authentication profile contains an ordered list of VIA authentication profiles. The web authentication profile is used by end users to login to the VIA download page (https://<server-IP-address>/via) for downloading the VIA client. Only one VIA web authentication profile is available. If more than one VIA authentication profile is configured, users can view this list and select one during the client login.

Syntax

No parameters.

Usage Guidelines

Issue this command to view the authentication profiles associated with the default web authentication profile. Use it without the profile name to see the list of authentication profiles.

Examples

```
(host) #show aaa authentication via web-auth

VIA Web Authentication List
---------------------------
Name     References  Profile Status
----     ----------  --------------
default  2

Total:1

(host) #show aaa authentication via web-auth default

VIA Web Authentication "default"
--------------------------------
Parameter                   Value
---------                   -----
VIA Authentication Profiles  via1
```

The output of this command includes the following parameters:

Parameter	Description
`VIA Authentication Profiles`	This is the name of the VIA authentication profile. The value column displays the order of priority in which the profiles are displayed in the VIA client login.

Related Commands

Command	Description	Mode
`aaa authentication via web-auth`	Use **`aaa authentication via web-auth`** to configure the parameters displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication vpn

```
show aaa authentication vpn [default|default-cap|default-rap]
```

Description

This command displays VPN authentication settings, including authentication roles and servers.

Usage Guidelines

Issue this command to identify the default role assigned to VPN users, the name of the group of servers used to authenticate the VPN users, and the maximum number of authentication failures allowed before the user is blacklisted.

Example

The following example displays configuration details for VPN authentication default, default-cap and default-rap.

```
(host) #show aaa authentication vpn default

VPN Authentication Profile "default"
------------------------------------
Parameter                    Value
---------                    -----
Default Role                 default-vpn-role
Server Group                 default
Max Authentication failures  2

(TechPubs) #show aaa authentication vpn default-cap

VPN Authentication Profile "default-cap" (Predefined)
-----------------------------------------------------
Parameter                    Value
---------                    -----
Default Role                 ap-role
Server Group                 internal
Max Authentication failures  0

(TechPubs) #show aaa authentication vpn default-rap

VPN Authentication Profile "default-rap" (Predefined (changed))
---------------------------------------------------------------
Parameter                    Value
---------                    -----
Default Role                 default-vpn-role
Server Group                 default
Max Authentication failures  0
```

The output of this command includes the following parameters:

Parameter	Description
Default Role	The default role to be assigned to VPN users.
Server Group	The name of the server group that performs the authentication.
Max Authentication failures	Number of times a user attempted to authenticate, but failed.

Related Commands

Command	Description	Mode
`aaa authentication via auth-profile`	Use the command **`aaa authentication via auth-profile`** to configure the settings displayed in the output of this show command.	Config mode

Command History

Version	Description
ArubaOS 3.0	Command introduced.
ArubaOS 5.0	The **default-cap** and **default-rap** profiles were introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	The PEFV license and the base operating system.	Enable or Config mode on master or local controllers

show aaa authentication wired

```
show aaa authentication wired
```

Description

View wired authentication settings for a client device that is directly connected to a port onthe controller.

Usage Guidelines

This command displays the name of the AAA profile currently used for wired authentication.

Example

The following example shows the current wired profile for the controller is a profile named “secure_profile_3.”

```
(host) #show aaa authentication wired

Wired Authentication Profile
----------------------------
Parameter    Value
---------    -----
AAA Profile  Secure_profile_3
```

Related Commands

Command	Description	Mode
`aaa authentication wired`	Use the command **`aaa authentication wired`** to configure the settings displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication wispr

```
show aaa authentication wispr <profile-name)
```

Description

This command shows information for a WISPr authentication profiles. Issue this command without the **<profile-name>** option to display the entire WISPr Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed WISPr authentication configuration information for that profile.

Parameter	Description
<profile-name>	The name of an existing MAC authentication profile.

Examples

The output of the example below shows two WISPr authentication profiles, **default** and **WISPR1**, which are referenced two times by other profiles. the **Profile Status** columns are blank, indicating that these profiles are both user-defined. (If a profile is predefined, the value **Predefined** appears in the Profile Status column.)

```
(host) #show aaa authentication wispr

WISPr Authentication Profile List
-----------------------------
Name         References  Profile Status
----         ----------  --------------
default      2
WISPr1  2

Total:2
```

The following example displays configuration details for the WISPr authentication profile “WISPr1”.

```
(host) #show aaa authentication wispr WISPr1

WISPr Authentication Profile "WISPr1"
-------------------------------------
Parameter                           Value
---------                           -----
Default Role                        guest
Server Group                        default
Logon wait minimum wait             5 sec
Logon wait maximum wait             10 sec
logon wait CPU utilization threshold  60 %
WISPr Location-ID ISO Country Code    US
WISPr Location-ID E.164 Country Code  1
WISPr Location-ID E.164 Area Code     408
WISPr Location-ID SSID/Zone           Corp1
WISPr Operator Name                   MyCompany
WISPr Location Name                   Sunnyvale
```

The output of this command includes the following parameters:

Parameter	Description
Default Role	The default role to be assigned to users that have completed WISPr authentication.
Server Group	The name of the server group that performs the authentication.

Parameter	Description
`Logon wait minimum wait`	If the controller's CPU utilization has surpassed the **Login wait CPU utilization threshold value,** the **Logon wait minimum wait** parameter defines the minimum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 5 seconds.
`Logon wait maximum wait`	If the controller's CPU utilization has surpassed the logon **wait CPU utilization threshold** value, the **Logon wait maximum wait** parameter defines the maximum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 10 seconds.
`WISPr Location-ID E.164 Area Code`	The E.164 Area Code in the WISPr Location ID.
`WISPr Location-ID E.164 Country Code 1`	The 1-3 digit E.164 Country Code in the WISPr Location ID.
`WISPr Location-ID ISO Country Code`	The ISO Country Code in the WISPr Location ID.
`WISPr Location-ID SSID/Zone`	The SSID/network name in the WISPr Location ID.
`WISPr Location Name`	A name identifying the hotspot location. If no name is defined, the default ap-name is used.
`WISPr Operator Name`	A name identifying the hotspot operator.

Related Commands

Command	Description	Mode
`aaa authentication wispr`	Configure WISPr authentication values on your controller.	Config mode on master or local controllers.

Command History

This command was introduced in ArubaOS 3.4.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication-server all

```
show aaa authentication-server all
```

Description

View authentication server settings for both external authentication servers and the internal controller database.

Usage Guidelines

The output of this command displays statistics for the Authentication Server Table, including the name and address of each server, server type and configured authorization and accounting ports.

Examples

The following command shows information for the internal Authentication server, and another RADIUS server named RADIUS-1.

```
(host) #show aaa authentication-server all

Auth Server Table
-----------------
Name      Type    IP addr         AuthPort  AcctPort  Status   Requests
----      ----    -------         --------  --------  ------   --------
Internal  Local   10.168.254.221  n/a       n/a       Enabled  5
SMOKERAD  Radius  10.4.101.123    5555      5556      Enabled  1
```

The following data columns appear in the output of this command:

Parameter	Description
Name	Name of the authentication server.
Type	The type of authentication server. ArubaOS supports LDAP, RADIUS and TACACS+ servers, in addition to its own local, internal authentication server.
IP addr	IP address of the server, in dotted-decimal format.
AuthPort	Port number used for authentication. An LDAP server uses port 636 for LDAP over SSL, and port 389 for SSL over LDAP, Start TLS operation andclear text. The default RADIUS authentication port is port 1812.
AcctPort	Accounting port on the server. The default RADIUS accounting port is port 1813.
AcctPort	Accounting port on the server.
Status	Shows whether the Authentication server is enable or disabled.
Requests	Number of authentication requests received by the server.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication-server internal

```
show aaa authentication-server internal [statistics]
```

Description

View authentication server settings for the internal controller database.

Examples

The output of the command below shows that the internal authentication server has been disabled.

```
(host) #show aaa authentication-server internal

Internal Server
---------------
Host      IP addr         Retries  Timeout  Status
----      -------         -------  -------  ------
Internal  10.168.254.221  3        5        Disabled
```

The following data columns appear in the output of this command:

Parameter	Description
`Host`	Name of the internal authentication server.
`IP addr`	Address of the internal server, in dotted-decimal format.
`Retries`	Number of retries allowed before the server stops attempting to authenticate a request.
`timeout`	Timeout period, in seconds.

Include the **statistics** parameter to display additional details for the internal server.

```
(host) #show aaa authentication-server internal statistics

Internal Database Server Statistics
-----------------------------------
PAP Requests            8
PAP Accepts             8
PAP Rejects             0
MSCHAPv2 Requests       0
MSCHAPv2 Accepts        0
MSCHAPv2 Rejects        0
Mismatch Response       0
Users Expired           1
Unknown Response        0
Timeouts                1
AvgRespTime (ms)        0
Uptime (d:h:m)          4:3:32
SEQ first/last/free     1,255,255
```

The following data columns appear in the output of this command:

Parameter	Description
PAP Requests	Number of PAP requests received by the internal server.
PAP Accepts	Number of PAP requests accepted by the internal server.
PAP Rejects	Number of PAP requests rejected by the internal server.
MSCHAPv2 Requests	Number of MSCHAPv2 requests received by the internal server.

Parameter	Description
MSCHAPv2 Accepts	Number of MSCHAPv2 requests accepted by the internal server.
MSCHAPv2 Rejects	Number of MSCHAPv2 requests rejected by the internal server.
Mismatch Response	Number of times the server received an authentication response to a request after another request had been sent.
Users Expired	Number of users that were deauthenticated because they stopped responding.
Unknown Response	Number of times the server did not recognize the response, possibly due to internal errors.
Timeouts	Number of times that the controller timed out an authentication request.
AvgRespTime (ms)	Time it takes the server to respond to an authentication request, in seconds.
Uptime (d:h:m)	Time elapsed since the last server reboot.
SEQ first/last/free	This internal buffer counter keeps track of the requests to the authentication server.

Related Commands

Command	Description	Mode
`aaa authentication-server internal`	Issue the command **`aaa authentication-server internal`** to use the internal database on a local controller for authenticating clients.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication-server ldap

```
show aaa authentication-server ldap [<ldap_server_name>]
```

Description

Display configuration settings for your LDAP servers.

Syntax

Parameter	Description
<ldap_server_name>	Name that identifies an LDAP server.

Examples

The output of the example below displays the LDAP server list with the names of all the LDAP servers. The **References** column lists the number of other profiles that reference an LDAP server, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #aaa authentication-server ldap

LDAP Server List
----------------
Name   References  Profile Status
----   ----------  --------------
ldap1  5
ldap2  3
ldap3  1

Total:3
```

Include the **<ldap_server_name>** parameter to display additional details for an individual server.

```
(host) #show aaa authentication-server ldap ldap1

LDAP Server "ldap1"
-------------------
Parameter                 Value
---------                 -----
Host                      10.1.1.234
Admin-DN                  cn=corp,cn=Users,dc=1m,dc=corp,dc=com
Admin-Passwd              ********
Allow Clear-Text          Disabled
Auth Port                 389
Base-DN                   cn=Users,dc=1m,dc=corp,dc=com
Filter                    (objectclass=*)
Key Attribute             sAMAccountName
Timeout                   20 sec
Mode                      Enabled
Preferred Connection Type ldap-s
```

The output of this command includes the following parameters:

Parameter	Description
host	IP address of the LDAP server
Admin-DN	Distinguished name for the admin user who has read/search privileges across all of the entries in the LDAP database.

Parameter	Description
`Admin Passwd`	Password for the admin user.
`Allow Clear-Text`	If enabled, this parameter allows clear-text (unencrypted) communication with the LDAP server.
`Auth Port`	Port number used for authentication. Port 636 will be attempted for LDAP over SSL, while port 389 will be attempted for SSL over LDAP, Start TLS operation and clear text.
`Base-DN`	Distinguished Name of the node which contains the required user database.
`Filter`	Filter that should be applied to search of the user in the LDAP database (default filter string is: i(objectclass=*)î).
`Key attribute`	Attribute that should be used as a key in search for the LDAP server.
`Timeout`	Timeout period of a LDAP request, in seconds.
`Mode`	Shows whether this server is **Enabled** or **Disabled**.
`Preferred Connection Type`	Preferred type of connection to the server. Possible values are • Clear text • LDAP-S • START-TLS

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication-server radius

```
show aaa authentication-server radius [<rad_server_name>|statistics]
```

Description

Display configuration settings for your RADIUS servers.

Syntax

Parameter	Description
<rad_server_name>	Name that identifies a RADIUS server.

Examples

The output of the example below displays the RADIUS server list with the names of all the RADIUS servers. The **References** column lists the number of other profiles that reference a RADIUS server, and the **Profile Status** column indicates whether the profile is predefined. User-defined servers will not have an entry in the **Profile Status** column. To view additional statistics for all RADIUS servers, include the **statistics** parameter.

```
(host) #aaa authentication-server radius

RADIUS Server List
----------------
Name           References  Profile Status
----       ----------  --------------
IAS1       5
SMOKERAD   3

Total:2
```

Include the **<rad_server_name>** parameter to display additional details for an individual server.

```
(host) #show aaa authentication-server radius SMOKERAD

RADIUS Server "SMOKERAD"
------------------------
Parameter    Value
---------    -----
Host         10.4.101.123
Key          ********
Auth Port    5555
Acct Port    5556
Retransmits  3
Timeout      5 sec
NAS ID       SMOKETEST
NAS IP       N/A
Use MD5      Disabled
Mode         Enabled
```

The output of this command includes the following parameters:

Parameter	Description
host	IP address of the RADIUS server
Key	Shared secret between the controller and the authentication server.

Parameter	Description
`Acct Port`	Accounting port on the server.
`auth port`	Authentication port on the server.
`Retransmits`	Maximum number of retries sent to the server by the controller before the server is marked as down.
`Timeout`	Maximum time, in seconds, that the controller waits before timing out the request and resending it.
`NAS ID`	Network Access Server (NAS) identifier to use in RADIUS packets.
`NAS IP`	NAS IP address to send in RADIUS packets. If you do not configure a server-specific NAS IP, the global NAS IP is used.
`Use MD5`	If enabled, the RADIUS server will use a MD5 hash of cleartext password.
`Mode`	Shows whether this server is **Enabled** or **Disabled**.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication-server tacacs

```
show aaa authentication-server tacacs [<tacacs_server_name>]|statistics
```

Description

Display configuration settings for your TACACS+ servers.

Syntax

Parameter	Description
<tacacs_server_name>	Name that identifies an TACACS+ server.
statistics	Displays accounting, authorization, and authentication request and response statistics for the TACACS server.

Examples

The output of the example below displays the TACACS+ server list with the names of all the TACACS+ servers. The **References** column lists the number of other profiles that reference a TACACS+ server, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #aaa authentication-server tacacs

TACACS Server List
----------------
Name           References  Profile Status
----          ----------  --------------
LabAuth    5
TACACS1     3

Total:2
```

Include the <tacacs_server_name> parameter to display additional details for an individual server.

```
(host) #show aaa authentication-server tacacs tacacs1

TACACS Server "tacacs1"
---------------------
Parameter    Value
---------    -----
Host         10.1.1.16
Key          ********
TCP Port     49
Retransmits  3
Timeout      20 sec
Mode         Enabled
```

The output of this command includes the following parameters:

Parameter	Description
host	IP address of the TACACS+ server
Key	Shared secret between the controller and the authentication server.
TCP Port	TCP port used by the server.

Parameter	Description
`Retransmits`	Maximum number of retries sent to the server by the controller before the server is marked as down.
`Timeout`	Maximum time, in seconds, that the controller waits before timing out the request and resending it.
`Mode`	Shows whether this server is **Enabled** or **Disabled**.

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 6.0	The **Statistics** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa authentication-server windows

```
show aaa authentication-server windows [<windows_server_name>]
```

Description

Display configuration settings for your Windows servers.

Syntax

Parameter	Description
<windows_server_name>	Name that identifies a Windows server.

Examples

The output of the example below displays the Windows server list with the names of all the Windows servers used for NTLM authentication. The **References** column lists the number of other profiles that reference a Windows server, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #aaa authentication-server tacacs

Windows Server List
---------------
Name           References  Profile Status
----          ----------  --------------
NTLM       1
Windows2   1

Total:2
```

Include the <windows_server_name> parameter to display additional details for an individual server.

```
(host) #show aaa authentication-server windows Windows2

Windows Server "windows"
------------------------
Parameter       Value
---------       -----
Host            172.21.18.170
Mode            Enabled
Windows Domain  MyCompanyDomain
```

The output of this command includes the following parameters:

Parameter	Description
host	IP address of the Windows server
Mode	Shows whether this server is **Enabled** or **Disabled**.
Windows Domain	Name of the Windows domain to which this server is assigned.

Command History

This command was introduced in ArubaOS 3.4.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa tacacs-accounting

```
show aaa tacacs-accounting
```

Description

Show configuration information for TACACS+ accounting servers.

Usage Guidelines

This command displays TACACS+ data for your controller if you have previously configured a TACACS+ server and server group. The output includes the current TACACS+ accounting mode (enabled or disabled), and the name of the TACACS+ server group.

Example

The output of the **show aaa accounting tacacs** command displays configuration information for a TACACS+ accounting server. The output of this command includes the following parameters:

```
(host) #show aaa accounting tacacs
TACACS Accounting Configuration
-------------------------------
Parameter      Value
---------      -----
Mode           Enabled
Commands       configuration
Server-Group   tacacs1
```

Parameter	Description
`Mode`	Shows whether this server group is **Enabled** or **Disabled**.
`Commands`	Displays the types of commands that are reported to the TACACS server group. • **action** reports action commands only. • **all** reports all commands. • **configuration** reports configuration commands only • **show** reports show commands only
`Server-Group`	Shows whether this server is **Enabled** or **Disabled**.

Related Commands

Command	Description	Mode
`aaa authentication-server tacacs`	Configure the TACACCS+ accounting feature.	Config mode
`aaa server-group`	Add a configured authentication server to an ordered list in a server group, and configure server rules to derive a user role, VLAN ID or VLAN name from attributes returned by the server during authentication	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa bandwidth-contracts

```
show aaa bandwidth-contracts
```

Description

This command shows the contract names, ID numbers and Rate limits for your bandwidth contracts.

Example

The output of the following command shows that the bandwidth contract **VLAN** has a configured rate of 6 Mbps, and the contract **User** has a rate of 2048 Kbps.

```
(host) #show aaa bandwidth-contracts

Bandwidth Contracts
-------------------
Contract  Id  Rate (bits/second)
--------  --  -----------------
VLAN       1   6000000
User       2   2048000

Total contracts = 2
Per-user contract total = 4096
Per-user contract usage = 0
```

Related Commands

Command	Description	Mode
`aaa bandwidth-contract`	Use this command to define contracts to limit traffic for a user or VLAN.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa derivation-rules

```
show aaa derivation-rules [server-group <group-name>|user <name>]
```

Syntax

Parameter	Description
<group-name>	Name of a server group
<name>	Name of a user rule group

Description

Show derivation rules based on user information or configured for server groups.

Example

The output of the following command shows that the server group group1 has the internal database configured as its authentication server, and that there is a single rule assigned to that group. You can omit the **<group-name>** parameter to show a table of all your server groups.

```
(host) #show aaa derivation-rules server-group group1

Server Group

Name      Inservice  trim-FQDN  match-FQDN
----      ---------  ---------  ----------
Internal  Yes        No

Server Rule Table
-----------------
Priority  Attribute  Operation  Operand   Action    Value  Total Hits  New Hits
--------  ---------  ---------  -------   ------    -----  ----------  --------
1         Filter-Id  equals     nsFilter  set vlan  111    24          0
Rule Entries: 1
```

The following data columns appear in the output of this command:

Parameter	Description
Name	Name of the authentication server assigned to this server group
Inservice	Specifies if the server is in service or out-of-service.
trim-FDQN	If enabled, user information in an authentication request is edited before the request is sent to the server.
match-FDQN	If enabled, the authentication server is associated with a specified domain.
Priority	The priority in which the rules are applied. Rules at the top of the list are applied before rules at the bottom.
Attribute	This is the attribute returned by the authentication server that is examined for **Operation** and **Operand** match

Parameter	Description
Operation	This is the match method by which the string in **Operand** is matched with the attribute value returned by the authentication server. • **contains** – The rule is applied if and only if the attribute value contains the string in parameter **Operand**. • **starts-with** – The rule is applied if and only if the attribute value returned starts with the string in parameter **Operand**. • **ends-with** – The rule is applied if and only if the attribute value returned ends with the string in parameter **Operand**. • **equals** – The rule is applied if and only if the attribute value returned equals the string in parameter **Operand**. • **not-equals** – The rule is applied if and only if the attribute value returned is not equal to the string in parameter **Operand**. • **value-of** – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied.
Operand	This is the string to which the value of the returned attribute is matched.
Action	This parameter identifies whether the rule sets a server group role (**set role**) or a VLAN (**set vlan**).
Value	Sets the user role or VLAN ID to be assigned to the client if the condition is met.
Total Hits	Number of times the rule has been applied since the last server reboot.
New Hits	Number of times the rule has been applied since the **show aaa derivation-rules** command was last issued.

To display derivation rules for a user group, include the **user <name>** parameter. You can also display a table of all user rules by including the **user** parameter, but omitting the **<name>** parameter.

```
(host) #show aaa derivation-rules user

User Rule Table
---------------
Priority  Attribute  Operation  Operand  Action    Value  Total Hits  New Hits   Description
--------  ---------  ---------  -------  ------    -----  ----------  --------   -----------
1         location   equals     ap23     set role  guest  56          18         guestrole1
```

The following data columns appear in the output of this command:

Parameter	Description
Priority	The priority in which the rules are applied. Rules at the top of the list are applied before rules at the bottom.
Attribute	This is the attribute returned by the authentication server that is examined for **Operation** and **Operand** match.

Parameter	Description
Operation	This is the match method by which the string in **Operand** is matched with the attribute value returned by the authentication server. • **contains** – The rule is applied if and only if the attribute value contains the string in parameter **Operand**. • **starts-with** – The rule is applied if and only if the attribute value returned starts with the string in parameter **Operand**. • **ends-with** – The rule is applied if and only if the attribute value returned ends with the string in parameter **Operand**. • **equals** – The rule is applied if and only if the attribute value returned equals the string in parameter **Operand**. • **not-equals** – The rule is applied if and only if the attribute value returned is not equal to the string in parameter **Operand**. • **value-of** – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied.
Operand	This is the string to which the value of the returned attribute is matched.
Action	This parameter identifies whether the rule sets a server group role (**set role**) or a VLAN (**set vlan**).
Value	Sets the user role or VLAN ID to be assigned to the client if the condition is met.
Total Hits	Number of times the rule has been applied since the last server reboot.
New Hits	Number of times the rule has been applied since the **show aaa derivation-rules** command was last issued.
Description	This optional parameter describes the rule. If no description was configured then it does not appear when you view the User Table.

Related Commands

Command	Description	Mode
`aaa derivation-rules`	Use `aaa derivation-rules` to define the parameters displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa dns-query-period

```
show aaa dns-query-period <minutes>
```

Description

View the configured interval between DNS requests sent from the controller to the DNS server.

Syntax

No parameters

Usage Guidelines

If you define a RADIUS server using the FQDN of the server rather than its IP address, the the controller will periodically generate a DNS request and cache the IP address returned in the DNS response. By default, DNS requests are sent every 15 minute, but the interval can be changed using the aaa dns-query-period command. Issue the **show aaa dns-query-period** command to view the current DNS query interval.

Example

This command shows that the controller will send a DNS query every 30 minutes.

```
(host) # show aaa dns-query-period
DNS Query Interval = 30 minutes
```

Related Commands

To configure the DNS query interval, issue the command aaa dns-query-period.

Command History

This command was available in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show aaa fqdn-server-names

```
show aaa fqdn-server-names
```

Description

Show a table of IP addresses that have been mapped to fully qualified domain names (FQDNs).

Syntax

No parameters.

Usage Guidelines

If you define a RADIUS server using the FQDN of the server rather than its IP address, the the controller will periodically generate a DNS request and cache the IP address returned in the DNS response. Issue this command to view the IP addreses that currently correlate to each RADIUS server FQDN.

Example

The output of this command shows the IP addresses for two RADIUS servers.

```
(host) #show aaa fqdn-server-names

Auth Server FQDN names
----------------------
FQDN   IP Address  Refcount
----      ----------  --------
myhost1.example.com192.0.2.32
myhost2.example.com192.0.2.53
```

Related Commands

To configure a RADIUS authentication server using that server's fully qualified domain name, use the command aaa authentication-server radius.

Command History

This command was available in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show aaa main-profile

```
show aaa main-profile summary
```

Description

Show a summary of all AAA profiles.

Example

The output of the **show aaa main-profile summary** command shows roles, server group settings, and wire-to-wireless-roaming statistics for each AAA profile.

```
(host) #show aaa main-profile summary

AAA Profile summary
-------------------
Name          role   mac-auth  dot1x-auth   rad-acct  XML-api   RFC3576    UDR-group  ww-roam
----          ----   --------  ----------   --------  -------   -------    ---------  ------
aaa_dot1x     logon  macprof2  dot1x        RADIUS    10.3.1.15 10.3.15.2  Usr1       Disable
default       logon  macprof2  dot1x        RADIUS    10.3.1.15 10.3.15.2  Usr1       Disable
defaultguest  guest  macprof1  default      RADIUS    10.3.1.15 10.3.15.2  Usr2       Disable
```

The following data columns appear in the output of this command:

Parameter	Description
Name	Name of the AAA profile.
role	Role for unauthenticated users.
mac-auth	Name of the server group used for MAC authentication.
dot1x-auth	Name of the server group used for dot1x authentication.
rad-act	Name of the server group used for RADIUS authentication.
XML-api	IP address of a configured XML API server.
RFC3576	IP address of a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576.
UDR-group	Name of the user derivation rule profile.
ww-roam	Shows if wired-to-wireless roaming is enabled or disabled.

Related Commands

Command	Description	Mode
`aaa profile`	Use **`aaa profile`** define the parameters displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa password-policy mgmt

```
show aaa password-policy mgmt [statistics]
```

Description

Show the current password policy for management users.

Syntax

Parameter	Description
`statistics`	Include this optional parameter to show the numbers of failed login attempts and any lockout periods for management user accounts.

Examples

The output of the **show aaa password-policy mgmt** command below shows that the current password policy requires a management user to have a password with a minimum of 9 characters, including one numeric character and one special character.

```
(host) #show aaa password-policy mgmt

Mgmt Password Policy
--------------------
Parameter Value
--------- -----
Enable password policy Yes
Minimum password length required 9
Minimum number of Upper Case characters 0
Minimum number of Lower Case characters 0
Minimum number of Digits 1
Minimum number of Special characters (!, @, #, $, %, ^, &, *, <, >, {, }, [, ], :, ., comma, |, +, ~, `) 1
Username or Reverse of username NOT in Password No
Maximum Number of failed attempts in 3 minute window to lockout user 0
Time duration to lockout the user upon crossing the "lock-out" threshold 3
Maximum consecutive character repeats 0
```

The following data columns appear in the output of this command:

Parameter	Description
Enable password policy	Shows if the defined policy has been enabled
Minimum password length required	Minimum number of characters required for a management user password. The default setting is 6 characters.
Minimum number of Upper Case characters	The maximum number of uppercase letters required for a management user password. By default, there is no requirement for uppercase letters in a password, and the parameter has a default value of 0.
Minimum number of Lower Case characters	The maximum number of lowercase letters required for a management user password. By default, there is no requirement for lowercase letters in a password, and the parameter has a default value of 0.
Minimum number of Digits	Minimum number of numeric digits required in a management user password. By default, there is no requirement for digits in a password, and the parameter has a default value of 0.
Minimum number of Special characters	Minimum number of special characters required in a management user password. By default, there is no requirement for special characters in a password, and the parameter has a default value of 0.

Parameter	Description
Username or Reverse of username NOT in Password	If **Yes**, a management user's password cannot be the user's username or the username spelled backwards. If **No**, the password can be the username or username spelled backwards.
Maximum Number of failed attempts in 3 minute window to lockout user	Number of times a user can unsuccessfully attempt to log in to the controller before that user gets locked out for the time period specified by the **lock-out threshold** below. By default, the password lockout feature is disabled, and the default value of this parameter is 0 attempts.
Time duration to lockout the user upon crossing the "lock-out" threshold	Amount of time a management user will be "locked out" and prevented from logging into the controller after exceeding the maximum number of failed attempts setting show above. The default lockout time is 3 minutes.
Maximum consecutive character repeats	The maximum number of consecutive repeating characters allowed in a management user password. By default, there is no limitation on the numbers of character that can repeat within a password, and the parameter has a default value of 0 characters.

Include the optional **statistics** parameter to show failed login statistics in the Management User table. The example below shows that a single failed login attempt locked out the root user **admin14**, and displays the time when that user can attempt to login to the controller again.

```
(host) #show aaa password-policy mgmt statistics

Management User Table
---------------------
USER    ROLE   FAILED_ATTEMPTS  STATUS
----    ----   ---------------  ------
admin14 root   1                Locked until 12/1/2009 22:28
```

Related Commands

Command	Description	Mode
`aaa profile`	Use **`aaa profile`** define the parameters displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 3.4.2.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa profile

```
show aaa profile <profile-name>
```

Description

Show configuration details for an individual AAA profile.

Example

The output of the following command shows roles, servers and server group settings, and wire-to-wireless-roaming statistics for each AAA profile.

```
(host) #show ap profile aaa_dot1x

AAA Profile "aaa_dot1x"
-----------------------
Parameter                          Value
---------                          -----
Initial role                       logon
MAC Authentication Profile         macprof2
MAC Authentication Default Role    guest
MAC Authentication Server Group    svrgrp
802.1X Authentication Profile      dot1x
802.1X Authentication Default Role guest
802.1X Authentication Server Group Internal
RADIUS Accounting Server Group     RADIUS
XML API server                     10.3.1.15
RFC 3576 server                    10.3.15.2
User derivation rules Usr1
Wired to Wireless Roaming          Enabled
SIP authentication role            N/A
```

The following data columns appear in the output of this command:

Parameter	Description
Name	The name of the AAA profile.
Initial Role	Role for unauthenticated users.
MAC Authentication Profile	Name of the MAC authentication profile.
MAC Authentication Default Role	Configured role assigned to the user after MAC authentication.
MAC Authentication Server Group	Name of the server group used for MAC authentication.
8021.X Authentication Profile	Name of the 802.1x authentication profile.
8021.X Authentication Default Role	Configured role assigned to the user after 802.1x authentication.
8021.X Authentication Server Group	Name of the server group used for 802.1x authentication.
RADIUS Accounting Server Group	Name of the server group used for RADIUS authentication.
XML API server	IP address of a configured XML API server.
RFC 3576 server	IP address of a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576.
User derivation rules	Name of the user derivation rule profile.
Wired to Wireless Roaming	Shows whether Wired to Wireless Roaming is **Enabled** or **Disabled**.

Parameter	Description
SIP authentication role	For controllers with an installed PEFNG license, this parameter displays the configured role assigned to a session initiation protocol (SIP) client upon registration.

Related Commands

Command	Description	Mode
`aaa profile`	Use the command **`aaa profile`** to define AAA profiles.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa radius-attributes

```
show aaa radius-attributes
```

Description

Show RADIUS attributes recognized by the controller.

Example

The output of the following command shows the name, currently configured value, type, vendor and RADIUS ID for each attribute.

```
(host) #show aaa radius-attributes

Dictionary
----------
Attribute                     Value  Type     Vendor     Id
---------                     -----  ----     ------     --
MS-CHAP-NT-Enc-PW             6      String   Microsoft  311
Suffix                        1004   String
Menu                          1001   String
Acct-Session-Time             46     Integer
Framed-AppleTalk-Zone         39     String
Connect-Info                  77     String
Acct-Ouput-Packets            48     Integer
Aruba-Location-Id             6      String   Aruba      14823
Service-Type                  6      Integer
Rad-Length                    310    Integer
CHAP-Password                 3      String
Aruba-Template-User           8      String   Aruba      14823
Event-Timestamp               55     Date
Login-Service                 15     Integer
Exec-Program-Wait             1039   String
Tunnel-Password               69     String
Framed-IP-Netmask             9      IP Addr
Acct-Output-Gigawords         53     Integer
MS-CHAP-CPW-2                 4      String   Microsoft  311
Acct-Tunnel-Packets-Lost      86     Integer
    ...
```

Related Commands

Command	Description	Mode
`aaa profile`	Use the command **`aaa profile`** to define AAA profiles.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa rfc-3576-server

```
show aaa rfc-3576-server [statistics|<udp-port>]
```

Description

Show configuration details for an RFC-3576 server, which is a RADIUS server that can send user disconnect and change-of-authorization (CoA) messages, as described in RFC 3576.

Example

This first example shows that there are two configured servers in the RFC 3567 Server List. The **References** column lists the number of other profiles with references to the RFC 3567 server, and the **Profile Status** column indicates whether the server is predefined. User-defined servers will not have an entry in the **Profile Status** column.

```
(host) #show aaa rfc-3567-server

RFC 3576 Server List
--------------------
Name       References  Profile Status
----       ----------  --------------
10.2.14.6  2
```

To view details for all RFC 3576 servers, include the **statistics** parameter.

```
(host) #show aaa rfc-3576-server statistics

RADIUS RFC 3576 Statistics
--------------------------
Statistics           10.1.2.3  10.1.2.34
----------           --------  ---------
Disconnect Requests  13 3
Disconnect Accepts   12  3
Disconnect Rejects   1   0
No Secret            0         0
No Session ID        0         0
Bad Authenticator    0         0
Invalid Request      0         0
Packets Dropped      0         2
Unknown service      0         0
CoA Requests         1  0
CoA Accepts          1  0
CoA Rejects          0         0
No permission        0         0

Packets received from unknown clients: 0
Packets received with unknown request: 0
Total RFC3576 packets Received       : 0
```

The output of the **show aaa rfc-3576-server statistics** command includes the following parameters:

Parameter	Description
Disconnect Requests	Number of disconnect requests sent by the server.
Disconnect Accepts	Number of disconnect requests sent by the server that were accepted by the user.
Disconnect Rejects	Number of disconnect requests sent by the server that were rejected by the user.
No Secret	Number of authentication requests that did not contain a RADIUS secret.
No Session ID	Number of authentication requests that did not contain a session ID.

Parameter	Description
Bad Authenticator	Number of authentication requests that contained a missing or invalid authenticator field in the packet.
Invalid Request	Number of invalid requests.
Packets Dropped	Number of packets dropped.
Unknown service	Number of requests for an unknown service type.
CoA Requests	Number of requests for a Change of Authorization (CoA).
CoA Accepts	Number of times a CoA request was accepted.
CoA Rejects	Number of times a CoA request was rejected.
No permission	Number of requests for a service that has been defined, but has not been administratively enabled.

Related Commands

Command	Description	Mode
`aaa rfc-3576-server`	Define RFC 3576 server profiles.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa server-group

```
show aaa server-group [<group-name>|summary]
```

Description

Show configuration details for your AAA server groups.

Syntax

Parameter	Description
<group-name>	The name of an existing AAA server group.

Usage Guidelines

Issue this command without the **<group-name>** or **summary** options to display the entire server group list, including profile status and the number of references to each profile.The **References** column lists the number of other profiles that reference a server group, and the **Profile Status** column indicates whether the server group is predefined. User-defined server groups will not have an entry in the Profile Status column. Examples

This first example shows that there are five configured server groups

```
(host) #show aaa server-group summary

Server Group List
-----------------
Name                    References  Profile Status
----                    ----------  --------------
auth-profile-2          1
coltrane-server-group   1
default                 25
group1                  0
internal                0           Predefined

Total:5
```

.To view additional statistics for all server groups, include the **statistics** parameter.

```
(host) #show aaa server-group summary
Server Groups
-------------
Name                    Servers  Rules  hits  Out-of-service
----                    -------  -----  ----  --------------
auth-profile-2          1        0      0
coltrane-server-group   1        0      0
default                 1        0      0
group1                  1        1      0
internal                1        1      0
```

The output of the show aaa server-group summary command includes the following parameters:

Parameter	Description
name	Name of an existing AAA server group.
Servers	Number of servers in the group.
Rules	Number of rules configured for the server group.

Parameter	Description
hits	Number of hits for the server's rules.
Out-of-Service	Indicates whether the server is active, or out of service. Active servers may not have an entry in the Out-of-Service column.

To display detailed authorization, role and vlan statistics for an individual server group, include the name of the group for which you want more information.

```
(host) #show aaa server-group summary group1

Fail Through:No

Auth Servers
------------
Name      Server-Type  trim-FQDN  Match-Type  Match-Op  Match-Str
----      -----------  ---------  ----------  --------  ---------
rad1      Radius       No         authstring  equals    company_eng
rad3      Radius       No         authstring  equals    company_qa

Role/VLAN derivation rules
--------------------------
Priority  Attribute  Operation  Operand  Action    Value
--------  ---------  ---------  -------  ------    -----
1         class      contains   admin    set role  root
```

The output of the **show aaa server-group <group-name>** command includes the following parameters:

Parameter	Description
Name	Specifies if the server is in service or out-of-service.
Server-Type	If enabled, user information in an authentication request is edited before the request is sent to the server.
trim-FDQN	If enabled, user information in an authentication request is edited before the request is sent to the server.
Match-Type	If the match type is **authstring** he authentication server associates with a match rule that the controller can compare with the user/client information in the authentication request. A **fdqn** match type associates the authentication server with a specified domain. An authentication request is sent to the server only if there is an exact match between the specified domain and the <domain> portion of the user information sent in the authentication request.

Parameter	Description
Match-Op	This is the match method by which the string in **Match-Str** is matched with the attribute value returned by the authentication server. • **contains** – The rule is applied if and only if the attribute value contains the string in parameter **Operand**. • **starts-with** – The rule is applied if and only if the attribute value returned starts with the string in parameter **Operand**. • **ends-with** – The rule is applied if and only if the attribute value returned ends with the string in parameter **Operand**. • **equals** – The rule is applied if and only if the attribute value returned equals the string in parameter **Operand**. • **not-equals** – The rule is applied if and only if the attribute value returned is not equal to the string in parameter **Operand**. • **value-of** – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied
Match-Str	This is the string to which the value of the returned attribute is matched.
Priority	The priority in which role or VLAN derivation rules are applied. Rules at the top of the list are applied before rules at the bottom.
Attribute	For role or VLAN derivation rules, this is the attribute returned by the authentication server that is examined for **Operation** and **Operand** match.
Operation	For role or VLAN derivation rules, this is the match method by which the string in **Operand** is matched with the attribute value returned by the authentication server. • **contains** – The rule is applied if and only if the attribute value contains the string in parameter **Operand**. • **starts-with** – The rule is applied if and only if the attribute value returned starts with the string in parameter **Operand**. • **ends-with** – The rule is applied if and only if the attribute value returned ends with the string in parameter **Operand**. • **equals** – The rule is applied if and only if the attribute value returned equals the string in parameter **Operand**. • **not-equals** – The rule is applied if and only if the attribute value returned is not equal to the string in parameter **Operand**. • **value-of** – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied.
Operand	For role or VLAN derivation rules, this is the string to which the value of the returned attribute is matched.
Action	This parameter identifies whether the derivation rule sets a server group role (**set role**) or a VLAN (**set vlan**).
Value	Sets the user role or VLAN ID to be assigned to the client if the rule condition is met.

Related Commands

Command	Description	Mode
`aaa server-group`	Use **`aaa server-group`** to configure the settings displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa state ap-group

```
show aaa state ap-group
```

Description

Show the names and ID numbers of your AP groups

Example

This first example shows that the selected controller has two defined AP groups.

```
(host) #show aaa state ap-group

AP Group Table
--------------
Name  ID
----  --
ap1   1
ap2   2
```

Related Commands

Command	Description	Mode
`aaa server-group`	Use **`aaa server-group`** to define the AP groups displayed in the output of this show command	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

.

show aaa state configuration

```
show aaa state configuration
```

Description

Display authentication state configuration information, including the numbers of successful and failed authentications.

Example

This example shows authentication settings and values for a controller with no current users.

```
(host) #show aaa state configuration

Authentication State
--------------------
Name                         Value
----                         -----
Switch IP                    10.6.2.253
Master IP                    10.100.103.253
Switch Role                  local
Current/Max/Total Users      129/234/4058
Current/Max/Total Stations   121/190/367550
Captive Portal Users         4
802.1x Users                 119
VPN Users                    0
MAC Users                    0
Stateful 802.1x Users        0
Tunneled users               0
Configured user roles        21
Configured session ACL       41
Configured destinations      32
Configured services          77
Configured Auth servers      9
Auth server in service       9
Radius server timeouts       7062

Successful authentications
--------------------------
Web  MAC  VPN  802.1x  Krb  RadAcct  SecureID  Stateful-802.1x  Management
---  ---  ---  ------  ---  -------  --------  ---------------  ----------
138  0    0    10117   0    0        0         0                0

Failed authentications
----------------------
Web  MAC  VPN  802.1x  Krb  RadAcct  SecureID  Stateful-802.1x  Management
---  ---  ---  ------  ---  -------  --------  ---------------  ----------
48   0    0    32235   0    0        0         0                0

Idled users              = 3366
Mobility                 = Enabled
fast age                 = Disabled
Bandwidth contracts       = 2/1
IP takeovers             = 21
Ping/SYN/Session attacks = 0/0/0
```

The output of the **show aaa state configuration** command includes the following parameters:

Parameter	Description
Switch IP	IP address of the local controller.
Master IP	IP address of the master controller.
Switch Role	Role assigned to the controller on which you issued the **show aaa state** command.
Current/Max/Total Users	Current number of users on the controller/Maximum number of users that can be assigned to the controller at any time/Total number of users that have been assigned to the controller since the last controller reboot.
Current/Max/Total Stations	Current number of stations registered with the controller/Maximum number of stations that can be registered with the controller at any time/Total number of stations that have registered the controller since the last controller reboot.
Captive Portal Users	Number of current users authenticated via captive portal.
802.1x Users	Number of current users authenticated via 802.1x authentication.
VPN Users	Number of current users authenticated via VPN authentication.
MAC Users	Number of current users authenticated via MAC authentication.
Stateful 802.1x Users	Number of current users authenticated via stateful 802.1x authentication.
Tunneled users	Number of stations in tunneled forwarding mode, where 802.11 frames are tunneled to the controller using generic routing encapsulation (GRE).
Configured user roles	Number of configured user roles.
Configured session ACL	Number of configured session ACLs.
Configured destinations	Number of destinations configured using the `netdestination` command.
Configured services	Number of service aliases configured using the `netservice` command.
Configured Auth servers	Number of configured authentication servers.
Auth server in service	Number of authentication servers currently in service.
Radius server timeouts	Number of times the RADIUS server did not respond to the authentication request.
Web	Total number of captive portal authentications or authentication failures since the last controller reset.
MAC	Total number of MAC authentications or authentication failures since the last controller reset.
VPN	Total number of VPN authentications or authentication failures since the last controller reset.
802.1x	Total number of 802.1x authentications or authentication failures since the last controller reset.
Krb	Total number of Kerberos authentications or authentication failures since the last controller reset.
RadAcct	Total number of RADIUS accounting verifications or accounting failures since the last controller reset.
SecureID	Number of authentication verifications or failures using methods which use one-time passwords. (For example, EAP-GTC being used as the inner EAP protocol of EAP-PEAP.)
Stateful-802.1x	Total number of Stateful 802.1x authentications or authentication failures since the last controller reset.

Parameter	Description
Management	Total number of Management user authentications or authentication failures since the last controller reset.
Idled users	Total number of users that are not broadcasting data to an AP.
Mobility	Shows whether the IP mobility feature has been enabled or disabled on the controller.
fast age	When the **fast age** feature allows the controller actively sends probe packets to all users with the same MAC address but different IP addresses. The users that fail to respond are purged from the system. This parameter shows if fast aging of user table entries has been enabled or disabled.
Bandwidth contracts	Number of configured bandwidth contracts on the controller.
IP takeovers	Number of times a two different stations have attempted to use the same IP address (IP spoofing).
Ping/SYN/Session attacks	Number of reported ping, SYN and session attacks.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa state debug-statistics

```
show aaa state debug statistics
```

Description

show debug statistics for controller authentication, authorization and accounting.

Syntax

No parameters.

Example

The following example displays debug statistics for a variety of authentication errors.

```
(host) #show aaa state debug-statistics
user miss: ARP=47, 8021Q=5216, non-IP=0, zero-IP=0, loopback=0
user miss: mac mismatch=0, spoof=269 (74), drop=390, ncfg=0
Idled users = 3376
Idled users due to MAC mismatch = 0
Logon lifetime iterations = 4501, entries deleted = 121
SIP authentication messages received 29227, dropped 29227
Missing auth user deletes: 0
```

The output of this command includes the following parameters:

Parameter	Description
ARP	Number of ARP packets sent between the datapath and the controlpath.
8021q	Number of 802.1q (VLAN tag) packets sent between the datapath and the controlpath.
non-ip	Number of non-ip type packets sent between the datapath and the controlpath.
zero-ip	Number packets sent without an internet protocol (IP).
loopback	If **1**, the controller has a defined loopback address. If **0**, a loopback address has not yet been configured.
mac mismatch	Number of users that were not authenticated due to MAC mismatches.
spoof	Number of users that were not authenticated due to spoofed IP addresses.
drop	Number of user authentication attempts that were dropped.
ncfg	Number of packets sent between datapath and controlpath, where the authentication module has not completed the initialization required to process the traffic.
idled users	Number of inactive stations that are not broadcasting data to an AP.
idled users due to MAC mismatch	For internal use only.
Logon lifetime iteration	Number of users deleted for lack of activity.
SIP authentication message	Number of session initiation protocol (SIP) authentication messages received.
Missing auth user deletes	Number of users removed from the datapath by the auth module, even without a mapping entry in control path. This counter can help identify problems with messages sent between the controlpath and the datapath.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local or local controllers

show aaa state messages

Description

Display numbers of authentication messages sent and received.

Syntax

No parameters.

Usage Guidelines

This command displays a general overview of authentication statistics. To view authentication information for specific profiles such as a captive-portal, MAC or 801.x authentication profile, issue the commands specific to those features.

Example

The output of this command displays tables of statistics for PAPI, RAW socket and Sibyte messages.

```
(host) #show aaa state messages
PAPI Messages
-------------
Msg ID  Name                    Since last Read  Total
------  ----                    ---------------  -----
5004    set master ip           2                2
7005    Set switch ip           1                1
7007    Set VLAN ip             5                5
66      delete xauth vpn users  1                1

RAW socket Messages
-------------------
Msg ID  Name                         Since last Read  Total
------  ----                         ---------------  -----
1       raw PAP req                  188              188
33      captive portal config        11113            11113
59      TACACS ACCT config for cli   1                1
60      TACACS ACCT config for web   1                1

Sibyte Messages
---------------
Opcode  Name        Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
------  ----        --------------------  ----------  --------------------  ----------
2       bridge      21                    21          0                     0
4       session     4877                  4877        0                     0
11      ping        768                   768         768                   768
13      8021x       114563                114563      229126                229126
15      acl         803                   803         0                     0
16      ace         5519                  5519        0                     0
17      user        781821                781821      0                     0
27      bwm         3                     3           0                     0
29      wkey        27109                 27109       4                     4
42      nat         1                     1           0                     0
43      user tmout  4164                  4164        4160                  4160
56      forw unenc  1787103               1787103     0                     0
64      auth        5268                  5268        5267                  5267
94      aesccm key  17885                 17885       0                     0
111     dot1x term  196813                196813      151161                151161
114     rand        1614                  1614        1612                  1612
126     eapkey      1316231               1316231     2632462               2632462

114     rand        2                     2           0                     0
```

The output of this command contains the following parameters:

Parameter	Description
`Msg ID`	ID number for the message type
`Name`	Message name
`Since last Read`	Number of messages received since the buffer was last read.
`Total`	Total number of message received since the controller was last reset.
`opcode`	Code number of the message type.
`Sent Since last Read`	Number of messages sent since the buffer was last read.
`Sent Total`	Total number of message sent since the controller was last reset.
`Recv Since last Read`	Number of messages received since the buffer was last read.
`Recv Total`	Total number of message received since the controller was last reset.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show aaa state station

```
show aaa state station <A:B:C:D:E:F>
```

Description

Display AAA statistics for a station.

Syntax

Parameter	Description
<A:B:C:D:E:F>	MAC address of a station/

Example

The example below shows statistics for a station with four associated user IP addresses. The output of this command shows station data, the AAA profiles assigned to the station, and the station's authentication method.

```
(host) #show aaa state station 00:21:5c:85:d0:4b

Association count = 1, User count = 4
User list = 10.1.10.10 10.6.5.168 192.168.229.1 192.168.244.1
essid: ethersphere-wpa2, bssid: 00:1a:1e:8d:5b:31 AP name/group: AL40/corp1344 PHY: a, ingress=0x10e8
(tunnel 136)
vlan default: 65, assigned: 0, current: 65 cached: 0, user derived: 0, vlan-how: 0
name: MYCOMPANY\tgonzales, role:employee (default:logon, cached:employee, dot1x:), role-how: 1, acl:51/0,
age: 00:02:50
Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-MD5, server: vortex
dot1xctx:1 sap:1
Flags: mba=0
AAA prof: default-corp1344, Auth dot1x prof: default, AAA mac prof:, def role: logon
ncfg flags udr 1, mac 0, dot1x 1
Born: 1233767066 (Wed Feb  4 09:04:26 2009
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show aaa state user

```
show aaa state user <A.B.C.D>
```

Description

Display statistics for an authenticated user.

Syntax

Parameter	Description
<A.B.C.D>	IP address of a user.

Example

The example below shows statics for a user with the IP address 10.1.10.11. The output of this command shows user data, the user's authentication method. and statistics for assigned roles, timers and flags.

```
(host) #show aaa state user 10.1.10.11
Name: MYCOMPANY\tsenter, IP: 10.1.10.11, MAC: 00:21:5c:85:d0:4a, Role:employee, ACL:51/0, Age: 00:01:46
Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-MD5, server: vortex
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: Default
VLAN Derivation: Matched user rule
Idle timeouts: 0, ICMP requests sent: 0, replies received: 0, Valid ARP: 0
Mobility state: Associated, HA: Yes, Proxy ARP: No, Roaming: No Tunnel ID: 0 L3 Mob: 0
Flags: internal=0, trusted_ap=0, delete=0, l3auth=0, l2=1 mba=0
Flags: innerip=0, outerip=0, guest=0, station=0, download=1, nodatapath=0
Auth fails: 0, phy_type: a-HT, reauth: 0, BW Contract: up:0 down:0, user-how: 1
Vlan default: 65, Assigned: 0, Current: 65 vlan-how: 0
Mobility Messages: L2=0, Move=0, Inter=0, Intra=0, ProxyArp=0, Flags=0x0
Tunnel=0, SlotPort=0x1018, Port=0x10e2 (tunnel 130)
Role assigned: n/a, VPN: n/a, Dot1x:  Name: employee role-how: 0
Essid: ethersphere-wpa2, Bssid: 00:1a:1e:11:6b:91 AP name/group: AL31/corp1344 Phy-type: a-HT
RadAcct sessionID:n/a
RadAcct Traffic In 0/0 Out 0/0 (0:0/0:0:0:0,0:0/0:0:0:0)
Timers: arp_reply 0, spoof reply 0, reauth 0
Profiles AAA:default-corp1344, dot1x:default, mac: CP: def-role:'logon' sip-role:''
ncfg flags udr 0, mac 0, dot1x 0
Born: 1233772328 (Wed Feb  4 10:32:08 2009)
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show aaa sygate-on-demand (deprecated)

```
show aaa sysgate-on-demand
```

Syntax

No parameters.

Command History

Release	Modification
ArubaOS 3.0	Command introduced.
ArubaOS 3.4	Command deprecated.

show aaa tacacs-accounting

Description

Show TACACS accounting configuration.

Syntax

No parameters.

Example

The example below shows that TACACS accounting has been enabled, and that the TACACS server is in the server group acct-**server**.

```
(host) #show aaa tacacs-accounting
TACACS Accounting Configuration
-------------------------------
Parameter      Value
---------      -----
Mode           Enabled
Server-Group   acct-server
```

The output of this command includes the following parameters:

Parameter	Description
Mode	Shows if the TACACS accounting feature is enabled or disable
Server-Group	The server group that contains the active TACACS server.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show aaa timers

Description

Show AAA timer values.

Syntax

No parameters

Example

The example below shows that the controller has all default timer values:

```
(host) #show aaa timers
User idle timeout = 6 minutes
Auth Server dead time = 10 minutes
Logon user lifetime = 5 minutes
```

Related Commands

Command	Description	Mode
`aaa timers`	Use `aaa timers` to define the settings displayed in the output of this show command.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show aaa xml-api server

```
show aaa xml-api server [<server_ip>]
```

Description

Show a list of XML servers used for authentication, authorization and accounting.

Syntax

Parameter	Description
<server_ip>	IP address of an XML API server. Include this parameter to see if a secret key is configured for the specified server.

Example

The output of this command shows that the controller has two configured XML API servers that are each referenced by two different AAA profiles. Note that user-defined servers will not have an entry in the **Profile Status** column.

```
(host) #show aaa xml-api statistics
XML API Server List
-------------------
Name      References  Profile Status
----      ----------  --------------
10.1.2.3  2
10.4.3.2  2
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show aaa web admin-port

```
show aaa web admin-port
```

Description

Show the port numbers of HTTP and HTTPS ports used for web administration.

Syntax

No parameters.

Example

The example below shows that the controller is configured to use HTTPS on port 4343, and HTTP on port 8888.

```
(host) #show aaa web admin-port
https port = 4343
http  port = 8888
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show aaa xml-api statistics

```
show aaa xml-api statistics
```

Description

Display statistics for an external XML API server.

Syntax

Parameter	Description
<server_ip>	IP address of XML API server.

Usage Guidelines

Issue this command to troubleshoot AAA problems and monitor usage on an XML server.

Example

The example below shows AAA statistics for an external XML server with the IP address 10.1.2.3. This command shows the number of times that a particular event has occurred per client. The first number is the total number of times that this event has occurred is displayed firs. The number of new events since the last time the counters were displayed is shown in parentheses.

```
(host) #show aaa xml-api statistics
Statistics                          10.1.2.3
----------                          --------
user_authenticate                   0 (0)
user_add                            0 (0)
user_delete                         0 (0)
user_blacklist                      0 (0)
user_query                          0 (0)
unknown user                        0 (0)
unknown role                        0 (0)
unknown external agent              0 (0)
authentication failed               0 (0)
invalid command                     0 (0)
invalid message authentication method  0 (0)
invalid message digest              0 (0)
missing message authentication      0 (0)
missing or invalid version number   0 (0)
internal error                      0 (0)
client not authorized               0 (0)
Cant use VLAN IP                    0 (0)
Invalid IP                          0 (0)
Cant use Switch IP                  0 (0)
missing MAC address                 0 (0)
Packets received from unknown clients: 0 (0)
Packets received with unknown request: 0 (0)
Requests Received/Success/Failed    :  0/0/0 (0/0/0)
```

The output of this command includes the following parameters:

Parameter	Description
user_authenticate	Number of users authenticated on the XML server since the last controller reboot.
user_add	Number of users added to the controller's user table.
user_delete	Number of users removed from the controller's user table.

Parameter	Description
user_blacklist	Number of denied user association requests.
user_query	Number of user queries performed.
unknown user	Number of unknown users.
unknown role	Number of unknown user roles.
unknown external agent	Number of requests by an unknown external agent.
authentication failed	Number of failed authentication requests.
invalid command	Number of invalid XML commands
invalid message authentication method	Number of XML commands with an invalid authentication method (when a key is configured on the controller).
invalid message digest	Number of XML commands with an invalid digest type (when a key is configured on the controller).
missing message authentication	Number of XML commands with an missing authentication method (when a key is configured on the controller).
missing or invalid version number	`Number of commands with a missing or invalid version number. The version number should always be 1.0.`
internal error	Number of internal server errors
client not authorized	Number of unauthorized clients
Cant use VLAN IP	Number of time a user IP is same as the VLAN IP.
Invalid IP	Number of XML commands with an invalid IP address.
Cant use Switch IP	Redirection to a IP failed, possibly because the source IP has been NATted.
missing MAC address	Number of XML commands with a missing MAC address.
Packets received from unknown clients	Number of packets received from unknown clients.
Packets received with unknown request	Number of packets received with unknown request
Requests Received/Success/ Failed	Total number of requests received / number of successful requests / number of failed requests

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show acceleration

```
aaa authentication
show acceleration
   cifs {ap-name <ap-name>}|{ipaddr <ip-addr>}
   configuration {ap-name <ap-name>}|{ipaddr <ip-addr>}
   connections {ap-name <ap-name>}|{ipaddr <ip-addr>}
   counters all {ap-name <ap-name>}|{ipaddr <ip-addr>}
   debug {buffers|heap|trace-buffer}|{ap-name <ap-name>}|{ipaddr <ip-addr>}
   mapi {ap-name <ap-name>}|{ipaddr <ip-addr>}
   protocol{cifs|http|mapi}|{acceleration|bandwidth {ap-name <ap-name>}|{ipaddr <ip-
   addr>}}
   proxy {ap-name <ap-name>}|{ipaddr <ip-addr>}
```

Description

This command shows the Application Acceleration Service feature statistics.

Syntax

Parameter	Description
`cifs`	The Cached File Information system for the AP.
`configuration`	Application acceleration configuration information for the AP.
`connections`	Active connections for the AP.
`counters all`	Non-zero statistics for the AP.
`debug`	Shows acceleration application statistics for troubleshooting purposes.
`buffers`	Buffer allocation histogram statistics for the AP.
`heap`	Heap allocation histogram statistics for the AP.
`trace-buffer`	Trace buffer statistics. for the AP.
`mapi`	Shows the messaging API state for AP.
`protocol`	Shows protocol acceleration and bandwidth counter statistics for CIFS, HTTP and MAPI.
`proxy`	Shows active proxied requests for AP.
`ap-name <ap-name>`	Name of the AP.
`ipaddr <ip-addr>`	IP address.

Usage Guidelines

Use the **show application acceleration** command to display various application acceleration AP statistics for troubleshooting purposes. Use the command acceleration to configure a RAP to use the Application Acceleration Service feature to increase application performance. Refer to chapter titled, "Application Acceleration Module," in the *ArubaOS 5.0 User Guide* for detailed information about using this feature.

Example

This example displays all acceleration counters for the AP "ap123."

```
(A3200) #show acceleration counters all ap-name ap123

All Non-Zero Counters
Heap Statistics:
        Current Entries:          3     Maximum Entries:      25088
        High Water Mark:          3     Total Entries:            3
        Current Bytes:        12324     Maximum Bytes:      8388608
Socket Statistics:
        Current Entries:          1     Maximum Entries:        256
        High Water Mark:          1     Total Entries:        12204
Buffer Statistics:
        Current Entries:          2     Maximum Entries:        512
        High Water Mark:          3     Total Entries:            4

Request Statistics:
        Current Entries:          1     Maximum Entries:        256
        High Water Mark:          1     Total Entries:        12204
        RxQ High Water:           1     TxQ High Water:           0
Peer Statistics:
        Updates:                  0     Update Errors:        12204
```

Related Commands

Command	Description	Mode
acceleration	Use the acceleration command to configure the Application Acceleration Service. This feature improves application performance.	Config mode

Command History

This command was introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Application-Acceleration license	Enable or Config mode on master or local controllers

show acl ace-table

```
show acl ace-table {ace <0-1999>}|{acl <1-2700>}
```

Description

Show an access list entry (ACE) table for an access control list (ACL).

Syntax

Parameter	Description
`ace <0-1999>`	Show a single ACE entry.
`acl <1-2700>`	Show all ACE entries for a single ACL.

Example

The following example shows that there are eighteen access control entries for ACL 1.

```
(host) #show acl ace-table acl 1
  1020: any any  1  0-65535  0-65535  f80001:permit
  1021: any any  17  0-65535  53-53  f80001:permit
  1022: any any  17  0-65535  8211-8211  f80001:permit
  1023: any any  17  0-65535  8200-8200  f80001:permit
  1024: any any  17  0-65535  69-69  f80001:permit
  1025: any any  17  0-65535  67-68  f80001:permit
  1026: any any  17  0-65535  137-137  f80001:permit
  1027: any any  17  0-65535  138-138  f80001:permit
  1028: any any  17  0-65535  123-123  f80001:permit
  1029: user 10.6.2.253 255.255.255.255  6  0-65535  443-443  f80001:permit
  1030: user any  6  0-65535  80-80   d1f90,0000 f80021:permit dnat
  1031: user any  6  0-65535  443-443   d1f91,0000 f80021:permit dnat
  1032: any any  17  0-65535  500-500  f80001:permit
  1033: any any  50  0-65535  0-65535  f80001:permit
  1034: any any  17  0-65535  1701-1701  f80001:permit
  1035: any any  6  0-65535  1723-1723  f80001:permit
  1036: any any  47  0-65535  0-65535  f80001:permit
  1037: any any  0  0-0  0-0  f180000:deny
```

Related Commands

Configure ACLs using the command **`ip access-list session`**.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

show acl acl-table

```
show acl acl-table <1-2700>
```

Description

Display information for a specified access control list (ACL).

Syntax

Parameter	Description
`acl-table <1-2700>`	Specify the number of the ACL for which you want to view information.

Example

The following example displays the ACL table for the controller.

```
(host) #show acl acl-table acl 1

AclTable
--------
ACL  Type  ACE Index  Ace Count  Name   Applied
---  ----  ---------  ---------  ----   -------
1    role  1459       18         logon  0

Total free ACE entries = 3591
Free ACE entries at the bottom = 2552
Next ACE entry to use = 1480 (table 1)
Ace entries reused 622 times
ACL count 64, tunnel acl 0

Ace entries reused 373 times
ACL count 64, tunnel acl 0
```

The output of this command displays the following parameters:

Parameter	Description
ACL	Number of the specified ACL
Type	Shows the ACL type: • **role**: Access list is used to define a user role. • **mac**: MAC ACLs allow filtering of non-IP traffic. This ACL filters on a specific source MAC address or range of MAC addresses. • **session**: Session ACLs define traffic and firewall policies on the controller. • **ether-type**: This type of ACL filters on the Ethertype field in the Ethernet frame header, and is useful when filtering non-IP traffic on a physical port. • **standard**: Standard ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source address of the packet.
ACE Index	Starting index entry for the ACL's access control entries
ACE count	Number of access control entries in the ACL
Name	Name of the access control list
Applied	Number of times the ACL was applied to a role.
Total free ACE entries	The total number of free ACE entries. This includes available ACE entries at the bottom of the list, as well as free ACE entries in the middle of the table from previous access list entries that were later removed.

Parameter	Description
Free ACE entries at the bottom	The total number of free ACE entries at the bottom of the list.
Next ACE entry to use	Ace number of the first free entry at the bottom of the list.
ACE entries reused	For internal use only.
ACL count	Total number of defined ACLs
Tunnel ACL	Total number of defined tunnel ACLs.

The following example displays the ACL table for ACL 1.

```
(host) #show acl ace-table acl 1
Acl Table
--------
ACL  Type  ACE Index  Ace Count  Name   Applied
---  ----  ---------  ---------  ----   -------
1    role  1020       18         logon  0

Total free ACE entries = 3591
Free ACE entries at the bottom = 2991
Next ACE entry to use = 1041 (table 1)
Ace entries reused 373 times
ACL count 64, tunnel acl 0
```

Related Commands

Configure ACLs using the command `ip access-list session`.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

show acl hits

```
show acl hits
```

Description

Show internal ACL hit counters.

Syntax

No parameters.

Usage Guidelines

Issue this command to see the number of times an access control list defined a user's role, or traffic and firewall policies for a user session.

Example

In the example below, the output of the *User Role ACL Hits* table is shown in two separate tables to allow the output to fit on a single page of this document. In the actual controller command-line interface, the *User Role ACL Hits* table is shown in a single, wide table.

```
(host) #show acl ace-table acl 1
User Role ACL Hits
------------------
Role            Policy               Src           Dst
----            ------               ---           ---
logon           control              any           any
logon           control              any           any
logon                                any           any
visitor         vp-control           any           any
visitor         vp-control           any           any
visitor         vp-access            any           any
visitor         vp-access            user          mswitch-master
visitor         vp-access            any           any

User Role ACL Hits
------------------
Service       Action   Dest/Opcode  New Hits  Total Hits  Index
-------       ------   -----------  --------  ----------  -----
svc-icmp      permit                0         6           5052
svc-dhcp      permit                0         2           5057
0             deny                  0         53          5069
svc-dns       permit                9         46079       4885
svc-dhcp      permit                0         788         4886
svc-icmp      permit                0         536         4887
svc-http      permit                0         41          4889
6 9100-9100   permit                0         31          4892
Port Based Session ACL
----------------------
Policy     Src                    Dst  Service  Action  Dest/Opcode  New Hits  Total Hits  Index
------     ---                    ---  -------  ------  -----------  --------  ----------  -----
validuser  10.1.1.0 255.255.255.0  any  any      deny                0         214         4655
validuser  any                     any  any      permit              6         2502        4656

Port ACL Hits
-------------
ACL  ACE  New Hits  Total Hits  Index
---  ---  --------  ----------  -----
5     22       0           14    2382
```

The output of this command includes the following information:

Parameter	Description
Role	Name of the role assigned by the ACL.
Policy	Name of the policy used by the ACL
Src	The traffic source, which can be one of the following: • *<alias>*: Name of a user-defined alias for a network host, subnetwork, or range of addresses. • **any**: match any traffic. • **host**: specify a single host IP address. • **network**: specify the IP address and netmask. • **user**: represents the IP address of the user.
Dst	The traffic destination, which can be one of the following: • *<alias>*: Name of a user-defined alias for a network host, subnetwork, or range of addresses. • **any**: match any traffic. • **host**: specify a single host IP address. • **network**: specify the IP address and netmask. • **user**: represents the IP address of the user.
Service	Network service, which can be one of the following: • IP protocol number (0-255) • name of a network service (use the show netservice command to see configured services) • **any**: match any traffic • **tcp**: specify the TCP port number (0-65535) • **udp**: specify the UDP port number (0-65535)
Action	Action if rule is applied, which can be one of the following: • **deny**: reject packets • **dst-nat**: perform destination NAT on packets • **dual-nat**: perform both source and destination NAT on packets • **permit**: forward packets • **redirect**: specify the location to which packets are redirected • **src-nat**: perform source NAT on packets
Dest/Opcode	The datapath destination ID.
New Hits	Number of ACL hits that occurred since this command was last issued.
Total Hits	Total number of ACL hits recorded since the controller last reset.
Index	Index number of the ACL.
ACL	ACL number
ACE	ACE number
New Hits	Number of times the ACL was applied since this command was last issued.
Total Hits	Number of times the ACL was applied since the controller was last reset.
Index	Index number of the ACL.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers

show adp config

```
show adp config
```

Description

Show Dell Discovery Protocol (ADP) configuration settings.

Syntax

No parameters.

Example

The following example shows that the controller has all default settings for ADP.

```
(host) #show adp config
ADP Configuration
-----------------
key        value
---        -----
discovery  enable
igmp-join  enable
igmp-vlan  0
```

The output of this command includes the following parameters:

Parameter	Description
discovery	Dell APs send out periodic multicast and broadcast queries to locate the master controller. If the APs are in the same broadcast domain as the master controller and ADP is enabled on the controller, the controller automatically responds to the APs' queries with its IP address. This command shows whether ADP is enabled or disabled on the controller.
igmp-join	Shows whether the controller has enabled or disabled the sending of Internet Group Management Protocol (IGMP) join requests.
igmp-vlan	ID of the VLAN to which IGMP reports are sent. If this value is set to 0, the controller will use the default route VLAN used.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show adp counters

```
show adp counters
```

Description

Show Dell Discovery Protocol (ADP) counters.

Syntax

No parameters.

Example

The following example shows the ADP counter table for the controller.

```
(host) #show adp counters
ADP Counters
------------
key           value
---           -----
IGMP Join Tx  1
IGMP Drop Tx  0
ADP Tx        0
ADP Rx        0
```

The output of this command includes the following parameters:

Parameter	Description
`IGMP Join Tx`	Number of Internet Group Management Protocol (IGMP) join requests sent by the controller.
`IGMP Drop Tx`	Number of Internet Group Management Protocol (IGMP) drop requests sent by the controller.
`ADP Tx`	Number of ADP responses sent to APs.
`ADP Rx`	Number of multicast and broadcast queries received from APs trying to locate the master controller.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap active

```
show ap active [ap-name <ap-name>|{arm-edge dot11a|dot11g|voip-
only}|dot11a|dot11g|essid <essid>|ip-addr <ip-addr>|{type access-point|air-
monitor|(sensor dot11a|dot11g|voip-only)}|voip-only
```

Description

Show all active APs registered to a controller.

Syntax

Parameter	Description
`ap-name <ap-name>`	View data for an AP with a specified name.
`arm-edge`	Show the state of ARM edge APs.
`dot11a`	Show 802.11a radio information.
`dot11g`	Show 802.11g radio information.
`voip-only`	Show AP information filtered by associated/active VoIP clients.
`essid <essid>`	View data for a specific ESSID (Extended Service Set Identifier). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
`ip-addr <ip-addr>`	View data for an AP with a specified IP address by entering an IP address in dotted-decimal format.
`type`	Show AP information filtered by type of AP.
`access-point`	Show information for Access Points only.
`air-monitor`	Show information for Air Monitors only.
`sensor`	Show only RFprotect Sensor information.
`voip-only`	Show AP information filtered by associated/active VoIP clients.

Usage Guidelines

This command displays details for all active APs on the controller. If an AP on your network *does not* appear in this table, it may have been classified as an inactive AP for any of the following reasons:

- The AP is configured with a missing or incorrect VLAN. (For example, the AP is configured to use a tunneled SSID of VLAN 2 but the controller doesn't have a VLAN 2.)
- The AP has an unknown AP group.
- The AP has a duplicate AP name.
- An AP with an external antenna is not provisioned with external antenna gain settings.
- Both radios on the AP are disabled.
- No virtual APs are defined on the AP.
- The AP has profile errors. Issue the command `show profile errors" for details.
- The GRE tunnel between the AP and the controller was blocked by a firewall after the AP became active.
- The AP is temporarily down while it is upgrading its software. The AP will become active again after upgrading.

- An AP has conflicting configuration settings. For example, if the AP system profile on a single radio dual-band AP configures the radio uses 802.11g, but the virtual AP profile on the AP is set to use 802.11a, the AP might not appear to be active.
- A remote AP model 5WN or 2WG attempted to connect to a controller without using IPSec.

Example

The output of the command in the example below shows that the controller sees six active APs.

```
(host)# show ap active

Active AP Table
---------------
Name    Group          IP Address    11g       11g Ch/EIRP/MaxEIRP  11a 11a Ch/EIRP/MaxEIRP      AP
Type  Flags  Uptime
                                     Clients                        Clients
----    -----          ----------     -----   -------------------  ------    ----------------    ---
----  -----  ------
AL31    corp1344       10.6.1.202      0      AP:HT:1/8.5/33       0        AP:HT:149+/19/36     125
```

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
11g Clients	Number of 802.11g clients using the AP.
11g Ch/EIRP/MaxEIRP	802.11g radio channel used by the AP/current effective Isotropic Radiated Power (EIRP) / maximum EIRP.
11a Clients	Number of 802.11a clients using the AP.
11a Ch/EIRP/MaxEIRP	802.11a radio channel used by the AP/current EIRP/maximum EIRP.
AP Type	AP model type.
Flags	This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the **show ap active** command. • a = Reduce ARP packets in the air • A = Enet1 in active/standby mode • B = Battery Boost On • d = Drop Mcast/Bcast On or Disconnected Sensor • D = Disconn. Extra Calls On • E = Wired AP enabled • K = 802.11K Enabled • L = Client Balancing Enabled • M = Mesh • N = 802.11b protection disabled • P = PPPOE • R = Remote AP • R- = The remote AP requires captive portal authentication. Once this authentication is successfully completed, the **R-** flag changes to **R**. • S = RFprotect Sensor • U = USB modem • X = Maintenance Mode

Column	Description
`Uptime`	Number of hours, minutes and seconds since the last controller reboot or bootstrap, in the format *hours:minutes:seconds*.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap allowed-channels

```
show ap allowed-channels [<ap-name>|<country-code>|<ip-addr>]
```

Description

This command shows configuration information for Captive portal authentication profiles.

Syntax

Parameter	Description
<ap-name>	Name of an AP.
<country-code>	Specify a country code to display allowed channels for that country.
<ip-addr>	IP address of an AP, in dotted-decimal format.

Usage Guidelines

Specify the country code for your controller during initial setup. Changing the country code causes the valid channel lists to be reset to the defaults for that country.

Examples

The output of this example shows all allowed channels for the country code **US**.

```
(host)# show ap allowed-channels US

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

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap ap-group

```
show ap ap-group {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show the AP group settings for an individual AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Usage Guidelines

Use this command to display the contents of an AP's group profile. If you know the name of the group whose profile settings you want to view, use the command **show ap-group <profile-name>**. To view a list of all configured AP groups on your controller, use the command **show ap-group**.

Examples

In the example below, the output of this command lists the profiles associated with the AP group **Corp13**.

```
(host) #show ap ap-group AP2
AP group "corp13"
-------------------
Parameter                           Value
---------                           -----
Virtual AP                          corp13-guest
Virtual AP                          corp13-ether-wpa2
Virtual AP                          corp13-ether-voip
Virtual AP                          corp13-ether-comm
802.11a radio profile               default
802.11g radio profile               default
Wired AP profile                    default
Ethernet interface 0 link profile   default
Ethernet interface 1 link profile   default
AP system profile                   corp13
VoIP Call Admission Control profile default
802.11a Traffic Management profile  N/A
802.11g Traffic Management profile  N/A
Regulatory Domain profile           corp13-channel-profile
SNMP profile                        default
RF Optimization profile             handoff-aggressive
RF Event Thresholds profile         default
IDS profile                         ids-low-setting
Mesh Radio profile                  default
   Mesh Cluster profile                    N/A
```

Related Commands

Command	Description	Mode
ap-group	Configure your AP groups and AP group profiles.	Config mode

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap arm history

```
show ap arm history {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

For each interface on an AP, show the history of channel and power changes due to Adaptive Radio Management (ARM).

Syntax

Parameter	Description
`ap-name <ap-name>`	Show ARM history for an AP with a specific name.
`bssid <bssid>`	Show ARM history for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show ARM history for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

Adaptive Radio Management (ARM) can automatically change channel and power levels based on a number of factors such as noise levels and radio interference. The output of the **show ap arm history** command shows you an AP's channel and power changes over time, and the reason why those changes took place.

```
(host)# #(ethersphere-lms3) #show ap arm history ap-name AP-16
Interface :wifi0
ARM History
-----------
Reason  Old channel  New channel  Old Power  New Power  Last change
------  -----------  -----------  ---------  ---------  -----------
P-      153-         153-         12         9          3d:14h:56m:48s
P+      153-         153-         9          12         3d:13h:44m:7s
P+      153-         153-         12         15         3d:13h:23m:5s
P+      153-         153-         15         18         3d:13h:16m:32s
P+      153-         153-         18         21         3d:11h:42m:42s
P-      153-         153-         21         15         3d:8h:16m:12s

Interface :wifi1
ARM History
-----------
Reason  Old channel  New channel  Old Power  New Power  Last change
------  -----------  -----------  ---------  ---------  -----------
P-      11           11           15         12         3d:18h:22m:28s
P+      11           11           12         15         3d:18h:17m:27s
P-      11           11           15         12         3d:18h:9m:9s
P+      11           11           12         15         3d:17h:48m:41s
P+      11           11           15         18         3d:17h:44m:34s
P-      11           11           18         15         3d:17h:39m:11s
P-      11           11           15         12         3d:17h:32m:39s
P+      11           11           12         15         3d:17h:26m:15s
I: Interference, R: Radar detection, N: Noise exceeded, E: Error threshold exceeded, INV: Invalid Channe
Containment, M: Empty Channel, P+: Increase Power, P-: Decrease Power, OFF: Turn off Radio, ON: Turn on
```

The output of this command includes the following information:

Parameter	Description
`Reason`	This column displays one of the following code to indicate why the channel or power change was made. • **I**: Interference • **R**: Radar detected • **N**: Noise exceeded • **E**: Error threshold exceeded • **INV**: Invalid Channel • **G**: Rogue AP Containment • **M**: Empty Channel • **P+**: Increase Power • **P-**: Decrease Power • **OFF**: Turn off Radio • **ON**: Turn on Radio The Reason key appears at the bottom of the ARM History table.
`Old Channel`	Channel number used by the AP interface before the ARM change.
`New Channel`	Channel number used by the AP interface after the ARM change.
`Old Power`	Power level of the AP interface before the ARM change.
`New Power`	Power level of the AP interface after the ARM change.
`Last Change`	Time elapsed since the change, in the format *days:hours:minutes:seconds*.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap arm neighbors

```
show ap arm neighbors {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show the ARM settings for an AP's neighbors.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

The output of this command shows ARM neighbor information for both the **wifi1** and **wifi0** interfaces on AP **ap70_1**.

```
(host)# show ap arm neighbors ap70_1

Interface:wifi1
00:1b:2f:e6:1c:d0:known-interfering/SNR-1/CH-1
00:19:e3:31:55:f2:known-interfering/SNR-7/CH-1
00:1f:f3:01:4d:3f:known-interfering/SNR-1/CH-1
00:18:39:96:b4:16:known-interfering/SNR-0/CH-1
00:11:24:ec:49:05:known-interfering/SNR-0/CH-1

Interface:wifi0
00:19:7e:4d:8a:1d:known-interfering/SNR-0/CH-1
00:19:a9:ce:13:90:interfering/SNR-0/CH-4
00:19:7e:4d:80:df:known-interfering/SNR-0/CH-1
00:11:24:90:17:d4:known-interfering/SNR-0/CH-1
00:16:b6:f4:59:94:known-interfering/SNR-0/CH-1
00:14:51:6d:d1:d5:known-interfering/SNR-0/CH-1
```

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap arm rf-summary

```
show ap arm rf-summary {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show the state and statistics for all channels being monitored by an individual AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show channel data for an AP with a specific name.
`bssid <bssid>`	Show channel data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show channel data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

The output of this command shows detailed information for the individual channels being monitored and statistics for each AP interface. Use this command verify an AP's RF health, or to determine why multiple APs in the same area are on the same channel.

```
(host)# show ap arm rf-summary ap-name ap21
Channel Summary
---------------
channel  retry  low-speed  non-unicast  frag  bwidth  phy-err  mac-err  noise  cov-idx  intf_idx
-------  -----  ---------  -----------  ----  ------  -------  -------  -----  -------  --------
1        0      0          0            0     0       0        0        0      1/1      27/12//12/0
48       0      0          0            0     0       0        0        0      0/0      0/0//4/1
165      5      3          3            42    720     0        1        112    10/0     41/0//0/1
6        0      100        50           0     0       0        12       100    10/0     60/10//0/4
11       0      0          0            0     0       0        0        0      4/2      29/13//17/0
149      0      0          0            0     0       0        0        0      0/0      0/0//5/0
36       0      0          0            0     0       0        0        0      0/0      0/0//20/1
153      0      0          0            0     0       0        0        0      0/0      0/0//0/2
40       0      0          0            0     0       0        0        0      0/0      0/0//2/7
44       0      0          0            0     0       0        0        0      0/0      0/0//4/2

Interface Name           :wifi0
Current ARM Assignment   :165/21
Target Coverage Index    :10
Covered channels a/g     :0/0
Free channels a/g        :7/0
ARM Edge State           :enable
Last check channel/pwr   :22m:12s/9m:17s
Last change channel/pwr  :22m:12s/16m:55s
Next Check channel/pwr   :0s/2m:41s

Interface Name           :wifi1
Current ARM Assignment   :6/6
Target Coverage Index    :10
Covered channels a/g     :0/2
Free channels a/g        :0/1
ARM Edge State           :enable
Last check channel/pwr   :7h:53m:19s/2m:21s
```

The output of this command includes the following information:

Parameter	Description
`channel`	Number of a radio channel used by the AP.

Parameter	Description
retry	Number of 802.11 retry frames sent because a client failed to send an ACK.
low-speed	Number of frames sent at a data rate of 18 Mbps or slower.
non-unicast	The number of non-unicast frames sent on the channel.
frag	Number of fragmented packets
bwidth	Current bandwidth, in kbps.
phy-err	Number of PHY errors on the channel.
mac-err	Number of MAC errors on the channel.
noise	Current noise level, in -dBm.
cov-idx	The AP uses this metric to measure RF coverage. The coverage index is calculated as x/y, where "x" is the AP's weighted calculation of the Signal-to-Noise Ratio (SNR) on all valid APs on a specified 802.11 channel, and "y" is the weighted calculation of the Dell APs SNR the neighboring APs see on that channel.
intf_idx	The AP 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 AP sees on its selected channel. • Metric value "b" is the interference the AP sees on the adjacent channel. • Metric value "c" is the channel interference the AP's neighbors see on the selected channel. • Metric value "d" is the interference the AP's neighbors see on the adjacent channel • To calculate the total Interference Index for a channel add "a+b+c+d".
Interface Name	Name of the fastethernet or gigabit ethernet interface
Current ARM Assignment	Current channels assigned by the AP's ARM profile.
Target Coverage Index	Ideal value of coverage index an AP tries to achieve on its channel.
Covered channels a/g	Number of channels that are currently being used by an AP's BSSIDs.
Free channels a/g	Number of channels that are available to an AP because that channel has a lower interference index.
ARM Edge State	If enabled, ARM-enabled APs on the network edge will not become Air Monitors.
Last check channel/ pwr	Time elapsed since the AP checked its channel and power settings, in *hour:minute:second* format.
Last change channel/ pwr	Time elapsed since the AP changed its channel and power settings, in *hour:minute:second* format.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap arm scan-times

```
show ap arm scan-times {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show AM channel scan times for an individual AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show channel scan data for an AP with a specific name.
`bssid <bssid>`	Show channel scan data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show channel scan data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

The output of this command shows scan times for every channel on an AP with the IP address 10.15.10.37.

```
(host)# show ap arm scan-times ip-addr 10.15.10.37

Channel Scan Time
-----------------
channel  assign-time  scans-attempted  scans-rejected  dos-scans  flags  timer-tick
-------  -----------  ---------------  --------------  ---------  -----  ----------
36       8579         349              0               0          DVACT  50598
40       2365         349              0               0          DVACT  50610
44       2495         349              0               0          DVACT  50621
48       9714         349              0               0          DVACT  50656
52       0            349              0               0          DA     50643
56       0            349              0               0          DA     50655
60       0            348              0               0          DA     50519
64       0            348              0               0          DA     50530
149      5546         348              0               0          DVACT  50542
153      2310         348              0               0          DVACT  50553
157      6094         348              0               0          DVACT  50565
161      3014         348              0               0          DVACT  50576
165      10538        348              0               0          DVACT  50587
1        4194         97               0               0          DVACT  50594
2        0            97               0               0          DAC    50604
3        0            97               0               0          DAC    50615
4        0            97               0               0          DAC    50627
5        0            97               0               0          DC     50638
6        4076         97               0               0          DVACT  50656
7        0            96               0               0          DAC    50538
8        0            97               0               0          DC     50549
9        0            97               0               0          DC     50561
10       0            97               0               0          DAC    50572
11       3710         97               0               0          DVACT  50583
```

The output of this command includes the following parameters:

Parameter	Description
`channel`	A radio channel on the specified AP.
`Assign-time`	The amount of time that an AP has been on a channel.
`scans-attempted`	The number of times an AP has attempted to scan another channel
`scans-rejected`	The number of times an AP attempted to scan a channel, but was unable to scan because the scan was halted by the power save, voice aware or load aware ARM features.
`dos-scans`	The number of times an AP enabled with the rogue aware scanning feature had to contain a rogue device on a channel.
`flags`	The flags column displays additional relevant information about the channel. The flags key appears at the bottom of the Channel Scan Time table.
`timer tick`	Timer tick at which the last scan was attempted.
`last-scan-channel`	The last channel scanned by the AP
`current-scan-channel`	The AP's current channel.
`last-dos-channel`	The last channel that had to be contained because a rogue device was detected on that channel.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap arm state

```
show ap arm state [ap-name <ap-name>|dot11a|dot11g|ip-addr <ip-addr>]
```

Description

Display Adaptive Radio Management (ARM) information for an individual AP's neighbors, or show all available data for any neighboring AP using an 802.11a or 802.11g radio type.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show aggregate ARM Neighbor Information for a specific AP.
`dot11a`	Show aggregate ARM Neighbor Information for all APs using an 802.11a radio.
`dot11g`	Show aggregate ARM Neighbor Information for all APs using an 802.11g radio.
`ip-addr <ip-addr>`	Show aggregate ARM Neighbor Information for a AP with a specific IP address by entering its IP address in dotted-decimal format.

Usage Guidelines

The output of the **show ap arm state** command shows 802.11a and 802.11g information for all APs. Include an AP name or IP address to show data for just a single AP, or use the **dot11a** or **dot11g** keywords to show data for all APs using that radio type.

Examples

The output of this command shows 802.11a information for all neighboring APs.

```
(host)# show ap arm state

AP-AL39:10.6.1.206:48:19:23-Edge:enable
Neighbor Data
-------------
Name  IP Address  SNR  Assignment
----  ----------  ---  ----------
AL33  10.6.1.205  32   48/10

AP-AL33:10.6.1.205:48:10:23-Edge:disable
Neighbor Data
-------------
Name  IP Address  SNR  Assignment
----  ----------  ---  ----------
AL39  10.6.1.206  42   48/19
AL19  10.6.1.212  29   161/19
AL31  10.6.1.202  25   153/16
AL25  10.6.1.196  13   153/16
AL29  10.6.1.204  26   153/19
```

The output of this command includes the following information

Column	Description
`Name`	Name of an AP.
`IP address`	IP address of an AP.

Column	Description
SNR	Signal-to-noise (SNR) ratio. SNR is the power ratio between an information signal and the level of background noise.
`Assignment`	The AP's current channel assignment.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap association

```
show ap association [ap-name <ap-name>|ap-group <ap-group>|bssid <bssid>|channel
<channel>|client-mac <client-mac>|essid <essid>|ip-addr <ip-addr>|phy {a|b|g}|voip-
only]
```

Description

Show the association table for an AP group or for an individual AP.

Syntax

Parameter	Description
`ap-group <ap-group>`	Show AP associations for a specific AP group. You can also include the **channel**, **essid** or **voip-only** keywords to further filter the output of this command.
`ap-name <ap-name>`	Show AP associations for a specific AP. You can also include the **essid**, **phy** or **voip-only** keywords to further filter the output of this command.
`bssid <bssid>`	Show the AP associations for an specific AP Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`channel <channel>`	Show AP associations for an individual channel by specifying the channel for which you want to view information.
`client-mac <client-mac>`	Show the AP associations for a specific MAC address by entering the MAC address of a client for which you want to view association information.
`essid <essid>`	Show AP associations for an Extended Service Set Identifier (ESSID). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
`ip-addr <ip-addr>`	Show AP associations for a specific AP by entering an IP address in dotted-decimal format. You can also include the **essid**, **phy** or **voip-only** keywords to further filter the output of this command.
`phy`	Include the **phy** [**a**|**b**|**g**] keywords to show associations for a specific 802.11 radio type, either 802.11a, 802.11b or 802.11g.
`voip-only`	Show VoIP client information only.

Usage Guidelines

Use this command to check if user is connected to an AP. This command validates whether the client is associated and indicates the last AP to which it was connected. If the flags column shows an 'A', the client is currently associated with that AP. Alternately, if the client is not currently associated, the AP with the smallest value of association time is the last AP used by the client.

Example

Use the **show ap association client-mac** command to verify that a user has associated with an AP, or to determine last AP to which the client was connected. The output of this command in the example below shows the association table for the client with the MAC address 00:13:fd:5c:7c:59. If the flags column in the output of this command shows an 'A', the client associated last to that AP. Alternately, the AP with the smallest value of association time is the last AP to which the client had associated.

In the example below, the output of this command has been broken into two separate tables to better fit this page. In the actual output of the command, this information is shown in a single, wide table.

```
(host) #show ap association client-mac  00:13:fd:5c:7c:59

Flags: W: WMM client, A: Active, R: RRM client
PHY Details: HT: High throughput; 20: 20MHz; 40: 40MHz
             ss:  spatial streams

Association Table
-----------------

Association Table
-----------------
------------------
Name  bssid              mac               auth  assoc  aid  l-int  essid
----  -----              ---               ----  -----  ---  -----  -----
AL12  00:1a:1e:11:5f:11  00:21:5c:50:b1:ed  y     y      12   10     ethersphere-wpa2
AL5   00:1a:1e:88:88:31  00:19:7d:d6:74:93  y     y      6    10     ethersphere-wpa2


vlan-id  tunnel-id  phy            assoc  time  num assoc  Flags
```

The output of this command includes the following information:

Column	Description
Name	Name of an AP
bssid	The AP Basic Service Set Identifier (BSSID)
mac	MAC address of the AP
auth	This column displays a **y** if the AP has been configured for 802.11 authorization frame types. Otherwise, it displays an **n**.
assoc	This column displays a **y** if the AP has been configured for 802.11 association frame types. Otherwise, it displays an **n**.
aid	802.11 association ID. A client receives a unique 802.11 association ID when it associates to an AP.
1-int	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
essid	Name that uniquely identifies the AP's Extended Service Set Identifier (ESSID).
vlan-id	Identification number of the AP's VLAN.
tunnel-id	Identification number of the AP's tunnel.
assoc. time	Amount of time the client has associated with the AP, in the format *hours:minutes:seconds*.
num assoc	Number of clients associated with the AP.
flags	This column displays any flags for this AP. The list of flag abbreviations is included in the output of the **show ap association** command.

Related Commands

Command	Description	Mode
show ap debug association-failure (deprecated)	If the output of this show command indicates that a client is not associating with an AP, use `show ap debug association-failure (deprecated)` to determine why a client is not associated with an AP.	Config mode
show ap debug mgmt-frames (deprecated)	If the output of this show command indicates that a client is not associating with an AP, use `show ap debug mgmt-frames (deprecated)` to determine why a client is not associated with an AP.	Config mode

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap association remote

```
show ap association remote [ap-name <ap-name>|ap-group <ap-group>|bssid <bssid>|channel
<channel>|essid <essid>
```

Description

Display the association table for an individual AP or group of APs in bridge mode.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show AP associations for a specific remote AP.
`ap-group <ap-group>`	Show AP associations for a specific group of remote APs.
`bssid <bssid>`	Show the AP associations for an specific AP Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`channel <channel>`	Show remote AP associations for a specific channel.
`essid <essid>`	Show remote AP associations for an Extended Service Set Identifier (ESSID). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.

Examples

The output of the command below shows the association table for clients in the AP group **group1**.

```
show ap association remote ap-group group1

Flags: W: WMM client, A: Active, R: RRM client
PHY Details: HT: High throughput; 20: 20MHz; 40: 40MHz
             ss:  spatial streams

Association Table
-----------------
Name bssid             mac              auth  assoc aid  l-int  essid  vlan-id  tunnel-id phy
assoc.time  num assoc  Flags
---- -----             ---              ----  ----- ---  -----  -----  -------  --------- ---  ----
```

The output of this command includes the following information:

Column	Description
`Name`	Name of an AP
`bssid`	The AP Basic Service Set Identifier (BSSID)
`mac`	MAC address of the AP
`auth`	This column displays a **y** if the AP has been configured for 802.11 authorization frame types. Otherwise, it displays an **n**.
`assoc`	This column displays a **y** if the AP has been configured for 802.11 association frame types. Otherwise, it displays an **n**.
`aid`	802.11 association ID. A client receives a unique 802.11 association ID when it associates to an AP.
`1-int`	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.

Column	Description
`essid`	Name that uniquely identifies the AP's Extended Service Set Identifier (ESSID).
`vlan-id`	Identification number of the AP's VLAN.
`tunnel-id`	Identification number of the AP's tunnel.
`phy`	The RF band in which the AP should operate: **g** = 2.4 GHz **a** = 5 GHz
`assoc. time`	Amount of time the client has associated with the AP, in the format *hours:minutes:seconds*.
`num assoc`	Number of clients associated with the AP.
`flags`	This column displays any flags for this AP. The list of flag abbreviations is included in the output of the **show ap association remote** command.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap authorization-profile

```
show ap authorization-profile [<profile-name>]
```

Description

This command shows information for AP authorization profiles.

Syntax

Parameter	Description
<profile-name>	The name of an an existing AP authorization profile.

Usage Guidelines

The AP authorization profile specifies which configuration should be assigned to a remote AP that has been provisioned but not yet authenticated at the remote site. By default, these yet-unauthorized APs are put into the temporary AP group **authorization-group** and assigned the predefined profile **NoAuthApGroup**. This configuration allows the user to connect to an unauthorized remote AP via a wired port then enter a corporate username and password. Once a valid user has authorized the AP and the remote AP will be marked as authorized on the network. The remote AP will then download the configuration assigned to that AP by it's permanent AP group.

Issue this command without the **<profile-name>** option to display the entire AP authorization profile list, including profile status and the number of references to each profile. Include a profile name to display the authorization group defined for that profile.

Examples

The following example lists all AP authorization profiles. The **References** column lists the number of other profiles with references to that authorization profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined AP authorization profiles will not have an entry in the **Profile Status** column.

```
(host) #show ap authorization-profile

AP Authorization profile List
-----------------------------
Name           References  Profile Status
----           ----------  --------------
Noauthprofile  1
default        2           Predefined (editable)

Total:2
```

To display the authentication group for an individual profile, include the <profile> parameter. The example below shows the profile details for the AP authorization profile **Default**.

```
(host) #show ap authorization-profile default

AP Authorization profile "default" (Predefined (editable))
----------------------------------------------------------
Parameter               Value
---------               -----
AP authorization group  NoAuthApGroup
```

The output of the **show ap authorization** command includes the following parameters:

Parameter	Value
`AP authorization group`	Name of a configuration profile to be assigned to the group unauthorized remote APs.

Related Commands

Command	Description	Mode
ap authorization-profile	This command defines a temporary configuration profile for remote APs that are not yet authorized on the network.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap blacklist-clients

```
show ap blacklist-clients
```

Description

Show a list of clients that have been denied access.

Usage Guidelines

Use the stm CLI command to add or remove users from a blacklist. Additionally, the **dot1x authentication**, **VPN authentication** and **MAC authentication** profiles allow you to automatically blacklist a client if machine authentication fails.

Examples

The output of this command shows that the controller has a single user-defined blacklisted client.

```
(host)# show ap blacklist-clients

Blacklisted Clients
-------------------
STA                reason        block-time(sec)  remaining time(sec)
---                ------        ---------------  -------------------
00:1E:37:CB:D4:52  user-defined  2480             Permanent
```

The output of this command includes the following information:

Column	Description
STA	MAC address of the blacklisted client.
reason	The reason that the user was blacklisted. • **user-defined:** User was blacklisted due to blacklist criteria were defined by the network administrator • **mitm-attack**: Blacklisted for a man in the middle (MITM) attack; impersonating a valid enterprise AP. • **ping-flood**: Blacklisted for a ping flood attack. • **session-flood**: Blacklisted for a session flood attack. • **syn-flood**: Blacklisted for a syn flood attack. • **session-blacklist:** User session was blacklisted • **IP spoofing**: Blacklisted for sending messages using the IP address of a trusted client. • **ESI-blacklist**: An external virus detection or intrusion detection application or appliance blacklisted the client. • **CP-flood**: Blacklisting for flooding with fake AP beacons. • **UNKNOWN**: Blacklist reason unknown.
block-time (sec)	Amount of time the client has been blocked, in seconds.
remaining time(sec)	Amount of time remaining before the client will be allowed access to the network again.

Related Commands

Command	Description	Mode
stmadd-blacklist-client stmremove-blacklist-client <macaddr>	Manually add or remove clients from a blacklist.	Config mode

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap bss-table

```
show ap bss-table [ap-name <ap-name>|bssid <bssid>|essid <essid>|ip-addr <ip-addr>|port
<port>\<slot>]
```

Description

Show an AP's Basic Service Set (BSS).

Syntax

Parameter	Description
`ap-name <ap-name>`	Show the BSS table for a specific AP.
`bssid <bssid>`	Show the BSS table for an specific AP Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`essid <essid>`	Show the BSS table for an Extended Service Set Identifier (ESSID). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
`ip-addr <ip-addr>`	Show the BSS table for a specific AP by entering an IP address in dotted-decimal format.
`port <port>/<slot>`	Show the BSS table for a specific port and slot on an AP. The slot and port numbers should be separated by a forward slash (/).

Usage Guidelines

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

Example

The output of this command shows the BSS table for the seven active APs using the controller.

```
show ap bss-table

Dell AP BSS Table
-----------------
bss              ess       s/p   ip         phy   type ch/EIRP/max-EIRP cur-cl  ap name in-t(s) tot-
t    mtu acl-state
---      --- ----  ---       ---    ---- ------------     ------  ------  ------  ------ --- --------
00:0b:86:cc:d8:40  corp-ap   1/3 192.0.2.0  g     ap 11/16.5/33        0     3.70.17   0     50s
1500  -
00:0b:86:cc:d8:41  testbed1  1/3 192.0.2.10  g     ap   11/16.5/33    1     3.70.17   0     50s
1500  -
00:0b:86:9b:49:c8  corp-ap   1/0 192.0.2.11  a     ap 165/15.5/36        0     3.85.15   0     2m:0s
   1578  -
00:1a:1e:81:aa:50  corp-ap   1/0 192.0.2.12  a-HT  ap   44+/19/230     3.125.14  0     14m:0s 1578
```

The output of this command includes the following information:

Column	Description
bss	The AP Basic Service Set Identifier (BSSID). This is usually the MAC address of the AP
ess	The AP Extended Service Set Identifier (ESSID).

Column	Description
s/p	The controller port used by the AP, in the format <slot>/<port>. The **<slot>** number is always 1. The **<port>** parameter refers to the network interfaces that are embedded in the front panel of the W-3000 Controller Series Multi-Service Controller. Port numbers start at 0, from the left-most position.
ip	IP address of an AP.
phy	An AP 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 AP is working as an access point (AP) or air monitor (AM).
ch/EIRP/max-EIRP	Radio channel used by the AP/current effective Isotropic Radiated Power (EIRP) /maximum EIRP.
cur-cl	Current number of clients on the AP.
ap name	Name of the AP.
in-t(s)	Number of seconds that an AP has been inactive.
tot-t	An AP's total active time, in seconds.
mtu	Maximum Transmission Unit (MTU) size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
acl-state	An access control list (ACL) can enable or disable an AP during specific time ranges. • **Disabled**: An ACL with time restrictions is currently **disabled** (so the AP is enabled). • **Enabled**: An ACL with time restrictions is currently **enabled** (so the AP is disabled). • This data column will display a dash (**-**) if no ACLs are currently configured for the AP.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap bw-report

```
show ap bw-report {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show the bandwidth reporting table for a specific AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show bandwidth data for an AP with a specific name.
`bssid <bssid>`	Show bandwidth data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show bandwidth data for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Examples

The output of the following command shows the Dell AP bandwidth table for an AP with the IP address 192.0.2.170.

```
show ap bw-report ip-addr 192.0.2.170

Bandwidth report for AP "AL16" radio 0
--------------------------------------
Virtual AP                Allocated Share  Actual Share  Offered Load  Delivered Load
----------                ---------------  ------------  ------------  --------------
corp1344-guest            0%               0%            0 kbps        0 kbps
corp1344-ethersphere-wpa2 0%               0%            0 kbps        0 kbps
Average Throughput:0 kbps

Bandwidth report for AP "AL16" radio 1
--------------------------------------
Virtual AP                  Allocated Share  Actual Share  Offered Load  Delivered Load
----------                  ---------------  ------------  ------------  --------------
corp1344-guest              0%               0%            0 kbps        0 kbps
corp1344-ethersphere-voip   0%               0%            0 kbps        0 kbps
corp1344-ethersphere-vocera 0%               0%            0 kbps        0 kbps
Average Throughput:0 kbps
```

The output of this command includes the following information for all radios on the AP:

Column	Description
`Virtual AP`	Name of a Virtual AP
`Allocated Share`	Maximum percentage of total bandwidth available to that Virtual AP.
`Actual Share`	Actual percentage of total bandwidth used by a Virtual AP.
`Offered Load`	Attempted throughput for the Virtual AP, in kbps.
`Delivered Load`	Actual throughput for the Virtual AP, in kbps. This value may be less than the offered load if the Virtual AP has used all its allocated bandwidth.
`Average Throughput`	Average throughput for the virtual AP, in kbps.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap client status

```
show ap client status <client-mac>
```

Description

Show the current status of a specific client.

Syntax

Parameter	Description
`<client-mac>`	MAC address of a client

Examples

The output of the command shows the status of an individual client in the STA (station) table.

```
(host) #show ap client status  00:13:fd:42:32:38

STA Table
---------
bssid              auth  assoc  aid  l-int  essid      vlan-id  tunnel-id
-----              ----  -----  ---  -----  -----      -------  ---------
00:1a:1e:a3:02:c9  y     y      7    10     corp-wpa2  65       0x10c0
State Hash Table
----------------
bssid              state       reason
-----              -----       ------
00:1a:1e:a3:02:c9  auth-assoc  0
```

The output of this command includes the following information:

Column	Description
`bssid`	Basic Service Set ID (BSSID) of the client.
`auth`	This column displays a **y** if the AP has been configured for 802.11 authorization frame types. Otherwise, it displays an **n**.
`assoc`	This column displays a **y** if the AP has been configured for 802.11 association frame types. Otherwise, it displays an **n**.
`aid`	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
`l-int`	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
`essid`	Extended Service Set ID (ESSID) of the client.
`vlan-id`	VLAN ID of the VLAN used by the client
`tunnel-id`	Identification number for the tunnel
`state`	If the client has been both authorized and associated, this data column will display **auth-assoc**. If the client has only been authorized, this data column will display **auth**.
`Reason`	If the client failed to authenticate, this data column lists the reason code for 802.11 authentication failure

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap config

```
show ap config {ap-group <ap-group>}|{ap-name <ap-name>}|{essid <essid>}
```

Description

Show a large list of configuration settings for an ap-group or an individual AP.

Syntax

Parameter	Description
ap-group <ap-group>	Display configuration settings for an AP group.
ap-name <ap-name>	Display configuration settings for an AP with a specific name.
essid <essid>	Display configuration settings for an AP with a specific Extended Service Set Identifier (ESSID). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.

Examples

The example output below shows just some of the configuration settings displayed in the output of this command.

```
show ap config ap-group apgroup14
----------------------------------------------------
Parameter                                802.11g         802.11a         Source
---------                                -------         -------         ------
LMS IP                                   N/A            N/A            ap system-profile
"default"
Backup LMS IP                           N/A            N/A            ap system-profile
"default"
LMS Preemption                           Disabled        Disabled        ap system-
profile "default"
LMS Hold-down Period                    600 sec        600 sec        ap system-profile
"default"
Master controller IP address             N/A            N/A            ap system-profile
"default"
RF Band                                 g              g              ap system-profile
"default"
Double Encrypt                          Disabled       Disabled       ap system-profile
"default"
Native VLAN ID                          1              1              ap system-profile
"default"
SAP MTU                                 N/A            N/A            ap system-profile
"default"
Bootstrap threshold                      8              8              ap system-profile
"default"
Request Retry Interval                  10 sec         10 sec         ap system-profile
"default"
Maximum Request Retries                 10             10             ap system-profile
"default"
Keepalive Interval                      60 sec         60 sec         ap system-profile
"default"
Dump Server                             N/A            N/A            ap system-profile
"default"
Telnet                                  Disabled       Disabled       ap system-profile
```

The output of this command includes the following parameters.

Parameter	Description
LMS IP	The IP address of the local management switch (LMS)—the Dell controller which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network.
Backup LMS IP	For multi-controller networks, this parameter displays the IP address of a backup to the IP address specified with the lms-ip parameter.
LMS Preemption	When this parameter is enabled, the local management switch automatically reverts to the primary LMS IP address when it becomes available.
LMS Hold-down Period	Time, in seconds, that the primary LMS must be available before an AP returns to that LMS after failover.
Master controller IP address	For multi-controller networks, this parameter displays the IP address of the master controller.
RF Band	For dual-band radios, this parameter displays the RF band in which the AP should operate: • **g** = 2.4 GHz • **a** = 5 GHz
Double Encrypt	This parameter applies only to remote APs. Double encryption is used for traffic to and from a wireless client that is connected to a tunneled SSID. When enabled, all traffic is re-encrypted in the IPsec tunnel. When disabled, the wireless frame is only encapsulated inside the IPsec tunnel.
Native VLAN ID	Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).
SAP MTU	Maximum Transmission Unit (MTU) size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
Bootstrap threshold	Number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP rebootstraps. On the controller, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.
Request Retry Interval	Interval, in seconds, between the first and second retries of AP-generated requests. If the configured interval is less than 30 seconds, the interval for subsequent retries is increased up to 30 seconds.
Maximum Request Retries	Maximum number of times to retry AP-generated requests, including keepalive messages. After the maximum number of retries, the AP either reboots or tries the IP address specified by the backup LMS IP address (if configured).
Keepalive Interval	Time, in seconds, between keepalive messages from the AP
Dump Server	(For debugging purposes.) Displays the server to receive the core dump generated if an AP process crashes.
Telnet	Reports whether telnet access the AP is enabled or disabled.
SNMP sysContact	SNMP system contact information.
RFprotect Server IP	The IP address of the RFprotect server for this AP or group
RFprotect Backup Server IP	The IP address of the RFprotect backup server for this AP or group
AeroScout RTLS Server	Displays whether or not the AP will send RFID tag information to an AeroScout real-time asset location (RTLS) server.
Ortronics Walljack	Displays whether the external Ethernet port on the Ortronics Wi-Jack Duo AP is enabled or disabled.

Parameter	Description
Ortronics LED off Time-out	Automatically turns off the LEDs 5 minutes after the AP boots up.
Ortronics Low Temp	The low-temperature threshold for the Ortronics AP. If the temperature reaches this threshold, the maximum transmit power is restored to four.
Ortronics High Temp	The high-temperature threshold for the Ortronics AP. The maximum transmit power range is 0— 4, with a default of 4. If the AP temperature meets or exceeds this threshold, the maximum transmit power is reduced by one until it reaches zero.
RTLS Server configuration	Displays whether or not the AP will send RFID tag information to an RTLS server.
Remote-AP DHCP Server VLAN	Shows the VLAN ID of the remote-AP DHCP server used when controller is unreachable.
Remote-AP DHCP Server Id	Shows the IP Address of the DHCP DNS Server.
Remote-AP DHCP Default Router	Shows the IP Address of the DHCP Default Router.
Remote-AP DHCP Pool Start	Shows the IP Address used as start of DHCP Pool.
Remote-AP DHCP Pool End	Shows the IP Address used as end of DHCP Pool.
Remote-AP DHCP Pool Netmask	Shows the netmask of DHCP Pool.
Remote-AP DHCP Lease Time	Shows the length of leases, in days (0 means infinite).
Heartbeat DSCP	DSCP value of AP heartbeats (0-63).
Session ACL	Shows the access control list (ACL) applied on the uplink of a remote AP.
Maintenance Mode	Shows if Maintenance mode is enabled or disabled. If enabled, APs stop flooding unnecessary traps and syslog messages to network management systems or network operations centers when deploying, maintaining, or upgrading the network. The controller still generates debug syslog messages if debug logging is enabled.
Radio enable	Shows if the AP's radio is enabled or disabled.
Mode	Shows the operating modes for the AP. • **ap-mode**: Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN. • **am-mode**: Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.
High throughput enable (radio)	Shows if high-throughput (802.11n) features on the 2.4 GHz frequency band are enabled or disabled.
Channel	Shows the channel number for the AP's 802.11a/802.11n physical layer.
Beacon Period	Shows the time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Transmit Power	Shows the current transmission power level.
Advertise 802.11d and 802.11h Capabilities	This column reports whether or not the AP will advertise its 802.11d (Country Information) and 802.11h (TPC or Transmit Power Control) capabilities
Enable CSA	Displays whether or not the AP has enabled channel switch announcements (CSAs) for 802.11h.
CSA Count	Number of channel switch announcements that must be sent before the AP will switch to a new channel.

Parameter	Description
Management Frame Throttle interval	Average interval that rate limiting management frames are sent from this radio, in seconds. If this column displays a zero (**0**) rate limiting is disabled for this AP.
Management Frame Throttle Limit	Maximum number of management frames that can come from this radio in each throttle interval.
ARM/WIDS Override	Shows if Adaptive Radio Management (ARM) and Wireless IDS functions are enabled or disabled. If a radio is configured to operate in Air Monitor mode, then these functions are always enabled, regardless of this option.
Protection for 802.11b Clients	Displays whether or not protection for 802.11b clients is enabled or disabled.
Assignment	Displays whether or not ARM channel and power assignment has been enabled or disabled.
Allowed bands for 40MHz channels	Forty MHz channels may be used on the specified radio bands (802.11a or 802.11g).
Client Aware	Shows if the client aware feature has been enabled or disabled for this AP. If enabled, AP will not change channels when there are active clients.
Max Tx Power	Maximum transmission power for this AP, in dBm.
Min Tx Power	Minimum transmission power for this AP, in dBm.
Multi Band Scan	Shows if the multi-band scan feature has been enabled or disabled on this AP. If enabled, single-radio APs will try to scan across bands for Rogue AP detection
Rogue AP Aware	Shows if the rogue AP awareness feature has been enabled or disabled on this AP. If enabled, the AP will try to contain off-channel Rogue APs
Scan Interval	This column indicates, in seconds, how often the AP will leave its current channel to scan other channels in the band if scanning is enabled
Active Scan	Displays whether or not the active scan feature is enabled. **NOTE:** This option elicits more information from nearby APs, but also creates additional management traffic on the network. **Active Scan** is disabled by default, and should *not be enabled* except under the direct supervision of Dell Support.
Scanning	Shows if scanning is enabled or disabled for this AP. If this option is disabled, the following other options will also be disabled: • Multi Band Scan • Rogue AP Aware • Voip Aware Scan • Power Save Scan
Scan Time	The amount of time, in milliseconds, an AP will drift out of the current channel to scan another channel. The supported range for this setting is 0-2,147,483,647 seconds. Best practices are to configure a scan time between 50-200 msec.
VoIP Aware Scan	Shows if VoIP aware scanning is enabled or disabled. If you use voice handsets in the WLAN, **VoIP Aware Scan** should be enabled in the ARM profile so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that **Scanning** is also enabled.
Power Save Aware Scan	Shows if the power save aware scan is enabled or disabled. If enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode. Default: enabled
Ideal Coverage Index	The Dell coverage index metric is a weighted calculation based on the RF coverage for all DellAPs and neighboring APs on a specified channel. The **Ideal Coverage Index** specifies the ideal coverage that an AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be.

Parameter	Description
Acceptable Coverage Index	For multi-band implementations, the **Acceptable Coverage Index** specifies the minimal coverage an AP it should achieve on its channel. The denser the AP deployment, the lower this value should be.
Free Channel Index	The current free channel index value. The Dell Interference index metric measures interference for a specified channel and its surrounding channels. This value is calculated and weighted for all APs on those channels (including 3rd-party APs). An AP will only move to a new channel if the new channel has a lower interference index value than the current channel. **Free Channel Index** specifies the required difference between the two interference index values before the AP moves to the new channel. The lower this value, the more likely it is that the AP will move to the new channel.
Backoff Time	After an AP changes channel or power settings, it waits for this backoff time interval before it asks for a new channel/power setting.
Error Rate Threshold	The minimum percentage of PHY errors and MAC errors in the channel that will trigger a channel change.
Error Rate Wait Time	Minimum time in seconds the error rate on the AP has to exceed its defined error rate threshold before it triggers a channel change.
Noise Threshold	Maximum level of noise in a channel that triggers a channel change.
Noise Wait Time	Minimum time in seconds the noise level has to exceed the Noise Threshold before it triggers a channel change on the AP.
Minimum Scan Time	Minimum number of times a channel must be scanned before it is considered for assignment. Best practices are to configure a **Minimum Scan Time** between 1-20 scans.
Load aware Scan Threshold	The **Load Aware Scan Threshold** is the traffic throughput level an AP must reach before it stops scanning. Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high.
Mode Aware Arm	Shows if the mode-aware ARM feature has been enabled or disabled for this AP. If enabled, ARM will turn the AP into an Air Monitors (AMs) if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (e.g. less than 60 feet apart).
40 MHz intolerance	The specified setting allows ARM to determine if 40 MHz mode of operation is allowed on the 5 GHz or 2.4 GHz frequency band only, on both frequency bands, or on neither frequency band.
Honor 40 MHz intolerance	Shows if 40 MHz intolerance is enabled or disabled. If enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.
Legacy station workaround	Shows if interoperability for misbehaving legacy stations is enabled or disabled.
ESSID	Name that uniquely identifies the Extended Service Set Identifier (SSID).
Encryption	Encryption type used on this AP.
DTIM Interval	Shows the interval, in milliseconds, between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed.
Basic Rates	Lists supported 802.11a rates, in Mbps, that are advertised in beacon frames and probe responses from this AP.
Transmit Rates	Lists 802.11a rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error/loss rate of the client.
Station Ageout Time	Time, in seconds, that a client is allowed to remain idle before being aged out.
Max Transmit Attempts	Maximum number of retries allowed for the AP to send a frame

Parameter	Description
RTS Threshold	Wireless clients transmitting frames larger than this threshold must issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS). This helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting.
Short Preamble	Shows if a short preamble for 802.11b/g radios is enabled or disabled for this AP. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble. Legacy client devices that use only long preamble generally can be updated to support short preamble.
Max Associations	Maximum number of wireless clients allowed to associate to the AP
Wireless Multimedia (WMM)	Shows if Wireless Multimedia (WMM) is enabled or disabled for this AP. WMM provides prioritization of specific traffic relative to other traffic in the network
WMM TSPEC Min Inactivity Interval	Displays the minimum inactivity time-out threshold of WMM traffic for this AP.
DSCP mapping for WMM voice AC	Displays the DSCP value used to map WMM video traffic.
DSCP mapping for WMM video AC	Displays the DSCP value used to map WMM voice traffic.
DSCP mapping for WMM best-effort AC	Displays the DSCP value used to map WMM best-effort traffic
DSCP mapping for WMM background AC	Displays the DSCP value used to map WMM background traffic.
902il Compatibility Mode	Shows if 902 il compatibility mode is enabled or disabled. (This parameter only needs to be enabled for APs with associated clients using NTT DoCoMo 902iL phones.)
Hide SSID	Shows if the feature to hide a SSID name in beacon frames is enabled or disabled.
Deny_Broadcast Probes	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.
Local Probe Response	Shows if local probe response is enabled or disabled on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients' probe requests. If this option is disabled, then the controller sends the 802.11 probe responses
Disable Probe Retry	If disabled, the AP will not resend probes if it does not get a response.
Battery Boost	Shows if the battery boost feature is enabled or disabled for the AP. If enabled, this feature converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval. The longer interval keeps associated wireless clients from activating their radios for multicast indication and delivery, leaving them in power-save mode longer and thus lengthening battery life
Drop Broadcast and Multicast	If this feature is enabled on an AP, it drops all downstream broadcast or multicast traffic to increase battery life.
WEP Key 1	Displays the static WEP key (1 of 4).
WEP Key 2	Displays the static WEP key (2 of 4).
WEP Key 3	Displays the static WEP key (3 of 4).
WEP Key 4	Displays the static WEP key (4 of 4).
WEP Transmit Key Index	Displays the key index that specifies which static WEP key is to be used.
WPA Hexkey	Displays the WPA pre-shared key (PSK).

Parameter	Description
WPA Passphrase	Displays the WPA passphrase with which the AP generates a pre-shared key (PSK).
Maximum Transmit Failures	Display the maximum number of transmission failures allowed before the client gives up.
BC/MC Rate Optimization	Shows if the AP has enabled or disabled scanning of all active stations currently associated to that AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate.
High throughput enable (SSID)	Shows if the AP has enabled or disabled the use of its high-throughput SSID in 40 MHz mode.
40 MHz channel usage	Determines if this high-throughput SSID allows high-throughput (802.11n) stations to associate.
MPDU Aggregation	Shows if the AP has enabled or disabled MAC protocol data unit (MDPU) aggregation.
Max transmitted A-MPDU size	Shows the maximum size, in bytes, of an A-MPDU that can be sent on the AP's high-throughput SSID.
Max received A-MPDU size	Shows the maximum size, in bytes, of an Aggregated-MAC Packet Data Unit (A-MPDU) that can be received on the AP's high-throughput SSID.
Min MPDU start spacing	Displays the minimum time between the start of adjacent MDPUs within an aggregate MDPU, in microseconds.
Supported MCS set	Comma-separated list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this high-throughput SSID.
Short guard interval in 40 MHz mode	Shows if the AP has enabled or disabled use of short guard interval in 40 MHz mode of operation.
Legacy stations	Shows if the AP has enabled or disabled the legacy stations option, which controls whether or not legacy (non-HT) stations are allowed to associate with the AP's SSID. By default, legacy stations are allowed to associate. **NOTE:** This setting has no effect on a BSS in which HT support is not available.
Allow weak encryption	Shows if the AP has enabled or disabled the weak encryption option. The use of TKIP or WEP for unicast traffic forces the use of legacy transmissions rates. Disabling this mode prevents the association of stations using TKIP or WEP for unicast traffic. This mode is disabled by default.
Virtual AP enable	Wireless LAN profiles configure WLANs in the form of virtual AP profiles. This parameter shows if the AP has enabled or disabled virtual APs.
Allowed band	Shows the band(s) on which to use the virtual AP: • a—802.11a band only (5 GHz) • g—802.11b/g band only (2.4 GHz) • all—both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz)
VLAN	Shows the VLAN(s) into which users are placed in order to obtain an IP address.
Forward mode	Shows the current forward mode (tunnel, bridge, split-tunnel, or decrypt-tunnel) for the virtual AP. This parameter controls whether 802.11 frames are tunneled to the controller using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the controller, and Internet access remains local). When an AP is configured to use the decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the controller, which then applies firewall policies to the user traffic. When the controller sends traffic to a client, the controller sends 802.3 traffic through the GRE tunnel to the AP, which then converts it to encrypted 802.11 and forwards to the client. Only 802.1x authentication is supported when configuring bridge or split tunnel mode.
Deny time range	Shows the time range for which the AP will deny access for a virtual AP.

Parameter	Description
Mobile IP	Shows if IP mobility has been enabled or disabled for the virtual AP.
HA Discovery on-association	If enabled, all clients of a virtual-ap will received mobility service on association.
DoS Prevention	Shows the status of the Dos Prevention option. If enabled, virtual APs ignore deauthentication frames from clients. This prevents a successful deauth attack from being carried out against the AP. This does not affect third-party APs.
Station Blacklisting	Shows if the virtual AP has enabled or disabled detection of denial of service (DoS) attacks, such as ping or SYN floods, that are not spoofed deauth attacks.
Blacklist Time	Shows the number of seconds that a client will be quarantined from the network after being blacklisted.
Authentication Failure Blacklist Time	Shows the time, in seconds, a client is blocked if it fails repeated authentication. If the virtual AP shows a value of 0, a blacklisted client is blocked indefinitely.
Fast Roaming	Shows if the AP has enabled or disabled fast roaming.
Strict Compliance	If enabled, the virtual AP denies client association requests if the AP and client station have no common rates defined. Some legacy client stations which are not fully 802.11-compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.
VLAN Mobility	Shows if a virtual AP has enabled or disabled VLAN (Layer-2) mobility
Remote-AP Operation	Shows when the virtual AP operates on a remote AP: • **always**—Permanently enables the virtual AP. • **backup**—Enables the virtual AP if the remote AP cannot connect to the controller. • **persistent**—Permanently enables the virtual AP after the remote AP initially **connects** to the controller. • **standard**—Enables the virtual AP when the remote AP connects to the controller. A remote AP should use **always** and **backup** for bridge SSIDs, and use **persistent** and **standard** for 802.1x, tunneled, and split-tunneled SSIDs.
Convert Broadcast ARP requests to unicast	If this option is enabled, all broadcast ARP requests are converted to unicast and sent directly to the client. You can check the status of this option using the **show ap active** and the **show datapath** tunnel command. If enabled, the output will display the letter **a** in the flags column.
Band Steering	Shows if band-steering has been enabled or disabled for a virtual AP. ARM's band steering feature encourages dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4GHz band for single band clients like VoIP phones. Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5GHz band than on the 2.4GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40MHz or 20MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.
VoIP Call Admission Control	Shows if WiFi VoIP Call Admission Control features are enabled or disabled.
VoIP Bandwidth based CAC	Shows the maximum bandwidth that can be handled by one radio, in kbps.
VoIP Call Capacity	Show the number of simultaneous calls that can be handled by one radio.
VoIP Bandwidth Capacity (kbps)	Shows the maximum bandwidth that can be handled by one radio, in kbps.
VoIP Call Handoff Reservation	Shows the percentage of call capacity reserved for mobile VoIP clients on call.

Parameter	Description
VoIP Send SIP 100 Trying	If enabled, the AP sends SIP 100 - trying messages to a call originator to indicate that the call is proceeding. This is useful when the SIP invite may be redirected through a number of servers before reaching the controller.
VoIP Disconnect Extra Call	If enabled, the AP disconnects calls that exceed the high capacity threshold by sending a deauthentication frame.
VOIP TSPEC Enforcement	Shows if validation of TSPEC requests for call admission controls is enabled or disabled.
VOIP TSPEC Enforcement Period	Displays the maximum time for the station to start a call after the TSPEC request.
VoIP Drop SIP Invite and send status code (client)	Displays the status code sent to the client when a SIP Invite is dropped. • **480**: Temporary Unavailable • **486**: Busy Here • **503**: Service Unavailable • **none**: Don't send SIP status code
VoIP Drop SIP Invite and send status code (server)	Displays the status code sent to the server when a SIP Invite is dropped. • **480**: Temporary Unavailable • **486**: Busy Here • **503**: Service Unavailable • **none**: Don't send SIP status code

Related Commands

Command	Description	Mode
ap system-profile rf dot11g-radio-profile rf arm-profile rf ht-radio-profile wlan ht-ssid-profile wlan virtual-ap wlan voip-cac-profile	The output of the `show ap config` command displays the content of the profile settings for an individual AP or AP group. Use the commands displayed in the column to the left to configure these parameters.	Enable and Config modes

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap coverage-holes

```
show ap coverage holes
```

Description

Show information for APs that have detected coverage holes in the wireless network.

Usage Guidelines

This command will only display coverage hole information if you have enabled coverage hole detection using the command **rf optimization-profile <profile> coverage-hole-detection**. The coverage hole detection feature requires the RF Protect license.

Examples

The output of this command

```
(host) #show ap coverage-holes
   Coverage Holes Detected
   -----------------------
   Name  BSSID              Radio  STA                  RSSI
   ----  -----              -----  ---                  ----
   ap12  00:1a:1e:c0:7f:fc   a      00:0b:86:c7:49:94     15
```

The output of this command includes the following information:

Column	Description
Name	Name of an AP that detected a coverage hole.
BSSID	Basic Service Set Identifier (BSSID) of an AP that detected a coverage hole.
Radio	The coverage hole is for this radio PHY type (**a** or **g**).
STA	MAC address of the station.
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.

Command History

Introduced in ArubaOS 2.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	RF Protect license	Enable or Config mode on master controllers

show ap database

```
show ap database {group <group>|inactive|indoor|local|long|outdoor|page <page>|sensors
[disconnected]|sort-by [ap-group|ap-ip|ap-type|fqln|provisioned|status
{up|down}|switch-ip]|sort-direction[ascending|descending]|start <start> |status
{up|down]|switch <switch-ip-addr>|unprovisioned}
```

Description

Show the list of access points in the controller's database.

Syntax

Parameter	Description
`group <group>`	Show data for a specified AP group.
`inactive`	Show only local APs with no active BSSIDs or wired AP interfaces.
`indoor`	Show only APs that have an installation mode set to “indoor.”
`local`	Show only APs on this controller.
`long`	Display the following additional data columns: • Wired MAC Address, • Serial # • Slot/Port • FQLN
`outdoor`	Show only APs that have an installation mode set to “outdoor.”
`page <page>`	Display a limited number of APs by entering the number of APs to be displayed in the output of this command.
`sensors`	Show only RFprotect sensors.
`disconnected`	Show only disconnected RFprotect sensors.
`sort-by`	Sort the output of this command by a specific data column.
`ap-group`	Sort by AP group name.
`ap-ip`	Sort by AP group name.
`ap-type`	Sort by AP model.
`fqln`	Sort by Fully Qualified Location Name (FQLN).
`provisioned`	Sort by provisioning statistics.
`status up|down`	If used with the **sort-by** keyword, **status** sorts the output of the command by status type (**up** or **down**.) Otherwise, use the **status** keyword to display APs with the specified status.
`switch-ip`	Sort by controller IP address.
`sort-direction`	Choose sort direction of AP list:.
`ascending`	Sort AP list in ascending order by name.
`descending`	Sort AP list in descending order by name.
`start <start>`	Start showing the AP index at the specified index number.
`status`	Show only APS with a given status as active or inactive.
`down`	Show only APs that are inactive.
`up`	Show only APs that are active.
`switch <switch-ip-addr>`	Show only APs registered with a specified controller by entering a controller IP address.
`unprovisioned`	Show only unprovisioned APs (using modifiers).

Usage Guidelines

Many of the parameters in this command can be used together to filter a large database of information down to just the AP data you want to see. For example, you can issue the **command show ap database group <group> local status up** to view a list of local APs within a specific AP group that are reporting an **up** status. Include the **sort-by** and **sort-direction** keywords to specify how the data is sorted in the output of this command.

Examples

The output of the command **show ap database** shows the controller's database of information for APs in the group **default**. The output also includes a description of the flag types that may appear in the **Flags** column.

```
show ap database group default
AP Database
-----------
Name          Group    AP Type  IP Address   Status         Flags  Switch IP
----          -----    -------  ----------   ------         -----  ---------
3.125.141112  default  125      192.0.2.12   Up 1h:48m:27s         10.4.97.4
3.125.142113  default  125      192.0.2.12   Up 1h:43m:6s          10.4.97.6
3.125.242115  default  125      192.0.2.13   Up 1h:41m:18s         10.4.97.10
3.60.161112   default  60       192.0.2.14   Up 1h:43m:20s         10.4.97.4
3.60.202108   default  60       192.0.2.15   Up 8h:7m:4s    R      10.4.97.4
3.61.101100   default  61       192.0.2.16   Up 7h:32m:13s  R      10.4.97.4
3.61.161113   default  61       192.0.2.17   Up 1h:43m:20s         10.4.97.4
3.65.101117   default  65       192.0.2.18   Up 8h:39m:7s   R      10.4.97.4
3.65.121108   default  65       192.0.2.29   Up 1h:55m:14s         10.4.97.4
3.65.292112   default  65       192.0.2.32   Up 1h:43m:42s         10.4.97.10
3.70.102116   default  70       192.0.2.43   Up 8h:23m:17s  R      10.4.97.4
3.70.131107   default  70       192.0.2.44   Up 1h:55m:10s         10.4.97.4
3.70.172103   default  70       192.0.2.56   Up 1h:42m:24s         10.4.97.6
3.85.152116   default  85       192.0.2.57   Up 1h:42m:56s         10.4.97.6
3.85.252117   default  85       192.0.2.58   Up 1h:43m:18s         10.4.97.10
AP-61-20      default  61       192.0.2.59   Up 21m:36s     o      10.3.47.189
Flags: U = Unprovisioned; N = Duplicate name; G = No such group; L = Unlicensed
       R = Remote AP; I = Inactive; X = Maintenance Mode; P = PPPoE AP
       S = RFprotect Sensor; d = Disconnected Sensor; H = Using 802.11n license
       M = Mesh node; Y = Mesh Recovery i = Indoor; o = Outdoor
Total APs:15
```

Related Commands

Command	Description	Mode
show ap database-summary	To display a more general summary overview of the AP registered to a controller, use the command `show ap database-summary`.	Enable and Config modes

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap database-summary

```
show ap database-summary
```

Description

Show a general summary of access point information for this controller.

Usage Guidelines

Use this command to show the current number of active APs and Air Monitors. This command is also useful for determining how many unprovisioned APs or duplicate APs are on the network. For full details on each AP registered to a controller, use the command show ap database.

Examples

The output of this command shows that this controller can detect a total of five APs, four up, and one down.

```
show ap database-summary

(host) #show ap database-summary

AP Database Summary
-------------------
AP Mode              Total Up  Total Down  Total Upgrading*  Total Rebooting*  RAP Up  RAP Down  RAP          RAP
                           Upgrading*   Rebooting*
------              --------  ----------  ----------------  ----------------  ------  --------  -----------  -------
Access Points        0         0           0                 0                 0       0         0            0
Air Monitors         0         0           0                 0                 0       0         0            0
Wired Access Points  0         0           0                 0                 0       0         0            0
Mesh Portals         0         0           0                 0                 0       0         0            0
Mesh Points          0         0           0                 0                 0       0         0            0
RFprotect Sensors    0         0           0                 0                 0       0         0            0

*Upgrading and Rebooting counts only reflect APs registered on this controller.

Unprovisioned Access Points:0
Duplicated AP Name:0
```

The output of this command includes the following information:

Column	Description
`Total Up`	Total number of APs with an *up* status.
`Total Down`	Total number of APs with a *down* status.
`IPSEC Up`	Total number of APs with an active (up) IPSEC tunnel.
`IPSEC Down`	Total number of APs with an inactive (down) IPSEC tunnel.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug association-failure (deprecated)

```
show ap debug association-failure [{ap-name <ap-name>}|{bssid <bssid>}|{client-mac
<client-mac>}|{essid <essid>}|{ip-addr <ip-addr>}]
```

Description

Display association failure information that can be used to troubleshoot problems on an AP.

Command History

Platforms	Licensing
ArubaOS 3.0	Command introduced
ArubaOS 5.0	Command deprecated

show ap debug bss-config

```
show ap debug bss-config [ap-name <ap-name>|bssid <bssid>||essid <essid>|ip-addr <ip-addr>|port <port>/<slot>]
```

Description

Show the configuration for each BSSID of an AP. This information can be used to troubleshoot problems on an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Filter the AP Config Table by AP name.
`bssid <bssid>`	Filter the AP Config Table by BSSID. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`essid <essid>`	Filter the AP Config Table by ESSID. An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
`ip-addr <ip-addr>`	Filter the AP Config Table by IP address by entering an IP address in dotted-decimal format.
`port <port>/<slot>`	Filter the AP Config Table by port and slot numbers. The slot and port numbers should be separated by a forward slash (/).

Examples

The output of this command shows the AP configuration table for a specific BSSID.

```
(host) #show ap debug bss-config
Dell AP Config Table
---------------------
bss                ess    vlan  ip          phy   type  fw-mode  max-cl  rates tx-rates  preamble
mtu  status  wmm
---                ---    ----  --          ---   ----  -------  ------  ----- --------  --------
---  ------  ---
00:1a:1e:11:24:c2  cera2  66    10.6.1.203  g-HT  ap    tunnel   64      0x3   0xfff     enable
0    enable  enable
```

The output of this command includes the following information:

Column	Description
`bss`	Basic Service Set (BSS) identifier, which is usually the AP's MAC address.
`ess`	Extended Service Set (ESS) identifier; a user-defined name for a wireless network.
`vlan`	The BSSID's VLAN number.
`IP`	The AP's IP address.
`phy`	One of the following 802.11 types • a • a-HT (high-throughput) • g • g-HT (high-throughput)
`type`	This column shows if the BSSID is for an access point (**ap**) or an air monitor (**am**).

Column	Description
fw-mode	The configured forward mode for the AP's virtual AP profile. • **bridge**: Bridge locally • **split-tunnel**: Tunnel to controller or NAT locally • **tunnel**: Tunnel to controller
max-cl	The maximum number of clients allowed for this BSSID.
preamble	Shows if short preambles are enabled for 802.11b/g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using a short preamble.
MTU	Maximum Transmission Unit (MTU) size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
status	Shows if this BSSID is enabled or disabled.
wmm	Shows if the BSSID has enabled or disabled WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF) WMM provides prioritization of specific traffic relative to other traffic in the network.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug bss-stats

```
show ap debug bss-stats [bssid <bssid>]
```

Description

Show debug and troubleshooting statistics from a specific BSSID of an AP.

Syntax

Parameter	Description
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.

Examples

The example below shows part of the output of the command **show ap debug bss-stats bssid <bssid>**.

```
(host) #show ap debug bss-stats bssid 00:1a:1e:11:5f:11
   BSSID Stats
   -----------
   Parameter            Value
   ---------            -----
   -------------------  General Per-radio Statistics
   -------------------  Transmit specific Statistics
   Frames Rcvd For TX   4263
   Tx Frames Dropped    613
   Frames Transmitted   3650
   Success With Retry   0
   Tx Mgmt Frames       451975
   Beacons Transmitted  447712
   Tx Probe Responses   4263
   Tx Data Frames       0
   Multicast Data       0
   Tx CTS Frames        0
   Dropped After Retry  613
   Dropped No Buffer    0
   Missed ACKs          613
   Long Preamble        4263
   Short Preamble       0
   Tx EAPOL Frames      0
   Tx 6 Mbps            3650
   Tx WMM [VO]          4263
```

The output of this command includes the following information:

Parameter	Description
`Frames Rcvd For TX`	Number of frames received for transmission.
`Tx Frames Dropped`	Number of transmission frames that were dropped.
`Frames Transmitted`	Number of frames successfully transmitted.
`Success With Retry`	Number of frames that were transmitted after being retried.
`Tx Mgmt Frames`	Number of management frames transmitted.
`Beacons Transmitted`	Number of beacons transmitted.

Parameter	Description
Tx Probe Responses	Number of transmitted probe responses.
Tx Data Frames	Number of transmitted data frames.
Multicast Data	Number of multicast and broadcast frames transmitted.
Tx CTS Frames	Number of clear-to-sent (CTS) frames transmitted.
Dropped After Retry	Number of frames dropped after an attempted retry.
Dropped No Buffer	Number of frames dropped because the AP's buffer was full.
Missed ACKs	Number of missed acknowledgements (ACKs).
Long Preamble	Number of frames sent with a long preamble.
Short Preamble	Number of frames sent with a short preamble.
Tx EAPOL Frames	Number of Extensible Authentication Protocol over LAN (EAPOL) frames transmitted.
Tx 6 Mbps	Number of frames transmitted at 6 Mbps.
Tx 9 Mbps	Number of frames transmitted at 9 Mbps.
Tx 12 Mbps	Number of frames transmitted at 12 Mbps.
Tx 18 Mbps	Number of frames transmitted at 18 Mbps.
Tx 24 Mbps	Number of frames transmitted at 24 Mbps.
Tx 36 Mbps	Number of frames transmitted at 36 Mbps.
Tx 48 Mbps	Number of frames transmitted at 48 Mbps.
Tx 54 Mbps	Number of frames transmitted at 54 Mbps.
Tx HT 108 Mbps	Number of frames transmitted at 108 Mbps.
Tx HT 120 Mbps	Number of frames transmitted at 120 Mbps.
Tx HT 162 Mbps	Number of frames transmitted at 162 Mbps.
Tx HT 180 Mbps	Number of frames transmitted at 180 Mbps.
Tx HT 216 Mbps	Number of frames transmitted at 216 Mbps.
Tx HT 240 Mbps	Number of frames transmitted at 240 Mbps.
Tx HT 243 Mbps	Number of frames transmitted at 243 Mbps.
Tx HT 270 Mbps	Number of frames transmitted at 270 Mbps.
Tx HT 300 Mbps	Number of frames transmitted at 300 Mbps.
Tx WMM	Number of Wifi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. **Tx WMM [BE]:** Best Effort **Tx WMM [BK]:** Background **Tx WMM [VO]:** VoIP **Tx WMM [VI]:** Video
	Number of Wifi Multimedia (WMM) VoIP packets transmitted.
UAPSD OverflowDrop	Number of packets dropped due to Unscheduled Automatic Power Save Delivery (U-APSD) overflow.
Last SNR	The last recorded signal-to-noise ratio.

Parameter	Description
Last SNR CTL0	The signal-to-noise ratio for the last received data packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR CTL1	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR CTL2	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR	Signal-to-noise ratio for the last received ACK packet.
Last ACK SNR CTL0	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR CTL1	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR CTL2	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR EXT0	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR EXT1	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR EXT2	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Frames Received	Number of frames received.
Rx Data Frames	Number of data frames received.
Null Data Frames	Number of null data frames received.
Rx Mgmt Frames	Number of management frames received.
Control Frames	Number of control frames received.
Frames To Me	Number of wireless frames received that are addressed to the specified BSSID.
Probe Requests	Number of probe requests.
PS Poll Frames	Number of Power Save poll frames
Rx 6 Mbps	Number of frames received at 6 Mbps.
Rx 9 Mbps	Number of frames received at 9 Mbps.
Rx 12 Mbps	Number of frames received at 12 Mbps.
Rx 18 Mbps	Number of frames received at 18 Mbps.
Rx 24 Mbps	Number of frames received at 24 Mbps.
Rx 36 Mbps	Number of frames received at 36 Mbps.
Rx 48 Mbps	Number of frames received at 48 Mbps.
Rx 54 Mbps	Number of frames received at 54 Mbps.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug client-mgmt-counters

```
show ap debug client-mgmt-counters
```

Description

Show the numbers of each type of message from an AP's clients. This information can be used to troubleshoot problems on an AP.

Examples

The output of the command

```
(host)#show ap debug client-mgmt-counters
   Counters
   --------
   Name                          Value
   ----                          -----
   Validate Client               512
   AP Stats Update Message       557750
   3087                          6
   Tunnel VLAN Membership        4493
   Update STA Tunnel Request     229
   Update STA Tunnel Response    229
   ARM Update                    808921
   ARM Propagate                 590567
   ARM Neighbor Assigned         55396
   STM SAP Down                  19
   AP Message                    192
   STA On Call Message           12164
   STA Message                   19750
   STA SIP authenticate Message  10919
   STA Deauthenticate            707
   Stat Update V3                441447
   VoIP CAC State Announcement   37185
   Remote AP State               371330
   AP Message Response           164
```

The output of this command includes the following information:

Parameter	Description
`Validate Client`	Number of times a client was validated.
`AP Stats Update Message`	Number of times an AP updated its statistics with the controller.
`3087`	(For internal use only)
`Tunnel VLAN Membership`	(For internal use only)
`Update STA Tunnel Request`	(For internal use only)
`Update STA Tunnel Response`	(For internal use only)
`ARM Update`	Number of times an AP has changed its adaptive radio management (ARM) settings.
`ARM Propagate`	(For internal use only)
`ARM Neighbor Assigned`	(For internal use only)

Parameter	Description
STM SAP Down	(For internal use only)
AP Message	(For internal use only)
STA On Call Message	Number of counters indicating that a station has an active phone call
STA Message	(For internal use only)
STA SIP authenticate Message	Number of messages indicating that a telephone has completed SIP registration and authentication.
STA Deauthenticate	Number of times a station sent a message to an AP to deauthenticate a client.
Stat Update V3	(For internal use only)
VoIP CAC State Announcement	Number of times a controller announces a call admission control (CAC) state change to the AP. Changes in CAC state could include the ability of call admission controls to accept more or fewer calls than previously configured.
Remote AP State	(For internal use only)
AP Message Response	(For internal use only)
assoc-req	Number of 802.11 association request management frames from the controller.
assoc-resp	Number of 802.11 association responses to the controller.
reassoc-req	Number of 802.11 reassociation requests to the controller.
reassoc-resp	Number of 802.11 reassociation responses from the controller.
disassoc	Number of 802.11 disassociation messages to the controller.
deauth	Number of 802.11 deauthorization messages from the controller.
sapcp	(For internal use only)

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug client-stats

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

Description

Show detailed statistics about a client.

Example

The command below displays statistics for packets both received from and transmitted to the specified client.

```
(host) #show ap debug client-stats 00:19:7e:89:fa:e7

  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
```

The output of this command includes the following information:

Parameter	Description
`Frames Rcvd For TX`	Number of frames received for transmission.
`Tx Frames Dropped`	Number of transmission frames that were dropped.

Parameter	Description
Frames Transmitted	Number of frames successfully transmitted.
Success With Retry	Number of frames that were transmitted after being retried.
Tx Mgmt Frames	Number of management frames transmitted.
Tx Probe Responses	Number of transmitted probe responses.
Tx Data Frames	Number of transmitted data frames.
Tx CTS Frames	Number of clear-to-sent (CTS) frames transmitted.
Dropped After Retry	Number of frames dropped after an attempted retry.
Dropped No Buffer	Number of frames dropped because the AP's buffer was full.
Missed ACKs	Number of missed acknowledgements (ACKs)
Long Preamble	Number of frames sent with a long preamble.
Short Preamble	Number of frames sent with a short preamble.
Tx EAPOL Frames	Number of Extensible Authentication Protocol over LAN (EAPOL) frames transmitted.
Tx <n> Mbps	Number of frames transmitted at <n> Mbps, where <n> is a value between 6 and 300.
Tx WMM	Number of Wifi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. **Tx WMM [BE]:** Best Effort **Tx WMM [BK]:** Background **Tx WMM [VO]:** VoIP **Tx WMM [VI]:** Video
UAPSD OverflowDrop	Number of packets dropped due to Unscheduled Automatic Power Save Delivery (U-APSD) overflow.
Last SNR	The last recorded signal-to-noise ratio.
Last SNR CTL0	The signal-to-noise ratio for the last received data packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR CTL1	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR CTL2	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR	Signal-to-noise ratio for the last received ACK packet.
Last ACK SNR CTL0	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR CTL1	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR CTL2	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR EXT0	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR EXT1	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Frames Received	Number of frames received.
Rx Data Frames	Number of data frames received.

Parameter	Description
`Null Data Frames`	Number of null data frames received.
`Rx Mgmt Frames`	Number of management frames received.
`PS Poll Frames`	Number of power save poll frames received.
`Rx <n> Mbps`	Number of frames received at <n> Mbps, where <n> is a value between 6 and 300.
`Tx WMM`	Number of Wifi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear 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

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug client-table

```
show ap debug client-table [ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>]
```

Description

Show clients associated to an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Filter the AP Config Table by AP name.
`bssid <bssid>`	Filter the AP Config Table by BSSID. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Filter the AP Config Table by IP address by entering an IP address in dotted-decimal format.

Usage Guidelines

The **Tx_Rate**, **Rx_Rate**, **Last_ACK_SNR**, and **Last_Rx_SNR** columns shown in the output of this command display valuable troubleshooting information for clients trying to connect to a specific AP. Use this command to verify that the transmit (Tx_Rate) and receive (Rx_Rate) rates are not too low, and that the signal-to-noise (SNR) ratio is acceptable.

Examples

The example below shows part of the AP configuration table for a specific BSSID. Additional parameters not displayed are described in the table below.

```
(host) #show ap debug client-table ap-name AP12
MAC               ESSID  BSSID          Assoc_State  HT_State  AID  PS_State  UAPSD        Tx_Pkts
Rx_Pkts  PS_Qlen  Tx_Retr
---               -----  -----          -----------  --------  ---  --------  -----        -------
    -------   ---      ----
00:17:f2:4d:01:e2 wpa2  00:1a:1e:11:5f:11  Associated   None    0x1  Awake    (0,0,0,0,N/A,0) 31463
22821    0        4289
00:14:a4:25:72:6d wpa2  00:1a:1e:11:5f:11  Associated   None    0x2  Awake    (0,0,0,0,N/A,0) 24691
45215    0        944
00:19:7e:66:89:38 wpa2  00:1a:1e:11:5f:11  Associated   None    0x4  Awake    (0,0,0,0,N/A,0) 7031
```

The output of this command includes the following information:

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

Parameter	Description
UAPSD	This parameter 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`	Number of packets transmitted by the client.
`Rx_Pkts`	Number of packets received by the client.
`PS-Qlen`	Power save queue length, in bytes.
`Tx_Retries`	Number of packets that the client had to resend due to an initial transmission failure.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug counters

```
show ap debug counters {ap-name <ap-name>|bssid <bssid>|group <group>|ip-addr <ip-addr>}
```

Description

Show AP message and reboot/bootstrap counters for an individual AP or AP group.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show debug counters for an AP with a specified name.
`bssid <bssid>`	Show debug counters for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`group <group>`	Show debug counters for an AP group.
`ip-addr <ip-addr>`	Show debug counters for an AP with a specified IP address by entering an IP address in dotted-decimal format.

Example

The output of this command can you how many times each AP has rebooted (a hard boot) or bootstrapped (a soft boot), the number of times configuration changes were sent from the controller, and the number of configuration changes acknowledged by that AP.

```
(host) #show ap debug counters group corp1
AP Counters
-----------
Name  Group  IP Address  Configs Configs AP Boots  AP Boots  Bootstraps  Reboots
                          Sent    Acked   Sent      Acked
----  -----  ----------  ------  ------- --------  --------  ----------  -------
AL1   corp1  10.6.1.209  1597    1597     0         0         1           0
AL10  corp1  10.6.1.198  165     165      0         0         2           1
AL12  corp1  10.6.1.200  195     195      0         0         1           0
AL15  corp1  10.6.1.197  1580    1580     0         0         1           0
AL16  corp1  10.6.1.199  73      73       0         0         1           0
AL19  corp1  10.6.1.212  8       8        0         0         1           0
Total APs :6
```

The output of this command includes the following information:

Column	Description
`Name`	Name of the AP.
`Group`	Name of the AP's group.
`IP Address`	IP address of the AP.
`Configs sent`	Number of times configuration changes have been sent to the AP.
`Configs Acked`	Number of times that the AP has acknowledged receiving a configuration change.
`Bootstraps`	Number of times the AP restarted. Bootstraps are also known as "soft" restarts.
`Reboots`	Number of times power to the AP cycled off and then on again. Reboots also known as "hard" restarts.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug crash-info

```
show ap debug crash-info {ap-name <ap-name>|ip-addr <ip-addr>}
```

Description

Show crash log information (if it exists) for an individual AP. The stored information is cleared from the flash after the AP reboots.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show crash information for an AP with a specified name.
`ip-addr <ip-addr>`	Show crash information for an AP with a specified IP address by entering an IP address in dotted-decimal format.

Example

The output of this command shows a partial sample crash log information for an AP named **MyAP**

```
(host) #show ap debug crash-info ap-name MyAP

<5>
<4>Aruba Networks
<4>ArubaOS Version x.x.x.x (build xxxx / label #xxxx)
<4>Built by p4build@cartman on 2010-07-29 at 14:44:06 PST (gcc version x.x.x
Cav
ium Networks Version: 1.4.0, build 58)
<4>CVMSEG size: 2 cache lines (256 bytes)
<4>Setting flash physical map for 16MB flash at 0x1ec00000
<4>Determined physical RAM map:
<7>On node 0 totalpages: 16384
<7>  DMA zone: 16384 pages, LIFO batch:3
<7>  DMA32 zone: 0 pages, LIFO batch:0
<7>  Normal zone: 0 pages, LIFO batch:0
<7>  HighMem zone: 0 pages, LIFO batch:0
<4>Primary instruction cache 32kB, virtually tagged, 4 way, 64 sets, linesize
12
8 bytes.
<4>Primary data cache 16kB, 64-way, 2 sets, linesize 128 bytes.
<4>Using 500.000 MHz high precision timer. cycles_per_jiffy=1000000
<6>Memory: 56636k/65536k available (1925k kernel code, 8840k reserved, 575k
data
, 2716k init, 0k highmem)
<4>Calibrating delay using timer specific routine.. 1000.32 BogoMIPS
(lpj=100032
2)
<4> available.
<4>Checking for the multiply/shift bug... no.
<4>Checking for the daddi bug... no.
<4>Checking for the daddiu bug... no.
<5>detected lzma initramfs
<5>initramfs: LZMA lc=3,lp=0,pb=2,dictSize=8388608,origSize=15217664
<5>LZMA initramfs
```

Command History

Introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug datapath

```
show ap debug datapath {ap-group <ap-group>|ap-name <ap-name>|bssid <bssid>|ip-addr
<ip-addr>}
```

Description

Show datapath tunnel parameters of an AP or AP group.

Syntax

Parameter	Description
`ap-group <ap-group>`	Show data path information for a specific AP group.
`ap-name <ap-name>`	Show data path information for an AP with a specific name.
`bssid <bssid>`	Show data path information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data path information for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Example

The output of the following command shows datapath tunnel parameters for an AP with the IP address 192.0.2.32.

```
(host) #show ap debug datapath 192.0.2.32

Datapath Parameters Table
-------------------------
essid    encr-alg        client-vlan-id  tunnel-id  gre-type  deny-bcast  num-clients
-----    --------        --------------  ---------  --------  ----------  -----------
guest       Open            63              0x10f6     0x8300    disable     0
voip     WPA2 8021X AES  66              0x1103     0x8310    disable     7
corpWPA2 PSK AES         66              0x10f1     0x8320    disable     0
guest    Open            63              0x10f7     0x8200    disable     1
wpa2     WPA2 8021X AES  65              0x10be     0x8210    enable      15
```

The output of this command includes the following information:

Column	Description
`ESSID`	The Extended Service Set Identifier is a unique name that identifies a wireless network
`encr-alg`	Encryption algorithm used by the network
`client-vlan-id`	ID of the network VLAN
`tunnel-id`	Identification number of the AP's tunnel.
`gre-type`	GRE tunnel type.
`deny-bcast`	If **enabled**, the AP will respond to broadcast probe requests. If **disabled**, the AP will not respond to these requests.
`num-clients`	Number of clients currently using the network.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug driver-log

```
show ap debug driver-log {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show an AP's driver logs.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`bssid <bssid>`	Show log information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Usage Guidelines

Use this command to review configuration changes made since the AP was last reset.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug log

```
show ap debug log {ap-group <ap-group>|ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show an AP's debug log.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`bssid <bssid>`	Show log information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Usage Guidelines

An AP's log files show configuration changes since the AP was last reset.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug mgmt-frames (deprecated)

Description

Show traced 802.11 management frames.

Command History

Version	Modification
ArubaOS 3.0	Command Introduced
ArubaOS 5.0	Command deprecated

show ap debug radio-stats

```
show ap debug radio-stats {ap-name <ap-name>|ip-addr <ip-addr>} radio {0|1} [advanced]
```

Description

Show aggregate radio debug statistics of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`radio {0|1}`	Specify the ID number of the radio for which you want to view statistics.
`advanced`	Include this parameter to display additional radio statistics.

Example

The output of this command displays general statistics for the radio, as well as statistics for transmitted and received frames.

```
(host) #show ap debug radio-stats ap-name AP12 radio 1
RADIO Stats
-----------
Parameter            Value
---------            -----
-------------------  General Per-radio Statistics
Total Radio Resets   0
Resets Beacon Fail   0
TX Power Changes     5
Channel Changes      2
Radio Band Changes   0
Current Noise Floor  95
11g Protection       0
-------------------  Transmit specific Statistics
Frames Rcvd For TX   2452151
Tx Frames Dropped    1736429
Frames Transmitted   4247212
...
   Success With Retry   0
   Tx Mgmt Frames       24174109
```

If you include the **advanced** option at the end of the **show ap debug radio-stats** command, the output of this command will include all the following parameters. If you omit the advanced option, the output will include less information, and the data will be displayed in a different order.

Parameter	Description
`Total Radio Resets`	Total number of times the radio reset.
`Resets Beacon Fail`	Number of times the radio reset due to beacon failure.
`Resets BeacQ Stuck`	An AP's radio typically sends a beacon every 100 milliseconds. If beacons are not sent at a regular interval or the radio experiences excessive noise, the beacon queue will reset. This parameter indicates the number of queue resets.
`Resets Fatal Intr`	Number of time the radio was reset because the AP hardware was unresponsive.
`Resets RX Overrun`	The number of radio resets due to Receive FIFO overruns.

Parameter	Description
Resets RF Gain	Number of radio resets due to gain changes.
Resets MTU Change	Number of times the radio reset due to a change in the Maximum Transmission Unit (MTU) value.
Resets TX Timeouts	Number of radio resets due to transmission timeouts (the radio doesn't transmit a signal within the required time frame.)
POE-Related Resets	If the radio power profile drops, an W-AP125 may not be able to support three transmit chains, and may drop to two chains only. This parameter displays the number of resets due to this type of power change.
External Reset	Number of times the AP has been reset because it was unplugged or its reset button was pressed.
TX Power Changes	Number of times the radio's transmission power changed.
Channel Changes	Number of times the radio's channel changed.
Radio Band Changes	Number of time the radio's band changed.
Current Noise Floor	The residual background noise detected by an AP. **NOTE:** Noise seen by an AP is reported as -dBm. Therefore, a noise floor of -100 dBm is smaller (lower) than a noise floor of -50 dBm. For most environments, the noise floor should be no greater than -80 dBm. Anything larger may indicate an interference problem which is drowning out good signals (data) in background noise.
Avail TX Buffers	An AP has a set number of buffers which it can use to buffer frames for nonresponsive power save clients. The total number of buffer frames depends upon the AP model type.
11g Protection	This parameter shows whether 802.11g protection has been enabled or disabled.
Last TX Antenna	This parameter indicates whether the last frame transmitted was sent on antenna 1 or antenna 0. This parameter can be useful for troubleshooting external antennas.
Last RX Antenna	This parameter indicates whether the last frame received was via antenna 1 or antenna 0. This parameter can be useful for troubleshooting external antennas.
Scan Requests	Total number of scan requests received by the AP.
Scan Rejects	Total number of scan rejected by the AP.
Load aware Scan Rejects	Load aware ARM preserves network resources during periods of high traffic by temporarily halting scanning if the load for the AP gets too high. The **load aware Scan Rejects** parameter shows the number of times the AP has rejected a scan because of the load aware scan feature.
PS aware Scan Rejects	If the ARM power-save aware scan feature is enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode. The p**s aware Scan Rejects** parameter shows the number of times the AP has rejected a scan because of the power-save aware scan feature.
Voice aware Scan Rejects	If you enable the VoIP Aware Scan feature in the AP's ARM profile, the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This **Voice aware scan Rejects** parameter shows the number of times the AP has rejected a scan because of the Voip aware scan feature.
Scan Success	Number of successful scans. To view scan details, use the command `show ap arm scan-times`.
EIRP	The value of this parameter is the transmission power level (in dBm) + the antenna gain value.
MAX EIRP	The max EIRP depends on AP capability and the regulatory domain constraint for the channel of operation. For example, in the US, Channels 36-48 have max EIRP of 23dBm
UAPSD Flush STA Wake	Number of times a client wakes from power-save mode and flushes the UAPSD queue.

Parameter	Description
UAPSD SP Set	The number of unique UAPSD Scheduled Period is started in response to UAPSD trigger frames.
UASPD Dup Trig	The number of times duplicate UAPSD trigger frames are received (i.e., retried UAPSD triggers that were received by the AP more than once).
UAPSD Recv frame for TX	The number of frames received for transmission over the air interface using UAPSD
UAPSD Ageout Drain	The number of time UAPSD queue is drained (i.e. frames are dropped) due to ageout.
UAPSD TX proc comp	The number of UAPSD frames that were successfully transmitted
UAPSD SP In prog	The number of times a trigger frame was received while a Scheduled Period (SP) was already in progress based on an earlier trigger frame.
UAPSD QOS NULL TX	The number of times the AP had to respond with a QoS Null Data frame in response to a UAPSD trigger because AP did not have Data frame queued for that client
UAPSD TX HW Queued	The number of frames (Data and Null Data) that were transferred to the radio HW for transmission, in response to UAPSD triggers.
UAPSD SP Reset	The number of times the UAPSD Scheduled Period (SP) in progress is reset or cancelled.
Frames Rcvd For TX	Number of frames received for transmission.
Tx Frames Dropped	Number of transmission frames that were dropped.
Frames Transmitted	Number of frames successfully transmitted.
PS Unicast	Number of power save unicast frames
DTIM Broadcast	Number of broadcast frames with DTIM values.
Success With Retry	Number of frames that were transmitted after being retried.
Tx Mgmt Frames	Number of management frames transmitted.
Beacons Transmitted	Number of beacons transmitted.
Tx Probe Responses	Number of transmitted probe responses.
Tx Data Frames	Number of transmitted data frames.
Multicast Data	Number of multicast and broadcast frames transmitted.
Tx CTS Frames	Number of clear-to-sent (CTS) frames transmitted.
DTIM Timeouts	Number of broadcast frames with DTIM data that were not answered by a client.
Dropped After Retry	Number of frames dropped after an attempted retry.
Dropped No Buffer	Number of frames dropped because the AP's buffer was full.
Dropped UAPSD	Number of dropped Unscheduled Automatic Power Save Delivery (UAPSD) frames.
Missed ACKs	Number of missed acknowledgement frames.
Failed Beacons	Number of times a radio failed to transmit a beacon at the scheduled interval (100ms).
Multi-Beacon Fail	Number of times multiple consecutive beacons failed to transmit.
Long Preamble	Number of frames sent with a long preamble.
Short Preamble	Number of frames sent with a short preamble.
Beacon Interrupts	Number of broadcast beacons that were interrupted.
TX Interrupts	Number of transmission interrupts.

Parameter	Description
FIFO Underrun	The number of Receive FIFO overruns.
Allocated Desc	Number of allocated transmit descriptors.
Freed Desc	Number of freed transmit descriptors.
Tx EAPOL Frames	Number of Extensible Authentication Protocol over LAN (EAPOL) frames transmitted
Tx AGGR Good	Number of aggregated frames successfully transmitted.
Tx AGGR Unaggr	Number of non-aggregate frames transmitted due to unavailability of additional frames for aggregation at the time of transmission.
Tx <number> Mbps	Number of frames transmitted at the specified rate (in Mbps).
Tx <number> Mbps [Long]	Number of frames with a long preamble transmitted at the specified rate.
Tx <number> Mbps [Short]	Number of frames with a short preamble transmitted at the specified rate.
Tx HT <number> Mbps	Number of high-throughput frames transmitted at the specified rate.
Tx WMM	Number of Wifi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. **Tx WMM [BE]:** Best Effort **Tx WMM [BK]:** Background **Tx WMM [VO]:** VoIP **Tx WMM [VI]:** Video
UAPSD OverflowDrop	Number of packets dropped due to Unscheduled Automatic Power Save Delivery (U-APSD) overflow.
TX Timeouts	Number of transmission timeouts
Lost Carrier Events	Number of carrier sense timeouts.
Last SNR	The last recorded signal-to-noise ratio.
Last SNR CTL0	The signal-to-noise ratio for the last received data packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR CTL1	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR CTL2	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR EXT0	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR EXT1	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR EXT2	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR	Signal-to-noise ratio for the last received ACK packet.
Last ACK SNR CTL0	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR CTL1	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR CTL2	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.

Parameter	Description
Last ACK SNR EXT0	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR EXT1	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR EXT2	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Frames Received	Number of frames received.
Good Frames	Number of frames received with no errors.
Bad Frames	Number of bad or error frames received.
Rx Clear 1s	The percentage of time no activity was seen on the air in the last 1 second.
Rx Clear 4s	The percentage of time no activity was seen on the air in the last 4 seconds.
Rx Clear 64s	The percentage of time no activity was seen on the air in the last 64 seconds.
Discarded Events	Number of non-802.11 events that were detected and discarded during normal operation.
ARM Scan Frames	Number of scan frames sent for the adaptive radio management (ARM) feature.
Rx Data Frames	Data frames received
Null Data Frames	Null data frames received
Rx Mgmt Frames	Management frames received
Control Frames	Control frames received.
Frames To Me	Number of wireless frames received that are addressed to the specified BSSID.
Broadcast Frames	Number of broadcast frames received.
Beacons Received	Number of beacons received
Probe Requests	Number of Probe requests received.
Rx Probe Responses	Number of Probe responses received.
Rx RTS Frames	Ready To Send (RTS) frames received. These frames are sent when a computer has data to transmit.
Rx CTS Frames	Clear To Send (CTS) frames received. This type of frame are used to verify that a client is ready to receive information.
ACK Frames	Number of acknowledgement frames received.
PS Poll Frames	Power-Save Poll (PS-Poll) frames received. When a client exits a power-saving mode, it transmits a PS-Poll frame to the AP to retrieve any frames buffered while it was in power-saving mode.
CRC Errors	Cyclic Redundancy Check (CRC) is a data sequence that is sent with a frame to help verify if all the data received correctly. Possible CRC error causes include: • Hardware malfunction • Loose or unconnected cables • RF interference, such as overlapping access point coverage on a channel or interfering 2.4-GHz signals from devices like microwave ovens • and wireless handset phones
PLCP Errors	Physical Layer Convergence Protocol (PLCP) errors.
Rx Frames Dropped	Number of received frames that were dropped.

Parameter	Description
`PHY Events`	The number of Physical Layer Events, that are not 802.11 packets, detected by radio as part of its normal receive operation.
`RADAR Events`	Number of times an AP detects a radar signature. Dell APs are DFS-compliant detects a radar signature, it will change its channel.
`RX Interrupts`	The number of receive interrupts received by the CPU from the radio.
`RX Overrun`	The number of Receive FIFO overruns.
`Rx <number> Mbps`	Packets received at the specified rate (in Mbps).
`Rx <number> Mbps (Long)`	Packets with a long preamble received at the specified rate.
`Rx <number> Mbps (Short)`	Packets with a short preamble received at the specified rate.
`Rx HT <number> Mbps`	Number of high-throughput packets received at the specified rate.
`Rx WMM [BE]`	Number of Wifi Multimedia (WMM) packets received for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. **`Rx WMM [BE]`:** Best Effort **`Rx WMM [BK]`:** Background **`Rx WMM [VO]`:** VoIP **`Rx WMM [VI]`:** Video

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug received-config

```
show ap debug received-config {ap-group <ap-group>|ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show the configuration the AP downloaded from the controller.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`bssid <bssid>`	Show log information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Example

The output of this command displays configuration information for each interface. The example below shows only part of the output for this command. Additional parameters not displayed are described in the table below.

```
(host) #show ap debug received-config ap-name AP12

Downloaded Config for WIFI 0
----------------------------
Item                                Value
----                                -----
BSSID                               00:1a:1e:11:5f:10
LMS IP                              10.6.2.250
Master IP                           10.100.103.2
Mode                                AP Mode
QBSS Probe Response                 Allow Access
Native VLAN ID                      1
SAP MTU                             1500 bytes
Heartbeat DSCP                      0
High throughput enable (radio)      Enabled
Channel                             40-
Beacon Period                       100 msec
Transmit Power                      15 dBm
Advertise TPC Capability            Disabled
Enable CSA                          Disabled
CSA Count                           4
Management Frame Throttle interval  1 sec
Management Frame Throttle Limit     20
Active Scan                         Disabled
VoIP Aware Scan                     Enabled
Power Save Aware Scan               Enabled
Load aware Scan Threshold           1250000 Bps
40 MHz intolerance                  Disabled
Honor 40 MHz intolerance            Enabled
Legacy station workaround           Disabled
Country Code                        US
ESSID                               guest
...
```

The output of this command includes the following information:

Parameter	Description
BSSID	The BSSID of the AP.
LMS IP	The LMS IP is the IP address of the local controller used by the AP for client data processing.
Master IP	For environments with multiple controllers, the master controller is the central configuration and management point for all local controllers.
Mode	Shows the operating modes for the AP. ap-mode: Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN. am-mode: Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.
QBSS Probe Response	Quality-of-service BSS (QBSS).
Native VLAN ID	The ID number of the Native VLAN.
SAP MTU	The Maximum Transmission Unit (MTU) for the GRE tunnel.
Heartbeat DSCP	DSCP value for the heartbeat traffic between the AP and the controller.
High throughput enable (radio)	Shows if high-throughput (802.11n) features on tare enabled or disabled on the radio.
Channel	Shows the channel number for the AP's 802.11a/802.11n physical layer.
Beacon Period	Shows the time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Transmit Power	Shows the current transmission power level.
Advertise TPC Capability	If enabled, the AP will advertise its Transmit Power Control (TPC) capability.
Enable CSA	Displays whether or not the AP has enabled channel switch announcements (CSAs) for 802.11h.
CSA Count	Number of channel switch announcements that must be sent before the AP will switch to a new channel.
Management Frame Throttle interval	Average interval that rate limiting management frames are sent from this radio, in seconds. If this column displays a zero (**0**), rate limiting is disabled for this AP.
Management Frame Throttle Limit	Maximum number of management frames that can come from this radio in each throttle interval.
Active Scan	Displays whether or not the active scan feature is enabled. This option elicits more information from nearby APs, but also creates additional management traffic on the network. **Active Scan** is disabled by default, and should *not be enabled* except under the direct supervision of Dell Support.
VoIP Aware Scan	Shows if VoIP aware scanning is enabled or disabled. If you use voice handsets in the WLAN, **VoIP Aware Scan** should be enabled in the ARM profile so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that **Scanning** is also enabled.
Power Save Aware Scan	Shows if the power save aware scan is enabled or disabled. If enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode.
Load aware Scan Threshold	The **Load Aware Scan Threshold** is the traffic throughput level an AP must reach before it stops scanning. Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high.
40 MHz intolerance	The specified setting allows ARM to determine if 40 MHz mode of operation is allowed on the 5 GHz or 2.4 GHz frequency band only, on both frequency bands, or on neither frequency band.

Parameter	Description
Honor 40 MHz intolerance	Shows if 40 MHz intolerance is enabled or disabled. If enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.
Legacy station workaround	Shows if interoperability for misbehaving legacy stations is enabled or disabled.
Country Code	Display the country code for the AP. The country code specifies allowed channels for that country.
ESSID	An Extended Service Set Identifier (ESSID), for the AP.
Encryption	Encryption type used on this AP.
WPA2 Pre-Auth	802.11x settings are **enabled** or **disabled**.
DTIM Interval	Number of beacons that should elapse before an AP sends beacon broadcasts for power save clients.
802.11a Basic Rates	Minimum data rate required for a client to associate with the AP. For an 802.11a radio, this value can be 6, 12 and 24 802.11 data rates. 802.11b/g radios will report a value of 1 and 2 802.11 data rates.
802.11a Transmit Rates	802.11 data rate at which the AP will transmit data to its clients. This value can be 6-54 for 802.11a radios, and 1-54 for 802.11b/g radios.
Station Ageout Time	Number of seconds a station may be idle before it is deauthorized from an AP.
Max Transmit Attempts	maximum number of times the AP will attempt to retransmit data.
RTS Threshold	The minimum packet size at which the AP will issue a request-to-send (RTS) before sending the packet.
Max Associations	The maximum number of clients allowed to associated with the AP
Wireless Multimedia (WMM)	Shows if Wireless Multimedia (WMM) is enabled or disabled for this AP. WMM provides prioritization of specific traffic relative to other traffic in the network.
WMM TSPEC Min Inactivity Interval	Displays the minimum inactivity time-out threshold of WMM traffic for this AP.
DSCP mapping for WMM voice AC	Displays the DSCP value used to map WMM video traffic.
DSCP mapping for WMM video AC	Displays the DSCP value used to map WMM voice traffic.
DSCP mapping for WMM best-effort AC	Displays the DSCP value used to map WMM best-effort traffic
DSCP mapping for WMM background AC	Displays the DSCP value used to map WMM background traffic.
Hide SSID	Shows if the feature to hide a SSID name in beacon frames is **enabled** or **disabled**.
Deny_Broadcast Probes	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.
Local Probe Response	Shows if local probe response is enabled or disabled on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients' probe requests. If this option is disabled, then the controller sends the 802.11 probe responses
Disable Probe Retry	Shows if the AP has enabled or disabled MAC-level retries for probe response frames. By default this parameter is enabled, which mean that MAC level retries for probe response frames is disabled.

Parameter	Description
Maximum Transmit Failures	Display the maximum number of transmission failures allowed before the client gives up.
BC/MC Rate Optimization	Shows if the AP has enabled or disabled scanning of all active stations currently associated to that AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate.
High throughput enable (SSID)	Shows if the AP has enabled or disabled the use of its high-throughput SSID in 40 MHz mode.
40 MHz channel usage	Determines if this high-throughput SSID allows high-throughput (802.11n) stations to associate.
MPDU Aggregation	Shows if the AP has enabled or disabled MAC protocol data unit (MDPU) aggregation.
Max transmitted A-MPDU size	Shows the maximum size, in bytes, of an A-MPDU that can be sent on the AP's high-throughput SSID.
Max received A-MPDU size	Shows the maximum size, in bytes, of an Aggregated-MAC Packet Data Unit (A-MPDU) that can be received on the AP's high-throughput SSID.
Min MPDU start spacing	Displays the minimum time between the start of adjacent MDPUs within an aggregate MDPU, in microseconds.
Supported MCS set	Comma-separated list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this high-throughput SSID.
Short guard interval in 40 MHz mode	Shows if the AP has enabled or disabled use of short guard interval in 40 MHz mode of operation.
VLAN	VLAN ID used by the SSID.
Forward mode	Shows the current forward mode (bridge, split-tunnel, or tunnel) for the virtual AP. This parameter controls whether 802.11 frames are tunneled to the controller using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the controller, and Internet access remains local). Only 802.1x authentication is supported when configuring bridge or split tunnel mode.
Band Steering	Shows if band-steering has been enabled or disabled for a virtual AP. ARM's band steering feature encourages dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4GHz band for single band clients like VoIP phones. Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5GHz band than on the 2.4GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40MHz or 20MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug remote association

```
show ap debug remote association [ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>]
```

Description

Show the AP association table to identify the remote clients associated to each AP.

Syntax

Parameter	Description
`ap-group <ap-group>`	Show remote client associations for a specific AP group.
`ap-name <ap-name>`	Show remote client associations for a specific AP.
`bssid <bssid>`	Show remote client associations for an specific AP Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.

Usage Guidelines

Use this command to verify if a remote user is connected to an AP, and to validate the AP to which is connected.

Example

The output of this command displays information about the remote clients associated with an AP with the IP address 192.0.2.32.

```
(host) #show ap debug remote association ip-addr 192.0.2.32

Flags: W: WMM client, A: Active, R: RRM client

PHY Details: HT: High throughput; 20: 20MHz; 40: 40MHz
             <n>ss: <n> spatial streams

Association Table
-----------------
Name bssid             mac             auth assoc aid  l-int  essid  vlan-id  tunnel-id phy  assoc. num   Flags
                                                 time   assoc
---- ----------------  ----------------- -- --    ---  ----  -----  ----     ------     ---  -----  ----  ------
AP71 00:0a:23:c1:d4:11 00:16:6d:08:1s:f1 y  y     1    10    t-lab  111      0x108e     a    23s    1     A
Num Clients:1
```

The output of this command includes the following information:

Column	Description
`Name`	Name of an AP.
`bssid`	The AP Basic Service Set Identifier (BSSID).
`mac`	MAC address of the AP.
`auth`	This column displays a **y** if the AP has been configured for 802.11 authorization frame types. Otherwise, it displays an **n**.
`assoc`	This column displays a **y** if the AP has been configured for 802.11 association frame types. Otherwise, it displays an **n**.
`aid`	802.11 association ID. A client receives a unique 802.11 association ID when it associates to an AP.

Column	Description
1-int	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
essid	Name that uniquely identifies the AP's Extended Service Set Identifier (ESSID).
vlan-id	Identification number of the AP's VLAN.
tunnel-id	Identification number of the AP's tunnel.
assoc. time	Amount of time the client has associated with the AP, in the format hours:minutes:seconds.
num assoc	Number of clients associated with the AP.
flags	This column displays any flags for this AP. The list of flag abbreviations is included in the output of the **show ap association** command.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug shaping-table

```
show ap debug shaping-table {ap-name <ap-name>|ip-addr <ip-addr>}
```

Description

Show shaping information for clients associated to an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show shaping table information for a specific AP.
`ip-addr <ip-addr>`	Show shaping table information for a specific AP IP address by entering its IP address in dotted-decimal format.

Example

The following command shows the shaping table the an AP named ap22.

```
(host) #show ap debug shaping-table ap-name ap22

VAP station000
pktin   pktout  pktdrop pktqd   cmn[C:O:H]      drop    Numcl   TotCl   BWmgmt
0       0       0       0      0-0-0   0-0     0-0-0   0       0

d1      d2      d3      d4      d5      d6      d7      d8      d9
0       0       0       0       0       0       0       0       0

idx     tokens  last-t  in      out     drop    q       tx-t    rx-t    al-t    rate

idx     d1      d2      d3      d4      d5      d6      d7      d8      d9
0       0       0       0       0       0       0       0       0       0

VAP station001
pktin   pktout  pktdrop pktqd   cmn[C:O:H]      drop    Numcl   TotCl   BWmgmt
0       8144    0       0      0-0-0   0-0     0-2-0   2       0

d1      d2      d3      d4      d5      d6      d7      d8      d9
0       0       0       0       0       0       0       0       0

idx     tokens  last-t  in      out     drop    q       tx-t    rx-t    al-t    rate
1       0       0       0      2966     0       0       716     0       0       0
3       0       0       0      31       0       0       8       0       0       0

idx     d1      d2      d3      d4      d5      d6      d7      d8      d9
0       0       0       0       0       0       0       0       0       0
1       0       0       0       0       0       0       0       0       0
3       0       0       0       0       0       0       0       0       0
```

The output of this command includes the following information:

Column	Description
`pktin`	Number of packets received by the AP.
`pktout`	Number of packets sent by the AP.
`pktdrop`	Number of packets dropped by the AP.

Column	Description
pktqd	Number of packets queued.
cmn [C:O:H]	(For internal use only.)
drop	Number of CCK (802.11b) and OFDM (802.11a/g) packets dropped.
Numcl	Number of CCK (802.11b) and OFDM (802.11a/g) packets dropped.
TotCl	Total number of clients associated with the AP
Bwmgmt	This data column displays a 1 if the bandwidth management feature has been enabled. Otherwise, it displays a 0.
d<n>	(For internal use only.)
idx	Association ID.
tokens	This value represents the credits the station has to transmit tokens.
last-t	Number of tokens that were allocated to the station last time token allocation algorithm ran.
in	Number of packets received.
out	Number of packets sent.
drop	Number of dropped packets.
q	Number of queued packets
tx-t	Total time spent transmitting data.
rx-t	Total time spent receiving data.
al-t	Total time allocated for transmitting data to this station.
rate	(For internal use only.)

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug system-status

```
show ap debug system-status {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show detailed system status information for an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show system status data for an AP with a specific name.
`bssid <bssid>`	Show system status data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show system status data for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Usage Guidelines

The output of this command displays the following types of information (if it exists) for the selected AP:

Bootstrap information	Per-radio statistics	Ethernet duplex/speed settings
Descriptor Usage	Encryption statistics	Tunnel heartbeat stats
Interface counters	AP uptime	Boot version
MTU discovery	memory usage	LMS information
ARP cache	Kernel slab statistics	Power status
Route table	Interrupts	CPU type
Interface Information	Crash Information	

The following parameters are included in the output of this command, and can help troubleshoot problems on an AP or wireless network.

Parameter	Description
The **Failed** column in the **Descriptor Usage** section	This parameter can tell you if the AP is dropping packets.
Interface Information table	This parameter can tell you if the ethernet network is working properly. This table should not show an excessive number of errors.
AP Uptime table	Low values in this table can indicate problems with the wired network, or with the AP itself.
Tunnel Heartbeat table	This table can indicate the health of the underlying wired network.
Rebootstrap Information table /**Reboot Information** table	A large number of reboots can mean that the AP has hardware problems.

Command History

Release	Modification
ArubaOS 5.0	Crash information parameter was introduced.
ArubaOS 3.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap debug trace-addr

```
show ap debug trace-addr
```

Description

Show MAC addresses in the trace buffer.

Usage Guidelines

Use this command to troubleshoot wireless clients that are being traced for 802.11 communication

Examples

The output of the command shows the **Trace List** table. If no wireless clients are being traced, this table will be empty.

```
(host) #show ap debug trace-addr

Trace List
----------
MAC Address
-----------
00:1a:1e:c5:ca:b4
00:1a:1e:c5:d6:46
00:1a:1e:c5:d7:40
00:1a:1e:c5:d7:64
00:1a:1e:c5:d9:56
00:1a:1e:c5:d9:b0
```

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap details

```
show ap details [advanced]{ap-name <ap-name>|bssid <bssid>|ip-addr <ip-
addr>|installation}
```

Description

Show detailed provisioning parameters and hardware and operating information and for a specific AP.

Syntax

Parameter	Description
`advanced`	Include the following additional data in the output of this command: • switch message counts • AP group information • Virtual AP operating information
`ap-name <ap-name>`	Show data for a specific AP by entering the name of the AP for which you want to display information.
`bssid <bssid>`	Show data for an AP with the specified BSSID. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with the specified IP address.

Examples

The example below shows part of the output for the command **show ap details ap-name <ap-name>**.

```
(host) # show ap details ap-name AP32
   AP "AL39" Basic Information
   ---------------------------
   Item            Value
   ----            -----
   AP IP Address   10.6.1.206
   LMS IP Address  10.6.2.253
   Group           corp1344
   Location Name   N/A
   Status          Up
   Up time         4d:12h:47m:32s

   AP "AL39" Hardware Information
   ------------------------------
   Item                Value
   ----                -----
   AP Type             125
   Serial #            AD0054972
   Wired MAC Address   00:1a:1e:c9:17:38
   Radio 0 BSSID       00:1a:1e:11:73:90
   Radio 1 BSSID       00:1a:1e:11:73:80
   Enet 1 MAC Address  00:1a:1e:c9:17:39

   AP "AL39" Operating Information
   -------------------------------
   Item                 Value
```

The output of this command includes the following information:

Column	Description
AP IP Address	IP address of the AP
LMS IP Address	The IP address of the local management switch (LMS)—the Dell controller which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network.
Group	Name of the AP's AP group.
Location Name	Location of the AP.
Status	Current status of the AP, either **Up** or **Down**.
Up time	Number of hours, minutes and seconds since the last controller reboot or bootstrap, in the format *hours:minutes:seconds*.
Installation	AP Installation mode. The AP can be default (the factory set AP installation type, indoor or outdoor.
AP Type	AP model
Serial #	Serial number for the AP
Wired MAC address	MAC address of the wired interface.
Radio 0 BSSID	Basic Service Set Identifier (BSSID) of the AP's radio 0. This is usually the radio's MAC address.
Radio 1 BSSID	Basic Service Set Identifier (BSSID) of the AP's radio 1. This is usually the radio's MAC address.
Enet 1 MAC address	MAC address of the AP's ethernet port.
AP State	Displays the AP's current operational state.
Entry created	Timestamp showing the time the AP registered with the controller.
Last activity	Timestamp showing the last time the AP communicated with the controller. An AP typically sends keepalive messages every minute.
Reboots	Number of times power to the AP cycled off and then on again. Reboots also known as "hard" restarts.
Bootstraps	Number of times the AP restarted. Bootstraps are also known as "soft" restarts.
Bootstrap threshold	Number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP rebootstraps. On the controller, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.
Slot/Port	The controller port used by the AP, in the format <slot>/<port>. The **<slot>** number is always 1. The **<port>** parameter refers to the network interfaces that are embedded in the front panel of the W-3000 Controller Series Multi-Service Controller. Port numbers start at 0, from the left-most position.
High throughput	Shows if high-throughput (802.11n) features are **enabled** or **disabled**.
Mode	Shows the operating modes for the AP. • **AP**: Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN. • **AM**: Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.

Column	Description
Band	The RF band in which the AP should operate: • 802.11g = 2.4 GHz • 802.11a = 5 GHz
Channel	Channel number for the AP 802.11a/802.11n physical layer. The available channels depend on the regulatory domain (country).
Secondary Channel	The secondary channel number for the AP. The secondary channel is a 20 MHz channel used in conjunction with the primary channel to create a 40 MHz channel for high-throughput clients. High-throughput capable APs use only the primary channel to communicate with 20 MHz clients. The secondary channel is used for transmissions with 40 MHz capable high-throughput clients.
EIRP	Current effective Isotropic Radiated Power (EIRP).
AP Name	Name of the AP.
AP Group	AP group to which the AP belongs.
Location name	Fully-qualified location name (FQLN) for the AP.
SNMP sysLocation	User-defined description of the location of the AP, as defined with the command **provision-ap syslocation**.
Master	Name or IP address for the master controller.
Gateway	IP address of the default gateway for the AP.
Netmask	Netmask for the AP's IP address.
IP Addr	IP address for the AP.
Dns IP	IP address of the DNS server.
Domain Name	Domain name used by the AP.
Server Name	DNS name of the controller from which the AP boots.
Server IP	IP address of the controller from which the AP boots
Antenna gain for 802.11a	Antenna gain for 802.11a (5GHz) antenna.
Antenna gain for 802.11g	Antenna gain for 802.11g (2.4GHz) antenna.
Antenna for 802.11a	Antenna use for 5 GHz (802.11a) frequency band. • 1: AP uses antenna 1 • 2: AP uses antenna 2 • both: AP uses both antennas
Antenna for 802.11g	Antenna use for 2.4 GHz (802.11g) frequency band. • 1: AP uses antenna 1 • 2: AP uses antenna 2 • both: AP uses both antennas
IKE PSK	The IKE pre-shared key.
PPPOE User Name	Point-to-Point Protocol over Ethernet (PPPoE) user name for the AP.
PPPOE Password	PPPoE password for the AP.
PPPOE Service Name	PPPoE service name for the AP.
USB User Name	The PPP username provided by the cellular service provider.
USB Password	A PPP password, if provided by the cellular service provider.

Column	Description
USB Device Type	The USB driver type.
USB Device Identifier	The USB device identifier.
USB Dial String	The dial string for the USB modem.
USB Initialization String	The initialization string for the USB modem.
USB TTY device path	The TTY device path for the USB modem.
Mesh Role	If the mesh role is “none,” the AP is operating as a thin AP. An AP operating as a mesh node can have one of two roles: mesh portal or mesh point.
Installation	The type of installation (**indoor** or **outdoor**). The **default** parameter indicates that the ArubaOS automatically selects an installation mode based upon the AP’s model type.
Latitude	Latitude coordinates of the AP, in the format *Degrees Minutes Seconds* (DMS).
Longitude	Longitude coordinates of the AP, in the format *Degrees Minutes Seconds* (DMS).
Altitude	Altitude, in meters, of the AP. This parameter is supported on outdoor APs only.
Antenna bearing for 802.11a	Horizontal coverage distance of the 802.11a (5GHz) antenna from true north, from 0-360 degrees. **NOTE:** This parameter is supported on outdoor APs only. The horizontal coverage pattern does not consider the elevation or vertical antenna pattern.
Antenna bearing for 802.11g	Horizontal coverage distance of the 802.11g (2.4GHz) antenna from true north, from 0-360 degrees. **NOTE:** This parameter is supported on outdoor APs only. The horizontal coverage pattern does not consider the elevation or vertical antenna pattern.
Antenna tilt angle for 802.11a	The angle of the 802.11a (5GHz) antenna. This parameter can range from between -90 degrees and 0 degrees for downtilt, and between +90 degrees and 0 degrees for uptilt.
Antenna tilt angle for 802.11g	The angle of the 802.11g (2.4GHz) antenna. This parameter can range from between -90 degrees and 0 degrees for downtilt, and between +90 degrees and 0 degrees for uptilt.
Mesh SAE	Shows if the AP has enabled or disabled Secure Attribute Exchange (SAE) on a mesh network. This setting is disabled by default.

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	Introduced support for mesh parameters, additional antenna parameters, and AP location parameters.
ArubaOS 3.4	Introduced support for the following parameters: • installation • mesh-sae • set-ikepsk-by-addr • usb-dev • usb-dial • usb-init • usb-passwd • usb-tty • usb-type • usb-user
ArubaOS 5.0	The **mesh-sae** parameter no longer displays the **sae-default** setting if the parameter is disabled. Only the **sae-disable** option indicates that this parameter is currently in its default disabled state.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap enet-link-profile

```
show ap enet-link-profile [<profile>]
```

Description

Show a list of all Ethernet Link profiles.

Usage Guidelines

Include a profile name to display details for the specified Ethernet Link Profile, or omit the <profile> parameter to display a list of all Ethernet Link profiles.

Example

This command shows the speed of the Ethernet interface and the current duplex mode for the ethernet link profile “default”:

```
(host) #show ap enet-link-profile default

AP Ethernet Link profile "default"
----------------------------------
Parameter  Value
---------  -----
Speed      auto
Duplex     auto
```

The output of this command includes the following parameters:

Parameter	Description
Speed	The speed of the Ethernet interface. This value can be either **10 Mbps**, **100 Mbps**, **1000 Mbps** (1 Gbps), or **auto** (auto-negotiated).
Duplex	The duplex mode of the AP’s Ethernet interface. This value can be either **full**, **half**, or **auto** (auto-negotiated).

Related Commands

Command	Description	Mode
ap enet-link-profile	This command configures an AP Ethernet link profile.	Config mode

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap essid

```
show ap essid
```

Description

Show a Extended Service Set Identifier (ESSID) summary for the controller, including the numbers of APs and clients associated with each ESSID.

Examples

The output of the command in the example below shows statistics for four configured ESSIDs.

```
(host) #show ap essid
ESSID Summary
-------------
ESSID   APs  Clients  VLAN(s)  Encryption
-----   ---  -------  -------  ----------
vocera  21   0        66       WPA2 PSK AES
voip    23   52       66,64    WPA2 8021X AES
guest   49   6        63       Open
wpa2    26   88       65,64    WPA2 8021X AES
Num ESSID:4
```

The output of this command includes the following information:

Column	Description
ESSID	An Extended Service Set Identifier (ESSID) is the identifying name of an 802.11 wireless network.
APs	Number of APs associated with the ESSID.
VLAN(s)	VLAN IDs of the VLANs for the ESSID.
Encryption	The layer-2 authentication and encryption used on this ESSID to protect access and ensure the privacy of the data transmitted to and from the network.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap ht-rates

```
show ap ht-rates bssid <bssid>
```

Description

Show high-throughput rate information for a basic service set (BSS).

Syntax

Parameter	Description
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.

Examples

The output of this command shows high-throughput rates for each supported MCS value. These values are applicable to high-throughput (802.11n-capable) APs only.

```
Host) #show ap ht-rates bssid 00:1a:1e:1e:5a:10

AP "AL12" Radio 0 BSSID 00:1a:1e:1e:5a:10 High-throughput Rates (Mbps)
----------------------------------------------------------------------
MCS  Streams  20 MHz  40 MHz  40 MHz SGI
---  -------  ------  ------  ----------
  0   1          6.5    13.5    15.0
  1   1         13.0    27.0    30.0
  2   1         19.5    40.5    45.0
  3   1         26.0    54.0    60.0
  4   1         39.0    81.0    90.0
  5   1         52.0   108.0   120.0
  6   1         58.5   121.5   135.0
  7   1         65.0   135.0   150.0
  8   2         13.0    27.0    30.0
  9   2         26.0    54.0    60.0
 10   2         39.0    81.0    90.0
 11   2         52.0   108.0   120.0
 12   2         78.0   162.0   180.0
 13   2        104.0   216.0   240.0
 14   2        117.0   243.0   270.0
 15   2        130.0   270.0   300.0
```

The output of this command includes the following information:

Column	Description
`MCS`	A Modulation Coding Scheme (MCS) values supported on this high-throughput SSID.
`Streams`	Number of spatial streams used by the MCS index value.
`20 MHz`	802.11n data rates for the MCS for 20 Mhz transmissions.
`40 MHz`	802.11n data rates for the MCS for 40 Mhz transmissions.
`40 MHz SGI`	802.11n data rates for the MCS for 40 Mhz transmissions using a short guard interval.

Command History

Introduced in ArubaOS 3.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap image version

```
show ap image version [ap-name <ap-name>|ip-addr <ip-addr>]
```

Description

Display an AP's image version information.

Syntax

Parameter	Description
`ap-name <ap-name>`	View image version information for an AP with a specific name.
`ip-addr <ip-addr>`	View image version information for an AP with a specific IP address. Enter the address of the AP in dotted-decimal format.

Usage Guidelines

By default, this command displays image version information for all APs associated with the controller. To view image version information for a single AP, specify an AP using the **ap-name** or **ip-addr** parameters

Example

The output in the example below shows the current running image version as well as the image version stored in the controller's flash memory.

```
(host) #show ap image version ip-addr 192.0.2.45

Access Points Image Version
---------------------------
AP             Running Image Version String
--             ----------------------------
10.6.1.200    3.3.2.5 Wed Oct 22 10:46:42 PDT 2008
Flash Image Version String           Matches  Num Matches  Num Mismatches  Bad Checksums  Image Load Status
---------------------------          -------  ----------   --------------  -------------  ----------------
3.3.2.5 Wed Oct 22 10:46:42 PDT 2008 Yes      3            1               0              Done
```

The output of this command includes the following information:

Column	Description
`AP`	Name or IP address of an AP
`Running Image Version String`	String identifying the number of the image version currently running on the AP, as well as the date on which that version was created.
`Flash Image Version String`	String identifying the number of the image version in the AP's flash memory, as well as the date on which that version was created.
`Matches`	If **yes**, the running image version matches the image version currently in the AP's flash memory. If **no**, the two image versions do not match.
`Num Matches`	Number of times the running image version matched the flash image version after a reboot.
`Num Mismatches`	Number of times the running image version did not match the flash image version after a reboot. If the images do not match, the AP will upgrade to the flash image.
`Bad Checksums`	Number of bad checksum calculations due to an invalid or corrupted image file.

Column	Description
`Image Load Status`	Current status of the AP following an upgrade. **Done**: This status indicates that the controller reset after the upgrade was performed, or the upgrade was performed after the AP first registered with the controller. **Completed**: The AP was updated after it was registered to the controller, and after the controller's last reset. If AP shows a status of **completed**, it will also display the time it took it update that AP. **In progress:** The AP is currently updating its image.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap license-usage

```
show ap license-usage
```

Description

Show AP license usage information.

Examples

The output of the command below shows that controller has 82 remaining unused AP licenses.

```
(host) #show ap license-usage
Total AP Licenses                       : 128
AP Licenses Used                        : 3
Unused AP Licenses                      : 125
Licenses used for Campus AP's           : 3
Available Campus AP's                   : 29
Licenses used for Remote AP's           : 0
Available Remote AP's                   : 116
Total Ortronics AP Licenses             : 128
Ortronics AP Licenses Used              : 0
Total Indoor Mesh AP's Supported        : 128
Indoor Mesh AP's Active                 : 0
Total Outdoor Mesh AP's supported       : 128
Outdoor Mesh AP's Active                : 0
Total RF Protect Licenses               : 128
RF Protect Licenses Used                : 3
Total 802.11n-120abg Licenses   : 128
802.11n-120abg Licenses Used    : 0
Total 802.11n-121abg Licenses   : 128
802.11n-121abg Licenses Used    : 0
Total 802.11n-124abg Licenses   : 128
802.11n-124abg Licenses Used    : 0
Total 802.11n-125abg Licenses   : 128
802.11n-125abg Licenses Used    : 0
```

The output of this command includes the following information:

Parameter	Description
`Total AP Licenses`	Total number of AP licenses currently available on the controller.
`AP licenses used`	Number of AP licenses used by individual APs.
`Unused AP Licenses`	Number of AP licenses unused and currently available.
`Total RAP Licenses`	Total number of Remote AP (RAP) licenses currently available on the controller.
`RAP licenses used`	Number of RAP licenses currently used by Remote APs.
`Total Indoor Mesh AP Licenses`	Total number of Indoor Mesh AP (IMP) licenses currently available on the controller. The output of this command shows information for indoor mesh licenses, even though these licenses are not required in this version of ArubaOS.
`Indoor Mesh AP Licenses Used`	Number of IMP licenses currently used by Indoor Mesh APs. The output of this command shows information for indoor mesh licenses, even though these licenses are not required in this version of ArubaOS.
`Total Outdoor Mesh AP Licenses`	Total number of Outdoor Mesh AP (MAP) licenses currently available on the controller.
`Outdoor Mesh AP Licenses Used`	Number of MAP licenses currently used by Outdoor Mesh APs.

Parameter	Description
`Total 802.11n-120abg Licenses`	Total number of high-throughput (802.11n-capable) licenses available for 120abg APs.
`802.11n-120abg Licenses Used`	Number of high-throughput (802.11n-capable) licenses currently used by 120abg APs
`Total 802.11n-121abg Licenses`	Total number of high-throughput (802.11n-capable) licenses available for 121abg APs.
`802.11n-121abg Licenses Used`	Number of high-throughput (802.11n-capable) licenses currently used by 121abg APs
`Total 802.11n-124abg Licenses`	Total number of high-throughput (802.11n-capable) licenses available for 124abg APs.
`802.11n-124abg Licenses Used`	Number of high-throughput (802.11n-capable) licenses currently used by 124abg APs
`Total 802.11n-125abg Licenses`	Total number of high-throughput (802.11n-capable) licenses available for 125abg APs.
`802.11n-125abg Licenses Used`	Number of high-throughput (802.11n-capable) licenses currently used by 125abg APs

Command History

Release	Modification
ArubaOS 3.0	Command Introduced.
ArubaOS 3.3	The following parameters were introduced: • Total 802.11n-120abg Licenses • 802.11n-120abg Licenses Used • Total 802.11n-121abg Licenses • 802.11n-121abg Licenses Used • Total 802.11n-124abg Licenses • 802.11n-124abg Licenses Used • Total 802.11n-125abg Licenses • 802.11n-125abg Licenses Used

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system. The output of this command varies, according to the licenses currently installed on the controller.	Enable or Config mode on master controllers

show ap load-balancing

```
show ap load balancing
```

Description

Show the load-balancing information for each AP with load balancing enabled.

Examples

The output of the command in the example below shows details for a single AP enabled with the load-balancing feature.

```
(host) #show ap load-balancing
Load Balance Enabled Access Point Table
---------------------------------------
bss                  ess         name  s/p  ip          phy  chan  cur-cl  util(kbps)
---                  ---         ----  ---  --          ---  ----  ------  ----------
00:0b:86:cc:8e:4e  Wireless_1  mp22  2/24 10.3.148.12 a-HT 413   3       14
```

The output of this command includes the following information:

Column	Description
BSS	The Basic Service Set (BSS) Identifier for the AP. This is usually the APs MAC address.
ESS	The Extended Service Set (ESS) Identifier is the user-defined name of an 802.11 wireless network.
s/p	The controller slot and port used by the AP, in the format <slot>/<port>. The <slot> number is always 1. The **<port>** parameter refers to the network interfaces that are embedded in the front panel of the W-3000 Controller Series Multi-Service Controller. Port numbers start at 0, from the left-most position.
ip	IP address of the AP
phy	One of the following 802.11 types • a • a-HT (high-throughput) • g • g-HT (high-throughput)
chan	Channel number for the AP 802.11a/802.11n physical layer. The available channels depend on the AP's regulatory domain (country).
cur-cl	Current number of clients on the AP.
util (kbps)	Current bandwidth utilization, in kbps.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap mesh active

```
show ap mesh active [<mesh-cluster>|{page <page>}|{start <start>}]
```

Description

Show active mesh cluster APs currently registered on this controller.

Syntax

Parameter	Description
<mesh-cluster>	Name of a mesh cluster profile.
page <page>	Limit the output of this command to a specific number of entries by entering the number of entries you want to display.
start <start>	Start displaying the index of mesh APs at a chosen index number by entering the index number of the AP at which command output should start.

Examples

The output of this command displays a list of all active mesh points and mesh portals.

```
(host) #show ap mesh active
Mesh Cluster Name: meshprofile1
------------------------------
Name  Group   IP Address    BSSID             Band/Ch/EIRP/MaxEIRP  MTU   Enet 0/1      Mesh Role
----  -----   ----------    -----             --------------------  ---   --------      ---------
mp1   mp1     10.3.148.245  00:1a:1e:85:c0:30  802.11a/157/19/36           Off/Off       Point
mp2   mp2     10.3.148.250  00:1a:1e:88:11:f0  802.11a/157/19/36           Bridge/Bridge Point
mp3   mp3     10.3.148.253  00:1a:1e:88:01:f0  802.11a/157/19/36           Bridge/Bridge Point
mpp   mpp125  10.3.148.252  00:1a:1e:88:05:50  802.11a/157/19/36     1578  -/Bridge      Portal

Parent  #Children  AP Type  Uptime
 ------  ---------  -------  ------
 mp3     0          125      13d:2h:25m:19s
 mpp     1          125      14d:21h:23m:49s
 mp2     1          125      14d:21h:14m:55s
 -       1          125      14d:19h:5m:3s


------  ---------  -------  ------
```

The output of this command includes the following information:

Column	Description
Name	Name of an AP.
Group	AP group which includes the specified AP.
IP Address	IP address of the AP.
BSSID	Basic Service Set Identifier (BSSID) for the AP. This is usually the AP's MAC address.
Band/Ch/EIRP/MaxEIRP	The RF band in which the AP should operate (**a** or **g**)/ Radio channel used by the AP/Current effective Isotropic Radiated Power (EIRP) /maximum EIRP
MTU	Maximum Transmission Unit (MTU) size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.

Column	Description
`Enet 0/1`	Shows the current mode of each wired interface. • **Bridge**: 802.11 frames are bridged into the local Ethernet LAN. • **Tunnel**: 802.11 frames are tunneled to the controller using generic routing encapsulation (GRE). • **Split-tunnel**: 802.11 frames are either bridged into the local Ethernet LAN or tunneled to the controller, depending upon their destination. • **Off**: Interface is not available for serving clients. If an AP has only one wired interface, the output of this command will display a dash (-) for the unavailable port.
`Mesh Role`	An AP operating as a mesh node can have one of two roles: mesh portal or mesh point.
`Parent`	If the AP is operating as a mesh point, this parameter displays the name of its parent mesh portal. Mesh portals will display a dash (-).
`#Children`	If the AP is operating as a mesh portal, this parameter shows the number of mesh point children associated with that mesh portal.
`AP type`	The AP model type.
`Uptime`	Number of hours, minutes and seconds since the last controller reboot or bootstrap, in the format *hours:minutes:seconds*.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the secure enterprise mesh solution for outdoor APs require the Outdoor Mesh license.	Enable or Config mode on master controllers

show ap mesh debug counters

```
show ap mesh debug counters {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show counters statistics for a mesh node.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show counter statistics for an AP with a specific name.
`bssid <bssid>`	Show counter statistics for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	View counter statistics for an AP with a specific IP address. Enter the IP address of the AP in dotted-decimal format.

Example

The example below shows the Mesh Packet Counters table for an AP named meshpoint1. The **Probe Resp**, **Assoc Req**, and **Assoc Resp** data columns show both the total number of counters and, in parenthesis, the number of requests or responses with high-throughput information elements (HE IEs).

```
(host) #show ap mesh debug counters ap-name meshpoint1
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     68865      68755      24         8(8 HT)     3(1 HT)    3(1 HT)    1         1
-       -       0
Child      68913      67373      6          8           2          2          0         1
2       0       2618886

Received Packet Statistics: Total 2890717, Mgmt 2618946 (dropped non-mesh 0), Data 271771 (dropped
unassociated 1)HT: pns=8 ans=1 pnr=0 ars=0 arr=1 anr=0

Recovery Profile Usage Counters
-------------------------------
```

The output of this command includes the following information:

Column	Description
`Interface`	Indicates whether the mesh interface connects to a **Parent** AP or a **Child** AP. Each row of data in the *Mesh Packet Counters* table shows counter values for an individual interface.
`Echo Sent`	Number of echo packets sent.
`Echo Recv`	Number of echo packets received.
`Probe Req`	Number of probe request packets sent from the interface specified in the **Mesh-IF** parameter.
`Probe Resp`	Number of probe response packets sent to the interface specified in the **Interface** parameter.
`Assoc Req`	Number of association request packets from the interface specified in the **Interface** parameter.

Column	Description
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

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on master controllers.

show ap mesh debug current-cluster

```
show ap mesh debug current-cluster {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Display information for the mesh cluster currently used by a mesh point or mesh portal.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show mesh cluster data for an AP with a specific name.
`bssid <bssid>`	Show mesh cluster data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show mesh cluster data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

The output of the command below shows mesh cluster profile configuration parameters for the mesh cluster currently used by an AP named "mp2."

```
(host) #show ap mesh debug current-cluster ap-name mp2

AP "mp2" Current Cluster Profile: default
-----------------------------------------
Item            Value
----            -----
Cluster Name    smettu-mesh
RF Band         a
Encryption      opensystem
WPA Hexkey      N/A
WPA Passphrase  ********
```

The output of this command includes the following information:

Column	Description
`Cluster Name`	Name of the mesh cluster using this profile
`RF band`	The RF band in which the mesh point or mesh portal operates: • **g** = 2.4 GHz • **a** = 5 GHz
`Encryption`	Data encryption setting for the mesh cluster profile. • **opensystem**—No authentication and encryption. • **wpa2-psk-aes**—WPA2 with AES encryption using a preshared key.
`WPA Hexkey`	The WPA pre-shared key (only for mesh cluster profiles using WPA2 with AES encryption).
`WPA Passphrase`	The WPA password that generates the preshared key (only for mesh cluster profiles using WPA2 with AES encryption).

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on master controllers

show ap mesh debug forwarding-table

```
show ap mesh forwarding-table {ap-name <ap-name>}|{ip-addr <ip-addr>}
```

Description

Show the forwarding table for a remote mesh point or remote mesh portal.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for a remote mesh node with a specific name.
`ip-addr <ip-addr>`	Show data for a remote mesh node with a specific IP address by entering its IP address in dotted-decimal format.

Usage Guidelines

This is an internal technical support command. Dell technical support may request that you issue this command to help analyze and troubleshoot problems with your mesh network.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on master controllers

show ap mesh debug hostapd-log

```
show ap mesh debug hostapd-log {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show the debug log messages for the **hostapd** process.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Usage Guidelines

This is an internal technical support command. Dell technical support may request that you issue this command to help analyze and troubleshoot problems with the **hostapd** process or your mesh network.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on master controllers

show ap mesh debug meshd-log

```
show ap mesh debug meshd-log {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
[<page>]
```

Description

Show the debug log messages for the **meshd** process.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`<page>`	Display page number 0, 1 or 2, where page 0 has the newest information and page 2 has the oldest. If this parameter is omitted, this command will display all meshd log information, oldest first.

Usage Guidelines

This is an internal technical support command. Dell technical support may request that you issue this command to help analyze and troubleshoot problems with the **meshd** process or your mesh network.

Command History

Release	Modification
ArubaOS 3.0	Command introduced.
ArubaOS 3.4	The **page** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on master controllers

show ap mesh debug provisioned-clusters

```
show ap mesh debug provisioned-clusters {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show cluster profiles provisioned on a mesh portal or mesh point.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for a mesh node with a specific name.
`bssid <bssid>`	Show data for a mesh node with a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for a mesh node with a specific IP address by entering an IP address in dotted-decimal format.

Example

The output of the command below shows statistics for the AP's mesh cluster profile and recovery cluster profile.

```
(host) #show ap mesh debug provisioned-clusters ap-name portal2

AP Portal Cluster Profile: mesh-cluster-profile
-----------------------------------------------
------------------------
Parameter       Value
---------       -----
Cluster Name    sw-ad-GB32
RF Band         a
Encryption      opensystem
WPA Hexkey      N/A
WPA Passphrase  ********


AP "Portal" Cluster Profile: Recovery Cluster Profile
-----------------------------------------------------
Item            Value
----            -----
Cluster Name    Recovery-ZF-xAPl5z-g15VN
RF Band         a
Encryption      pa2-psk-aes
WPA Hexkey      ********
WPA Passphrase  N/A
```

The output of this command displays the following information for the AP's mesh cluster profile and recovery cluster profiles:

Column	Description
`Cluster Name`	Name of the mesh cluster using this profile
`RF band`	The RF band in which the AP should operate: • **g** = 2.4 GHz • **a** = 5 GHz

Column	Description
`Encryption`	Data encryption setting for the mesh cluster profile. • **opensystem**—No authentication and encryption. • **wpa2-psk-aes**—WPA2 with AES encryption using a preshared key.
`WPA Hexkey`	The WPA pre-shared key (only for mesh cluster profiles using WPA2 with AES encryption).
`WPA Passphrase`	The WPA password that generates the preshared key (only for mesh cluster profiles using WPA2 with AES encryption).

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on master controllers

show ap mesh neighbors

```
show ap mesh neighbors {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>} [names]
```

Description

Show all mesh neighbors for an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show mesh neighbors for an AP with a specific name.
`bssid <bssid>`	Show mesh neighbors for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show mesh neighbors for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`names`	If you include this optional parameter, the **Portal** column in the output of this command will translate the BSSIDs of mesh parent and child APs to AP names (where available).

Example

In the example below, the output has been split into two tables to better fit on the page. In the actual command-line interface, the output appears in a single, wide table. The **Flags** column the output of this command indicates the high-throughput (HT) properties of the mesh node. In the example below, the string "HT-40MHzsgi-2ss" indicates that the node uses a 40MHz channel with a short guard interval (sgi) and sends 2 spatial streams (ss).

```
(host) #show ap mesh neighbors ap-name portal

Neighbor list
-------------
MAC                Portal             Channel  Age  Hops  Cost   Relation      Flags  RSSI  Rate Tx/Rx
---                ------             -------  ---  ----  ----   --------      -----  ----  ----------
00:0b:86:e8:09:d1  00:1a:1e:88:01:f0  157      0    1     11.00  C 3h:15m:42s  -      65    54/54
00:1a:1e:88:02:91  00:1a:1e:88:01:f0  157      0    1     4.00   C 3h:35m:30s  HL     59    300/300
00:0b:86:9b:27:78  Yes                157      0    0     12.00  N 3h:22m:46s  -      26    -
00:0b:86:e8:09:d0  00:1a:1e:88:01:f0  157      0    1     11.00  N 3h:15m:36s  -      65    -
00:1a:1e:88:02:90  00:1a:1e:88:01:f0  157+     0    1     2.00   N 3h:35m:6s   HL     59    -

A-Req  A-Resp  A-Fail  HT-Details       Cluster ID
-----  ------  ------  ----------       ----------
1      1       0       Unsupported      sw-ad-GB32
1      1       0       HT-40MHzsgi-2ss  sw-ad-GB322
0      0       0       Unsupported      mc1
0      0       0       Unsupported      sw-ad-GB32
0      0       0       HT-40MHzsgi-2ss  sw-ad-GB32

Total count: 5, Children: 2
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
```

The output of this command includes the following information:

Column	Description
MAC	MAC address of the mesh node.

Column	Description
Portal	By default, this column displays the BSSID of the mesh point. If you include the optional **names** parameter, this column will display AP names, if available. The AP names will include **[p]** (parent), or **[c]** (child) suffixes to indicate the role of the mesh BSSID.
Channel	Number of a radio channel used by the AP.
Age	Number of seconds elapsed since the AP heard from the neighbor.
Hops	Indicates the number of hops it takes traffic from the mesh node to get to the mesh portal. The mesh portal advertises a hop count of 0, while all other mesh nodes advertise a cumulative count based on the parent mesh node
Cost	A relative measure of the quality of the path from the AP to the controller. A lower number indicates a better quality path, where a higher number indicates a less favorable path (e.g, a path which may be longer or more congested than a path with a lower value.) For a mesh point, the path cost is the sum of the (parent path cost) + (the parent node cost) + (the link cost).
Relation	Shows the relationship between the specified AP and the AP on the neighbor list and the amount of time that relationship has existed. • **P** = Parent • **C** = Child • **N** = Neighbor • **B** = Blacklisted-neighbor
Flags	This parameter shows additional information about the mesh neighbor. The key describing each flag appears 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	Name of the Mesh cluster that includes the specified AP or BSSID.

Command History

Version	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4.1	The names **parameter** was introduced. The output of this command was also modified to include the **Rate Tx/Rx** column.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on master controllers

show ap mesh tech-support

```
show ap mesh tech-support ap-name <ap-name> <filename>
```

Description

Display all information for an AP, and save that information in a file on the controller

Syntax

Parameter	Description
`<ap-name>`	Name of an AP for which you want to create a report
`<filename>`	Filename for the report created by this command. The file can only be saved in the flash directory. If desired, you can use FTP or TFTP to copy the file to another destination.

Usage Guidelines

This command displays the output of the multiple mesh and debug CLI commands, then saves that data into a report file on the controller's flash drive, where it can be analyzed for debugging purposes. The information in this report includes the output of the following commands:

- show ap mesh neighbors
- show ap mesh debug current-cluster
- show ap mesh debug provisioned-clusters
- show ap mesh debug counters
- show ap mesh debug forwarding-table
- show ap mesh debug meshd-log
- show ap mesh debug hostapd-log

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Config mode on master controllers

show ap mesh topology

```
show ap mesh topology [long] [page <page>] [start <start>]
```

Description

Show the mesh topology tree.

Syntax

Parameter	Description
`long`	Include the names of a mesh portal's children in the output of this command
`page <page>`	Limit the output of this command to a specific number of entries by entering the number of entries you want to display.
`start <start>`	Start displaying the mesh topology tree at a chosen index number by entering the index number of the AP at which command output should start.

Example

An **(N)** in the **Mesh Role** column indicates the node is 11N capable. An **(N)** beside the parent name in the **Parent** column indicates that the mesh node's the parent is also 11N capable.

```
(host) #show ap mesh topology

Mesh Cluster Name: sw-ad-GB32
-----------------------------
Name Mesh Role   Parent  Path Cost  Node Cost  Link Cost  Hop Count  RSSI  Rate Tx/Rx  Last Update  Uplink Age  #Children
---- ---------   ------  ---------  ---------  ---------  ---------  ----  ----------  -----------  ----------  ---------
ad-ap Point (N)   mp3     2          0          0          1          61    300/270     6m:12s       3h:8m:7s    0
msc-1 Point       mp3     2          0          0          1          64    54/54       6m:36s       2h:48m:12s  0

Total APs :2
(R): Recovery AP. (N): 11N Enabled. For Portals 'Uplink Age' equals uptime.
```

The output of this command includes the following information:

Column	Description
`Name`	Name of the mesh node.
`Mesh Role`	An AP operating as a mesh node can have one of two roles: mesh portal or mesh point.
`Parent`	If the AP is operating as a mesh point, this parameter displays the name of its parent mesh portal.
`Path Cost`	A relative measure of the quality of the path from the AP to the controller. A lower number indicates a better quality path, where a higher number indicates a less favorable path (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).
`Node Cost`	A relative measure of the quality of the node, where a lower number of is more favorable than a higher number. This cost is related to the number of children on the specified node.
`Link Cost`	A relative measure of the quality of the link. For example, a more congested link will have a higher link cost than a similar, less-congested link.
`Hop Count`	Number of hops to the mesh portal.

Column	Description
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 mesh point transmits and receives at on its uplink. Note that the rate information is only as current as indicated in the **Last Update** column.
Last Update	Time elapsed since the mesh node last updated its statistics.
Uplink Age	Time elapsed since the mesh node became active in the mesh topology.
#Children	Number of children associated with a parent mesh point.

Command History

Version	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4.1	The output of this command was also modified to include the **Rate Tx/Rx** column.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on master controllers

show ap mesh-cluster-profile

```
show ap mesh-cluster-profile [<profile>]
```

Description

Show configuration settings for a mesh cluster profile.

Syntax

Parameter	Description
`<profile>`	Name of a mesh cluster profile

Usage Guidelines

The command **show ap mesh-cluster-profile** displays a list of all mesh cluster profiles configured on the controller, including the number of references to each profile and each profile's status. Include the optional <profile> parameter to show detailed settings for an individual mesh cluster profile.

Examples

The example below shows the configuration settings for the mesh cluster profile "meshcluster2".

```
(host) #show ap mesh-cluster-profile meshcluster2

Mesh Cluster profile "meshcluster2"
-----------------------------
Parameter       Value
---------       -----
Cluster Name    company-mesh
RF Band         a
Encryption      opensystem
WPA Hexkey      N/A
WPA Passphrase  N/A
```

The output of this command includes the following information:

Parameter	Description
`Cluster Name`	Name of the mesh cluster using this profile
`RF band`	The RF band in which the AP should operate: • **g** = 2.4 GHz • **a** = 5 GHz
`Encryption`	Data encryption setting for the mesh cluster profile. • **opensystem**—No authentication and encryption. • **wpa2-psk-aes**—WPA2 with AES encryption using a preshared key.
`WPA Hexkey`	The WPA pre-shared key (only for mesh cluster profiles using WPA2 with AES encryption).
`WPA Passphrase`	The WPA password that generates the preshared key (only for mesh cluster profiles using WPA2 with AES encryption).

Command History

Introduced in ArubaOS 3.2.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on master controllers

show ap mesh-ht-ssid-profile

```
show ap mesh-ht-ssid-profile [<profile>]
```

Description

Show configuration settings for a mesh high-throughput Service Set Identifier (SSID) profile.

Syntax

Parameter	Description
`<profile>`	Name of a mesh high-throughput SSID profile.

Usage Guidelines

High-throughput APs support additional settings not available in legacy APs. A mesh high-throughput SSID profile can enable or disable high-throughput (802.11n) features and 40 Mhz channel usage, and define values for aggregated MAC protocol data units (MDPUs) and Modulation and Coding Scheme (MCS) ranges.

The command **show ap mesh-ht-ssid-profile** displays a list of all mesh high-throughput SSID profiles configured on the controller, including the number of references to each profile and each profile's status. Include the optional **<profile>** parameter to show detailed settings for an individual mesh high-throughput SSID profile.

Examples

The example below shows the configuration settings for the mesh high-throughput radio profile "default".

```
(host) #show ap mesh-ht-ssid-profile default

Mesh High-throughput SSID profile "default"
-------------------------------------------
Parameter                           Value
---------                           -----
High throughput enable (SSID)       Enabled
40 MHz channel usage                Enabled
MPDU Aggregation                    Enabled
Max transmitted A-MPDU size         65535 bytes
Max received A-MPDU size            65535 bytes
Min MPDU start spacing              0 usec
Supported MCS set                   1-14
Short guard interval in 40 MHz mode Enabled
Legacy stations                     Allowed
Allow weak encryption               Disabled
```

The output of this command includes the following information:

Column	Description
`High throughput enable (SSID)`	Shows if 802.11n high-throughput features are enabled or disabled for this profile. By default, high-throughput features are enabled.
`40 MHz channel usage`	This parameter shows if the profile enables or disables the use of 40 MHz channels.
`MPDU Aggregation`	This parameter shows if the profile enables or disables MAC protocol data unit (MPDU) aggregation. High-throughput mesh APs are able to send aggregated MAC protocol data units (MDPUs), which allow an AP to receive a single block acknowledgment instead of multiple ACK signals. This option, which is enabled by default, reduces network traffic overhead by effectively eliminating the need to initiate a new transfer for every MPDU.

Column	Description
`Max transmitted A-MPDU size`	Maximum size of a transmitted aggregate MPDU, in bytes.
`Max received A-MPDU size`	Maximum size of a received aggregate MPDU, in bytes.
`Min MPDU start spacing`	Minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds.
`Supported MCS set`	A list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20MHz vs. 40MHz) and the number of spatial streams used by the mesh node.
`Short guard interval in 40 MHz mode`	This parameter shows if the profile enables or disables use of short (400ns) guard interval in 40 MHz mode. A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data.
`Legacy stations`	This parameter shows if the profile allows or disallows associations from legacy (non-HT) stations.
`Allow weak encryption`	Using TKIP or WEP encryption for unicast traffic forces legacy transmission rates on high-throughput APs. This option is disabled by default, preventing clients using TKIP or WEP for unicast traffic from associating with the mesh node.

Command History

Introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap mesh-radio-profile

```
show ap mesh-radio-profile [<profile>]
```

Description

Show configuration settings for a mesh radio profile.

Syntax

Parameter	Description
`<profile>`	Name of a mesh radio profile.

Usage Guidelines

The radio profile determines the radio frequency/channel used only by mesh nodes to establish mesh links. Mesh nodes operating in different cluster profiles can share the same radio profile. Conversely, mesh portals using the same cluster profile can be assigned different mesh radio profiles to achieve frequency separation.

The command **show ap mesh-radio-profile** displays a list of all mesh radio profiles configured on the controller, including the number of references to each profile and each profile's status. Include the optional <*profile*> parameter to show detailed settings for an individual mesh radio profile.

Example

The example below shows the configuration settings for the mesh cluster profile "default".

```
(host) #show ap mesh-radio-profile default
Mesh Radio profile "default"
----------------------------
Parameter                          Value
---------                          -----
Maximum Children                   6
Maximum Hop Count                  5
Heartbeat threshold                10
Link Threshold                     12
Reselection mode                   reselect-anytime
Metric algorithm                   distributed-tree-rssi
Retry Limit                        4
RTS Threshold                      2333 bytes
802.11a Transmit Rates             6 9 12 18 24 36 48 54
802.11g Transmit Rates             1 2 5 6 9 11 12 18 24 36 48 54
Mesh Private Vlan                  0
Allowed VLANs on mesh link         1
BC/MC Rate Optimization            Enabled
Mesh High-throughput SSID Profile  default
```

The output of this command includes the following information:

Parameter	Description
`Maximum Children`	The maximum number of children a mesh portal can accept.
`Maximum Hop Count`	The maximum number of hops allowed between a mesh point and a mesh portal.
`Heartbeat Threshold`	Indicates the maximum number of heartbeat messages that can be lost between neighboring mesh nodes before the mesh node is considered inactive and is dropped as a mesh neighbor.
`Link Threshold`	Indicates the threshold for the lowest acceptable Receive Signal Strength Indicator (RSSI) value. Links that drop below this threshold will have an increased link cost. Default: 12.

Parameter	Description
Reselection Mode	Specifies the one of the following methods used to find a better mesh link. • **startup-sub-threshold**: When bringing up the mesh network, mesh nodes have 3 minutes to find a better uplink. After that time, each mesh node evaluates alternative links only if the existing uplink falls below the configured threshold level (the link becomes a sub-threshold link). The reselection process is canceled if the average RSSI rises on the existing uplink rises above the configured link threshold. • **reselect-any-time:** Connected mesh nodes evaluate alternative mesh links every 30 seconds. If a mesh node finds a better uplink, the mesh node connects to the new parent to create an improved path to the mesh portal. • **reselect-never**: Connected mesh nodes do not evaluate other mesh links to create an improved path to the mesh portal. • **subthreshold-only**: Connected mesh nodes evaluate alternative links only if the existing uplink becomes a sub-threshold link.
Metric algorithm	Algorithm used by a mesh node to select its parent.
Retry Limit	Maximum number of times a mesh node can re-send a packet.
RTS Threshold	The packet size sent by mesh nodes. Mesh nodes transmitting frames larger than this threshold must issue request to send (RTS) and wait for other mesh nodes to respond with clear to send (CTS) to begin transmission. This helps prevent mid-air collisions.
802.11a Transmit Rates	Indicates the transmit rates for the 802.11a radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.
802.11g Transmit Rates	Indicates the transmit rates for the 802.11g radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.
Mesh Private Vlan	A VLAN ID for control traffic between an RMP and mesh nodes.
BC/MC Rate Optimization	If enabled, the mesh node will use the slowest associated mesh-point rate for broadcast/ multicast data (rather than minimum).
Mesh High-throughput SSID Profile	The High-throughput SSID Profile associated with this mesh radio profile.

Command History

Release	Modification
ArubaOS 3.2	Command Introduced.
ArubaOS 3.4	The **802.11g Portal channel** and **802.11a Portal channe**l parameters were deprecated, and the **Mesh High-throughput SSID Profile** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap monitor

```
show ap monitor active-laser-beams|ap-list|channel|client-list|ids-state|mesh-list|pot-ap-list|pot-client-list|routers|wired-mac {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>} {ap-bssid <ap-bssid>}|{enet-mac <enet-mac>}
```

Description

Show information for Dell Air Monitors.

Syntax

Parameter	Description
`active-laser-beams`	Show active laser beam generators. The output of this command shows a list of all APs that are actively performing policy enforcement containment such as rogue containment. This command can tell us which AP is sending out deauthorization frames, although it does not specify which AP is being contained.
`ap-list`	Show list of APs being monitored.
`arp-cache`	Show ARP Cache of learned IP to MAC binding
`channel`	Show state and stats of a specific channel.
`client-list`	Show list of client being monitored.
`ids-state`	Show IDS State.
`mesh-list`	Show list of Mesh APs being monitored.
`pot-ap-list`	Display the Potential AP table. The Potential AP table shows the following data: • **bssid**: the AP's Basic Service Set Identifier. • **channel**: The AP's current radio channel • **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 controller first recognized the AP. • **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-client-list`	Display 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 controller first recognized the client. • it: Client Idle time, expressed as a number of timer ticks.
`routers`	Show Router MAC Addresses learned. The output of this command includes the router's MAC address, IP address and uptime.
`wired-mac`	Show Wired MAC Addresses learned.
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`ap-bssid <ap-bssid>`	Include the optional **ap-bssid <ap-bssid>** parameters to show how the AP is monitoring information for another AP with a specific BSSID.
`enet-mac <enet-mac>`	Include the optional e**net-mac <enet-mac>** parameters to show how the AP is monitoring information for an interface with a specific ethernet MAC address.

Examples

The output of the command displays the Monitored AP Table, which lists all the APs monitored by a specified AP or BSSID.

```
(host) #show ap monitor ap-list  ap-name al12

Monitored AP Table
------------------
bssid              essid               chan  ap-type  phy-type        dos      mt      it  load-balance
-----              -----               ----  -------  --------        ---      --      --  ------------
00:1a:1e:11:5f:02  ethersphere-vocera  6     valid    80211b/g-HT-20  disable  787272  0   disable
00:1a:1e:11:5f:00  guest               6     valid    80211b/g-HT-20  disable  787272  0   disable
00:1a:1e:11:5f:11  ethersphere-wpa2    48    valid    80211a-HT-40    disable  786835  0   disable
00:1a:1e:11:5f:10  guest               48    valid    80211a-HT-40    disable  786835  0   disable
00:1a:1e:11:5f:01  ethersphere-voip    6     valid    80211b/g-HT-20  disable  787272  0   disable
00:1a:1e:11:6e:70  guest               48    valid    80211a-HT-40    disable  18543   0   disable
00:1a:1e:11:6e:71  ethersphere-wpa2    48    valid    80211a-HT-40    disable  18543   0   disable
00:1a:1e:88:90:42  employee4a          6     unknown  80211b/g        disable  3160    0   disable
00:1a:1e:88:90:41  guest4              6     unknown  80211b/g-HT-20  disable  3160    0   disable
00:1a:1e:88:90:40  employee4           6     unknown  80211b/g-HT-20  disable  3159    0   disable
00:1a:1e:8e:73:e1  guest10             6     unknown  80211b/g-HT-20  disable  941     0   disable
00:1a:1e:8e:73:e0  emplyee10           6     unknown  80211b/g-HT-20  disable  910     0   disable
00:1a:1e:8e:73:f0  emplyee10           48    unknown  80211a-HT-40    disable  252     0   disable
00:1a:1e:8e:73:f1  guest10             48    unknown  80211a-HT-40    disable  252     0   disable
00:1a:1e:8d:5b:30  guest               48    valid    80211a-HT-40    disable  189     0   disable
00:1a:1e:8d:5b:31  ethersphere-wpa2    48    valid    80211a-HT-40    disable  189     0   disable
00:1a:1e:85:89:20  employee8           11    unknown  80211b/g-HT-20  disable  9       9   disable
00:1a:1e:85:89:21  guest8              11    unknown  80211b/g-HT-20  disable  9       9   disable
00:1a:1e:88:dd:60  employee2           11    unknown  80211b/g-HT-20  disable  9       9   disable
0                                                 repeat
Length:19
Total:19
```

The output of this command includes the following information:

Column	Description
bssid	Basic Service Set Identifier for an AP. This is usually the AP's MAC address.
essid	Extended service set identifier that names a wireless network.
chan	Radio channel used by the BSSID
phy-type	Radio phy type. Possible types include: • 802.11a • 802.11a-HT-40 • 802.11b/g • 802.11b/g-HT-20
dos	Shows if the feature to contain DoS attacks has been enabled or disabled.
mt	Monitor time; the number of elapsed timer ticks since the AP first recognized the monitored AP.
it	AP idle time, the number of timer-ticks since the AP last saw any frames from the monitored AP.
load-balance	Shows if the load-balancing feature has been enabled on the AP.

Command History

Version	Modification
ArubaOS 3.0.	Command introduced

Version	Modification
ArubaOS 3.4.	The **ap-bssid** and **enet-mac** parameters were added to the **show ap monitor wired-mac** command.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap monitor association

```
show ap monitor association {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
<ap-bssid>
```

Description

Show the association table for an Air Monitor (AM).

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AM with a specific name.
`bssid <bssid>`	Show data for an AM with a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AM's MAC address.
`ip-addr <ip-addr>`	Show data for an AM with a specific IP address by entering its IP address in dotted-decimal format.
`<ap-bssid>`	BSSID of an AP.

Examples

The output of the command lists the MAC addresses associated with the Air Monitor BSSID.

```
(host) #show ap monitor association ap-name ap9 00:1a:1e:11:74:a1
Association Table
-----------------
mac               rsta-type  auth  phy-type
---               ---------  ----  --------
00:1d:d9:01:c4:50  valid      yes   80211a
00:17:f2:4d:01:e2  valid      yes   80211a
00:1f:3b:8c:28:89  valid      yes   80211a
00:1d:d9:05:05:d0  valid      yes   80211a
00:14:a4:25:72:6d  valid      yes   80211a
00:19:7d:d6:74:8d  valid      yes   80211a
```

The output of this command includes the following information:

Column	Description
`mac`	MAC address associated with the Air Monitor BSSID
`rsta-type`	Rogue station type: • **interfering**: Interfering station. • **valid**: Station is not a rogue station. • **DoS**: Station may have attempted a DoS attack.
`auth`	Displays a **yes** if the client has been authenticated.
`phy-type`	The RF band in which the AP should operate: **802.11g** = 2.4 GHz **802.11a** = 5 GHz

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap monitor debug

```
show ap monitor debug counters|status {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}

show ap monitor debug profile-config {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>} ap-radio|ap-system|arm|event-thresholds|ids-dos|ids-general|ids-impersonation|ids-signature-matching|ids-unauthorized-device|interference|regulatory-domain|rf-behavior
```

Description

Show information for an Air Monitor's current status, message counters, or profile settings.

Syntax

Parameter	Description
`counters`	Show Air Monitor (AM) message counters.
`status`	Show the status of an Air Monitor.
`ap-name <ap-name>`	Show data for an AM with a specific name.
`bssid <bssid>`	Show data for an AM with a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AM with a specific IP address by entering its IP address in dotted-decimal format.
`profile-config`	Show an Air Monitor profile configuration.
`ap-radio`	Show the Air Monitor radio configuration parameters, as defined in the AM's 802.11a, 802.11b, or high-throughput radio profiles.
`ap-system`	Show an Air Monitor's system configuration settings, as defined in it's AP System profile.
`arm`	Show an Air Monitor's Adaptive Radio Management (ARM) settings, as defined in its current ARM profile
`event-thresholds`	Show an Air Monitor Event Thresholds settings, as defined in its current RF Event Thresholds profile
`ids-dos`	Show an Air Monitor IDS DoS settings, as defined in its current IDS DoS profile.
`ids-general`	Show an Air Monitor IDS General Configuration settings, as defined in its IDS General profile.
`ids-impersonation`	Show an Air Monitor IDS Impersonation Configuration settings, as defined in its IDS Impersonation profile.
`ids-signature-matching`	Show an Air Monitor IDS Signature Matching configuration settings, as defined in its IDS Signature Matching profile
`ids-unauthorized-device`	Show an Air Monitor IDS Unauthorized Device configuration settings, as defined in its IDS Unauthorized Device profile.
`interference`	Show an Air Monitor's interference configuration settings, as defined in its current RF Optimization profile.
`regulatory-domain`	Show an Air Monitor's Regulatory Domain configuration settings, as defined in its Regulatory Domain profile.
`rf-behavior`	Show an Air Monitor RF Behavior Configuration

Examples

The output of the following command includes the *WLAN Interface*, *Data Structures*, *WLAN Interface Switch Status* and *RTLS Configuration* tables for the specified AP.

```
(host) #show ap monitor debug status ap-name ap12
WLAN Interface
--------------
bssid              scan    monitor  probe-type  phy-type        task   channel  pkts
-----              ----    -------  ----------  --------        ----   -------  ----
00:1a:1e:11:5f:10  enable  enable   sap         80211a-HT-40    tuned  153      496970814
00:1a:1e:11:5f:00  enable  enable   sap         80211b/g-HT-20  tuned  6        391278179

Wired Interface
---------------
mac                ip              gw-ip           gw-mac             status  pkts    macs gw-macs
tagged-pkts vlan
---                --              -----           ------             ------  ----    ---- -------
----------- ----
00:1a:1e:c9:15:f0  192.0.2.32.200  192.0.2.32.254  00:0b:86:08:e1:00  enable  101960  2    3
1  03           2
Global Counters
---------------
key                    value
---                    -----
Packets Read           888248993
Bytes Read             2819670134
Num Interrupts         681037971
Num Buffer Overflows   591393
Max PPS                16239
Cur PPS                1130
Max PPI                20
Cur PPI                2
Uptime                 3323085
AP Name                AL12
LMS IP                 192.0.2.250
Master IP              192.0.2.253
AP Type                125
Country Code           2

Data Structures
---------------
ap  sta  pap  psta  ch  msg-hash  ap-l
--  ---  ---  ----  --  --------  ----
20  40   17   55    24  21        20

Other Parameters
----------------
key                    value
---                    -----
WMS on Master          disabled
Stats Update Interval  60
Poll Interval          174000
Num Switches           1
Collect Stats          enabled

WLAN Interface Switch Status
----------------------------
Bssid              Type   Status  Last-reg  N-reg  Last-update  Next-update  N-updates  Last-ack
-----              ----   ------  --------  -----  -----------  -----------  ---------  --------
00:1a:1e:11:5f:10  local  up      3321891   3821   3322965      197          10368      3322965
00:1a:1e:11:5f:00  local  up      3321891   3821   3322917      187          10378      3322965
```

The output of this command includes the following information:

Column	Description
bssid	The Basic Service Set Identifier (BSSID) for the AP. This is usually the AP's MAC address.
scan	Indicates whether or not if active scanning is enabled on this AP.
monitor	Indicates whether the AP radio is currently enabled or disabled.
probe-type	This parameter displays one of the following options to show the AP is configured. • **sap**: Default AP setting. • **am**: AP is configured as an Air Monitor. • **m-portal**: AP is configured as a Mesh portal. • **m-point**: AP is configured as a Mesh point.
task	This parameter displays one of the following options to show the radio's current task: • **scan**: AP is scanning other channels. • **tuned**: AP is tuned on one channel. • **locate**: AP has been asked to locate a specific AP or client. • **pcap**: The AP is enabled with the Packet Capture feature.
channel	The radio channel currently used by an AP's WLAN interface.
pkts	Number of packets seen on the interface.
mac	MAC address for the AP's wired interface.
ip	The AP's IP address.
gw-ip	IP address for the AP's gateway.
gw-mac	MAC address for the AP's gateway.
status	Shows if the interface is currently enabled or disabled.
pkts	Number of packets seen on the AP's wired interface.
macs	Number of MAC addresses in the Wired MAC table for that interface.
gw-macs	Number of MAC addresses in the Wired MAC table for that interface.
tagged-pkts	Number VLAN-tagged packets sent to that interface.
vlan	The VLAN ID for the packets sent to that interface.
Packets read	Number of packets read by the AP since it was last reset.
Bytes read	Number of bytes read by the AP since it was last reset.
Num Intercepts	Number of interrupts from the AP's driver.
Num Buffer Overflows	Number of times excessive traffic has filled the AP's buffers.
Max PPS	Maximum throughput rate seen on the interface, in packets per second.
Cur PPS	Current throughput rate seen on the interface, in packets per second.
Max PPI	Maximum interrupt rate seen on the interface, in interrupts per second.
Cur PPI	Current interrupt rate seen on the interface, in interrupts per second.
Uptime	Number of seconds since the AP was last reset.
LMS IP	IP address of the AP's local controller.
Master IP	IP address of the AP's master controller.
AP type	AP model type.

Column	Description
Country Code	The AP's country code. Valid radio channels for your wireless network are based on your country code. If you change the AP's country code, the valid channels will be reset to the defaults for the new country.
ap	Number of other APs monitored by this AP.
sta	Number of clients and APs seen by this AP.
pap	Number of potential APs; APs which have transmitted a beacon, but have not yet been registered.
psta	Number of potential stations; AP has seen a MAC address from the station but hasn't yet received traffic from it.
ch	Number of channel entries in the channel table.
msg-hash	Number of different message types seen on the interface.
ap-l	(For internal use only)
WMS on Master	Indicates if the AP communicates to the wms process on a master or local controller. **enabled**: Communicates with a master controller. **disabled**: Communicates with a local controller only.
Stats Update Interval	If the AP is collecting statistics, this value is the interval in seconds in which the AP sends statistics to the WMS process on a controller.
Poll Interval	Interval, in milliseconds, that the AP sends RSSI updates to the WMS process on a controller.
Num Switches	Number of controllers to which this AP has access. If the value is 1, the AP has access to a master *or* a local controller. If the value is 2, the AP has access to a master *and* a local controller.
Collect Stats	If enabled, the AP will collect statistics to send the WMS process on its controller.
Bssid	BSSID of the radio.
Type	Indicates whether the controller type is **master** or **local**.
Status	If **up**, the AP can reach the controller. If **down**, the AP cannot reach the controller.
Last-reg	The time the AP last registered with the WMS process.
N-reg	Number of times the AP has registered with the WMS process.
Last-update	The last timer tick time the AP updated the WMS process.
Next-update	Interval between the last update and the next scheduled update.
N-updates	Number of updates sent to the WMS process.
Last-ack	Number of timer ticks since the AP received an acknowledgement from the WMS process.
Type	Type of RTLS server used by the AP, such as MMS or Aeroscout.
Server IP	IP address of the RTLS server.
Port	Port used by the RTLS server.
Frequency	Rate, in seconds, at which RTLS messages are sent to the server.
Active	Indicates if the server is active on the AP.

Command History

Version	Modification
ArubaOS 3.0.	Command introduced
ArubaOS 3.4.	The **tagged-pkts** and **vlan** parameters were added to the Wired Interface table in the output of the **show ap monitor debug status** command.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap monitor stats

```
show ap monitor stats advanced {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
client-mac <client-mac>

show ap monitor stats {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>} mac <mac>
```

Description

Show packet, signal and channel statistics for an AP or a client.

Syntax

Parameter	Description
`advanced`	Show advanced statistics for an AP or client.
`ap-name <ap-name>`	Show statistics for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`mac <mac>`	Show data for a specific MAC address by entering the MAC address of a client or AP.
`client-mac <client-mac>`	Show data for a specific client MAC address by entering the MAC address of a client.

Example

The output of the following command shows monitoring statistics for the AP al12, and a client with the MAC address 00:03:2a:02:6a:d7.

```
(host) #show ap monitor stats ap-name al12 mac 00:03:2a:02:6a:d7

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)
----------  ----------  -----------  -----  --------------
51          51          51           4      50
Monitored Time:6626
Last Packet Time:585500
Uptime:585502

DoS Frames
----------
tx  old-tx  rx  old-rx
--  ------  --  ------
0   0       0   0
Interference Baseline
---------------------
FRR  FRER
---  ----
17   4
Handoff Assist
--------------
rssi-index  cur-signal  old-cur-signal
----------  ----------  --------------
0           51          0
High Throughput Parameters
--------------------------
ht-type  primary-channel  sec-channel  gf-supported  40mhz-intolerance
-------  ---------------  -----------  ------------  -----------------
none     0                0            0             0
```

The output of this command includes the following information:

Column	Description
retry	Percent of 802.11 retry frames sent because a client failed to send an ACK.
Low-speed	Percent of frames sent at a data rate of 18 Mbps or slower.
non-unicast	Percent of non-unicast frames
recev-error	Percent of error frames of all frames seen in the last second.
frag	Rate of fragmented packets, in frames per second
bwth	Current bandwidth, in bps.
avg-signal	Average signal-to-noise ratio over the interval since the AP's last reset.
Low-signal	Lowest signal-to-noise ratio over the interval since the AP's last reset.
high-signal	Highest signal-to-noise ratio over the interval since the AP's last reset.
count	Number of packets seen on the AP over the interval since the AP's last reset.
Duration	Time over which the AP has measured RSSI values.
tx	The total number of deauthorization frames sent to this MAC address for containment in the interval from the AP's last reset until the current timer tick.
old-tx	The total number of deauthorization frames sent to this MAC address for containment until the previous timer tick.
rx	The total number of deauthorization frames spoofing the MAC address in the interval from the AP's last reset until the current timer tick.
old-rx	The total number of deauthorization frames sent to this MAC address for containment until the previous timer tick.
FRR	Frame retry rate, in frames per second.
FRER	Frame error retry rate, in frames per second.
rssi-index	This value indicates the number of consecutive timer ticks over which the value of the Receive Signal Strength Indicator (RSSI) of the client has reduced by more than 3 units. **NOTE:** This value is updated only if 'handoff-assist' is enabled in the AP's RF Optimization profile.
cur-signal	The Receive Signal Strength Indicator (RSSI) of the most recent frame received from the specified MAC address.
old-cur-signal	The most recent Receive Signal Strength Indicator (RSSI) of the MAC which is 3 lower or 5 higher than the current RSSI. **NOTE:** This value is updated only if 'handoff-assist' is enabled in the AP's RF Optimization profile
ht-type	This parameter indicates support for the following HT types: **no**: No support for high-throughput. **HT-20**: Support for 20 Mhz high-throughput only. **HT-40**: Support for 40 Mhz high-throughput.
primary-channel	Primary radio channel.
sec-channel	Secondary radio channel
gf-supported	If **1**, this AP supports greenfield mode. If **0**, greenfield is not supported.
40mhz-intolerance	Indicates whether the specified MAC address is 40 Mhz intolerant.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap pcap status

```
show ap pcap status {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show the status of outstanding packet capture (pcap) sessions.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.

Usage Guidelines

The Packet Capture (pcap) feature copies control path packets from the Dell Control Processor, providing visibility for packets to or from the controller.This provides a useful troubleshooting tool for diagnosing communication problems with elements such as a Radius server. You can retrieve these packets by issuing the command **tar logs**, and then viewing the file filter.pcap on the controller's flash drive.

Example

The example below shows the Packet Capture Sessions table for an AP named AP16.

```
(host) #show ap pcap status ap-name AP16
  Packet Capture Sessions
  -----------------------
  pcap-id  filter  type  intf              channel max-pkt-size  num-pkts  status       url  target
  -------  ------  ----  ----              ------- ------------  --------  ------       ---  ------
  1                raw   00:1a:1e:82:ab:b0  161                          in-progress
  10.3.9.225/5555
```

The output of this command includes the following information:

Column	Description
`pcap-id`	ID number of the packet capture session.
`filter`	Packet Capture filter specification.
`type`	A **raw** packet capture type indicates that the controller is streaming raw packets to an external viewer.
`intf`	BSSID of the interface for the PCAP session.
`channel`	Channel used by AP to capture packets.
`max-pkt-size`	Maximum size of all captured packets.
`num-pkts`	Number of packets captured during the session.
`status`	Shows the current status of the packet-capture session.
`url`	Packet capture data can be downloaded to this URL
`target`	IP address of the client station running Wildpacket's AiroPeek monitoring application

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap profile-usage

```
show ap profile-usage {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show a complete list of all profiles referenced by an individual AP or an AP BSSID.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.

Usage Guidelines

Use this command to monitor the configuration profiles in use by an AP or a specific BSSID. The output of this command shows the name of each profile type that is associated with the AP or BSSID, as well as the source that associates the profile with the AP.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap provisioning

```
show ap provisioning {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show provisioning parameters currently used by an AP

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address.

Example

The output of this command shows that the AP named **AP8** has mostly default parameters. These appear with the value N/A.

```
(host) #show ap provisioning ap-name AP8
   AP "mp2" Provisioning Parameters
   --------------------------------
   Item                            Value
   ----                            -----
   AP Name                         mp2
   AP Group                        mpp1
   Location name                   N/A
   SNMP sysLocation                N/A
   Master                          N/A
   Gateway                         N/A
   Netmask                         N/A
   IP Addr                         N/A
   DNS IP                          N/A
   Domain Name                     N/A
   Server Name                     Dell-master
   Server IP                       N/A
   Antenna gain for 802.11a        N/A
   Antenna gain for 802.11g        N/A
   Antenna for 802.11a             both
   Antenna for 802.11g             both
   IKE PSK                         N/A
   PAP User Name                   N/A
   PAP Password                    N/A
   PPPOE User Name                 N/A
   PPPOE Password                  N/A
   PPPOE Service Name              N/A
   USB User Name                   N/A
   USB Password                    N/A
   USB Device Type                 any
   USB Device Identifier           N/A
   USB Dial String                 N/A
   USB Initialization String       N/A
   USB TTY device path             N/A
   Mesh Role                       mesh-point
   Installation                    default
```

The output of this command includes the following information:

Column	Description
AP Name	Name of the AP.
AP Group	AP group to which the AP belongs.
Location name	Fully-qualified location name (FQLN) for the AP.
SNMP sysLocation	User-defined description of the location of the AP, as defined with the command **provision-ap syslocation**.
Master	Name or IP address for the master controller.
Gateway	IP address of the default gateway for the AP.
Netmask	Netmask for the AP's IP address.
IP Addr	IP address for the AP.
Dns IP	IP address of the DNS server.
Domain Name	Domain name used by the AP.
Server Name	DNS name of the controller from which the AP boots.
Server IP	IP address of the controller from which the AP boots
Antenna gain for 802.11a	Antenna gain for 802.11a (5GHz) antenna.
Antenna gain for 802.11g	Antenna gain for 802.11g (2.4GHz) antenna.
Antenna for 802.11a	Antenna use for 5 GHz (802.11a) frequency band. • **1**: AP uses antenna 1 • **2**: AP uses antenna 2 • **both**: AP uses both antennas
Antenna for 802.11g	Antenna use for 2.4 GHz (802.11g) frequency band. • **1**: AP uses antenna 1 • **2**: AP uses antenna 2 • **both**: AP uses both antennas
IKE PSK	IKE PSK The IKE pre-shared key.
PPPOE User Name	Point-to-Point Protocol over Ethernet (PPPoE) user name for the AP.
PPPOE Password	PPPoE password for the AP.
PPPOE Service Name	PPPoE service name for the AP.
Mesh Role	If the mesh role is "none," the AP is operating as a thin AP. An AP operating as a mesh node can have one of two roles: mesh portal or mesh point.
Latitude	Latitude coordinates of the AP, in the format *Degrees Minutes Seconds* (DMS).
Longitude	Longitude coordinates of the AP, in the format *Degrees Minutes Seconds* (DMS).
Altitude	Altitude, in meters, of the AP. This parameter is supported on outdoor APs only.
Antenna bearing for 802.11a	Horizontal coverage distance of the 802.11a (5GHz) antenna from true north, from 0-360 degrees. **NOTE:** This parameter is supported on outdoor APs only. The horizontal coverage pattern does not consider the elevation or vertical antenna pattern.

Column	Description
`Antenna bearing for 802.11g`	Horizontal coverage distance of the 802.11g (2.4GHz) antenna from true north, from 0-360 degrees. **NOTE:** This parameter is supported on outdoor APs only. The horizontal coverage pattern does not consider the elevation or vertical antenna pattern.
`Antenna tilt angle for 802.11a`	The angle of the 802.11a (5GHz) antenna. This parameter can range from between -90 degrees and 0 degrees for downtilt, and between +90 degrees and 0 degrees for uptilt.
`Antenna tilt angle for 802.11g`	The angle of the 802.11g (2.4GHz) antenna. This parameter can range from between -90 degrees and 0 degrees for downtilt, and between +90 degrees and 0 degrees for uptilt.
`Mesh SAE`	Shows if the AP has enabled or disabled Secure Attribute Exchange (SAE) on a mesh network.

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	Introduced support for mesh parameters, additional antenna parameters, and AP location parameters.
ArubaOS 3.4	Introduced support for the following parameters: • Installation • Mesh SAE • USB User Name • USB Password • USB Device Type • USB Device Identifier • USB Dial String • USB Initialization String • USB TTY device path
ArubaOS 5.0	The **mesh-sae** parameter no longer displays the **sae-default** setting if the parameter is disabled. Only the **sae-disable** option indicates that this parameter is currently in its default disabled state.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap radio-database

```
show ap radio-database [band a|g] [group <group>] [mode access-point|air-monitor|disabled|ht|ht-40mhz|legacy|sap-monitor] [sort-by ap-group|ap-ip|ap-name|ap-type|switch-ip] [sort-direction ascending|descending] [start <start>] [switch <switch-ip-addr>]
```

Description

Show radio information for Access Points visible to this controller.

Syntax

Parameter	Description
band	Show only APs with a radio operating in the specified band.
a	Show only APs with a radio operating in the 802.11a band (5 GHz).
g	Show only APs with a radio operating in the 802.11g band (2.4 GHz).
group <group>	Show only APs associated with the specified AP group
mode	Show only APs with a radio operating in the specified mode.
access-point	Show only APs operating as access points
air-monitor	Show only APs operating as air monitors.
disabled	Show only disabled APs.
ht	Show only high-throughput APs.
ht-40mhz	Show only 40 Mhz high-throughput APs
legacy	Show only legacy (not high-throughput) APs.
sap-monitor	Show only APs operating as SAP monitors
sort-by	Sort the output of this command by a specific data column
ap-group	Sort the output of this command by AP group name
ap-ip	Sort the output of this command by AP IP address
ap-name	Sort the output of this command by AP name
ap-type	Sort the output of this command by AP model type.
switch-ip	Sort the output of this command by controller ip address
sort-direction	Select a sort direction for the output of this command
ascending	Sort the output in ascending order.
descending	Sort the output in descending order.
start	Start displaying the output of this command at a chosen index number by entering the index number of the AP at which command output should start.
switch <switch-ip-addr>	Display information for APs associated with a specific controller by entering the IP address of that controller.

Example

The output of the command shows that the AP is aware of five other access points, three of which are active.

```
(host) #show ap radio-database

AP Radio Database
-----------------
Name            Group    AP Type  IP Address   Status          Flags  Switch IP     11g Mode/Chan/
EIRP/Cli  11a Mode/Chan/EIRP/Cli
----            -----    -------  ----------   ------          -----  ---------     ---------------
-------  ----------------------
mp3          default  125     10.3.129.96  Up 14h:45m:0s   M     10.3.129.232  AP(HT)/10/0/0
AP(HT)/100/4/0
sw-ad-ap124-11  default  124     10.3.129.99  Up 14h:43m:18s  M     10.3.129.232  AP(HT)/10/0/0
AP(HT)/100+/2/0
sw-ad-ap125-13  default  125     10.3.129.98  Up 14h:49m:36s  M     10.3.129.232  AP(HT)/10/2.5/0
AP(HT)/100/4/0
sw-ad-ap65-19   default  65       10.3.129.95  Down                  10.3.129.232

   Flags: U = Unprovisioned; N = Duplicate name; G = No such group; L = Unlicensed
          R = Remote AP; I = Inactive; X = Maintenance Mode; P = PPPoE AP; B = Built-in AP
          S = RFprotect Sensor; d = Disconnected Sensor; H = Using 802.11n license
          M = Mesh node; Y = Mesh Recovery
```

The output of this command includes the following information:

Column	Description
Name	Name of the AP.
Group	AP group to which the AP is associated.
AP Type	AP model type.
IP address	IP address of the AP.
Status	Current AP status. If the AP is currently up, this data column also shows the amount of time for which the AP has been active.
Flags	This column displays a letter that corresponds to some type of additional information for the AP. The key to the list of possible flags appears at the bottom of the output of this command.
Switch IP	IP address of the AP's controller.
11g Mode/Chan/EIRP/Cli	802.1g radio type and mode/802.11g radio channel used by the AP/current Effective Isotropic Radiated Power (EIRP)/Number of Clients associated with the radio
11a Mode/Chan/EIRP/Cli	802.1a radio type and mode/802.11a radio channel used by the AP/current Effective Isotropic Radiated Power (EIRP)/Number of Clients associated with the radio.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap regulatory-domain-profile

```
show ap regulatory-domain-profile [<profile-name>]
```

Description

Show the list of regulatory domain profiles, or the settings in an individual regulatory domain profile

Syntax

Parameter	Description
<profile-name>	Show data for a specific regulatory domain profile

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire regulatory domain profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three regulatory domain profiles. The **References** column lists the number of other profiles with references to the regulatory domain profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) # show ap regulatory-domain-profile

Regulatory Domain profile List
------------------------------
Name                            References  Profile Status
----                            ----------  --------------
corp-channel-profile            8
default                         10
channel-test 1

Total:3
```

This example displays the configuration settings for the profile **corp-channel-profile**. The output of this command shows the profile's country code and the valid channel and channel pairs for that profile.

```
(host) #show ap regulatory-domain-profile corp-channel-profile

Regulatory Domain profile "corp-channel-profile"
------------------------------------------------
Parameter                       Value
---------                       -----
Country Code                    US
Valid 802.11g channel           1
Valid 802.11g channel           6
Valid 802.11a channel           36
Valid 802.11a channel           40
Valid 802.11a channel           44
Valid 802.11a channel           48
Valid 802.11a channel           149
Valid 802.11a channel           153
Valid 802.11g 40MHz channel pair  N/A
Valid 802.11a 40MHz channel pair  36-40
Valid 802.11a 40MHz channel pair  44-48
   Valid 802.11a 40MHz channel pair  149-153
```

The output of this command includes the following information:

Column	Description
Country Code	Code that represents the country in which the APs will operate. The country code determines the 802.11 wireless transmission spectrum.
Valid 802.11g channel	Selected 802.11b/g channel available for use by an AP using the specified regulatory domain profile. These channels are limited to those valid for the profile's country code.
Valid 802.11a channel	Selected 802.11a channel available for use by an AP using the specified regulatory domain profile. These channels are limited to those valid for the country code.
Valid 802.11g 40MHz channel pair	Selected 802.11b/g 40 MHz channel pair available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.
Valid 802.11a 40MHz channel pair	Selected 802.11a 40 MHz channel pair available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap remote counters

```
show ap remote counters {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show the numbers of message counters for Remote APs

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. You must specify an AP's BSSID, which is usually the AP's MAC address
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address.

Examples

Use this command to determine the number of message counters recorded for each counter type seen by the remote AP. The output of the command in the example below shows counters for Remote AP State and VoIP CAC State Announcements.

```
(host) #show ap remote counters ap-name al22

Counters
--------
Name                          Value
----                          -----
Remote AP State               62851
VoIP CAC State Announcement   13605
```

The output of this command includes the following information:

Column	Description
`Name`	Name of the counter type.
`Value`	Number of counters recorded since the AP was last reset.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap remote debug flash-config

```
show ap remote debug flash-config {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
acls|{vap <vap>|vaps
```

Description

Show the remote AP configuration stored in flash memory.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show debugging data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`acls`	Display ACLs of offline Virtual APs (VAPs).
`vap <vap>`	Display the configuration of a specific offline VAP by entering the name of an VAP.
`vaps`	Display the current number of offline VAPs.

Example

The output of this command can be used to debug problems with a remote AP. The command below shows statistics for an AP with the IP address `192.0.2.64.`

```
(host) #show ap remote debug flash-config ip-addr 192.0.2.64 acls
Offline ACLs
------------
Item               Value
----               -----
Native VLAN        1
DHCP VLAN          N/A
DHCP ADDR          192.168.11.1
DHCP POOL NETMASK  255.255.255.0
DHCP POOL START    192.168.11.2
DHCP POOL END      192.168.11.254
DHCP DNS SERVER    0.0.0.0
DHCP ROUTER        192.168.11.1
DHCP DNS DOMAIN    mycompany
DHCP LEASE         0
Session ACL        N/A
Session ACL Name   N/A
Session ACL Count  N/A
Session Aces       N/A
ACL 1              1
ACL 1 Name         logon
ACL 1 Count        21
Aces 1             16 1 4294
...
```

The output of this command includes the following information:

Column	Description
Native VLAN	VLAN ID of the native VLAN.
DHCP VLAN	VLAN ID of Remote AP DHCP server used when the controller is unreachable.
DHCP ADDR	IP Address used as DHCP Server Identifier.
DHCP POOL NETMASK	Netmask of the DHCP server pool.
DHCP POOL START	IP Address used as the start of a range of addresses for a DHCP pool.
DHCP POOL END	IP Address used as the end of a range of addresses for a DHCP pool.
DHCP DNS SERVER	IP Address for the DHCP DNS server.
DHCP ROUTER	IP Address for the DHCP default router.
DHCP DNS DOMAIN	Domain name for the DHCP DNS server.
DHCP LEASE	Length of DHCP DNS leases in days. If this parameter displays a zero (0) the DHCP lease is has no defined end.
Session ACL	Name of the ACL applied to the user session.
Session ACL name	Name of the ACL applied to the user session.
Session ACL count	Number of rules in the applied to the user session.
Session Aces	A list of the individual rules in the session ACL.
ACL 1	This parameter shows the position of an individual ACL.
ACL1 Name	Name of the ACL in the first position.
ACL1 Count	Number of rules in the specified ACL.
ACL1 Aces	A list of the individual rules in the specified ACL.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap remote debug mgmt-frames

```
show ap remote debug mgmt-frames {ap-name <ap-name>}|{bssid <bssid>|{ip-addr <ip-addr>}
[client-mac <client-mac>] [count <count>]
```

Description

Show traced 802.11 management frames for a remote AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show debugging information for a specific AP.
`bssid <bssid>`	Show debugging information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address
`ip-addr`	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`client-mac`	Show the AP associations for a specific MAC address by entering the MAC address of the client.
`count <count>`	Limit the amount of information displayed by specifying number of frames to appear in the output of this command.

Examples

Use this command to debug 802,1 authentication on a remote AP. The example below shows that a client successfully associated with the remote AP, then was later deauthenticated.

```
(host) #show ap remote debug mgmt-frames ap-name AP32

Traced 802.11 Management Frames
-------------------------------
Timestamp        stype       SA                DA                BSS               signal  Misc
---------        -----       --                --                ---               ------  ----
Oct 30 11:20:19  deauth      00:23:6c:2f:9a:85  00:1a:1e:11:56:40  00:1a:1e:11:56:40  0      STA has
left and is deauthenticated
Oct 30 11:04:39  assoc-resp  00:1a:1e:11:56:40  00:23:6c:2f:9a:85  00:1a:1e:11:56:40  15
Success
Oct 30 11:04:39  assoc-req   00:23:6c:2f:9a:85  00:1a:1e:11:56:40  00:1a:1e:11:56:40  0       -
```

The output of this command includes the following information:

Column	Description
`Timestamp`	The time the management frame was sent
`stype`	One of the following 802.11 frame types: auth: Authorization frame deauth: Deauthorization frame assoc-resp: Association response assoc-req: Association request
SA	Source MAC address.
DA	Destination MAC address.
BSS	Basic Service Set Identifier (BSSID) of the AP

Column	Description
signal	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.
Misc	Additional information describing the client's action.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap spectrum ap-list

```
show ap spectrum ap-list {ap-name <ap-name>}|{ip-addr <ip-addr>}
   ap-bssid <bssid>
   channel <channel>
   essid <essid>
   limit <number>
   or
   page <number>
   freq-band 2.4ghz|5ghz
   sort <sort>
   start <index>
```

Description

This command shows spectrum data seen by an access point that has been converted to a spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`channel <channel>`	View spectrum information for a specific radio channel.
`essid <essid>`	View spectrum information for a specific ESSID.
`limit <number>`	Limit the displayed output to the specified number of entries
`or`	Use this parameter to display information that meets either of two criteria, such as a specified ESSID or channel.
`page <number>`	Enter a number from 10-100 (inclusive) to specify the number of entries that should appear in each page of the output for this command. For example, if the output of this command has 100 entries and you select a page value of 20, the output will appear in 5 pages each with 20 entries. If you selected a page value of 10, the output would appear in 10 pages with 10 entries.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 Ghz.
`sort <sort>`	Sort the output by the specified data column
`start <index>`	Start displaying the output at specific spectrum index value.

Usage Guidelines

The Spectrum Analysis feature provides visibility into RF coverage, allowing you to troubleshoot RF interference and identify 802.11 devices on the network. Issue this command to display and sort APs seen by a specific spectrum monitor.

Examples

The output of this example shows spectrum data seen by spectrum monitor ap123. The output in the example below has been divided into two tables to better fit this document. In the ArubaOS CLI, the output appears as a single, long table.

```
(host)# show ap spectrum ap-list ap-name ap123

Spectrum AP Table
-----------------
bssid              essid          spectrum-id  chan  phy-type        signal(dBm)
-----              -----          -----------  ----  --------        ---------------
00:0b:86:cd:22:d0  ECSD Wireless  2            161   80211a          62
00:0b:86:cb:cf:30  ECSD Wireless  3            157   80211a          68
00:0b:86:f6:f6:a0  osuwireless    3            1     80211b/g        48
00:0b:86:f6:f6:a1  osuvoice       4            1     80211b/g        47
00:0b:86:f6:f6:a2  osuguest       5            1     80211b/g        45

avg-rssi(dB) curr-rssi(dB) ibss  add-time             last-seen
--------     ---------     ----  --------             -----------
29           31            no    2010-05-16 17:41:36  2010-05-18 13:39:38
24           25            no    2010-05-16 17:41:36  2010-05-18 14:19:03
37           38            no    2010-05-16 17:41:36  2010-05-18 15:06:02
38           38            no    2010-05-16 17:41:36  2010-05-18 15:04:23
37           40            no    2010-05-16 17:41:36  2010-05-18 15:07:32
```

The output of this command includes the following information:

Column	Description
`bssid`	Basic Service Set Identifier for an AP. This is usually the AP's MAC address.
`essid`	Extended service set identifier that names a wireless network.
`spectrum-id`	Identifier assigned to the device by the spectrum monitor
`chan`	Radio channel used by the BSSID
`freq-band`	Radio phy type. Possible types include: • 2.4 GHz • 5 GHz
signal (dBm)	Strength of the signal received by the device, in dBm.
avg-rssi	The average signal-to-noise ratio seen by the AP.
curr-rssi	Most recent signal-to-noise ratio seen by the AP.
ibss	Shows if ad-hoc BSS is enabled or disabled. It will be enabled if the bssid has detected an ad-hoc BSS (an ibss bit in an 802.11 frame).
add-time	Time when the AP was first detected by the spectrum monitor.
last-seen	Time when the AP was last seen by the spectrum monitor.

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum channel-metrics

```
show ap spectrum channel-metrics {ap-name <ap-name>}|{ip-addr <ip-addr>} freq-band
2.4ghz|5ghz
```

Description

This command shows channel quality, availability and utilization metrics as seen by a spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Usage Guideline

This chart displays channel utilization data, showing the percentage of each channel that is currently being used by Wi-Fi devices, and the percentage of each channel being used by non-Wi-Fi devices and 802.11 adjacent channel interference (ACI).

Note: ACI refers to the interference on a channel created by a transmitter operating in an adjacent channel. A transmitter on a nonadjacent or partially overlapping channel may also cause interference, depending on the transmit power of the interfering transmitter and/or the distance between the devices. In general, ACI may be caused by a Wi-Fi transmitter or a non-Wi-Fi interferer. However, whenever the term ACI appears in Spectrum Analysis graphs, it refers to the ACI caused by Wi-Fi transmitters. The channel utilization option in the Channel Metrics Chart shows the percentage of the channel utilization due to both ACI and non-Wi-Fi interfering devices. Unlike the ACI shown in the show ap spectrum interference-power output, the ACI shown in this graph indicates the percentage of channel time that is occupied by ACI or unavailable for Wi-Fi communication due to ACI.

.The Channel Metrics table can also show channel availability, the percentage of each channel that is available for use, or display the current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands. In the spectrum analysis feature, channel quality is a relative measure that indicates the ability of the channel to support reliable Wi-Fi communication. Channel quality, which is represented as a percentage in this chart, is a weighted metric derived from key parameters that can affect the communication quality of a wireless channel, including noise, non-Wi-Fi (interferer) utilization and duty-cycles, and certain types of retries. Note that channel quality is not directly related to Wi-Fi channel utilization, as a higher quality channel may or may not be highly utilized.

Examples

The output of this example shows part of the channel metrics table for channels seen by the spectrum monitor ap123,.

```
(host)# show ap spectrum channel-metrics ap-name ap123 freq-band 2.4GHz

Channel Metrics Table
---------------------
Channel  Quality(%)  Availability(%)  Utilization(%)  WiFi Util(%)  Interference Util(%)
-------  ----------  ---------------  --------------  ------------  --------------------
1        97          57               43              40            3
2        80          58               42              22            20
3        63          58               42              5             37
4        71          57               43              16            27
5        88          54               46              36            10
6        98          51               49              47            2
7        88          54               46              35            11
8        69          56               44              14            30
9        60          57               43              3             40
10       30          29               71              1             70
11       0           0                100             0             100
12       25          50               50              0             50
13       50          99               1               0             1
14       99          99               1               0             1
1+/5-    63          54               46              36            10
2+/6-    63          51               49              47            2
3+/7-    63          51               49              47            2
4+/8-    69          51               49              47            2
5+/9-    60          51               49              47            2
6+/10-   30          29               71              1             70
7+/11-   0           0                100             0             100

Interference Util:Utilization by non-Wi-Fi Interference + WiFi ACI (Adjacent Channel Interference)
```

The output of this command includes the following information:

Column	Description
channel	An 802.11a or 82.11g radio channel.
Quality(%)	Current relative quality of selected channels in the 802.11a or 802.11g radio bands, as determined by the percentage of packet retries, the current noise floor, and the duty cycle for non-Wi-Fi devices on that channel.
Availability(%)	The percentage of the channel currently available for use.
Utilization(%)	The percentage of the channel being used.
WiFi Util(%)	The percentage of the channel currently being used by wifi devices.
Interference Util(%)	The percentage of the channel currently being used by non-Wi-Fi interference + wifi ACI (Adjacent Channel Interference)

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum channel-summary

```
show ap spectrum channel-summary {ap-name <ap-name>}|{ip-addr <ip-addr>} freq-band
2.4ghz|5ghz
```

Description

This command displays a summary of the 802.11a or 802.11g channels seen by a spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either **2.4 GHz** or **5 GHz**.

Usage Guidelines

This table can display data aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference and the signal-to-noise-and-interference Ratio (SNIR).

SNIR is the ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Examples

The output of the example below shows information for 802.11a radio channels seen by the spectrum monitor ap999.

```
(host)# show ap spectrum channel-summary ap-name ap999 freq-band 5ghz

Channel Summary Table
---------------------
Channel  KnownAPs  UnknownAPs  Util(%)  MaxAPSignal(dBm)  MaxInterference(dBm)  SNIR(dB)
-------  --------  ----------  -------  ----------------  --------------------  -------
149      69        0           5        -39               -69                   30
153      20        0           100      -42               -60                   18
157      56        0           6        -53               -59                   6
161      54        0           4        -43               -71                   28
165      32        0           3        -27               -70                   43
149+     69        0           100      -39               -60                   21
157+     20        0           6        -43               -59                   16
```

The output of this command includes the following information:

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Known APs	Number of valid APs identified on the radio channel.
UnKnown APs	Number of invalid or rogue APs identified on the radio channel.
Channel Util (%)	Percentage of the channel currently in use.
Max AP Signal (dBm)	Signal strength of the AP that has the maximum signal strength on a channel.

Column	Description
Max Interference(dBm)	Signal strength of the non-Wi-Fi device that has the highest signal strength.
SNIR (db)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum client-list

```
show ap spectrum client-list {ap-name <ap-name>}|{ip-addr <ip-addr>}
   ap-bssid <bssid>
   channel <channel>
   essid <essid>
   limit <limit>
   mac <mac-addr>
   or
   page <page>
   freq-band 2.4ghz|5ghz
   start <start>
```

Description

This command shows details for clients seen by a specified spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`ap-bssid <bssid>`	View information for a client with a specific BSSID.
`channel <channel>`	view information for clients on a specific radio channel.
`essid <essid>`	View information for clients using a specific ESSID.
`limit <limit>`	Limit the output of this command to the specified number of clients.
`mac <mac-addr>`	View information for a client with a specific MAC address.
`start <start>`	Limit the output of this command to clients that with the specified index number or lower.
`limit <number>`	Limit the displayed output to the specified number of entries
`or`	Use this parameter to display information that meets either or two criteria, such as a specified ESSID or channel.
`page <number>`	Enter a number from 10-100 (inclusive) to specify the number of entries that should appear in each page of the output for this command. For example, if the output of this command has 100 entries and you select a page value of 20, the output will appear in 5 pages each with 20 entries. If you selected a page value of 10, the output would appear in 10 pages with 10 entries.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either **2.4 GHz** or **5 GHz**.

Usage Guidelines

Use this command to view channel and signal information for wireless clients seen by the spectrum monitor.

Examples

The example shows that the spectrum monitor **ap999** sees eight different clients on channel 149. The output in the example below has been divided into two tables to better fit this document. In the ArubaOS CLI, the output appears as a single, long table.

```
(host)# show ap spectrum client-list ap-name ap999 channel 149

Spectrum Client Table
---------------------
mac                bssid              essid              spectrum-id  channel  phy-type
---                -----              -----              -----------  -------  --------
00:14:a4:d1:34:63  00:24:6c:80:48:79  ethersphere-wpa2   14           149      80211a
00:19:7d:3a:96:d9  00:24:6c:80:7b:c9  ethersphere-wpa2   198          149      80211a
00:16:cf:af:3e:e1  00:24:6c:80:48:79  ethersphere-wpa2   80           149      80211a
00:1c:26:5b:a7:ac  00:24:6c:81:8b:19  ethersphere-wpa2   125          149      80211a
00:21:6b:c6:b2:12  00:24:6c:80:48:79  ethersphere-wpa2   118          149      80211a-HT-40
00:21:6a:9c:0e:36  00:24:6c:81:8b:19  ethersphere-wpa2   121          149      80211a
00:21:6a:51:e4:30  00:1a:1e:87:c1:91  ethersphere-wpa2   164          149      80211a-HT-40
00:24:d6:65:a9:e6  00:24:6c:80:48:7a  ethersphere-voip   222          149      80211a-HT-40

signal(dBm)       add-time             last-seen
---------------   --------             -----------
-71               2010-05-17 09:53:47  2010-05-17 12:36:54
-66               2010-05-17 12:01:01  2010-05-17 12:36:42
-74               2010-05-17 09:54:59  2010-05-17 12:35:55
-79               2010-05-17 10:23:29  2010-05-17 12:37:28
-66               2010-05-17 10:17:05  2010-05-17 12:31:58
-72               2010-05-17 10:20:05  2010-05-17 12:37:30
-63               2010-05-17 11:07:21  2010-05-17 12:29:01
-69               2010-05-17 12:37:25  2010-05-17 12:37:25

start:0
Length:8
Total:8
```

The output of this command includes the following information:

Column	Description
mac	MAC address of the client.
bssid	Basic Service Set Identifier for a client. This is usually the device's MAC address.
essid	Extended service set identifier that names a wireless network.
spectrum-id	Identifier assigned to the client by the spectrum monitor.
chan	Radio channel used by the BSSID
phy-type	Radio phy type. Possible types include: • 802.11a • 802.11a-HT-40 • 802.11b/g • 802.11b/g-HT-20
signal(dBm)	Client signal strength, in dBm.
add-time	Time when the client was first detected by the spectrum monitor.
last-seen	Time when the spectrum monitor last detected that the client was active.

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum debug

```
show ap spectrum debug {channel-info|channel-quality|classify|classify-fft|device-details|device-info|devices-seen} {ap-name <ap-name>}|{ip-addr <ip-addr>} freq-band {2.4ghz|5ghz}
```

Description

This command saves spectrum analysis channel information to a file on the spectrum monitor.

Syntax

Parameter	Description
`channel-info`	Save channel information for later analysis.
`channel-quality`	Save channel quality information for later analysis
`classify`	Save information on classification for later analysis.
`classify-fft`	Save information on classification and FFT data for later analysis.
`device-details`	Save device details for later analysis.
`device-info`	Save device information for later analysis.
`devices-seen`	Save information on devices seen by the spectrum monitor.
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`freq-band 2.4ghz|5ghz`	Save information for a specific radio type, either **2.4 GHz** or **5 GHz**.

Usage Guidelines

Use this command under the supervision of your Dell technical support representative to troubleshoot spectrum analysis issues or errors.

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum debug fft

```
show ap spectrum debug fft {ap-name <ap-name>}|{ip-addr <ip-addr>} freq-band
{2.4ghz|5ghz}
   avg
   duty-cycle
   fft-to-controller
   max
   normalized
   raw
   raw-normalized
```

Description

Save FFT (Fast Fourier Transform) power data to a file on the spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor.
`freq-band 2.4ghz|5ghz`	Save information for a specific radio type, either **2.4 GHz** or **5 GHz**.
`avg`	Save FFT average information.
`duty-cycle`	Save FFT duty-cycle data
`fft-to-controller`	Save the FFT max, average and duty-cycle data
`max`	Save the maximum FFT power measured for all samples taken over the last second.
`normalized`	Save normalized FFT information
`raw`	Save the raw FFT information received from driver
`raw-normalized`	Save FFT information received from driver and its normalized FFT

Usage Guidelines

Use this command under the guidance of an Dell technical support representative to troubleshoot FFT power issues seen on an W-AP105 or W-AP90 Series.

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum debug monitors

```
show ap spectrum debug monitors
```

Description

Show a detailed description of all spectrum monitors on the controller.

Syntax

No parameters

Examples

The output of this command shows a list of available spectrum monitors, a list of spectrum monitors currently subscribed to a spectrum client, message counters for subscribed spectrum monitors and the subscription history.

```
(host)# show ap spectrum debug monitors
List of Available Spectrum Monitors
-----------------------------------
AP name  Phy  Band
-------  ---  ----
ap999    G    2GHz
ap999    A    5GHz-lower
Total: 2

List of Subscriptions
---------------------
AP name  Band        Client IP      Subscribe Time          HTTPD pid  Last Data Sent  Send Failed
-------  ----        ---------      -------------           ---------  --------------  -----------
ap123    2GHz        10.100.100.67  2010-05-18 03:49:44 PM  1711       1s              0
ap123    5GHz-upper  10.100.100.67  2010-05-18 03:49:51 PM  1711       1s              0
Num Subscriptions: 2
Current Time: 2010-05-18 03:49:54 PM

Message Counters
----------------
AP name  Band        FFT Data  FFT Duty Cycle  Device Info  Device Details  Devices Seen  Channel Info
-------  ----        --------  --------------  -----------  --------------  ------------  ------------
ap123    2GHz        4         4               1            194             1             1
ap123    5GHz-upper  0         0               0            0               0             0

Subscription History
--------------------
Message          AP/Radio/Band          Client IP      HTTPD  Timestamp               Result
   pid
-------          -------------          ---------      ------ ---------               ------
Subscribe        "ap123"/1/2GHz         10.240.16.165  1701   2010-05-17 01:29:16 PM  Success
Re-subscribe     "ap123"/0/5GHz-upper   10.240.16.165  1700   2010-05-17 01:29:16 PM  Success
Unsubscribe-All  "ap123"/-/-            10.240.16.165  1701   2010-05-17 02:44:18 PM  Client Not found
Subscribe        "ap123"/1/2GHz         10.100.100.67  1716   2010-05-18 03:44:28 PM  Success
Re-subscribe     "ap123"/0/5GHz-upper   10.100.100.67  1718   2010-05-18 03:44:28 PM  Success
Unsubscribe      "ap123"/-/5GHz-upper   10.100.100.67  1702   2010-05-18 03:44:55 PM  Success
Unsubscribe      "ap123"/-/2GHz         10.100.100.67  1720   2010-05-18 03:44:57 PM  Success
Subscribe        "ap123"/1/2GHz         10.100.100.67  1704   2010-05-18 03:49:11 PM  Success
Re-subscribe     "ap123"/0/5GHz-upper   10.100.100.67  1701   2010-05-18 03:49:11 PM  Success
```

Usage Guidelines

Use this command under the guidance of an Dell technical support representative to troubleshoot spectrum analysis errors.

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum debug status

```
show ap spectrum debug status {ap-name <ap-name>}|{ip-addr <ip-addr>} freq-band
2.4ghz|5ghz
```

Description

This command shows detailed status and statistics for a spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view status information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view status information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Usage Guidelines

Use this command under the guidance of an Dell technical support representative to troubleshoot spectrum analysis errors.

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum device-duty-cycle

```
show ap spectrum device-duty-cycle {ap-name <ap-name>}|{ip-addr <ip-addr>} freq-band
2.4ghz|5ghz
```

Description

Shows the current duty cycle for devices on all channels being monitored by the spectrum monitor radio.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Usage Guidelines

The FFT Duty Cycle table in the output of this command shows the duty cycle for each radio channel. The duty cycle is the percentage of time each device type operates or transmits on that channel. For additional details about non-Wi-Fi device types shown in this table, see "Non-Wi-Fi Interferers" on page 687.

Note: This chart is only available for AP models W-AP105 and the W-AP90 Series.

Examples

The output of this command shows that video devices sent a signal on channels 153 and 157 during 99% of the last sample interval.

```
Device Duty Cycle Table (in %)
------------------------------
Device Type          149  153  157  161  165  149+  157+
-----------          ---  ---  ---  ---  ---  ----  ----
Generic Interferer   0    0    0    0    0    0     0
WIFI                 5    0    5    12   8    0     12
Microwave            0    0    0    0    0    0     0
Bluetooth            0    0    0    0    0    0     0
Generic Fixed Freq   0    0    0    0    0    0     0
Cordless Phone FF    0    0    0    0    0    0     0
Video                0    99   99   0    0    0     0
Audio                0    0    0    0    0    0     0
Generic Freq Hopper  0    0    0    0    0    0     0
Cordless Network FH  0    0    0    0    0    0     0
Xbox                 0    0    0    0    0    0     0
Microwave Inverter   0    0    0    0    0    0     0
Cordless Base FH     5    5    5    5    5    0     0

Total:7
```

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum device-history

```
show ap spectrum device-history {ap-name <ap-name>}|{ip-addr <ip-addr>}
   freq-band 2.4ghz|5ghz
   [type audio-ff|bluetooth|cordless-base-fh|cordless-network-fh|cordless-phone-
   ff|generic-ff|generic-fh|generic-interferer|microwave|microwave-inverter|video|xbox]
```

Description

This command shows the history of the last 256 non-Wi-Fi devices.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.
`type`	Show information for one type of device only by specifying a non-Wi-Fi device.
`audio-ff`	View information for audio devices seen by the spectrum monitor.
`bluetooth`	View information for bluetooth devices seen by the spectrum monitor. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.
`cordless-base-fh`	View information for frequency-hopping cordless phone bases seen by the spectrum monitor.
`cordless-phone-ff`	View information for frequency-hopping cordless phones seen by the spectrum monitor.
`cordless-network-fh`	View information for frequency-hopping cordless network devices seen by the spectrum monitor.
`generic-ff`	View information for generic fixed-frequency devices seen by the spectrum monitor.
`generic-fh`	View information for generic frequency-hopping devices seen by the spectrum monitor.
`generic-interferer`	Show only generic interfering devices.
`microwave`	View information for microwave-emitting devices seen by the spectrum monitor. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.
`microwave-inverter`	View information for inverter microwave devices seen by the spectrum monitor. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.
`video`	View information for video devices seen by the spectrum monitor.
`xbox`	View information for Xbox devices seen by the spectrum monitor. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.

Usage Guidelines

Use this command to view channel, signal and duty-cycle information and add/delete times for the last 256 devices seen by the spectrum monitor.

Non-Wi-Fi Interferers

The following table describes each type of of non-Wi-Fi interferer detected by a spectrum monitor.

Non-Wi-Fi Interferer Type	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as *Fixed Frequency (Audio)*.
Fixed Frequency (Cordless Phones)	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as *Fixed Frequency (Cordless Phones)*.
Fixed Frequency (Video)	Video transmitters that continuously transmit video on a single frequency are classified as *Fixed Frequency (Video*). These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.
Fixed Frequency (Other)	All other fixed frequency devices that do not fall into one of the above categories are classified as *Fixed Frequency (Other*). Note that the RF signatures of the fixed frequency audio, video and cordless phone devices are very similar and that some of these devices may be occasionally classified as Fixed Frequency (Other).
Frequency Hopper (Cordless Base)	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (i.e., no active phone calls), the cordless base is classified as *Frequency Hopper (Cordless Base*).
Frequency Hopper (Cordless Network)	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as *Frequency Hopper (Cordless Network*). Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as *Frequency Hopper (Xbox*).
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into one of the above categories, it is classified as Frequency Hopper (Other). Some examples include IEEE 802.11 FHSS devices, game consoles and cordless/hands-free devices that do not use one of the known cordless phone protocols.
Microwave	Common residential microwave ovens with a single magnetron are classified as a *Microwave*. These types of microwave ovens may be used in cafeterias, break rooms, dormitories and similar environments. Some industrial, healthcare or manufacturing environments may also have other equipment that behave like a microwave and may also be classified as a Microwave device.
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as *Microwave (Inverter)*. Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as Microwave (Inverter). As in the the Microwave category described above, there may be other equipment that behave like inverter microwaves in some industrial, healthcare or manufacturing environments. Those devices may also be classified as Microwave (Inverter).
Generic Interferer	Any non-frequency hopping device that does not fall into one of the other categories described in this table is classified as a *Generic Interferer*. For example a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a Generic Interferer. Similarly wide-band interfering devices may be classified as Generic Interferers.

Example

The output of this example shows details for fixed-frequency video devices seen by the spectrum monitor.

```
(host)# show ap spectrum device-history ap-name ap123 freq-band 5ghz type video

Non-Wifi Device History Table
-----------------------------
Type   ID  Cfreq(Khz) Bandwidth(KHz)Channels-affected Signal-strength Duty-cycle Add-time             Delete-time
----   --  -----      ---------     ----------------- --------------- ---------- --------             -----------
Video  1   5745312    6000          149               76              99         2010-05-16 20:07:08  -
Video  2   5745312    6000          149               75              99         2010-05-16 20:07:39  2010-05-17 16:50:24
Video  3   5745312    6000          149               74              99         2010-05-16 20:20:25  2010-05-16 20:20:36
Video  4   5745312    6000          149               76              99         2010-05-16 20:32:44  2010-05-16 20:33:07
Video  5   5742031    6000          149               79              99         2010-05-16 20:33:43  2010-05-16 20:33:53
Video  6   5745312    6000          149               75              99         2010-05-16 20:34:08  2010-05-16 20:34:20
```

The output of this command includes the following information:

Column	Description
Type	Device type. This parameter can be any of the following: • audio FF (fixed frequency) • bluetooth • cordless base FH (frequency hopper) • cordless phone FF (fixed frequency • cordless network FH (frequency hopper) • generic FF (fixed frequency • generic FH (frequency hopper) • generic interferer • microwave • microwave inverter • video • xbox **NOTE:** For additional details about non-Wi-Fi device types shown in this table, see "Non-Wi-Fi Interferers" on page 687
ID	ID number assigned to the device by the spectrum monitor. A spectrum monitor assigns a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device, in Kilohertz.
Channels-affected	Radio channels affected by the wireless device, in Kilohertz.
Signal-strength	Strength of the signal sent from the device, in dBm.
Duty-cycle	Device duty cycle. This value represents the percent of time a the device broadcasts on the specified channel or frequency.
Add-time	Time at which the device was first detected.
Delete-time	Time at which the device was aged out.

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum device-list

```
show ap spectrum device-list {ap-name <ap-name>}|{ip-addr <ip-addr>}
   freq-band 2.4ghz|5ghz
   [type audio-ff|bluetooth|cordless-base-fh|cordless-network-fh|cordless-phone-
   ff|generic-ff|generic-fh|generic-interferer|microwave|microwave-inverter|video|xbox]
```

Description

Show a device summary table and channel information for non-Wi-Fi devices currently seen by the spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.
`type`	Show data for a specific device type only.
`audio-ff`	Show only audio fixed frequency devices.
`bluetooth`	Show only bluetooth devices. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.
`cordless-base-fh`	View information for frequency-hopping cordless phone bases seen by the spectrum monitor.
`cordless-phone-ff`	View information for frequency-hopping cordless phones seen by the spectrum monitor.
`cordless-network-fh`	View information for frequency-hopping cordless network devices seen by the spectrum monitor.
`generic-ff`	View information for generic fixed-frequency devices seen by the spectrum monitor.
`generic-fh`	View information for generic frequency-hopping devices seen by the spectrum monitor.
`generic-interferer`	Show only generic interfering devices.
`microwave`	Show only microwave devices. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.
`microwave-inverter`	Show only microwave inverter devices. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.
`video`	Show only video fixed frequency devices.
`xbox`	Show only xbox frequency hopper devices. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.

Usage Guidelines

Issue this command to view detailed information about currently active non-Wi-Fi devices on the network. Use the optional **type** parameter to display data for one specific device type only. For additional details about non-Wi-Fi device types shown in this table, see "Non-Wi-Fi Interferers" on page 687.

Examples

The output of this example shows that the spectrum monitor **ap123** is able to see data for a single non-Wi-Fi device on its 802.11a radio. Note that the output below is divided into two sections to better fit on the page of this document. In the ArubaOS CLI, this information is displayed in a single long table.

```
(host) #show ap spectrum device-list ap-name ap123 freq-band 5ghz
Non-Wifi Device List Table
--------------------------
Type               ID  Cfreq    Bandwidth  Channels-affected  Signal-strength
----               --  -----    ---------  -----------------  ---------------
Cordless Phone FH  3   5826093  80000      149 157 161 165    49

Duty-cycle  Add-time             Update-time
----------  --------             -----------
5           2010-05-17 10:04:53  2010-05-17 10:04:55
Total:1
Current Time:2010-05-17 10:04:56
```

The output of this command includes the following information:

Column	Description
Type	Device type. This parameter can be any of the following: • audio FF (fixed frequency) • bluetooth • cordless base FH (frequency hopper) • cordless phone FF (fixed frequency • cordless network FH (frequency hopper) • generic FF (fixed frequency • generic FH (frequency hopper) • generic interferer • microwave • microwave inverter • video • xbox **NOTE:** For additional details about non-Wi-Fi device types shown in this table, see "Non-Wi-Fi Interferers" on page 687
ID	ID number assigned to the device by the spectrum monitor. A spectrum monitor assigns a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device.
Channels-affected	Radio channels affected by the wireless device.
Signal-strength	Strength of the signal sent from the device, in dBm.
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add-time	Time at which the device was first detected.
Update-time	Time at which the device's status was updated.

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum device-log

```
show ap spectrum device-log {ap-name <ap-name>}|{ip-addr <ip-addr>}
   freq-band 2.4ghz|5ghz
   [type audio-ff|bluetooth|cordless-phone-ff|cordless-phone-fh|
   generic-ff|generic-fh|generic-interferer|microwave|microwave-inverter|video|xbox]
```

Description

This command shows a time log of add and delete events for non-Wi-Fi devices.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.
`type`	Show data for a specific device type only.
`audio-ff`	Show only audio fixed frequency devices.
`bluetooth`	Show only bluetooth devices. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.
`cordless-base-fh`	View information for frequency-hopping cordless phone bases seen by the spectrum monitor.
`cordless-phone-ff`	View information for frequency-hopping cordless phones seen by the spectrum monitor.
`cordless-network-fh`	View information for frequency-hopping cordless network devices seen by the spectrum monitor.
`generic-ff`	View information for generic fixed-frequency devices seen by the spectrum monitor.
`generic-fh`	View information for generic frequency-hopping devices seen by the spectrum monitor.
`generic-interferer`	Show only generic interfering devices.
`microwave`	Show only microwave devices. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.
`microwave-inverter`	Show only microwave inverter devices. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.
`video`	Show only video fixed frequency devices.
`xbox`	Show only xbox frequency hopper devices. **NOTE:** This option is available only for 2.4 GHz spectrum monitor radios.

Usage Guidelines

Use this table to show a time log of when non-Wi-Fi devices were added to and deleted from the Wi-fi Device log table. For additional details about non-Wi-Fi device types shown in this table, see "Non-Wi-Fi Interferers" on page 687.

Examples

The output of this example shows that the spectrum monitor **ap123** logged data for four frequency-hopping cordless base devices seen by its 802.11g radio. Note that the output below is divided into two sections to better fit on the page of this document. In the ArubaOS CLI, this information is displayed in a single long table.

```
(host) #show ap spectrum device-log ap-name ap123 freq-band 5ghz cordless-base-fh

Non-Wifi Device Log Table
-------------------------
Device Type       ID  Added/Deleted  Signal Strength  Duty Cycle  Center Freq
-----------       --  -------------  ---------------  ----------  -----------
Cordless Base FH  1   Added          78               5           5773281
Cordless Base FH  1   Deleted        78               5           5747343
Cordless Base FH  2   Added          78               5           5757656
Cordless Base FH  2   Deleted        78               5           5760469
Cordless Base FH  3   Added          80               5           5802813
Cordless Base FH  3   Deleted        80               5           5802813
Cordless Base FH  4   Added          80               5           5770781

Start Freq  End Freq  Channels Affected     Bandwidth
----------  --------  -----------------     ---------
5733281     5813281   153                   80000
5707343     5787343   149 153 157 161 165   80000
5717656     5797656   153                   80000
5720469     5800469   153 157 161 165       80000
5762813     5842813   161                   80000
5762813     5842813   161                   80000
5730781     5810781   153                   80000

Total:7
Current Time:2010-05-17 12:04:54
```

The output of this command includes the following information:

Column	Description
Device Type	Type of non-Wi-Fi device detected by the spectrum monitor.
ID	The spectrum ID number assigned to that device. A spectrum monitor assigns a unique spectrum ID per device type.
Added/Deleted	The non-Wi-Fi Device Log Table can show signal data for a device when that device was added or removed from the log table.
Signal Strength	Strength of the signal sent by the device.
Duty Cycle	Device duty cycle. This value represents the percent of time a signal is broadcast on a specific channel or frequency.
Center Freq	Center frequency of the signal sent by the device.
Start Freq	Lowest signal frequency sent by the device.
End Freq	Highest signal frequency sent by the device.
Channels affected	Radio channels affected by the device signal.
Bandwidth	Amount of signal bandwidth used by the device, in kilohertz.

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum device-summary

```
show ap spectrum device-summary {ap-name <ap-name>}|{ip-addr <ip-addr>} freq-band
2.4ghz|5ghz
```

Description

This command shows the numbers of wi-fi and non-Wi-Fi device types on each channel monitored by a spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Usage Guidelines

Use this command to show the types of devices that the spectrum monitor can detect on each channel it monitors. For additional details about non-Wi-Fi device types shown in this table, see "Non-Wi-Fi Interferers" on page 687.

Examples

The output of this example shows that the spectrum monitor **ap123** is able to detect 61wi-fi devices on channel 149g.

```
(host) #show ap spectrum device-summary ap-name ap123 freq-band 5ghz

Device Summary Table
--------------------
Device               149  153  157  161  165
-------              ---  ---  ---  ---  ---
Unknown              0    0    0    0    0
WIFI                 61   6    14   29   9
Microwave            0    0    0    0    0
Bluetooth            0    0    0    0    0
Generic Fixed Freq   0    0    0    0    0
Cordless Phone FF    0    0    0    0    0
Video                0    0    0    0    0
Audio                0    0    0    0    0
Generic Freq Hopper  0    0    0    0    0
Cordless Phone FH    0    0    0    0    0
Xbox                 0    0    0    0    0
Microwave Inverter   0    0    0    0    0
Total:12
```

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum interference-power

```
show ap spectrum interference-power {ap-name <ap-name>}|{ip-addr <ip-addr>} freq-band
2.4ghz|5ghz [<chan-width>]
```

Description

This command shows the interference power detected by a 802.11a or 80211g radio on a spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.
`<chan-width>`	Specify **20MHz** or **40MHz** to select the channel width for which you want to view information. If you do not specify a channel width, the output of this command will display the default 20MHz setting.

Usage Guidelines

This table displays information about AP power levels, channel noise and adjacent channel interference seen on each channel by a spectrum monitor radio.

The output of this command displays the noise floor of each selected channel in dBm. The noise floor of a channel depends on the noise figure of the RF components used in the radio, temperature, presence of certain types of interferers or noise, and the width of the channel. For example, in a clean environment, the noise floor of a 20 MHz channel will be around -95 dBm and that of a 40 MHz channel will be around -92 dBm. Certain types of fixed frequency continuous transmitters such as video bridges, fixed frequency phones, and wireless cameras typically elevate the noise floor as seen by the Wi-Fi radio. Other interferers such as the frequency hopping phones, Bluetooth and Xbox devices may not affect the noise floor of the radio. A Wi-Fi radio can only reliably decode Wi-Fi signals that are a certain dB above the noise floor and therefore estimating and understanding the actual noise floor of the radio is critical to understanding the reliability of the RF environment.

The ACI column displayed in the Interference Power Chart displays adjacent-channel interference (ACI) power levels based on the signal strength(s) of the Wi-Fi APs on adjacent channels. A higher ACI value in Interference Power Chart does not necessarily mean higher interference since the AP that is contributing to the maximum ACI may or may not be very actively transmitting data to other clients at all times. The ACI power levels are derived from the signal strength of the beacons.

Examples

The output of this example shows interference power levels for each channel seen by the spectrum monitor ap123.

```
(host)# show ap spectrum interference-power ap-name ap123 freq-band 5ghz

Interference Power Table
------------------------
Channel  Noise Floor(dBm)  Max AP Signal(dBm)  Max AP SSID        Max AP BSSID       ACI(dBm)  Max Interference(dBm)
-------  ----------------  ------------------  -----------        ------------       --------  ---------------------
149      -91               -40                 ethersphere-wpa2   00:24:6c:80:7b:c9  -77       -71
153      -63               -42                 guest              00:1a:1e:87:c1:90  -63       -58
157      -92               -48                 alpha              00:1a:1e:50:01:30  -74       -60
161      -94               -39                 00:24:6C:C0:15:EB  00:24:6c:81:57:c8  -61       -70
165      -93               -26                 sw-jfb-attack      00:1a:1e:9b:1d:c8  -74       -69
149+     -60               -40                 ethersphere-wpa2   00:24:6c:80:7b:c9  -0        -58
157+     -89               -39                 00:24:6C:C0:15:EB  00:24:6c:81:57:c8  -0        -60
```

The output of this command includes the following information:

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Noise Floor (dBm)	Current noise floor recorded on the channel.
Max AP Signal (dBm)	Power level of the AP on the channel with the highest signal power.
Max AP SSID	SSID of the AP on the channel with the highest signal power.
Max AP BSSID	BSSID of the AP on the channel with the highest signal power.
ACI (dBm)	Adjacent channel interference level detected by the spectrum monitor.
Max Interference Power (dBm)	Signal strength of the non-Wi-Fi device that has the highest signal strength.

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum local-override

```
show ap spectrum local-override
```

Description

This command shows a list of AP radios currently converted to spectrum monitors via the spectrum local-override list

Syntax

No parameters

Examples

The output of this example shows that three APs each have two radios defined as spectrum monitors.

```
(host)# show ap spectrum debug monitors

Spectrum Local Override Profile
-------------------------------
Parameter       Value
---------       -----
Override Entry  AP ap125 band 2ghz
Override Entry  AP ap125 band 5ghz-upper
Override Entry  AP ap105 band 2ghz
Override Entry  AP ap105 band 5ghz-upper
Override Entry  AP apcorp1 band 2ghz
Override Entry  AP APcorp1 band 5ghz-middle
```

The Value column in the output of this command includes the following information:

Parameter	Description
AP	Name of an AP configured as a spectrum monitor.
band	Spectrum band that the spectrum monitor radio is currently monitoring. Possible values are: • 2GHz • 5GHz-lower • 5GHz-middle • 5GHz-upper

Related Commands

Command	Description	Mode
`ap spectrum local-override`	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.	Config mode on master or local controllers
`rf dot11a-radio-profile mode spectrum-mode`	Set a 802.11a radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers
`rf dot11g-radio-profile mode spectrum-mode`	Set a 802.11g radio so the device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	Config mode on master or local controllers

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum monitors

```
show ap spectrum monitors
```

Description

This command shows a list of APs terminating on the controller that are currently configured as spectrum monitors.

Syntax

No parameters

Examples

The output of this example shows that the 802.11a radio on a spectrum monitor named **ap123** is sending spectrum analysis data to a client with the IP address 10.240.16.177.

```
(host)# show ap spectrum debug monitors
List of Sensors
---------------
AP name  Phy  Band        Client IP      Subscribe Time
-------  ---  ----        ---------      --------------
ap123    G    2GHz        10.240.16.177  2010-06-09 04:51:38 PM
ap123    A    5GHz-upper  10.240.16.177  2010-06-09 04:51:34 PM

Num Sensors:2
```

The output of this command includes the following information:

Column	Description
AP name	Name of an AP configured as a spectrum monitor
Phy	The radio's PHY type. Possible values are **A** for 802.11a and **G** for 802.11b/g,
Band	Spectrum band that the spectrum monitor radio is currently monitoring. Possible values are: • 2GHz • 5GHz-lower • 5GHz-middle • 5GHz-upper
Client IP	IP address of the client to which the spectrum monitor is sending data.
Subscribe time	Time at which the spectrum monitor was connected to the client.

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ap spectrum technical-support

```
show ap spectrum technical-support ap-name <ap-name> <filename>
```

Description

Save spectrum data for later analysis by technical support.

Syntax

Parameter	Description
`<ap-name>`	Save technical support information for a specific spectrum monitor.
`<filename>`	Name of the file to which this data should be saved. This file does not have to already exist on the controller, the **show ap spectrum technical-support** command will create this file.

Usage Guidelines

Use this command under the supervision of your Dell technical support representative to troubleshoot spectrum analysis issues or errors.

Command History

Introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap spectrum-load-balancing

```
show ap spectrum-load-balancing [group <group>]
```

Description

Show spectrum load balancing information for an AP with this feature enabled.

Syntax

Parameter	Description
`group <group>`	Filter this information to show only data for the specified spectrum load balancing domain.

Examples

The output of the command below shows the APs currently using the spectrum load-balancing domain **default-1**.

```
(host) #show ap spectrum-load-balancing group default-1

Spectrum Load Balancing Group
-----------------------------
Name     IP Address       Domain     Assignment  Clients
----     ----------       ------     ----------  -------
ap121-1  192.168.151.253  default-1  149/21      3
ap124-1  192.168.151.254  default-1  48/15       3
ap125-1  192.168.151.251  default-1  44/15       2
```

The output of this command includes the following information:

Column	Description
`Name`	Name of an AP
`IP address`	AP IP address
`Domain`	Name of the spectrum load balancing domain assigned to the AP
`Assignment`	Current channel and power assignment for the AP.
`Clients`	Number of clients currently using the AP.

Command History

Introduced in ArubaOS 3.3.2.14.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap system-profile

```
show ap system-profile <profile>
```

Description

Show an AP's system profile settings.

Syntax

Parameter	Description
`<profile>`	Name of a system profile.

Examples

The output of the command below shows the current configuration settings for the default system profile.

```
(host) #show ap system profile default

AP system profile "default"
---------------------------
Parameter                          Value
---------                          -----
LMS IP                             192.0.2.90
Backup LMS IP                      N/A
LMS Preemption                     Disabled
LMS Hold-down Period               600 sec
Master controller IP address       N/A
LED operating mode (AP-12x only)   normal
RF Band                            a
Double Encrypt                     Disabled
Native VLAN ID                     1
SAP MTU                            N/A
Bootstrap threshold                8
Request Retry Interval             10 sec
Maximum Request Retries            10
Dump Server                        192.0.2.41
Telnet                             Enabled
SNMP sysContact                    N/A
RFprotect Server IP                N/A
RFprotect Backup Server IP         N/A
AeroScout RTLS Server              192.0.2.32.104:1411
RTLS Server configuration          N/A
Heartbeat DSCP                     0
Session ACL                        N/A
Corporate DNS Domain               N/A
Maintenance Mode                   Disabled
Remote-AP Local Network Access     Disabled
```

The output of this command includes the following information:

Column	Description
`LMS IP`	The IP address of the local management switch (LMS)—the Dell controller which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network.
`Backup LMS IP`	For multi-controller networks, this parameter displays the IP address of a backup to the IP address specified with the lms-ip parameter.
`LMS Preemption`	When this parameter is enabled, the local management switch automatically reverts to the primary LMS IP address when it becomes available.

Column	Description
LMS Hold-down Period	Time, in seconds, that the primary LMS must be available before an AP returns to that LMS after failover.
Master controller IP address	For multi-controller networks, this parameter displays the IP address of the master controller.
LED operating mode (AP-12x only)	Displays the LED operating mode for W-AP120 series APs. LEDs display as usual in the default **normal** operating mode, but are all turned off in **off** mode.
RF Band	For dual-band radios, this parameter displays the RF band in which the AP should operate: • **g** = 2.4 GHz • **a** = 5 GHz
Double Encrypt	This parameter applies only to remote APs. Double encryption is used for traffic to and from a wireless client that is connected to a tunneled SSID. When enabled, all traffic is re-encrypted in the IPsec tunnel. When disabled, the wireless frame is only encapsulated inside the IPsec tunnel.
Native VLAN ID	Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).
SAP MTU	Maximum Transmission Unit (MTU) size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
Bootstrap threshold	Number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP rebootstraps. On the controller, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.
Dump Server	(For debugging purposes.) Displays the server to receive the core dump generated if an AP process crashes.
Telnet	Reports whether telnet access the AP is enabled or disabled.
SNMP sysContact	SNMP system contact information.
RFprotect Server IP	The IP address of the RFprotect server for this AP or group
RFprotect Backup Server IP	The IP address of the RFprotect backup server for this AP or group
AeroScout RTLS Server	IP address of an AeroScout real-time asset location (RTLS) server.
Heartbeat DSCP	DSCP value of AP heartbeats (0-63).
Session ACL	Shows the access control list (ACL) applied on the uplink of a remote AP.
Corporate DNS Domain	DNS name used by the corporate network.
Maintenance Mode	Shows if Maintenance mode is enabled or disabled. If enabled, APs stop flooding unnecessary traps and syslog messages to network management systems or network operations centers when deploying, maintaining, or upgrading the network. The controller still generates debug syslog messages if debug logging is enabled.
Remote-AP Local Network Access	Shows if Remote-AP Local Network Access is enabled or disabled. By enabling this option, the clients that are connected to a RAP can communicate. Note: By default, the Remote-AP Local Network Access will be disabled.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap tech-support

```
show ap tech-support ap-name <name> [<filename>]
```

Description

Display all information for an AP, or save that information to a file on the controller. This information can be used by Dell technical support to diagnose a problem with an AP.

Syntax

Parameter	Description
`<name>`	Name of the AP for which you want to view tech support data.
`<filename>`	Save the output of this command into a file on the controller with the specified filename.

Usage Guidelines

This is an internal technical support command. Dell technical support may request that you issue this command to help analyze and troubleshoot problems with an AP or your wireless network.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap vlan-usage

```
show ap vlan-usage [{ap-name <ap-name>}|{bssid <bssid>|{essid <essid>|{ip-addr <ip-addr>}]
```

Description

Show the numbers of clients on each vlan.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show VLAN data for an AP with a specific name.
`bssid <bssid>`	Show VLAN data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`essid <essid>`	Show VLAN data for a specific Extended Service Set Identifier (ESSID). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
`ip-addr <ip-addr>`	Show VLAN data for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Examples

The output of this command displays the **VLAN Usage** table.

```
(host) #show ap vlan-usage
   VLAN Usage Table
   ----------------
   VLAN ID  Clients
   -------  -------
   64       1
   65       32
   66       44
```

The output of this command includes the following information:

Column	Description
`VLAN ID`	ID number of the wireless VLAN
`Clients`	Number of clients currently using the specified VLAN.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap wired stats

```
show ap wired stats {ap-name <ap-name>} | {ip-addr <ip-addr>}|{client-ip <client-ip>} |
{client-mac <client-mac>}
```

Description

Shows statistics for RAP wired clients.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show wired RAP statistics for a specified AP name.
`ip-addr <ip-addr>`	Show wired RAP statistics for a specified AP by entering an IP address in dotted-decimal format.
`client-ip <client-ip>`	Show wired RAP statistics for a specified client IP address.
`client-mac <client-mac>`	Show wired RAP statistics for a specified client MAC address

Example

```
(host) #show ap wired stats ap-name rap5wn client-mac 00:14:d1:19:3c:0b

RAP Wired User Statistics
-------------------------
Counter               Value
-------               -----
Slot                  0
Port                  1
VLAN                  1
TX Packets            78
TX Bytes              7894
RX Packets            37
RX Bytes              5352
TX Broadcast Packets  36
TX Broadcast Bytes    4410
TX Multicast Packets  22
TX Multicast Bytes    1990
```

The output of this command includes the following information:

Column	Description
`Slot`	Slot number
`Port`	Port number
`VLAN`	Associated VLAN number
`TX Packets`	Number of packets sent
`TX Bytes`	Number of bytes sent
`RX Packets`	Number of packets received
`RX Bytes`	Number of bytes received

Column	Description
`TX Broadcast Packets`	Number of broadcast packets sent
`TX Broadcast Bytes`	Number of broadcast bytes sent
`TX Multicast Packets`	Number of multicast packets sent
`TX Multicast Bytes`	Number of multicast bytes sent

Command History

Introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap wired-ap-profile

```
show ap wired-ap-profile [<profile>]
```

Description

Show a list of all wired AP profiles, or display the configuration parameters in a specific wired AP profile.

Syntax

Parameter	Description
`<profile>`	Name of a wired AP profile.

Usage Guidelines

The command show ap wired-ap-profile displays a list of all wired AP profiles, including the number of references to each profile and the profile status. If you include the optional <profile> parameter, the command will display detailed information for that one profile.

Example

The output of this command shows the configuration parameters for the wired AP profile “default”.

```
(host) #show ap wired-ap-profile default

Wired AP profile "default"
--------------------------
Parameter                 Value
---------                 -----
Wired AP enable           Disabled
Forward mode              tunnel
Switchport mode           access
Access mode VLAN          1
Trunk mode native VLAN    1
Trunk mode allowed VLANs  1-4094
Trusted                   Not Trusted
Broadcast                 Broadcast
```

The output of this command includes the following information:

Column	Description
`Wired AP enable`	Indicates whether the wired AP profile is **enabled** or **disabled**.
`Forward mode`	The configured forward mode for the profile. • **bridge**: Bridge locally • **split-tunnel**: Tunnel to controller or NAT locally • **tunnel**: Tunnel to controller
`Switchport mode`	The profile’s switching mode. • **access**: Set access mode characteristics of the interface. • **mode**: Set trunking mode of the interface. • **trunk**: Set trunk mode characteristics of the interface.
`Access mode VLAN`	VLAN ID of the access mode VLAN.
`Trunk mode native VLAN`	VLAN ID of the native VLAN.
`Trunk mode allowed VLANs`	Range of allowed VLAN IDs for the native VLAN.

Column	Description
Trusted	Shows if the wired port on an AP using this profile is a trusted port. Possible values are **Trusted** or **Not Trusted**.
Broadcast	If set to **broadcast**, the wired AP port will forward broadcast traffic. If the parameter displays **Do Not Broadcast**, broadcast traffic will not be forwarded.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap wired-port-profile

```
show ap wired-port-profile
```

Description

Shows all AP wired port profiles and their status.

Syntax

No parameters.

Example

The output of this show command shows the

```
(host) (config) #show ap  wired-port-profile

AP wired port profile List
--------------------------
Name             References  Profile Status
----             ----------  --------------
default          3
NoAuthWiredPort  4           Predefined (editable)
shutdown         3           Predefined

Total:3
```

The output of this command includes the following information:

Column	Description
Name	Name of the listed wired port profile
References	Number of references
Profile Status	Status of the listed profile

Command History

This command was introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap wmm-flow

```
show ap wmm-flow [{ap-name <ap-name>}|{bssid <bssid>}|{essid <essid>}|{ip-addr <ip-addr>}] dotlla|dotllg
```

Description

Show the Wireless Multimedia (WMM) flow table.

Syntax

Parameter	Description
`ap-name <ap-name>`	View an AP with a specified name.
`bssid <bssid>`	View data for an AP with a specific BSSID (Basic Service Set Identifier). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`essid <essid>`	View data for a specific ESSID (Extended Service Set Identifier). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
`ip-addr <ip-addr>`	View an AP with a specified IP address by entering an IP address in dotted-decimal format.
`dot11a`	Show the WMM flow table for a 802.11a radio.
`dot11g`	Show the WMM flow table for a 802.11g radio.

Usage Guidelines

WMM, or Wireless Multimedia Extensions, are a subset of the 802.11e standard. WMM provides for four different types of traffic classification: voice, video, best effort, and background, with voice having the highest priority and background the lowest. Issue the **show ap wmm-flow** command to view WMM flow data for all APs. Include any of the optional parameters described in the table above to filter the table by a specific AP, radio channel (a or g), or both an ap and radio type.

Example

The example below shows WMM flow data for all APs.

```
(host) #show ap wmm-flow

WMM Flow Table
--------------
AP Name    ESSID  Client             Description
-------    -----  ------             -----------
AP125-srk  NOE    00:90:7a:06:1f:5b  tsid 6:prio 6:inactivity 2157352960 us:bidir:apsd:normalack:tclas prio 6 ip DIP-
192.168.101.194 DP-32514 DSCP-48:one-match
AP125-srk  NOE    00:90:7a:06:1f:5b  tsid 0:prio 0:inactivity 100000000 us:bidir:apsd:normalack:no-match

Num Flows:0
```

The output of this command includes the following parameters:

Column	Description
`AP name`	Name of an AP with recorded WMM flows
`ESSID`	Extended Service Set Identifier (ESSID) of a wireless network.
`Client`	MAC address of the client.

Column	Description

Description	The description is a long string that includes the following information.
	• **TSID:** The transmitting subscriber identification number. The TSID should match the priority level for each flow.
	• **Priority**: One of the following IEEE 802.1p priority values:
	  ▪ 0-1 = Best Effort
	  ▪ 2-3 = Background
	  ▪ 4-5 = Video
	  ▪ 6-7 = Voice
	• **Inactivity**: Tspec inactivity threshold, in microseconds.
	• **<country code>**: AP country code, e.g. US.
	• **bdir**: flow is bidirectional.
	• **apsd**: flow has enabled auto power save delivery.
	• **<ack>**: Displays the ack policy negotiated for the flow. Possible values are:
	  ▪ normalack
	  ▪ noack
	  ▪ blockack
	  ▪ resack (reserved ack)
	• **DIP**: Destination IP address for the flow.
	• **DP**: Destination IP Port specified in the TCLAS for flow negotiation.
	• **DCSP**: The Differentiated Services Code Point (DSCP) priority value that matches the flows 802.1p priority.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap-group

```
show ap-group [<ap-group>]
```

Description

Show settings for an AP group.

Syntax

Parameter	Description
<ap-group>	The name of an AP group.

Usage Guidelines

Issue this command without the optional **<ap-group>** parameter to display the entire AP group list, including profile status for each profile. Include an AP group name to display detailed configuration information for that AP group profile.

Example

This first example shows that the controller has nine configured AP groups. The **Name** column lists the names of all configured AP groups. the **Profile Status** column indicates whether the AP group is predefined. (User-defined profiles will not have an entry in the **Profile Status** column.)

```
(host) #show ap-group
AP group List
-------------
Name               Profile Status
----               --------------
corp-office
branch-office-am
corp
corp1
Corp1-AM
Corp1-AM-Ch11
Corp1-AM-Ch6
corp1-AP85
corp1-lab

Total: 9
```

Include an AP group name to display a complete list of configuration settings for that profile. The example below shows settings for the AP group **corp1**.

```
(host) #show ap-group corp1
AP group "corp1"
------------------
Parameter                           Value
---------                           -----
Virtual AP                          corp1-guest
Virtual AP                          corp1-wpa2
802.11a radio profile               default
802.11g radio profile               profile1-g
Wired AP profile                    default
Ethernet interface 0 link profile   default
Ethernet interface 1 link profile   default
AP system profile                   corp1344
VoIP Call Admission Control profile default
802.11a Traffic Management profile  N/A
802.11g Traffic Management profile  N/A
Regulatory Domain profile           corp1344-channel-profile
SNMP profile                        default
RF Optimization profile             handoff-aggressive
RF Event Thresholds profile         default
IDS profile                         ids-low-setting
Mesh Radio profile                  default
Mesh Cluster profile                N/A
```

The output of this command includes the following parameters:

Parameter	Description
Virtual AP	Virtual AP profile that which configures a specified WLAN.
802.11a radio profile	Profile that defines 802.11a radio settings for the AP group.
802.11g radio profile	Profile that defines 802.11g radio settings for the AP group.
Wired AP profile	Profile that defines wired port settings for APs assigned to the AP group.
Ethernet interface 0 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
Ethernet interface 1 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
AP system profile	Name of the AP system profile for the AP group.
VoIP Call Admission Control profile	Name of the AP system profile for the AP group.
802.11a Traffic Management profile	Name of the 802.11a WLAN traffic management profile for the AP group.
802.11g Traffic Management profile	Name of the 802.11g WLAN traffic management profile for the AP group.
Regulatory Domain profile	Name of the regulatory domain profile for the AP group.
SNMP profile	Name of the SNMP profile for the AP group.
RF Optimization profile	Name of the RF optimization profile for the AP group.
RF Event Thresholds profile	Name of the RF event thresholds profile for the AP group.
IDS profile	IDS profile for the AP group.
Mesh Radio profile	Mesh radio profile assigned to the AP group.
Mesh Cluster profile	Mesh cluster profile assigned to the AP group.

Related Commands

Configure AP group settings using the command ap-group.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master controllers

show ap-name

```
show ap-name [<ap-name>]
```

Description

Show a list of AP names. Include the **<ap-name>** parameter to display detailed configuration information for that AP.

Syntax

Parameter	Description
<ap-name>	The name of an AP.

Example

This first example shows that the controller has eight registered APs. The **Name** column lists the names of each registered AP. Note that APs are all user-defined, so they will not have an entry in the **Profile Status** column.

```
(host) #show ap-group
AP name List
------------
Name            Profile Status
----            --------------
mp3
sw-ad-ap124-11
sw-ad-ap125-13
sw-ad-ap125-15
sw-ad-ap125-17
sw-ad-ap125-18
sw-ad-ap125-19
sw-ad-ap125-3

Total: 8
```

Include an AP name to display a complete list of configuration settings for that AP. If the AP has default settings, the value may appear as N/A. The AP in the example below has all default profile settings

```
(host) #show ap-group corp1
AP name "mp3"
-------------
Parameter                           Value
---------                           -----
Virtual AP                          N/A
Excluded Virtual AP                 N/A
802.11a radio profile               N/A
802.11g radio profile               N/A
Wired AP profile                    N/A
Ethernet interface 0 link profile   N/A
Ethernet interface 1 link profile   N/A
AP system profile                   N/A
VoIP Call Admission Control profile N/A
802.11a Traffic Management profile  N/A
802.11g Traffic Management profile  N/A
Regulatory Domain profile           N/A
RF Optimization profile             N/A
RF Event Thresholds profile         N/A
IDS profile                         N/A
Mesh Radio profile                  N/A
Mesh Cluster profile                N/A
Excluded Mesh Cluster profile       N/A
```

The output of this command includes the following parameters:

Parameter	Description
Virtual AP	Virtual AP profile that which configures a specified WLAN.
Excluded Virtual AP	Excludes the specified mesh cluster profile from this AP.
802.11a radio profile	Profile that defines 802.11a radio settings for the AP.
802.11g radio profile	Profile that defines 802.11g radio settings for the AP.
Wired AP profile	Profile that defines wired port settings for APs assigned to the AP.
Ethernet interface 0 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
Ethernet interface 1 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
AP system profile	Name of the AP system profile for the AP.
VoIP Call Admission Control profile	Name of the AP system profile for the AP.
802.11a Traffic Management profile	Name of the 802.11a WLAN traffic management profile for the AP group.
802.11g Traffic Management profile	Name of the 802.11g WLAN traffic management profile for the AP.
Regulatory Domain profile	Name of the regulatory domain profile for the AP.
RF Optimization profile	Name of the RF optimization profile for the AP.
RF Event Thresholds profile	Name of the RF event thresholds profile for the AP.
IDS profile	IDS profile for the AP.
Mesh Radio profile	Mesh radio profile assigned to the AP.
Mesh Cluster profile	Mesh cluster profile assigned to the AP.

Parameter	Description
Excluded Mesh Cluster profile	Excludes the specified mesh cluster profile from this AP.

Related Commands

Configure AP settings using the command ap-name.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show arp

```
show arp
```

Description

Show Address Resolution Protocol (ARP) entries for the controller.

Syntax

No parameters

Example

This example shows configured static ARP entries for the controller.

```
(host) #show arp
Protocol        Address         Hardware Address        Interface
Internet        10.3.129.98     00:1A:1E:C0:80:28       vlan1
Internet        10.3.129.253    00:0B:86:42:35:80       vlan1
Internet        10.3.129.250    00:1A:92:45:DB:00       vlan1
Internet        10.3.129.99     00:1A:1E:C0:1C:60       vlan65
Internet        10.3.129.96     00:1A:1E:C0:80:1E       vlan65
Internet        10.3.129.254    00:0B:86:02:EE:00       vlan1
```

The output of this command includes the following parameters:

Parameter	Description
`Protocol`	Protocol using ARP. Although the controller will most often use ARP to translate IP addresses to Ethernet MAC addresses, ARP may also be used for other protocols, such as Token Ring, FDDI, or IEEE 802.11, and for IP over ATM.
`Address`	IP address of the device.
`Hardware Address`	MAC address of the device.
`Interface`	Interface used to send ARP requests and replies.

Related Commands

Add a static Address Resolution Protocol (ARP) entry using the command **`show arp`**.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master and local controllers

show audit-trail

```
show audit-trail {<number>]
```

Description

Show the controller's audit trail log.

Syntax

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.

Example

By default, the audit trail feature is enabled for all commands in configuration mode. The example below shows the most recent ten audit log entries for the controller.

```
(host) # show audit-trail 10
Feb  5 06:13:17  cli[1239]: USER: admin has logged in from 10.240.16.118.
Feb  5 06:20:13  cli[1239]: USER: admin connected from 10.240.16.118 has logged out.
Feb  5 06:24:37  cli[1239]: USER: admin has logged in from 10.240.16.118.
Feb  5 06:37:01  cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap "mp-only" no vap-enable > -- command
executed successfully
Feb  5 06:37:14  cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap "mp-a-only" no vap-enable > -- command
executed successfully
Feb  5 06:37:20  cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap "default" no vap-enable > -- command
executed successfully
Feb  5 06:37:29  cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap "mpp-a-only" no vap-enable > -- command
executed successfully
Feb  5 06:46:10  cli[1239]: USER:admin@10.3.129.250 COMMAND:<interface gigabitethernet "1/2" port monitor
igigabitethernet "1/1" > -- command executed successfully
Feb  5 06:57:44  cli[1239]: USER:admin@10.3.129.250 COMMAND:<ap system-profile "default" heartbeat-dscp 12 > -- command
executed successfully
Feb  5 07:05:48  cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap "mp-a-only" vap-enable > -- command executed
successfully
```

Related Commands

Enable or disable the audit trail feature using the command **`audit-trail`**.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes. Audit trails can only be enabled on master controllers

show auth-tracebuf

```
show auth-tracebuf [count <1-250] [failures] [mac <address>]
```

Description

Show the trace buffer for authentication events.

Syntax

Parameter	Description
count <1-250>	limit the output of the command to the specified number of packets.
failures	Filter the output of this command to display only authentication failures
mac <address>	Filter the output of this command to display only information for a specified MAC address.

Usage Guidelines

Use the output of this command to troubleshoot 802.1x authentication errors. Include the **<address>** parameter to filter data by the MAC address of the client which is experiencing errors. This command can tell you, for example, when 802.1x authentication completed and when keys were plumbed correctly.

Example

The example below shows the most recent ten trace buffer entries for the controller. Each row includes the following information:

```
(host) # show auth-tracebuf count 10
Auth Trace Buffer
-----------------
Feb  5 08:08:29  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic failure
Feb  5 08:08:30  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:30  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic failure
Feb  5 08:08:31  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:31  station-down          *   00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   -
Feb  5 08:08:31  station-up           *   00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   -    wpa2 psk aes
Feb  5 08:08:31  station-data-ready   *   00:09:ef:05:1e:b2  00:00:00:00:00:00  66  -
Feb  5 08:08:31  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:31  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic failure
Feb  5 08:08:32  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:32  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic failure
Feb  5 08:08:33  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:33  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic failure
Feb  5 08:08:34  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:34  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic failure
Feb  5 08:08:35  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:35  station-down          *   00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   -
```

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.
- BSSID/Server Name.
- The packet number.
- The packet length.

- Additional information (if available), e.g.username, encryption and WPA type, or reason for failure.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable or Config modes on master or local controllers

show banner

```
show banner
```

Description

Show the current login banner

Syntax

No parameters

Usage Guidelines

Issue this command to review the banner message that appears when you first log in to the controller's command-line or browser interfaces.

Example

```
(host) # show banner
This testlab controller is scheduled for maintenance starting Saturday night at 11 p.m.
```

Related Commands

Configure a banner message using the command banner motd.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show boot

```
show boot
```

Description

Display boot parameters, including the boot partition and the configuration file to use when booting the controller.

Syntax

No parameters.

Example

```
(host) # show boot
Config File: default.cfg
Boot Partition: PARTITION 1
```

Related Commands

Configure boot parameters using the command boot.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show cellular profile

```
show cellular profile [<name>] | [factory]
```

Description

Display the cellular profiles and profile settings.

Syntax

Parameter	Description
<name>	Enter the name of an existing cellular profile
factory	Display a list of factory supported cellular profiles.

Usage Guidelines

Issue this command without the **<name>** parameter to display configuration parameters for the entire list of available cellular profiles. Include a profile name to display configuration information for that one profile.

Example

The output of this command displays the Cellular Profile Table. The example below shows eight preconfigured cellular profiles.

```
(host) #show cellular profile

Cellular Profile Table
----------------------
Name                  Vend      Prod      Serial  Dialer   Tty      Driver  Priority  Modeswitch
----                  ----      ----      ------  ------   ---      ------  --------  ----------
Novatel_U720          1410      2110              evdo_us  ttyUSB0  option  default
Novatel_U727          1410      4100              evdo_us  ttyUSB0  option  default
Kyocera_KPC680        0c88      180a              evdo_us  ttyUSB0  option  default
Sierra_Compass_597    1199      0023              evdo_us  ttyUSB0  sierra  default
Pantech_UM175         106c      3714              evdo_us  ttyUSB1  option  default
Sierra_USBConn_881    1199      6856              gsm_us   ttyUSB0  option  default
USBConn_Mercury_C885  1199      6880              gsm_us   ttyUSB3  option  default
Globetrotter_Icon322  0af0      d033              gsm_us   ttyHS3   hso     default
Default cellular priority:      100
```

The output of this command includes the following parameters:

Parameters	Description
Name	Name of a cellular profile.
Vend	Vendor ID in hexadecimal
Prod	USB product ID in hexadecimal
Serial	USB device serial number.
Dialer	Name of a dialer group profile.
TTY	Modem TTY port.

Parameters	Description
Driver	One of the following cellular modem drivers: • **acm**: Linux ACM driver. • **hso**: Option High Speed driver. • **option**: Option USB data card driver (default). • **sierra**: Sierra Wireless driver.
Priority	Displays the cellular profile priority; profiles with the default priority of 100 will display the word **default** in the Priority column Range: 1 to 255. Default: 100
Modeswitch	One of two USB device modeswitch settings: • **eject**: Eject the CDROM device. • **rezero**: Send SCSI CDROM rezero command.

Command History

Introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
600 Series	Base operating system	Config or Enable mode on master or local controllers

show clock

```
show clock [summer-time|timezone]
```

Description

Display the system clock.

Syntax

Parameter	Description
`summer-time`	Show summer (daylight savings) time settings.
`timezone`	Show the configured timezone for the controller.

Usage Guidelines

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

The output below shows the current time on the controller clock.

```
(host) # show clock
Thu Feb  5 16:52:28 PST 2009
```

Related Commands

Configure clock settings using the commands clock set, clock summer-time recurring, and clock timezone.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show command-mapping

```
show command-mapping [reverse]
```

Description

Show the mapping new commands to deprecated commands.

Syntax

Parameter	Description
`reverse`	Sort the command map by deprecated command syntax. This command is useful to find the current command syntax for a deprecated command.

Usage Guidelines

The syntax of many commands changed after the release of ArubaOS 3.0. Use this command to display a list of current commands and their deprecated command equivalents. Include the **reverse** parameter sort the output of this table by the deprecated command syntax.

Example

The example below shows part of the output for this command. Note that a single new command may have replaced several older commands.

```
(host) # show command-mapping
Command Map
-----------
New Command                          Old Command
-----------                          -----------
show ap active                       show wlan ap
show ap arm neighbors                show ap arm-neighbors
show ap arm rf-summary               show am rf-summary
show ap arm scan-times               show am scan-times
show ap arm state                    show wlan arm
show ap association                  show stm association
                                     show wlan client
                                     show wlan remote-client
show ap blacklist-clients            show stm dos-sta
show ap bss-table                    show stm connectivity
show ap client status                show stm state
show ap coverage-holes               show rfsm coverage-holes
show ap database                     show ap global-list
                                     show sapm ap search
                                     show ap registered
show ap debug association-failure    show wlan association-failure
....
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show configuration

```
show configuration
```

Description

Show the saved configuration on the controller.

Syntax

No parameters.

Usage Guidelines

Issue this command to view the entire configuration saved on the controller, including all profiles, ACLs, and interface settings.

Example

The example below shows part of the output for this command.

```
(host) # show configuration
version 3.4
enable secret "0078b61601db950378d3d27a33c0b4d61f95b653ce9480a229"
telnet cli
prompt Lab12-800
loginsession timeout 0
hostname "sampleHost"
clock timezone PST -8
banner motd:
This controller is in Lab 12.

location "Building1.floor1"
mms config 0
controller config 1173

ip access-list eth 200
```

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show controller-ip

```
show controller-ip
```

Description

Show controller's country and domain upgrade trail.

Syntax

No parameters.

Example

The output of this command shows the controller's IP address and VLAN interface ID.

```
(host) # show controller-ip

Switch IP Address: 10.168.254.221
Switch IP is configured to be Vlan Interface: 1
```

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show country

```
show country [trail]
```

Description

Show controller's country and domain upgrade trail.

Syntax

Parameter	Description
`trail`	Display the record showing how the switch was reconfigured for it's current country domain when the controller hardware was upgraded.

Usage Guidelines

A controller's country code sets the regulatory domain for the radio frequencies that the APs use. This value is typically set during the controller's initial setup procedure. Use this command to determine the country code specified during setup.

Example

The output of this command shows the controller's country, model and hardware types.

```
(host) # show country

Country:US
Model:-US
Hardware:Restricted US
```

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show cp-bwcontracts

```
show cp-bwcontract
```

Description

Display a list of Control Processor (CP) bandwidth contracts for whitelist ACLs.

Syntax

No parameters.

Example

The *CP bw contracts* table lists the contract names, the ID number assigned to each contract, and its defined traffic rate in bits per second.

```
(host) #show cp-bwcontracts

CP bw contracts
---------------
Contract     Id    Rate (bits/second)
--------     --    ------------------
limit        4098  2000000000
newcontract  4097  1000000000
```

Related Commands

Command	Description	Mode
`cp-bandwidth-contract`	This command configures a bandwidth contract traffic rate which can then be associated with a whitelist session ACL.	Enable or Config modes
`firewall cp`	This command creates a new whitelist ACL and can associate a bandwidth contract with that ACL.	Enable or Config modes

Command History

This command was introduced in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license.	Config mode on master controllers

show cpuload

```
show cpuload [current]
```

Description

Display the controller CPU load for application and system processes.

Syntax

Parameter	Description
`current`	Include this optional parameter at the request of Dell technical support to display additional CPU troubleshooting statistics.

Example

This example shows that the majority of the controller's CPU resources are not being used by either application (user) or system processes.

```
(host) #show cpuload
user 6.9%, system 7.7%, idle 85.4%
```

The output of this command includes the following parameters:

Parameter	Description
`user`	Percentage of controller CPU resources used by application processes.
`system`	Percentage of controller CPU resources used by system processes.
`idle`	Percentage of unused controller CPU resources.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show crypto dp

```
show
show crypto dp [peer <source-ip>]
```

Descriptions

Displays crypto data packets.

Syntax

Parameter	Description
dp	Shows crypto latest datapath packets. The output is sent to crypto logs.
peer <source-ip>	Clears crypto ISAKMP state for this IP.

Usage Guidelines

Use this command to send crypto data packet information to the controller log files, or to clear a crypto ISAKMP state associated with a specific IP address.

Examples

The command show crypto dp sends debug information to CRYTPO logs.

```
(host) # show crypto

Datapath debug output sent to CRYPTO logs.
```

Related Commands

Command	Description	Mode
crypto isakmp	Use this command to configure Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP)	Enable and Config modes

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show crypto dynamic-map

```
show crypto dynamic-map [tag <dynamic-map-name>]
```

Descriptions

Displays IPsec dynamic map configurations.

Syntax

Parameter	Description
`dynamic-map`	IPsec dynamic maps configuration.
`tag <dynamic-map-name>`	A specific dynamic map.

Usage Guidelines

Dynamic maps enable IPsec SA negotiations from dynamically addressed IPsec peers. Once you have defined a dynamic map, you can associate that map with the default global map using the command crypto map global-map.

Examples

The command **show crypto dynamic-map** shows IPsec dynamic map configuration.

```
(host) #show crypto dynamic-map

Crypto Map Template"default-dynamicmap" 10000
         lifetime: [300 - 86400] seconds, no volume limit
         PFS (Y/N): N
         Transform sets={ default-transform }
```

Related Commands

Command	Description	Mode
`crypto dynamic-map`	Use this command to configure a dynamic map.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show crypto ipsec

```
show crypto ipsec {mtu|sa[peer <peer-ip>]|transform-set [tag <transform-set-name>]}
```

Descriptions

Displays the current IPsec configuration on the controller.

Syntax

Parameter	Description
mtu	IPsec maximum mtu.
sa	Security associations.
peer <peer-ip>	IPsec security associations for a peer.
transform-set	IPsec transform sets.
tag <transform-set-name>	A specific transform set.

Usage Guidelines

The command **show crypto ipsec** displays the Maximum Transmission Unit (MTU) size allowed for network transmissions using IPsec security. It also displays the transform sets that define a specific encryption and authentication type.

Examples

The command **show crypto transform-set** shows the transform sets default-transform and default-ml-transform.

```
(host) #show crypto ipsec transform-set

Transform set default-transform: { esp-3des esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-ml-transform: { esp-3des esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
```

Related Commands

Command	Description	Mode
crypto ipsec	Use this command to configure IPsec parameters.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show crypto isakmp

```
show crypto isakmp {groupname}|{key}|{policy}|{sa[peer <peer-ip>]|stats}
```

Descriptions

This command displays Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Syntax

Parameter	Description
`groupname`	Show the IKE Aggressive group name.
`key`	Show the IKE pre-shared keys.
`policy`	Show the IKE configured policies.
`sa`	Show the security associations
`peer <peer-ip>`	Shows crypto isakmp security associations for this IP.
`stats`	Show the IKE statistics.

Usage Guidelines

Use the show crypto key command to view the IKE pre-shared keys.

Examples

The command **show crypto isakmp stats** shows the IKE statistics.

```
(host) #show crypto isakmp stats

Main Mode Initiator exchanges started/completed     = 0/0
Main Mode Responder exchanges started/completed     = 0/0
Aggr Mode Initiator exchanges started/completed     = 0/0
Aggr Mode Responder exchanges started/completed     = 0/0
Quick Mode Initiator exchanges started/completed    = 0/0
Quick Mode Responder exchanges started/completed    = 0/0
XAuth Type1 Responder exchanges started/completed   = 0/0
XAuth Type2 Responder exchanges started/completed   = 0/0
Mode-Config Responder exchanges started/completed   = 0/0
Phase1 SAs Current/Max/Total                        = 0/0/0
Phase2 SAs Current/Max/Total                        = 0/0/0
VPN Sessions Total/RAPs/Master-Local/Redundancy     = 0/0/0/0
VPN License Limits Total/Platform/Current/Violation = 16777215/16777215/0/0
Switch Role:                                          Master
CFGM triggers: Master/Local/Redund/Failed/Total     = 74682/0/0/0/74682
Redundancy changes: Master->Standby/Standby->Master = 0/0
FPAPPS TX messages: Tunnel-Up/Tunnel-Down           = 0/0
FPAPPS TX messages: cfg-map-add/cfg-map-del         = 0/0
FPAPPS TX messages: Peer-map-add/Peer-map-del       = 0/0
FPAPPS TX messages: SwitchIP-mapadd/SwitchIP-mapdel = 0/0
FPAPPS TX messages: New-SwitchIP-map-adds           = 0
Datapath To Control DPD Triggers Received           = 0
DPD Initiate Reqs-Sent/Re-Sent/Replies-Rcvd/Dropped = 0/0/0/0
```

Related Commands

Command	Description	Mode
`crypto isakmp`	Use this command to configure Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show crypto map

```
show crypto ipsec map
```

Descriptions

This command displays the IPsec map configurations.

Syntax

Parameter	Description
`map`	Show the IKE Aggressive group name.

Usage Guidelines

Use the show crypto map command to view configuration for global, dynamic and default map configurations.

Examples

The command **show crypto map** shows statistics for the global, dynamic and default maps.

```
(host) #show crypto map

Crypto Map "GLOBAL-MAP" 10000 ipsec-isakmp
Crypto Map Template"default-dynamicmap" 10000
         lifetime: [300 - 86400] seconds, no volume limit
         PFS (Y/N): N
         Transform sets={ default-transform }
Crypto Map "default-local-master-ipsecmap" 9999 ipsec-isakmp
Crypto Map Template"default-local-master-ipsecmap" 9999
         lifetime: [300 - 86400] seconds, no volume limit
         PFS (Y/N): N
         Transform sets={ default-ml-transform }
         Peer gateway: 0.0.0.0
         Interface: VLAN 0
         Source network: 0.0.0.0/0.0.0.0
         Destination network: 0.0.0.0/0.0.0.0
         Pre-Connect (Y/N): N
         Tunnel Trusted (Y/N): Y
```

Related Commands

Command	Description	Mode
`crypto map global-map`	Use this command to configure the default global map.	Config mode
`crypto dynamic-map`	Use this command to configure an existing dynamic map.	Config mode
`crypto map global-map`	Use this command to configure the default global map.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show crypto pki

```
show crypto pki csr
```

Descriptions

This command displays the certificate signing request (CSR) for the captive portal feature.

Syntax

Parameter	Description
`csr`	The certificate signing request.

Usage Guidelines

Use the **show crypto pki** command to view the CSR output.

Examples

The command **show crypto pki** shows output from the **crypto pki csr** command.

```
(host) #show crypto pki csr

Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=CA, L=Sunnyvale, O=sales, OU=EMEA,
CN=www.mycompany.com/emailAddress=myname@mycompany.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:e6:b0:f2:95:37:d0:18:c4:ee:f7:bd:5d:96:85:
                    49:a3:56:63:76:ee:99:82:fe:4b:31:6c:80:25:c4:
                    ed:c7:9e:8e:5e:3e:a2:1f:90:62:b7:91:69:75:27:
                    e8:29:ba:d1:76:3c:0b:14:dd:83:3a:0c:62:f2:2f:
                    49:90:47:f5:2f:e6:4e:dc:c3:06:7e:d2:51:29:ec:
                    52:8c:40:26:de:ae:c6:a0:21:1b:ee:46:b1:7a:9b:
                    dd:0b:67:44:48:66:19:ec:c7:f4:24:bd:28:98:a2:
                    c7:6b:fb:b6:8e:43:aa:c7:22:3a:b8:ec:9a:0a:50:
                    c0:29:b7:84:46:70:a5:3f:09
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        25:ce:0f:29:91:73:e9:cd:28:85:ea:74:7c:44:ba:b7:d0:5d:
        2d:53:64:dc:ad:07:fd:ed:09:af:b7:4a:7f:14:9a:5f:c3:0a:
        8a:f8:ff:40:25:9c:f4:97:73:5b:53:cd:0e:9c:d2:63:b8:55:
        a5:bd:20:74:58:f8:70:be:b9:82:4a:d0:1e:fc:8d:71:a0:33:
        bb:9b:f9:a1:ee:d9:e8:62:e4:34:e4:f7:8b:7f:6d:3c:70:4c:
        4c:18:e0:7f:fe:8b:f2:01:a2:0f:00:49:81:f7:de:42:b9:05:
        59:7c:e4:89:ed:8f:e1:3b:50:5a:7e:91:3b:9c:09:8f:b7:6b:
        98:80
-----BEGIN CERTIFICATE REQUEST-----
MIIB1DCCAT0CAQAwgZMxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTESMBAGA1UE
BxMJU3Vubnl2YWxlMQ4wDAYDVQQKEwVzYWxlczENMAsGA1UECxMERU1FQTEaMBgG
A1UEAxMRd3d3Lm15Y29tcGFueS5jb20xKDAmBgkqhkiG9w0BCQEWGXB3cmVkZHlA
YXJ1YmFuZXR3b3Jrcy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOaw
8pU30BjE7ve9XZaFSaNWY3bumYL+SzFsgCXE7ceejl4+oh+QYreRaXUn6Cm60XY8
CxTdgzoMYvIvSZBH9S/mTtzDBn7SUSnsUoxAJt6uxqAhG+5GsXqb3QtnREhmGezH
9CS9KJiix2v7to5DqsciOrjsmgpQwCm3hEZwpT8JAgMBAAGgADANBgkqhkiG9w0B
AQUFAAOBgQAlzg8pkXPpzSiF6nR8RLq30F0tU2TcrQf97Qmvt0p/FJpfwwqK+P9A
JZz0l3NbU80OnNJjuFWlvSB0WPhwvrmCStAe/I1xoDO7m/mh7tnoYuQ05PeLf208
cExMGOB//ovyAaIPAEmB995CuQVZfOSJ7Y/hO1BafpE7nAmPt2uYgA==
-----END CERTIFICATE REQUEST-----
```

Related Commands

Command	Description	Mode
`crypto pki`	Use this command to generate a certificate signing request (CSR) for the captive portal feature.	Enable mode
`crypto pki-import`	Use this command to import certificates for the captive portal feature.	Enable mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show crypto-local ipsec-map

```
show crypto-local ipsec [tag <ipsec-map-name>]
```

Description

Displays the current IPsec map configuration on the controller.

Syntax

Parameter	Description
`tag <ipsec-map-name>`	Display a specific IPsec map.

Usage Guidelines

The command **show crypto-local ipsec** displays the current IPsec configuration on the controller.

Examples

The command **show crypto-local ipsec-map** shows the default map configuration along with any specific IPsec map configurations.

```
(host) #show crypto-local ipsec-map

Crypto Map Template"default-local-master-ipsecmap" 9999
         lifetime: [300 - 86400] seconds, no volume limit
         PFS (Y/N): N
         Transform sets={ default-ml-transform }
         Peer gateway: 0.0.0.0
         Interface: VLAN 0
         Source network: 0.0.0.0/0.0.0.0
         Destination network: 0.0.0.0/0.0.0.0
         Pre-Connect (Y/N): N
         Tunnel Trusted (Y/N): Y
         Forced NAT-T (Y/N): N
Crypto Map Template"testmap" 3
         lifetime: [300 - 86400] seconds, no volume limit
         PFS (Y/N): N
         Transform sets={ default-transform }
         Peer gateway: 0.0.0.0
         Interface: VLAN 0
         Source network: 0.0.0.0/0.0.0.0
         Destination network: 0.0.0.0/0.0.0.0
         Pre-Connect (Y/N): N
         Tunnel Trusted (Y/N): N
         Forced NAT-T (Y/N): N
```

Related Commands

Command	Description	Mode
`crypto-local ipsec-map`	Use this command to configure IPsec mapping for site-to-site VPN.	Config mode

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show crypto-local isakmp

```
show crypto isakmp {ca-certificates}|{dpd}|{key}|{server-certificate}|{xauth}
```

Descriptions

This command displays Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Syntax

Parameter	Description
`ca-certificates`	Shows all the Certificate Authority (CA) certificate associated with VPN clients.
`dpd`	Shows the IKE Dead Peer Detection (DPD) configuration on the local controller.
`key`	Shows the IKE preshared key on the local controller for site-to-site VPN. This is includes keys configured by Fully Qualified Domain Name (FQDN) and local and global keys configured by address.
`server-certificate`	Shows all the IKE server certificates used to authenticate the controller for VPN clients.
`xauth`	Shows the IKE XAuth configuration for VPN clients.

Usage Guidelines

Use the **show crypto-local isakmp** command to view IKE parameters.

Examples

This example shows sample output for the **show crypto-local ca-certificate**, **show crypto-local dpd**, **show crypto-local key**, **show crypto-local server-certificate** and **show crypto-local xauth** commands .

```
(host) #show crypto-local isakmp ca-certificate
ISAKMP CA Certificates
----------------------
CA certificate name  Client-VPN  # of Site-Site-Maps
-------------------  ----------  -------------------


(host) #show crypto-local isakmp dpd
DPD is Enabled: Idle-timeout = 22 seconds, Retry-timeout = 2 seconds, Retry-attempts = 3


(host) #show crypto-local isakmp key
ISAKMP Local Pre-Shared keys configured by FQDN
-----------------------------------------------

FQDN of the host  Key
----------------  ---

ISAKMP Local Pre-Shared keys configured by FQDN
-----------------------------------------------

FQDN of the host  Key
----------------  ---

ISAKMP Local Pre-Shared keys configured by Address
--------------------------------------------------
IP address of the host  Subnet Mask Length  Key
----------------------  ------------------  ---

ISAKMP Global Pre-Shared keys configured by Address
---------------------------------------------------

IP address of the host  Subnet Mask Length  Key
----------------------  ------------------  ---


(OAW-4324) #show crypto-local isakmp server-certificate
ISAKMP Server Certificates
--------------------------
Server certificate name  Client-VPN  # of Site-Site-Maps
-----------------------  ----------  -------------------


(host) #show crypto-local isakmp xauth
IKE XAuth Enabled
```

Related Commands

Command	Description	Mode
`crypto-local isakmp ca-certificate`	Use this command to assign the Certificate Authority (CA) certificate used to authenticate VPN clients.	Config mode
`crypto-local isakmp dpd`	Use this command to configure IKE Dead Peer Detection (DPD) on the local controller.	Config mode
`crypto-local isakmp key`	Use this command to configure the IKE preshared key on the local controller for site-to-site VPN.	Config mode
`crypto-local isakmp server-certificate`	Use this command to assign the server certificate used to authenticate the controller for VPN clients.	Config mode
`crypto-local isakmp xauth`	Use this command to enable the IKE XAuth for VPN clients.	Config mode

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show crypto-local pki

```
show crypto pki {PublicCert|ServerCert|TrustedCA} <name> <filename>
```

Descriptions

This command displays imported certificate information.

Syntax

Parameter	Description
`PublicCert <name>`	Shows Public key information of a certificate. This certificate allows an application to identify an exact certificate.
`ServerCert <name>`	Shows Server certificate information. This certificate must contain both a public and a private key (the public and private keys must match). You can import a server certificate in either PKCS12 or x509 PEM format; the certificate is stored in x509 PEM DES encrypted format on the controller.
`TrustedCA <name>`	Shows trusted CA certificate information.This certificate can be either a root CA or intermediate CA. Dell encourages (but does not require) an intermediate CA's signing CA to be the controller itself.

Usage Guidelines

Use the **show crypto-local pki** command to view the name, original filename and reference count for an imported public, server or trusted CA certificates.

Example

This example displays information about an imported Server certificate. Both the Public and Trusted Ca certificate parameters display similar information.

```
(host) (config) #show crypto-local pki serverCert

Name(total=1)   Original Filename       Reference Count
==============  =================       ===============
sialdevice              2400a.pem                       1
```

Related Commands

Command	Description	Mode
`crypto-local pki`	This command is saved in the configuration file and verifies the presence of the certificate in the controller's internal directory structure.	Enable mode

Command History

This command was introduced in ArubaOS 3.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode.

show database

```
show database synchronization
```

Description

Shows database synchronization status.

Syntax

No parameters.

Usage Guidelines

Issue this command to show the status database synchronization status.

Example

This example shows a database synchronization status.

```
(host) #show database synchronize

Last synchronization time: Not synchronized since last reboot

Periodic synchronization is enabled and runs every 25 minutes
Synchronization includes RF plan data
```

Related Commands

Command	Description	Mode
`database synchronize`	Show the output of the database synchronize command.	Enable and Config modes

Command History

Release	Modification
ArubaOS 3.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master and local controllers

show datapath

```
show
   acl id <id-name> {ap-name <ap-name>}|{ip-addr <ip-address>}
   application {ap-name <ap-name>|counters|ip-addr <ip-address>}
   bridge {ap-name <ap-name>|counters|ip-addr <ip-address>|table}
   bwm table
   crypto counters
   debug {dma counters|trace-buffers}
   esi table
   frame {ap-name <ap-name>|counters|ip-addr <ip-address>}
   hardware {counters|statistics}
   ip-reassembly {ap-name <ap-name>|counters|ip-addr <ip-address>}
   lag table
   maintenance counters
   message-queue counters
   nat {ap-name <ap-name>|counters|ip-addr <ip-address>}
   port table
   route {ap-name <ap-name>|counters|ip-addr <ip-address>][table]}
   route-cache {ap-name <ap-name>|counters|ip-addr <ip-address>|table}
   services
   session {ap-name <ap-name>|counters}|{ip-addr <ip-address>|table}
   station [counters|mac <macaddr>|table]
   tcp {app <app>|counters|tunnel}
   tunnel [counters|table]
   user {ap-name <ap-name>|counters|ip-addr <ip-address>|table}
   utilization
   vlan {ap-name <ap-name>}|{ip-addr <ip-address>|table}
   wifi-reassembly counters
   wmm counters
```

Descriptions

Displays system statistics for your controller.

Syntax

Parameter	Description
`acl id <id-name>`	Displays datapath statistics associated with a specified ACL. The ACL index is found in the **show rights** command.
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-address>`	IP address of the AP
`application counters`	Shows application counters and errors generated by applications running on a particular AP. These include stateful firewall application layer statistics.
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-address>`	IP address of the AP.
`bridge`	Shows bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for an AP.
`ap-name <ap-name>`	Name of the AP. Shows MAC address, VLAN, assigned VLANs, destination and flags information.
`counters`	Shows datapath bridge table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures and max link length.
`ip-addr <ip-address>`	IP address of the AP. Shows MAC address, VLAN, assigned VLANs, destination and flags information.
`table <macaddr>`	Displays the current high, maximum, and total number of bridge table entries for the Dell controller.
`bwm table`	Shows bandwidth management table entry statistics such as CPU, contract, Bits/sec, policed, available bytes, queued bytes and packets.
`crypto counters`	Displays crypto parameter statistics including crypto, IPSEC, PPTP, WEP, TKIP, AESCCM, WEP CRC, crypto hardware , XSEC, DOT1X and L2TP information.
`debug`	Displays datapath debug details. These are low-level datapath details.
`dma counters`	DMA counters are displayed.
`trace-buffers`	Debug trace-buffer tables are displayed.
`esi table`	Displays the contents of the datapath ESI server table entries including server, IP, MAC, destination, VLAN, type, session and flag information.
`frame counters`	Displays frame statistics that are received and transmitted from the datapath of the controller.
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-address>`	IP address of the AP.
`hardware`	Displays datapath hardware counters and hardware packet statistics information.
`counters`	Hardware counters.
`statistics`	Hardware packet statistics.
`ip-reassembly`	Displays the contents of the IP Reassembly statistics table.
`ap-name <ap-name>`	Name of the AP.
`counters`	IP reassembly counters.
`ip-addr <ip-address>`	IP address of the AP
`lag table`	Displays contents of the datapath link aggregation group (LAG) or port channel table.

Parameter	Description
`maintenance counters`	Displays datapath maintenance statistics.
`message-queue counters`	Displays statistics of messages received by a CPU from other datapath CPUs (only CPUs that receive messages and non-zero statistics are shown).
`nat`	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.
`ap-name <ap-name>`	Name of AP.
`counters`	Nat counters.
`ip-addr <ip-address>`	IP address of the AP.
`port table`	Displays the datapath port-vlan untrusted status and table session entries.
`untrusted-vlan <slot/port>`	Show if there are untrusted vlan entries for the indicated slot and port.
`vlan-table <slot/port>`	Displays the VLAN and its corresponding Session ACL for a particular slot and port.
`route`	Displays datapath route table statistics.
`ap-name <ap-name>`	Name of the AP.
`counters`	Displays route table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures and max link length.
`ip-addr <ip-address>`	Address of IP.
`table`	Displays route table entries such as IP, mask, gateway, cost, VLAN and flags.
`verbose`	Displays all detailed route table entries including IP, mask, gateway, cost, VLAN, flags, Internal VerNum Index.
`route-cache`	Displays datapath route cache table statistics.
`ap-name <ap-name>`	Name of the AP.
`counters`	Displays route cache table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures and max link length.
`ip-addr <ip-address>`	Address of IP.
`table`	Displays route cache table entries such as IP, mask, gateway, cost, VLAN and flags.
`verbose`	Displays all detailed route cache table entries including IP, mask, gateway, cost, VLAN, flags, Internal VerNum Index.
`services`	Displays the datapath services table statistics including protocol, port and service.
`session`	Displays datapath session statistics
`ap-name <ap-name>`	Name of AP
`counters`	Displays counters statistics including current entries, high water mark, maximum entries, total entries, allocation failures, duplicate entries, cross linked entries, number of reverse entries and maximum link length.
`ip-addr <ip-address>`	Address of IP
`table`	Displays all the IP flows of a wireless device or Dell AP. Statistics include table entries including source IP, destination IP, protocol, SPort, DPort, Cntr, priority, ToS, age, destination, TAge and flags.
`station`	Displays datapath station association table statistics.

Parameter	Description
counters	Display the current and high water mark amount of 802.11 associated wireless devices on an Dell controller. Values output from this command represent the water-marks since the last boot of the controller. This is the same value obtainable from the Num Associations output from the show stm connectivity command.
mac <macaddr>	Hardware address, in hexadecimal format.
tcp	Displays contents of the tcp tunnel table. This command displays all tcp tunnels that are terminated by the controller,
app <app>	Name of the application.
counters	Displays the tcp tunnel statistics.
tunnel	Displays the tcp tunnel table.
table	This command displays the Datapath Station Table Statistics detail. Display all associated wireless devices on the Dell controller with their corresponding AP BSSID and VLAN ID. Displays the wireless device is associated with the correct encryption type (if the device is associated to an AP BSSID that has encryption enabled and verifies whether the Dell controller is having a problem in decrypting the wireless device's frames.
tunnel	Displays contents of the datapath tunnel table. This command displays all the tunnels that are terminated by the controller, including Dell APs' GRE tunnels. For example, a GRE tunnel is created and terminated on the Dell controller for every SSID/BSSID configured on the Dell AP.
counters	Tunnel counters.
table	Tunnel 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.
ap-name <ap-name>	Name of AP.
counters	User counters.
ip-addr <ip-address>	IP address of the AP.
table	User table statistics.
utilization	Displays the current CPU utilization of all datapath CPUs.
vlan	Displays VLAN table information such as VLAN memberships inside the datapath including L@ tunnels which tunnel L2 traffic.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-address>	IP address of AP.
table	Displays VLAN number, flag, port and datapath VLAN multicast entries.
wifi-reassembly counters	Displays wifi reassembly counters including CPU, current entries, high water-mark, maximum entries, total entries and allocation failures.
wmm counters	Displays VOIP statistics including the number of uplink and downlink resets.

Usage Guidelines

Use the **show datapath** command to display various datapath statistics for debugging purposes.

Example

In this example, the show datapath user counters command displays datapath user table statistics. .

```
(host) #show datapath user counters

Datapath User Table Statistics
------------------------------
Current Entries      2
Pending Deletes      0
High Water Mark      2
Maximum Entries      8191
Total Entries        143
Allocation Failures  0
Invalid Users        0
Max link length      1
```

Command History

Version	Description
ArubaOS 3.0	Command introduced
ArubaOS 5.0	The **tcp** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show destination

```
show destination <string>
```

Description

Display the aliases for default and user-defined network destinations.

Syntax

Parameter	Description
`string`	Optional parameter to view details of a specific destination alias.

Example

This example displays the network destinations configured in the controller.

```
(host) #show destination
controller
----------
Position  Type  IP addr      Mask/Range
--------  ----  -------      ----------
1         host  10.16.15.1

user
----
Position  Type     IP addr           Mask/Range
--------  ----     -------           ----------
1         network  255.255.255.255   0.0.0.0

mswitch
-------
Position  Type  IP addr      Mask/Range
--------  ----  -------      ----------
1         host  10.16.15.1

any
---
Position  Type     IP addr   Mask/Range
--------  ----     -------   ----------
1         network  0.0.0.0   0.0.0.0
```

The output of this command includes the following parameters:

Parameter	Description
`Position`	Displays the priority position of the alias.
`Type`	The rule type of the destination alias.
`IP addr`	The IP address configured in the alias. This can be a network address, host address or a range.
`Mask/Range`	Network mark or the IP address range.

Command History

This command was available in ArubaOS 1.0.

Replaced with `netdestination` in 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	You must have a PEFNG license to configure or view a destination.	Enable or Config mode on master and local controllers

show dialer group

```
crypto-local
   show dialer group
```

Description

Display dialer group information.

Syntax

No parameters.

Usage Guidelines

Displays the Dialer Group Table with the current dialing parameters.

Example.

```
(host) #show dialer group
Dialer Group Table
------------------
Name     Init String                       Dial String
----     -----------                       -----------
evdo_us  ATQ0V1E0                          ATDT#777
gsm_us   AT+CGDCONT=1,"IP","ISP.CINGULAR"  ATD*99#
```

Command History

Introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
Aruba 600 controllers	Base operating system	Config mode on master and local controllers

show dir

```
crypto-local
show dir usb: disk <disk-name><filesystem-path>
```

Description

Display the list of directories in the specified disk and the filesystem path.

Syntax

Parameter	Description
<disk-name>	Name of the USB device. If you do not know the name of the USB disk, issue the command **show usb-storage** to view a list of device names.
<filesystem-path>	The USB file system path.

Example

The command below displays the USB directory list for a device named **SEGATE-HJ1235_p1**.

```
(host) #(show dir usb: SEGATE-HJ1235_p1/docs

USB directory list
------------------
Permission     Size   Time Stamp    Directory Name
----------     ----  -------------- --------------
drwxr-xr-x      0     May 13 09:39  samba
```

The output of this command includes the following parameters:

Parameter	Description
Permission	Read, write and execute permissions for the directory.
Size	Size of the directory.
Time Stamp	Date and time that the directory was last modified.
Directory Name	Name of the directory on the USB device.

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
Aruba 600 controllers	Base operating system	Config mode on master and local controllers

show dot1x ap-table

```
show dot1x ap-table
```

Description

Shows the 802.1x AP table.

Syntax

No parameters.

Example

Issue this command to display details from the AP table.

```
AP Table
--------
MAC               IP         Essid       Type AP name           Vlan Enc          Stations Forwarding-
Mode       Profile         Acl
---               --          -----       ---- -------           ---- ---          --------- ---------
------       -------          ---
00:1a:1e:87:ff:c0 10.3.9.242              AP   00:1a:1e:c0:7f:fc 0    -            0
```

The output of this command includes the following parameters:

Parameter	Description
`MAC`	The MAC address of the AP
`IP`	The IP address of the AP
`Essid`	The AP's ESSID
`Type`	Device type
`AP name`	Name of the AP
`Vlan`	Number of VLANs associated with the specified AP
`Enc`	AP's encryption method
`Stations`	Number of stations associated with the specified AP
`Forwarding Mode`	Forwarding mode used by the specified AP
`Profile`	AP profile
`Acl`	Number of ACLs this AP belongs to

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show dot1x ap-table aes

```
show dot1x ap-table aes
```

Description

Shows the AES keys of all APs.

Syntax

No parameters.

Example

Issue this command to display AES keys of all APs.

```
AP Table Showing AES Keys
-------------------------
AP-MAC             GTK/Size/Slot
------             -------------
00:1a:1e:87:ff:d0  * * * * * * * */128-Bit/1
00:1a:1e:87:ff:d1  * * * * * * * */128-Bit/1
```

The output of this command includes the following parameters:

Parameter	Description
`AP-MAC`	AP MAC address
`GTK/Size/Slot`	GTK: The group temporal key Size: Size of the AES key Slot: Slot number

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show dot1x ap-table dynamic-wep

```
show dot1x ap-table dynamic-wep
```

Description

Shows the dynamic WEP keys of all APs.

Syntax

No parameters.

Example

Issue this command to display dynamic keys of all APs.

```
Dynamic-WEP Key Information
---------------------------
AP-MAC  Key1/Size/Slot  Key2/Size/Slot
------  --------------  --------------
Num APs: 0
```

The output of this command includes the following parameters:

Parameter	Description
`AP-MAC`	AP MAC address
`Key1/Size/Slot`	Key1: The WEP key Size: Size of the WEP key Slot: Slot number
`Key12/Size/Slot`	Key2: The WEP key Size: Size of the WEP key Slot: Slot number

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show dot1x ap-table static-wep

```
show dot1x ap-table static-wep
```

Description

Shows the static WEP keys of all APs.

Syntax

No parameters.

Example

Issue this command to display the static WEP keys of all APs

```
Static-WEP Key Information
--------------------------
AP-MAC  Key1/Size  Key2/Size  Key3/Size  Key3/Size
------  ---------  ---------  ---------  ---------
```

The output of this command includes the following parameters:

Parameter	Description
AP-MAC	AP's MAC address
Key1/Size	WEP key 1 and its size
Key2/Size	WEP key 2 and its size
Key3/Size	WEP key 3 and its size
Key3/Size	WEP key 3 and its size

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show dot1x ap-table tkip

```
show dot1x ap-table tkip
```

Description

Displays a table of TKIP keys on the controller.

Syntax

No parameters.

Example

Issue this command to display all TKIP keys.

```
AP Table Showing TKIP Keys
--------------------------
AP-MAC             GTK/Size/Slot
------             -------------
00:1a:1e:6f:e5:10  * * * * * * * */256-Bit/1
Num APs: 1
```

The output of this command includes the following parameters:

Parameter	Description
AP-MAC	AP MAC Address
GTK/Size/Slot	GTK: The group temporal key Size: Size of the AES key Slot: Slot number

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show dot1x counters

```
show dot1x counters
```

Description

Displays a table of dot1x counters.

Example

Issue this command to display all dot1x count information.

```
 802.1x Counters

AP
 Sync Request..................4
 Sync Response.................3
 Up............................4
 Down..........................1
 Resps.........................4
 Acl...........................53
Station
 Sync Request..................9
 Sync Response.................9
 Up............................2321
 Down..........................2272
 Unknown.......................72
EAP
 RX Pkts.......................4811
 Dropped Pkts..................4497
 TX Pkts.......................5253
WPA
 Message-1.....................2484
 Message-2.....................63
 Message-3.....................63
 Message-4.....................63
 Group Message-1...............63
 Group Message-2...............63
 Rx Failed.....................2418
 IE Mismatches.................4836
 Key Exchange Failures.........602
WPA2
 Message-1.....................2630
 Message-2.....................13
 Message-3.....................13
 Message-4.....................13
 Rx Failed.....................2079
 IE Mismatches.................4158
 Key Exchange Failures.........549
Radius
```

The output of this command includes the following parameters:

Parameter	Description
AP • `Sync Request` • `Sync Response` • `Up` • `Down` • `Resps` • `Acl`	 • Number of sync requests sent • Number of sync responses sent • Number of times an AP has come up • Number of times an has gone down • Number of response messages sent to the AP due to an AP up message • Number of access control lists

Parameter	Description
Station • Sync Request • Sync Response • Up • Down • Unknown	• Number of sync requests sent to find all APs and stations that are connected • Number of sync responses received • Number of times a station (any station) connected to the AP • Number of times a station (any station) disconnected from the AP • Number of times a station attempted to start an EAP exchange before associating to an AP. In other words, the number of times the auth module saw the start of an EAP exchange before auth was notified that a station has associated an AP
EAP • RX Pkts • Dropped Pkts • TX Pkts	• Number of EAP packets received • Number of EAP packets dropped (ignored) for any reason, such as bad packet, length, EAP ID mismatch, etc. • Number of EAP packets sent
WPA • Message-1 • Message-2 • Message-3 • Message-4 • Group Message-1 • Group Message-2 • Rx Failed • IE Mismatches • Key Exchange Failures	• Number of WPA message-1s sent • Number of WPA message-2s sent • Number of WPA message-3s sent • Number of WPA message-4s sent • Number of WPA group message-1s sent • Number of WPA group message-2s sent • Number of WPA related EAP packets dropped for any reason • Number of WPA related EAP packets dropped because the station and controller have a different perception of what the connection details are • Number of key exchange failures
WPA2 • Message-1 • Message-2 • Message-3 • Message-4 • Rx Failed • IE Mismatches • Key Exchange Failures	• Number of WPA2 message-1s sent • Number of WPA2 message-2s sent • Number of WPA2 message-3s sent • Number of WPA2 message-4s sent • Number of WPA2 related EAP packets dropped for any reason • Number of WPA2 related EAP packets dropped because the station and controller have a different perception of what the connection details are • Number of key exchange failures
Radius • Accept	• Number of RADIUS accepts
Station Deauths	Number of stations deaths

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show dot1x supplicant-info

```
show dot1x supplicant-info <supplicant-mac> <ap-mac>
```

Description

Shows the details about a specific supplicant.

Example

Issue this command to display the details about a supplicant

```
Name                                MYCORPNETWORKS\ccutler
MAC Address                         00:19:7e:a9:8e:b0
AP MAC Address                      00:1a:1e:11:5f:11
Status                              Authentication Success
Unicast Cipher                      WPA2-AES
Multicast Cipher                    WPA2-AES
EAP-Type                            EAP-PEAP

Packet Statistics:
EAPOL Starts                        0
EAP ID Requests                     0
EAP ID Responses                    0
EAPOL Logoffs from station          0
EAP pkts to the station             2
EAP pkts from station               2
Unknown EAP pkts from station       0
EAP Successes sent                  0
EAP Failures sent                   0
Station failed to respond           0
Station NAKs                        0
Radius pkts to the server           0
Radius pkts from the server         0
Server failed to respond            0
Server rejects                      0
WPA/WPA2-Key Message1               1
WPA/WPA2-Key Message2               1
WPA/WPA2-Key Message3               1
WPA/WPA2-Key Message4               1
WPA-GKey Message1                   0
WPA-GKey Message2                   0
ID of the last EAP request          0
Length of the last EAP request      151
ID of the last EAP response         0
Length of the last EAP response     0
ID of the last radius request       0
Length of the last radius request   0
ID of the last radius response      0
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Supplicant name.
`MAC Address`	Supplicant MAC address.
`AP MAC Address`	AP MAC address.
`Status`	Supplicant's status.
`Unicast Cipher`	Supplicant's unicast cipher.
`Multicast Cipher`	Supplicant's multicast cipher.

Parameter	Description
EAP-Type	Supplicant's EAP-Type.
EAPOL Starts	Number of EAPOL starts.
EAP ID Requests	Number of EAP ID requests.
EAP ID Responses	Number of EAP ID responses.
EAPOL Logoffs from station	Number of EAPOL logoffs from the station.
EAP pkts to the station	Number of EAP packets sent to the station.
EAP pkts from station	Number of EAP packets sent from the station.
Unknown EAP pkts from station	Number of unknown EAP packets sent from the station.
EAP Successes sent	Number of EAP successes sent.
EAP Failures sent	Number of EAP failures sent.
Station failed to respond	Number of times the station failed to respond.
Station NAKs	Number of station negative-acknowledgement characters.
Radius pkts to the server	Number of radius packets set to the server.
Radius pkts from the server	Number of radius packets sent from the server.
Server failed to respond	Number of times the server failed to respond.
Server rejects	Number of times ac connection was rejected by the server.
WPA/WPA2-Key Message1	Number of WPA message-1s sent.
WPA/WPA2-Key Message2	Number of WPA message-2s sent.
WPA/WPA2-Key Message3	Number of WPA message-3s sent.
WPA/WPA2-Key Message4	Number of WPA message-4s sent.
WPA-GKey Message1	Number of WPA group message-1s sent.
WPA-GKey Message2	Number of WPA group message-2s sent.
ID of the last EAP request	The ID of the last EAP request.
Length of the last EAP request	The length of the last EAP request.
ID of the last EAP response	The ID of the last EAP response.
Length of the last EAP response	The length of the last EAP response.
ID of the last radius request	The ID of the last radius request.
Length of the last radius request	The length of the last radius request.

Parameter	Description
`ID of the last radius response`	The ID of the last radius response.
`Length of the last radius response`	The length of the last radius response.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show dot1x supplicant-info list-all

```
show dot1x supplicant-info list all
```

Description

Shows all 802.1x supplicants.

Syntax

No parameters.

Example

Issue this command to display all 802.1x supplicants as well as additional relevant information.

```
802.1x User Information
-----------------------
     MAC              Name     Auth  AP-MAC               Enc-Key/Type              Auth-Mode     EAP-
Type  Remote
------------       --------  ----  ------             -------------------       ------------   -----
----  ------
```

The output of this command includes the following parameters:

Parameter	Description
MAC	Supplicant MAC address
Name	Supplicant name
Auth	Shows if the supplicant authenticated successfully
AP-MAC	AP MAC address
Enc-Key/Type	Enc-Key: Supplicant's encryption key Type: Encryption type used by the supplicant
Auth-Mode	Authentication mode
EAP-Type	EAP type
Remote	Is the supplicant remote

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show dot1x supplicant-info pmkid

```
show dot1x supplicant-info pmkid <supplicant-mac>
```

Description

Shows the PMKIDs of the various stations on the controller.

Syntax

No parameters.

Example

Issue this command to display the PMKIDs of the various stations on the controller.

```
PMKID Table
 -----------
 Mac                Name           AP                PMKID
 ---                ----           --                -----
 00:03:7f:bf:12:ac  zoobar22  00:0b:86:a0:57:60  c2:7d:12:1a:1c:5b:40:f8:89:46:22:a5:ec:9b:fb:a6
 00:03:7f:bf:12:ac  zoobar22  00:0b:86:c0:04:88  bb:2d:e1:57:e1:b8:9b:a2:71:f5:98:ad:61:db:47:e7
```

The output of this command includes the following parameters:

Parameter	Description
MAC	Supplicant MAC address
Name	Supplicant name
AP	AP MAC address
PMKID	Station PMKID

Command History

This command was introduces in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show dot1x supplicant-info statistics

```
show dot1x supplicant-info statistics
```

Description

Shows the 802.1x statistics of the users.

Syntax

No parameters.

Example

Issue this command to display the 802.1x statistics of the users.

```
 802.1x Statistics
-----------------
Mac               Name   AP               Auth-Succs  Auth-Fails  Auth-Tmout  Re-Auths  Supp-Naks
UKeyRotations  MKeyRotations
---               ----   --               ----------  ----------  ----------  --------  ---------
-------------  -------------
```

The output of this command includes the following parameters:

Parameter	Description
MAC	Supplicant MAC address.
Name	Supplicant name.
AP	AP MAC address.
Auth-Succs	Number of successful authentications.
Auth-Fails	Number of authentication failures.
Auth-Tmout	Number of authentication timeouts.
Re-Auths	Number of reauthentications.
Supp-Naks	Number of negative-acknowledgement characters sent by the supplicant.
UKeyRotations	Number of unicast key rotations.
MKeyRotations	Number of multicast key rotations.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show esi groups

```
show esi groups [{group-name <groupname>|{ping-name <ping-name>}]
```

Description

Show ESI group information.

Syntax

Parameter	Description
group-name <groupname>	View the facility used when logging messages into the remote syslog server.
ping-name <ping-name>	Enter the name of a set of ping values to how the names of ESI groups using that set of ping attributes. Define a set of ESI ping values using the command `esi ping`.
server	Show the IP address of a remote logging server.

Usage Guidelines

The ESI parser is a mechanism for interpreting syslog messages from third party appliances such as anti-virus gateways. Use this command to view configured ESI server groups.

Example

This example below displays the name of each configured ESI group, including its ping definitions and ESI server.

```
(host) #show esi groups

ESI Group Table
---------------
Name       Tunnel ID  Ping      Flags  Servers
----       ---------  ----      -----  -------
anything   0x1042     pingset_1 C      0
cupertino  0x1043     -         C      0
Flags:
  C:Datapath Download complete
```

Related Commands

Platforms	Licensing	Command Mode
`esi group`	This command configures an ESI group.	Config mode on master or local controllers.
`esi ping`	This command specifies the ESI ping health check configuration.	Config mode on master or local controllers.
`esi server`	This command configures an ESI server.	Config mode on master or local controllers.

Command History

This command was introduced in ArubaOS 2.5.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show esi parser

```
show esi parser domains|rules|stats
```

Description

Show ESI parser information.

Syntax

Parameter	Description
domains	Show ESI parser domain information.
rules	Show ESI parser rule information.
stats	Show ESI parser rule stats.

Usage Guidelines

The ESI parser is a generic syslog parser on the controller that accepts syslog messages from external third-party appliances such as anti-virus gateways, content filters, and intrusion detection systems. It processes syslog messages according to user-defined rules and takes configurable actions on the corresponding system users.

ESI servers are configured into domains to which ESI syslog parser rules are applied.

Use the **`show esi parser domains`** command to show ESI parser domain information.

Example

The ESI Parser Domain Table in the example below shows that the controller has two ESI domains and two ESI servers.

```
(host) #show esi parser domains

ESI Parser Domain Table
-----------------------
Domain         ESI Servers   Peer Controllers
------         -----------   ----------------
corp_domain    172.21.5.50   10.3.132.14
remote_domain  192.84.66.30

Total number of servers configured: 2
```

Related Commands

Platforms	Licensing	Command Mode
`esi parser domain`	This command configures an ESI syslog parser domain.	Config mode on master or local controllers.
`esi parser rule`	This command creates or changes an ESI syslog parser rule.	Config mode on master or local controllers.
`esi parser rule-test`	This command allows you to test all of the enabled parser rules.	Config mode on master or local controllers.

Command History

This command was introduced in ArubaOS 3.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show esi ping

```
show esi ping [ping-name <ping-name>]
```

Description

Show settings for ESI ping health check attributes.

Syntax

Parameter	Description
ping-name <ping-name>	Include the optional **ping-name <ping-name>** parameters to display settings for one specified set of ping settings.

Example

This example below shows that the controller has three defined sets of ping attributes.

```
(host) #show esi groups

ESI Ping Table
--------------
Name        Frequency (sec)  Timeout (sec)  Retry Count  ID  Num Groups
----        ---------------  -------------  -----------  --  ----------
ping_att1   5                2              2            0   1
ESIping     5                2              2            1   0
ESIping2    50000            2              2            2   2
```

The output of this command includes the following information:

Column	Description
Name	Name of a group of ping settings.
`frequency`	Specifies the ping frequency in seconds.
`timeout`	Specifies the ping timeout in seconds.
`retry-count`	Specifies the ping retry count
ID	ID number assigned to the ping attributes when that set of attributes was defined.
Num Groups	Number of ESI groups to which this set of ping attributes is assigned.

Related Commands

Platforms	Licensing	Command Mode
`esi ping`	This command specifies the ESI ping health check configuration.	Config mode on master or local controllers.

Command History

This command was introduced in ArubaOS 2.5.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show esi servers

```
show esi servers [{group-name <groupname>|{server-name <server-name>}]
```

Description

Show configuration information for ESI servers.

Syntax

Parameter	Description
group-name <groupname>	Include this optional parameter to display information for all ESI servers assigned to a specific ESI group.
server-name <server-name>	Specify an ESI server name to view configuration information for just that server.

Usage Guidelines

By default, this command displays configuration settings for all ESI servers. You can include the name of an ESI group to view servers assigned to just that group, or specify a server name to view information for that server only.

Example

This example below displays configuration details for the ESI server name **forti_1**.

```
(host) #show esi servers server-name forti_1

ESI Server Table
----------------
Name     Trusted IP    Untrusted IP  Trusted s/p  Untrusted s/p  Group   Mode   NAT Port  ID  Flags
----     ----------    ------------  -----------  -------------  -----   ----   --------  --  -----
forti_1  10.168.173.2  10.168.171.3  -/-          -/-            default route  0         4   U
Flags:
  C :Datapath Download complete
  U :Server Up
  D :Server Down
  PT:Trusted Ping response outstanding
  PU:Untrusted Ping response outstanding
  HT:Health Check Trusted IP
  HU:Health Check Untrusted IP
  FT:Trusted Ping failed
  FU:Untrusted Ping failed
```

The output of this command includes the following information:

Column	Description
Name	Name of the ESI server.
Trusted IP	Displays the server IP address on the trusted network. As an option, you can also enable a health check on the specified address
Untrusted IP	Displays the server IP address on the untrusted network. As an option, you can also enable a health check on the specified address
Trusted s/p	Shows the slot and port connected to the trusted side of the ESI server; slot/port format.
Untrusted s/p	Shows the slot and port connected to the untrusted side of the ESI server.
Group	Name of the ESI group to which this server is assigned. If the server has not yet been assigned to a group, this column will be blank.
Mode	Specifies the ESI server mode of operation: bridge, nat, or route

Column	Description
Nat Port	Displays the NAT destination TCP/UDP port.
ID	ID number assigned to the server when it was first defined.
Flags	This data column displays any flags associated with this server. The flag key appears below the ESI Server Table.

Related Commands

Platforms	Licensing	Command Mode
esi server	This command configures an ESI server.	Config mode on master or local controllers.

Command History

This command was introduced in ArubaOS 2.5.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show faults

```
show fault [history]
```

Description

Display a list of faults, which are any problematic conditions of the ArubaOS software or hardware.

Syntax

Parameter	Description
history	Include this parameter to display a history of faults cleared by the controller or the operator.

Usage Guidelines

A controller can maintain a list of up to 100 faults. Once 100 faults have been logged, any faults arising after that are dropped. The controller maintains a history of the last 100 faults that have cleared. Every time a new fault clears clear, the oldest fault in the fault history is purged from the list.

Example

This example below shows all active faults the controller, including the time the fault occurred, the fault ID number, and a description of the problem.

```
(host) #show firewall

Active Faults
-------------
Time                 Number  Description
----                 ------  -----------
2009-03-02 18:13:08  93      Authentication Server vortex is down.
2009-03-02 18:13:08  94      Authentication Server vortex is down.
2009-03-02 18:13:08  95      Authentication Server vortex is down.
2009-03-02 18:13:08  96      Authentication Server vortex is down.
2009-03-02 18:13:08  97      Authentication Server corp1-supersvr is down.
2009-03-02 18:13:08  98      All authentication servers in server group sg-auth2 are brought back in service.
2009-03-02 18:13:08  99      Authentication Server corp1-supersvr is down.
2009-03-02 18:13:08  100     All authentication servers in server group sg-auth2 are brought back in service.
2009-03-02 18:13:08  101     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:08  102     All authentication servers in server group sg-auth2 are brought back in service.
2009-03-02 18:13:08  103     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:08  104     All authentication servers in server group sg-auth2 are brought back in service.
2009-03-02 18:13:08  105     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:08  106     All authentication servers in server group sg-auth2 are brought back in service.
2009-03-02 18:13:09  107     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:09  108     All authentication servers in server group sg-auth2 are brought back in service.
2009-03-02 18:13:09  109     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:09  110     All authentication servers in server group sg-auth2 are brought back in service.
2009-03-02 18:13:09  111     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:09  112     All authentication servers in server group sg-auth2 are brought back in service.
2009-03-02 18:13:09  113     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:09  114     All authentication servers in server group sg-auth2 are brought back in service.
2009-03-02 18:13:09  115     Authentication Server corp1-supersvr is down.
Total number of entries in the queue    :23
```

Related Commands

Command	Description	Mode
`clear fault <id>|all`	Manually clear a single fault by specifying the fault ID number, or clear all faults by including the **all** parameter.	Config mode

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show firewall

```
show firewall
```

Description

Display a list of global firewall policies.

Syntax

No parameters

Example

This example below shows all firewall policies currently configured on the controller.

```
(host) #show firewall

Global firewall policies
------------------------
Policy                                    Action    Rate     Slot/Port
------                                    ------    ----     ---------
Enforce TCP handshake before allowing data  Enabled
Prohibit RST replay attack                Enabled
Deny all IP fragments                     Enabled
Prohibit IP Spoofing                      Enabled
Monitor ping attack                       Enabled   20/sec
Monitor TCP SYN attack                    Disabled
Monitor IP sessions attack                Disabled
Deny inter user bridging                  Disabled
Log all received ICMP errors              Disabled
Per-packet logging                        Disabled
Session mirror destination                Disabled
Stateful SIP Processing                   Enabled
Allow tri-session with DNAT               Enabled
Disable FTP server                        No
GRE call id processing                    Disabled
Session Idle Timeout                      Disabled
Broadcast-filter ARP                      Disabled
WMM content enforcement                   Disabled
Session VOIP Timeout                      Disabled
Stateful H.323 Processing                 Enabled
Stateful SCCP Processing                  Enabled
Only allow local subnets in user table    Enabled
Monitor/police CP attacks                 Enabled   255/sec
Rate limit CP untrusted ucast traffic     Enabled   10 Mbps
Rate limit CP untrusted mcast traffic     Enabled   2 Mbps
Rate limit CP trusted ucast traffic       Enabled   80 Mbps
Rate limit CP trusted mcast traffic       Enabled   2 Mbps
Rate limit CP route traffic               Enabled   1 Mbps
Rate limit CP session mirror traffic      Enabled   1 Mbps
Rate limit CP auth process traffic        Enabled   1 Mbps
Deny inter user traffic                   Disabled
Session mirror IPSEC                      Disabled
```

The output of this command includes the following information:

Parameter	Description
`Enforce TCP handshake before allowing data`	If enabled, this feature prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network.
`Prohibit RST replay attack`	If enabled, this setting closes a TCP connection in both directions if a TCP RST is received from either direction.

Parameter	Description
Deny all IP fragments	If enabled, all IP fragments are dropped.
Prohibit IP Spoofing	When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.
Monitor ping attack	If enabled, the controller monitors the number of ICMP pings per second. If this value exceeds the maximum configured rate, the controller will register a denial of service attack.
Monitor TCP SYN attack	If enabled, the controller monitors the number of TCP SYN messages per second. If this value exceeds the maximum configured rate, the controller will register a denial of service attack.
Monitor IP sessions attack	If enabled, the controller monitors the number of TCP sessions requests per second. If this value exceeds the maximum configured rate, the controller will register a denial of service attack sessions.
Deny inter user bridging	If enabled this setting prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic.
Log all received ICMP errors	Shows if the controller will log received ICMP errors.
Per-packet logging	If active, and logging is enabled for the corresponding session rule, this feature logs every packet.
Session mirror destination	Destination to which mirrored packets are sent.
Stateful SIP Processing	Shows if the controller has enabled or disabled monitoring of exchanges between a voice over IP or voice over WLAN device and a SIP server. This option should be enabled only when thee is no VoIP or VoWLAN traffic on the network
Allow tri-session with DNAT	Shows if the controller allows three-way session when performing destination NAT.
Disable FTP server	If active, this feature disables the FTP server on the controller.
GRE callid processing	If active the controller creates a unique state for each PPTP tunnel.
Session Idle Timeout	Shows if a session idle timeout interval has been defined.
Broadcast-filter ARP	If enabled, this feature reduces the number of broadcast packets sent to VoIP clients, thereby improving the battery life of voice handsets.
WMM content enforcement	If traffic to or from the user is inconsistent with the associated QoS policy for voice, this feature reclassifies traffic to best effort and data path counters are incremented.
Session VOIP Timeout	If enabled, a idle session timeout is defined for sessions that are marked as voice sessions.
Stateful H.323 Processing	Shows if the controller has enabled or disabled stateful H.323 processing.
Stateful SCCP Processing	Shows if the controller has enabled or disabled stateful SCCP processing.
Only allow local subnets in user table	If enabled, the controller only adds IP addresses which belong to a local subnet to the user table.
Monitor/police CP attacks	If enabled, the controller monitors a misbehaving user's inbound traffic rate. If this rate is exceeded, the controller can register a denial of service attack.
Rate limit CP untrusted ucast traffic	Shows the inbound traffic rate
Rate limit CP untrusted mcast traffic	Displays the untrusted multicast traffic rate limit.

Parameter	Description
`Rate limit CP trusted ucast traffic`	`Displays the trusted unicast traffic rate limit.`
`Rate limit CP trusted mcast traffic`	`Displays the trusted multicast traffic rate limit.`
`Rate limit CP route traffic`	Displays the traffic rate limit for traffic that needs generated ARP requests.
`Rate limit CP session mirror traffic`	Displays the traffic rate limit for session mirrored traffic forwarded to the controller.
`Rate limit CP auth process traffic`	Displays the traffic rate limit for traffic forwarded to the authentication process.
`Deny inter user traffic`	If enabled, this setting disables the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic.
`Session mirror IPSEC`	If enabled, rrames are sent to IP address specified by the session-mirror-destination option.

Related Commands

Command	Description	Mode
`firewall`	This command configures firewall options on the controller.	Config mode
`firewall cp`	This command creates whitelist session ACLs	Config mode
`firewall cp-bandwidth-contract`	This command configures bandwidth contract traffic rate limits to prevent denial of service attacks.	Config mode

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers

show firewall-cp

```
show firewall-cp [internal]
```

Description

Displays the captive-portal (CP) firewall policies on the controller.

Syntax

No Parameters

Example

The output of this command shows the CP firewall policies.

```
(host) # show firewall-cp

CP firewall policies
--------------------
Protocol  Start Port  End Port  Permit/Deny  hits  contract
--------  ----------  --------  -----------  ----  --------
6         22          22        Permit       0
6         8081        8081      Permit       0
6         8082        8082      Permit       0
6         8083        8083      Permit       0
17        1812        1812      Permit       0
17        1813        1813      Permit       0
17        67          67        Permit       0
17        68          68        Permit       0
47        1           65535     Permit       0
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show gateway health-check

```
show gateway health-check
```

Description

Display the current status of the gateway health-check feature.

Syntax

No parameters.

Usage Guidelines

The gateway health check feature can only be enabled by Dell Technical Support.

Example

This example below shows that the gateway health-check feature has not been enabled on the controller.

```
(host) #show gateway health-check
Gateway health check not enabled
```

Related Commands

Command	Description	Mode
`gateway health-check disable`	Disable the gateway health check	Config mode

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers

show global-user-table count

```
show global-user-table
show global-user-table count
   [current-switch] <IP address>
   [authentication-method] {dot1x | mac | stateful-dot1x | vpn | web}
   [role] <role name>
   [bssid] <bssid MAC>
   [essid] <essid>
   [ap-name] <AP name>
   [phy-type] {a | b | g}
   [age] <starting time dd:hh:mm> <ending time dd:hh:mm>
```

Description

This command displays a count of global user based on the specified criteria.

Syntax

Parameter	Description
`current-switch`	Match IP address of the switch where the user is currently associated
`authentication-method`	Count users matching the specified authentication method
`role`	Count users matching the specified role
`bssid`	Count users matching the specified BSSID
`essid`	Count users matching the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
`ap-name`	Count users matching the specified AP name
`phy-type`	Count users matching the specified Phy type
`age`	Count users matching the specified age

Example

Issue this command to display a global user count.The output shown below is a result of the command **show global-user-table count current-switch <ip-address>**.

```
Complete results.
The number of global users : 2
```

The output includes the following parameters:

Parameter	Description
`The number of global users:`	Total number of global users meeting the specified criteria.

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms Master controller only	Base operating system	Enable or config mode on master controllers

show-global-user-table list

```
show global-user-table list
   [current-switch] <IP address>
   [authentication-method] {dot1x | mac | stateful-dot1x | vpn | web}
   [role] <role name>
   [bssid] <bssid MAC>
   [essid] <essid>
   [ap-name] <AP name>
   [phy-type] {a | b | g}
   [age] <starting time dd:hh:mm> <ending time dd:hh:mm>
   [not]
   [or]
   [rows]
   [sort] {sort_by_ap-name | sort_by_authtype | sort_by_bssid | sort_by_current-switch
   | sort_by_essid | sort_by_ip | sort_by_mac | sort_by_name | sort_by_phy-type |
   sort_by_role}{asc | desc}
   [start]
```

Description

This command displays a list of current users on a specified switch.

Syntax

Parameter	Description
current-switch	Match IP address of the switch where the user is currently associated
authentication-method	Count users matching the specified authentication method
role	Count users matching the specified role
bssid	Count users matching the specified BSSID
essid	Count users matching the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
ap-name	Count users matching the specified AP name
phy-type	Count users matching the specified Phy type
age	Count users matching the specified age
current-switch	Match IP address of the switch where the user is currently associated
authentication-method	Count users matching the specified authentication method
role	Count users matching the specified role
not	Show users that do not satisfy the given criteria
or	Show users that satisfy any of the given criteria
rows	Number of rows to show
sort	Sort the list based on a specified criteria, in ascending or descending order
start	Show user table starting from a specific row

Example

Issue this command to display a global user count. The output shown below is a result of the command **show global-user-table list current-switch <ip-address>**

```
Global Users
------------
    IP          MAC           Name   Current switch  Role         Age(d:h:m)  Auth    VPN link AP name
Essid Bssid Phy Profile
----------  ------------       ------  --------------  ----          ----------  ----    -------- ---
----  ----- ----- --- -------
```

The output includes the following parameters:

Parameter	Description
IP	IP address of user.
MAC	MAC address of user.
Name	User name.
Current Switch	IP address of the switch where the user is currently associated.
Role	User role.
Age	User age, displayed as *days:hours:minutes*.
Auth	Authentication method used by user.

Parameter	Description
`VPN Link`	IP address of the client VPN gateway.
`AP name`	AP name.
`Roaming`	Roaming status.
`Essid`	User's extended service set identifier (ESSID).
`Bssid`	User's basic service set identifier (BSSID).
`Phy`	User Phy type (*a*, *b* or *g*).
`Profile`	Profile name

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms Master controller only	Base operating system	Enable or config mode on master controllers

show guest-access-email

```
show guest-access-email
```

Description

This command shows a guest access email profile configuration.The guest access email process sends email to either the guest or the sponsor whenever a guest user account is created or when the Guest Provisioning user manually sends email from the Guest Provisioning page.

Syntax

No parameters.

Usage Guidelines

Issue this command to show the current guest access email profile parameters. The Parameter and **Value** columns show the configured SMTP server and SMTP ports. that process guest email.

```
(host) #show guest-access-email

Guest-access Email Profile
--------------------------
Parameter    Value
---------    -----
SMTP Server  10.1.1.4
SMTP Port    25
```

Related Commands

Command	Description	Mode
guest-access-email	This command shows a guest access email profile configuration.	Enable or Config modes
local-userdb-guest add	This command creates a guest user in a local user database.	Enable or Config modes

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show hostname

```
show hostname
```

Description

Show the hostname of the controller.

Syntax

No parameters.

Example

The output of this command shows the hostname configured for the controller. A hostname can contain alphanumeric characters, spaces, punctuation, and symbol characters.

```
(host) # show hostname
hostname is SampleHost.
```

Related Commands

Configure the controller's hostname using the command hostname.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available on master or local controllers

show ids dos-profile

```
show ids dos-profile <profile-name>
```

Description

Show an IDS Denial Of Service (DoS) Profile

Syntax

Parameter	Description
<profile-name>	Name of an IDS DoS profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire IDS DoS profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has four configured DoS profiles.

```
(host) # show ids dos-profile
IDS Denial Of Service Profile List
----------------------------------
Name                    References  Profile Status
----                    ----------  --------------
default                 1
ids-dos-disabled        1           Predefined
ids-dos-high-setting    1           Predefined
ids-dos-low-setting     1           Predefined
ids-dos-medium-setting  1           Predefined
```

This example displays the configuration settings for the profile **ids-dos-disabled**.

```
(host) # show ids dos-profile ids-dos-disabled
IDS Denial Of Service Profile "ids-dos-disabled" (Predefined)
-------------------------------------------------------------
Parameter                                   Value
---------                                   -----
Spoofed Deauth Blacklist                    Disabled
Detect AP Flood Attack                      false
AP Flood Threshold                          50
AP Flood Increase Time                      3 sec
AP Flood Detection Quiet Time               900 sec
Detect EAP Rate Anomaly                     false
EAP Rate Threshold                          60
EAP Rate Time Interval                      3 sec
EAP Rate Quiet Time                         900 sec
Detect Rate Anomalies                       false
Rate Thresholds for Assoc Frames            default
Rate Thresholds for Disassoc Frames         default
Rate Thresholds for Deauth Frames           default
Rate Thresholds for Probe Request Frames    default
Rate Thresholds for Probe Response Frames   default
Rate Thresholds for Auth Frames             default
Detect 802.11n 40MHz Intolerance Setting    false
Client 40MHz Intolerance Detection Quiet Time  900
```

The output of this command includes the following parameters:

Parameter	Description
Spoofed Deauth Blacklist	Shows if the profile has enabled or disabled detection of a deauth attack initiated against a client associated to an Dell AP. When such an attack is detected, the client is quarantined from the network to prevent a man-in-the-middle attack from being successful.
Detect Ap Flood Attack	Shows if the profile has enabled or disabled detection of flooding with fake AP beacons to confuse legitimate users and to increase the amount of processing needed on client operating systems.
AP Flood Threshold	Number of fake AP beacons that must be received within the flood increase time to trigger an alarm.
AP Flood Increase Time	Time, in seconds, during which a configured number of fake AP beacons must be received to trigger an alarm.
AP Flood Detection Quiet TIme	Time, in seconds, that must elapse before an second fake AP flood alarm may be triggered.
Detect EAP Rate Anomaly	Shows if the profile has enabled or disabled 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.
EAP rate Threshold	Number of EAP handshakes that must be received within the EAP rate time interval to trigger an alarm.
EAP Rate TIme Interval	Time, in seconds, during which the configured number of EAP handshakes must be received to trigger an alarm.
EAP Rate Quiet Time	Time, in seconds, that must elapse after an EAP rate anomaly alarm has been triggered before another identical alarm may be triggered.
Detect Rate Anomalies	Enables detection of rate anomalies.
Rate Thresholds for Assoc Frames	Rate threshold for associate request frames.
Rate Thresholds for Disassoc Frames	Rate threshold for disassociate frames.
Rate Thresholds for Deauth Frames	Rate threshold for deauthenticate frames.
Rate Thresholds for Probe Request Frames	Rate threshold for probe request frames.
Rate Thresholds for Probe Response Frames	Rate threshold for probe response frames.
Rate Thresholds for Auth Frames	Rate threshold for authenticate frames.
Detect 802.11n 40MHz Intolerance Setting	Shows if the profile has enabled or disabled detection of 802.11n 40 MHz intolerance setting, which controls whether stations and APs advertising 40 MHz intolerance will be reported.
Client 40MHz Intolerance Detection Quiet Time	Seconds of quiet time when the AP stops reporting intolerant STAs if they have not been detected).

Related Commands

Configure IDS DoS profiles using the command ids dos-profile.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config mode on master or local controllers

show ids general-profile

```
show ids general-profile <profile-name>
```

Description

Show an IDS General profile.

Syntax

Parameter	Description
`<profile-name>`	Name of an IDS General profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire IDS General profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has four configured General profiles.

```
(host) # show ids general-profile
IDS General Profile List
------------------------
Name                      References  Profile Status
----                      ----------  --------------
default                   3
ids-general-disabled      1           Predefined
ids-general-high-setting  1           Predefined
test1                     0

Total:4
```

This example displays the configuration settings for the profile **default**.

```
(host) # show ids general-profile default
IDS General Profile "default"
-----------------------------
Parameter                      Value
---------                      -----
Stats Update Interval          60 sec
AP Inactivity Timeout          5 sec
STA Inactivity Timeout         60 sec
Min Potential AP Beacon Rate   25 %
Min Potential AP Monitor Time  3 sec
Signature Quiet Time           900 sec
Wireless Containment           true
Debug Wireless Containment     false
Wired Containment              false
Mobility Manager RTLS        false
```

The output of this command includes the following parameters:

Parameter	Description
`Stats Update Interval`	Interval, in seconds, for the AP to update the controller with statistics. This setting takes effect only if the Dell Mobility Manager is configured. Otherwise, statistics update to the controller is disabled.
`AP Inactivity Timeout`	Time, in seconds, after which an AP is aged out.

Parameter	Description
STA Inactivity Timeout	Time, in seconds, after which a station is aged out.
Min Potential AP Beacon Rate	Minimum beacon rate acceptable from a potential AP, in percentage of the advertised beacon interval.
Min Potential AP Monitor Time	Minimum time, in seconds, a potential AP has to be up before it is classified as a real AP.
Signature Quiet Time	After a signature match is detected, the time to wait, in seconds, to resume checking.
Wireless Containment	Shows if the profile has enabled or disabled containment from the wireless side.
Debug Wireless Containment	Shows if the profile has enabled or disable debugging of containment from the wireless side.
Wired Containment	Shows if the profile has enabled or disable containment from the wired side.
Mobility Manager RTLS	Shows if RTLS communication with the configured mobility-manager is enabled or disabled.

Related Commands

Configure IDS General profiles using the command ids general-profile.

Command History

Version	Description
ArubaOS 3.0	Command Introduced
ArubaOS 5.0	Mobility Manager RTLS parameter introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config mode on master or local controllers

show ids impersonation-profile

```
show ids impersonation-profile <profile-name>
```

Description

Show an IDS Impersonation Profile.

Syntax

Parameter	Description
<profile-name>	Name of an IDS Impersonation profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire IDS Impersonation profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured Impersonation profiles.

```
(host) # show ids impersonation-profile
IDS Impersonation Profile List
------------------------------
Name                           References  Profile Status
----                           ----------  --------------
default                        3
ids-impersonation-disabled     1           Predefined
ids-impersonation-high-setting 1           Predefined
Total:3
```

This example displays the configuration settings for the profile **ids-impersonation-high-setting**.

```
(host) # show ids impersonation-profile ids-impersonation-high-setting
IDS Impersonation Profile “ids-impersonation-high-setting” (Predefined)
-----------------------------------------------------------------------
Parameter                     Value
---------                     -----
Detect AP Impersonation       true
Protect from AP Impersonation  true
Beacon Diff Threshold         50 %
Beacon Increase Wait Time     3 sec
```

The output of this command includes the following parameters:

Parameter	Description
Detect AP Impersonation	Shows of the profile has enabled or disabled detection of AP impersonation.
Protect from AP Impersonation	Shows if AP impersonation is enabled or disabled for the profile. When AP impersonation is detected, both the legitimate and impersonating AP are disabled using a denial of service attack.
Beacon Diff Threshold	Percentage increase in beacon rates that triggers an AP impersonation event.
Beacon Increase Wait Time	Time, in seconds, after the beacon difference threshold is crossed before an AP impersonation event is generated.

Related Commands

Configure IDS impersonation profiles using the command ids impersonation-profile.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config mode on master or local controllers

show ids profile

```
show ids profile <profile-name>
```

Description

Show an IDS profile.

Syntax

Parameter	Description
`<profile-name>`	Name of an IDS profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire IDS profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has five configured IDS Profiles.

```
(host) # show ids profile
IDS Profile List
----------------
Name                References  Profile Status
----                ----------  --------------
default             1
ids-disabled        0           Predefined
ids-high-setting    0           Predefined
ids-low-setting     5           Predefined
ids-medium-setting  0           Predefined

Total:5
```

This example displays the configuration settings for the profile **ids-low-setting**.

```
(host) # show ids profile ids-low-setting

IDS Profile "ids-low-setting" (Predefined)
------------------------------------------
Parameter                       Value
---------                       -----
IDS General profile             default
IDS Signature Matching profile  factory-default-signature
IDS DOS profile                 ids-dos-low-setting
IDS Impersonation profile       default
IDS Unauthorized Device profile default
```

The output of this command includes the following parameters:

Parameter	Description
`IDS General profile`	Name of a IDS General profile to be applied to an AP or AP group.
`IDS Signature Matching profile`	Name of a IDS Signature Matching profile to be applied to an AP or AP group.
`IDS DOS profile`	Name of a IDS Denial of Service profile to be applied to an AP or AP group.

Parameter	Description
`IDS Impersonation profile`	Name of a IDS Impersonation profile to be applied to an AP or AP group.
`IDS Unauthorized Device profile`	Name of a IDS Unauthorized Device profile to be applied to an AP or AP group.

Related Commands

Configure the IDS profile using the command ids profile.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config mode on master or local controllers

show ids rate-thresholds-profile

```
show ids rate-thresholds-profile <profile-name>
```

Description

Show an IDS Rate Thresholds profile.

Syntax

Parameter	Description
`<profile-name>`	Name of an IDS Rate Threshold profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire IDS Rate Threshold profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has eight configured IDS Rate Threshold Profiles.

```
(host) # show ids rate-thresholds-profile
IDS Rate Thresholds Profile List
--------------------------------
Name                              References  Profile Status
----                              ----------  --------------
def-assoc-thresholds              1
def-auth-thresholds               1
def-deauth-thresholds             1
def-disassoc-thresholds           1
def-probe-request-thresholds      1
def-probe-response-thresholds     1
default                           18
probe-request-response-thresholds 6           Predefined

Total:8
```

This example displays the configuration settings for the profile **probe-request-response-thresholds**.

```
(host) # show ids rate-thresholds-profile probe-request-response-thresholds
IDS Rate Thresholds Profile "probe-request-response-thresholds" (Predefined)
-------------------------------------------------------------------------------
Parameter             Value
---------             -----
Channel Increase Time  30 sec
Channel Quiet Time     900 sec
Channel Threshold      350
Node Time Interval     10 sec
Node Quiet Time        900 sec
Node Threshold         250
```

The output of this command includes the following parameters:.

Parameter	Description
`Channel Increase Time`	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.
`Channel Quiet Time`	The time that must elapse after a channel rate alarm before another identical alarm may be triggered. This option prevents excessive messages in the log file.

Parameter	Description
`Channel Threshold`	Number of a specific type of frame that must be exceeded within a specific interval in an entire channel to trigger an alarm.
`Node Time Interval`	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.
`Node Quiet Time`	The time that must elapse after a node rate alarm before another identical alarm may be triggered. This option prevents excessive messages in the log file.
`Node Threshold`	Number of a specific type of frame that must be exceeded within a specific interval for a particular client MAC address to trigger an alarm.

Related Commands

Configure the IDS DoS profile using the command show ids dos-profile.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config mode on master or local controllers

show ids signature-matching-profile

```
show ids signature-matching-profile <profile-name>
```

Description

Show an IDS Signature Matching profile.

Syntax

Parameter	Description
`<profile-name>`	Name of an IDS Signature Matching profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire IDS Signature Matching profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured Signature Matching profiles.

```
(host) # show ids signature-matching-profile
IDS Signature Matching Profile List
-----------------------------------
Name                         References  Profile Status
----                         ----------  --------------
default                      2
factory-default-signatures   3           Predefined

Total:2
```

This example displays the configuration settings for the profile **factory-default-signatures**.

```
(host) # show ids signature-matching-profile factory-default-signatures
IDS Signature Matching Profile "factory-default-signatures" (Predefined)
------------------------------------------------------------------------
Parameter      Value
---------      -----
IDS Signature  AirJack
IDS Signature  ASLEAP
IDS Signature  Deauth-Broadcast
IDS Signature  Netstumbler Generic
IDS Signature  Netstumbler Version 3.3.0x
IDS Signature  Null-Probe-Response
```

The output of this command includes the following parameters:

Parameter	Description
`IDS Signature`	Name of a signature profile. See "ids signature-profile" on page 239.

Related Commands

Configure the Signature Matching profile using the command ids signature-matching-profile.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config mode on master or local controllers

show ids signature-profile

```
show ids signature-profile <profile-name>
```

Description

Show an IDS signature profile.

Syntax

Parameter	Description
<profile-name>	Name of an IDS Signature profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire IDS Signature profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has eight configured Signature profiles.

```
(host) # show ids signature-profile

IDS Signature Profile List
--------------------------
Name                        References  Profile Status
----                        ----------  --------------
AirJack                     1           Predefined
ASLEAP                      1           Predefined
Deauth-Broadcast            1           Predefined
default                     1
Netstumbler Generic         1           Predefined
Netstumbler Version 3.3.0x  1           Predefined
Null-Probe-Response         1           Predefined
sample                      0

Total:8
```

This example displays the configuration settings for the profile **AirJack**.

```
(host) # show ids signature-profile
IDS Signature Profile "AirJack" (predefined)
--------------------------------------------
Parameter   Value
---------   -----
Frame Type  beacon SSID = AirJack
```

The output of this command includes the following parameters:

Parameter	Description
`Frame Type`	Type of 802.11 frame. For each type of frame, further parameters may be included to filter and detect only the required frames. • **assoc**: Association frame type. • **auth**: Authentication frame type. • **beacon**: Beacon frame type. • **control**: All control frames. • **data**: All data frames. • **deauth**: Deauthentication frame type. • **disassoc**: Disassociation frame type. • **mgmt**: Management frame type. • **probe-request**: Probe request frame type. • **probe-response:** Probe response frame type. • **ssid**: For beacon, probe-request, and probe-response frame types, the SSID as either a string or hex pattern. • **ssid-length**: For beacon, probe-request, and probe-response frame types, the length, in bytes, of the SSID.
`payload`	Pattern at a fixed offset in the payload of an 802.11 frame.
`sequence number`	Sequence number of the frame.
`src- mac`	Source MAC address in the 802.11 frame header.
`dst- mac`	Source MAC address in the 802.11 frame header.
`bssid`	BSSID field in the 802.11 frame header.

Related Commands

Configure the Signature profile using the command ids signature-profile.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config mode on master or local controllers

show ids unauthorized-device-profile

```
show ids unauthorized-device-profile <profile-name>
```

Description

Show an IDS Unauthorized Device Profile.

Syntax

Parameter	Description
<profile-name>	Name of an IDS Unauthorized Device profile

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire IDS Unauthorized Device profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has four configured Unauthorized Device profiles.

```
(host) # show ids unauthorized-device-profile
IDS Unauthorized Device Profile List
------------------------------------
Name                                 References  Profile Status
----                                 ----------  --------------
default                              2
ids-unauthorized-device-disabled     1           Predefined
ids-unauthorized-device-high-setting 1           Predefined
ids-unauthorized-device-medium-setting 1         Predefined

Total:4
```

This example displays the configuration settings for the profile **ids-unauthorized-device-disabled**.

```
(host) # show ids unauthorized-device-profile ids-unauthorized-device-disabled
IDS Unauthorized Device Profile "ids-unauthorized-device-disabled" (Predefined)
-------------------------------------------------------------------------------
Parameter                                   Value
---------                                   -----
Detect Adhoc Networks                       false
Protect from Adhoc Networks                 false
Detect Windows Bridge                       false
Detect Wireless Bridge                      false
Detect Devices with an Invalid MAC OUI      false
MAC OUI detection Quiet Time                900 sec
Adhoc Network detection Quiet Time          900 sec
Wireless Bridge detection Quiet Time        900 sec
Rogue AP Classification                     false
Overlay Rogue AP Classification             true
Valid Wired MACs                            N/A
Allow Well Known MAC                        N/A
Rogue Containment                           false
Suspected Rogue Containment                 false
Suspected Rogue Containment Confidence Level 60
Protect Valid Stations                      false
Detect Bad WEP                              false
Detect Misconfigured AP                     false
Protect Misconfigured AP                    false
Protect SSID                                false
Privacy                                     false
Require WPA                                 false
Valid 802.11g channel for policy enforcement 11
Valid 802.11a channel for policy enforcement 40
Valid MAC OUIs                              N/A
Valid and Protected SSIDs                   N/A
Protect 802.11n High Throughput Devices     false
Protect 40MHz 802.11n High Throughput Devices false
Detect Active 802.11n Greenfield Mode       false
```

The output of this command includes the following parameters:

Parameter	Description
`Detect AdHoc Networks`	Shows if the profile has enabled or disabled detection of adhoc networks.
`Protect from Adhoc Networks`	Shows if the profile has enabled or disabled protection from adhoc networks.
`Detect Windows Bridge`	Shows if the profile has enabled or disabled detection of Windows station bridging.
`Detect Wireless Bridge`	Shows if the profile has enabled or disabled detection of wireless bridging.
`Detect Devices with an Invalid MAC OUI`	Shows if the profile has enabled or disabled checking of the first three bytes of a MAC address, known as the organizationally unique identifier (OUI), assigned by the IEEE to known manufacturers.
`MAC OUI detection Quiet Time`	Time, in seconds, that must elapse after an invalid MAC OUI alarm has been triggered before another identical alarm may be triggered.
`Adhoc Network detection Quiet Time`	Time, in seconds, that must elapse after an adhoc network detection alarm has been triggered before another identical alarm may be triggered.
`Wireless Bridge detection Quiet Time`	Time, in seconds, that must elapse after a wireless bridge alarm has been triggered before another identical alarm may be triggered.
`Rogue AP Classification`	Shows if the profile has enabled or disabled rogue AP classification.
`Overlay Rogue AP Classification`	Shows if the controller allows APs that are plugged into the wired side of the network to be classified as “suspected rogue” instead of “rogue”.

Parameter	Description
Valid Wired MACs	List of valid and protected SSIDs.
Allow Well Known MAC	Shows if the profile allows devices with known MAC addresses to classify rogue APs.
Rogue Containment	Shows if the controller will automatically shut down rogue APs.
Suspected Rogue Containment	Shows if the controller will automatically treat suspected rogue APs as interfering APs.
Suspected Rogue Containment Confidence Level	Confidence level of suspected Rogue AP to trigger containment, expressed as a percentage.
Protect Valid Stations	Shows if the controller will allow valid stations to connect to a non-valid AP.
Detect Bad WEP	Shows if the profile has enabled or disabled detection of WEP initialization vectors that are known to be weak and/or repeating.
Detect Misconfigured AP	Shows if the profile has enabled or disabled detection of misconfigured APs.
Protect Misconfigured AP	Shows if the profile has enabled or disabled protection of misconfigured APs.
Protect SSID	Shows if the profile has enabled or disabled use of SSID by valid APs only.
Privacy	Shows if the profile has enabled or disabled encryption as a valid AP configuration.
Require WPA	Shows if the controller will flag any valid AP not using WPA as a misconfigured AP.
Valid 802.11g channel for policy enforcement	A list of valid 802.1b/g channels that third-party APs are allowed to use.
Valid 802.11a channel for policy enforcement	A list of valid 802.11a channels that third-party APs are allowed to use.
Valid MAC OUIs	A list of valid MAC Organizationally Unique Identifiers (OUIs).
Valid and Protected SSIDs	A list of valid and protected SSIDs.
Protect 802.11n High Throughput Devices	Shows if the profile enables or disables protection of high-throughput (802.11n) devices.
Protect 40MHz 802.11n High Throughput Devices	Shows if the profile enables or disables protection of high-throughput (802.11n) devices operating in 40 MHz mode.
Detect Active 802.11n Greenfield Mode	Shows if the profile enables or disables detection of high-throughput devices advertising greenfield preamble capability.

Related Commands

Configure the Unauthorized Device profile using the command ids unauthorized-device-profile.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config mode on master or local controllers

show image version

Description

Display the current system image version on both partition 0 and 1.

Syntax

No parameters.

Example

The following example shows that the controller is running ArubaOS 3.4 and booting off partition 0:0.

```
(host) #show image version
---------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : AOS-W 3.3.2.0
Build number            : 18661
Label                   : 18661
Built on                : 2008-06-12 04:24:34 PDT
---------------------------------
Partition               : 0:0 (/dev/hda1)
Software Version        : AOS-W 3.3.2.0
Build number            : 18661
Label                   : 18661
Built on                : 2008-06-12 04:24:34 PDT
```

The output of this command includes the following parameters:

Parameter	Description
Partition	Partition number and name. The default boot partition will display a **Default boot** notice by the partition name.
Software Version	Version of ArubaOS software running on the partition.
Build number	Build number for the software version.
Label	The label parameter can display additional information for the build. By default, this value is the software build number.
Built on	Date the software build was created.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show interface counters

```
show interface counters
```

Description

Displays a table of L2 interfaces counters.

Syntax

No parameters

Example

The example below shows the output of **show interface counters** on an W-600 Series Controller controller.

```
Port          InOctets     InUcastPkts     InMcastPkts     InBcastPkts
GE1/0        250559459         1664878               0              16
GE1/1       1615683022         1230973               0              16
GE1/2           204909            1511               0              16
GE1/3          2964355           22155               0              17
GE1/4       1612815178        12509415               0             228
GE1/6      23571170611        15545404               0               4
GE1/7      23562566444        15530432            8236             146

Port         OutOctets    OutUcastPkts    OutMcastPkts    OutBcastPkts
GE1/0       2504472376         2645877            8243           16770
GE1/1        169128719          820198            8243           17083
GE1/2          1881584           25785            8243           16771
```

The output of this command includes the following parameters:

Parameter	Description
`Port`	Port number.
`InOctets`	Number of octets received through the port.
`InUcastPkts`	Number of unicast packets received through the port.
`InMcastPkts`	Number of multicast packets received through the port.
`InBcastPkts`	Number of broadcast packets received through the port.
`OutOctets`	Number of octets sent through the port.
`OutUcastPkts`	Number of unicast packets sent through the port.
`OutMcastPkts`	Number of multicast packets sent through the port.
`OutBcastPkts`	Number of broadcast packets sent through the port.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show interface gigabitethernet

```
show interface gigabitethernet <slot/port>
```

Description

Displays information about a specified Gigabit ethernet port.

Syntax

Parameter	Description
counters	Displays L2 interface counters for the specified interface.
switchport	Displays L2 interface information.
untrusted-vlan	Displays port member vlan untrusted status.
xsec	Displays xsec configuration.

Examples

The example below shows the output of **show interface gigabitethernet 1/0**.

```
#show interface gigabitethernet 1/0

GE 1/0 is up, line protocol is up
Hardware is Gigabit Ethernet, address is 00:0B:86:F0:33:E1 (bia 00:0B:86:F0:33:E1)
Description: GE1/0 (RJ45 Connector)
Encapsulation ARPA, loopback not set
Configured: Duplex ( AUTO ), speed ( AUTO )
Negotiated: Duplex (Full), speed (100 Mbps)
MTU 1500 bytes, BW is 100 Mbit
Last clearing of "show interface" counters 23 day 4 hr 27 min 54 sec
link status last changed 15 day 3 hr 15 min 21 sec
    2049219 packets input, 112651020 bytes
    Received 911909 broadcasts, 0 runts, 0 giants, 0 throttles
    26 input error bytes, 0 CRC, 0 frame
    906926 multicast, 1137310 unicast
    185897 packets output, 58327172 bytes
```

The output of this command includes the following parameters:

Parameter	Description
GE 1/0 is...	Displays the status of the specified port.
line protocol is...	Displays the status of the line protocol on the specified port.
Hardware is....	Describes the hardware interface type.
address is...	Displays the MAC address of the hardware interface.
Description	The port type, name, and connector type.
Encapsulation	Encapsulation method assigned to this port.
loopback...	Displays whether or not loopback is set.
Configured	Configured transfer operation and speed.
Negotiated	Negotiated transfer operation and speed.
MTU bytes	MTU size of the specified port in bytes.

Parameter	Description
BW is...	Bandwidth of the link.
Last clearing of "show interface counters"	Time since "show interface counters" was cleared.
link status last changed...	Time since "show interface counters" was cleared. Below the time, all current counters related to the specified port are listed.
This port is...	Whether or not this port is trusted.
POE status of the port is...	The POE status of the specified port.

```
#show interface gigabitethernet 1/0

Port          InOctets     InUcastPkts     InMcastPkts     InBcastPkts
GE1/0        112670646         1137507          907019            4983

Port         OutOctets    OutUcastPkts    OutMcastPkts    OutBcastPkts
```

The output of this command includes the following parameters:

Parameter	Description
Port	Port number.
InOctets	Number of octets received through the port.
InUcastPkts	Number of unicast packets received through the port.
InMcastPkts	Number of multicast packets received through the port.
InBcastPkts	Number of broadcast packets received through the port.
OutOctets	Number of octets sent through the port.
OutUcastPkts	Number of unicast packets sent through the port.
OutMcastPkts	Number of multicast packets sent through the port.
OutBcastPkts	Number of broadcast packets sent through the port.

```
#show interface gigabitethernet 1/0 switchport

Name:  GE1/0
Switchport:  Enabled
Administrative mode:  static access
Operational mode:  static access
Administrative Trunking Encapsulation:  dot1q
Operational Trunking Encapsulation:  dot1q
Access Mode VLAN: 62 (VLAN0062)
Trunking Native Mode VLAN: 1 (Default)
```

The output of this command includes the following parameters:

Parameter	Description
Name	Port name.
Switchport	Whether or not switchport is enabled.
Administrative mode	Administrative mode .
Operational mode	Operational mode.
Administrative Trunking Encapsulation	Encapsulation method used for administrative trunking.
Operational Trunking Encapsulation	Encapsulation method used for operational trunking.
Access Mode VLAN	The access mode VLAN for the specified port.
Trunking Native Mode VLAN	The trunking native mode VLAN for the specified port.
Trunking Vlans Enabled	Number of trunking VLANs currently enabled.
Trunking Vlans Active	Number of trunking VLANs currently active.

```
#show interface gigabitethernet 1/0 untrusted-vlan

Name:  GE1/0
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the specified port.
Untrusted Vlan(s)	List of untrusted VLANs.

```
#show interface gigabitethernet 1/1 xsec
xsec vlan 7 is ACTIVE
```

The output of this command includes the following parameters:

Parameter	Description
xsec vlan 7 is ACTIVE	This states that xsec is active on the specified port as well as the associated VLAN.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show interface fastethernet

```
show interface fastethernet <slot/port>
```

Description

Displays information about a specified fast ethernet port.

Syntax

Parameter	Description
access-group	Displays access groups configured on this interface.
counters	Displays L2 interface counters for the specified interface.
switchport	Displays L2 interface information.
untrusted-vlan	Displays port member vlan untrusted status.
xsec	Displays xsec configuration.

Examples

The example below shows the output of **show interface fastethernet 1/0**.

```
FE 1/0 is up, line protocol is up
Hardware is FastEthernet, address is 00:0B:86:51:14:D1 (bia 00:0B:86:51:14:D1)
Description: fe1/0
Encapsulation ARPA, loopback not set
Configured: Duplex ( AUTO ), speed ( AUTO )
Negotiated: Duplex (Full), speed (100 Mbps)
MTU 1500 bytes, BW is 100 Mbit
Last clearing of "show interface" counters 15 day 21 hr 34 min 53 sec
link status last changed 15 day 21 hr 32 min 16 sec
    1122463 packets input, 196293018 bytes
    Received 661896 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input error bytes, 0 CRC, 0 frame
    661881 multicast, 460567 unicast
```

The output of this command includes the following parameters:

Parameter	Description
FE 1/0 is...	Displays the status of the specified port.
line protocol is...	Displays the status of the line protocol on the specified port.
Hardware is....	Describes the hardware interface type.
address is...	Displays the MAC address of the hardware interface.
Description	The port type, name, and connector type.
Encapsulation	Encapsulation method assigned to this port.
loopback...	Displays whether or not loopback is set.
Configured	Configured transfer operation and speed.
Negotiated	Negotiated transfer operation and speed.
MTU bytes	MTU size of the specified port in bytes.

Parameter	Description
BW is...	Bandwidth of the link.
Last clearing of “show interface counters”	Time since “show interface counters” was cleared. Below the time, all current counters related to the specified port are listed.
This port is...	Whether or not this port is trusted.
POE status of the port is...	The POE status of the specified port.

```
#show interface fastethernet 1/0 access-group

FE 1/0:

Port-Vlan Session ACL
---------------------
SessionACL             Vlan     Status
```

The output of this command includes the following parameters:

Parameter	Description
SessionACL	Session ACL name.
Vlan	VLAN number.
Status	ACL status.

```
#show interface fastethernet 1/0 counters


Port          InOctets     InUcastPkts     InMcastPkts     InBcastPkts
FE1/0        196310364          460655          661932              15

Port         OutOctets    OutUcastPkts    OutMcastPkts    OutBcastPkts
```

The output of this command includes the following parameters:

Parameter	Description
Port	Port number.
InOctets	Number of octets received through the port.
InUcastPkts	Number of unicast packets received through the port.
InMcastPkts	Number of multicast packets received through the port.
InBcastPkts	Number of broadcast packets received through the port.
OutOctets	Number of octets sent through the port.
OutUcastPkts	Number of unicast packets sent through the port.
OutMcastPkts	Number of multicast packets sent through the port.
OutBcastPkts	Number of broadcast packets sent through the port.

```
#show interface fastethernet 1/0 switchport

Name:  FE1/0
Switchport:  Enabled
Administrative mode:  trunk
Operational mode:  trunk
Administrative Trunking Encapsulation:  dot1q
Operational Trunking Encapsulation:  dot1q
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (Default)
```

The output of this command includes the following parameters:

Parameter	Description
Name	Port name.
Switchport	Whether or not switchport is enabled.
Administrative mode	Administrative mode.
Operational mode	Operational mode.
Administrative Trunking Encapsulation	Encapsulation method used for administrative trunking.
Operational Trunking Encapsulation	Encapsulation method used for operational trunking.
Access Mode VLAN	The access mode VLAN for the specified port.
Trunking Native Mode VLAN	The trunking native mode VLAN for the specified port.
Trunking Vlans Enabled	Number of trunking VLANs currently enabled.
Trunking Vlans Active	Number of trunking VLANs currently active.

```
#show interface fastethernet 1/0 untrusted-vlan

Name:  FE1/0
Untrusted Vlan(s)
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the specified port.
Untrusted Vlan(s)	List of untrusted VLANs.

```
#show interface fastethernet 1/1 xsec
xsec vlan 7 is ACTIVE
```

The output of this command includes the following parameters:

Parameter	Description
`xsec vlan 7 is ACTIVE`	This states that xsec is active on the specified port as well as the associated VLAN.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show interface loopback

```
show interface loopback
```

Description

Displays information about the loopback IP interface.

Syntax

No parameters

Example

The example below shows the output of **show interface loopback** on a W-600 Series Controller controller.

```
#show interface loopback

loopback interface is up line protocol is up
Hardware is Ethernet, address is 00:0B:86:51:14:D0
Internet address is 10.3.49.100  255.255.255.255
```

The output of this command includes the following parameters:

Parameter	Description
`loopback interface is...`	Status of the loopback interface.
`line protocol is...`	Status of the line protocol on the specified port.
`Hardware is...`	Hardware interface type.
`address is...`	MAC address of the loopback interface.
`Internet address is...`	IP address and subnet mask of the loopback interface.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show interface port-channel

```
show interface port-channel
```

Description

Displays information about a specified port-channel interface.

Syntax

Parameter	Description
`access-group`	Displays access groups configured on this interface.
`counters`	Displays L2 interface counters for the specified interface.
`untrusted-vlan`	Displays port member vlan untrusted status.
`xsec`	Displays xsec configuration.

Example

The example below shows the output of **show interface port-channel 0** on a controller.

```
Port-Channel 0 is administratively up
Hardware is Port-Channel, address is 00:00:00:00:00:00 (bia 00:0B:86:F0:36:B1)
Description: Link Aggregate (LACP)
Spanning Tree is disabled
VLAN membership:     1
Switchport priority: 0
Member port:
Last clearing of "show interface" counters 3 day 21 hr 23 min 6 sec
link status last changed 3 day 21 hr 23 min 6 sec
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input error bytes, 0 CRC, 0 frame
    0 multicast, 0 unicast
```

The output of this command includes the following parameters:

Parameter	Description
`Port-Channel 0 is...`	Status of the specified port.
`line protocol is...`	Status of the line protocol on the specified port.
`Hardware is....`	Hardware interface type.
`address is...`	MAC address of the hardware interface.
`Description`	The port type, name, and connector type. If the LAG is created by LACP, it is indicated as shown in the display output above. If the LAG is created by LACP, you can not statically add or delete any ports under that port channel. All other commands are allowed. If LACP is not shown, then the LAG is created by static configuration.
`Spanning Tree is...`	Spanning tree status on the specified port-channel.
`VLAN membership`	Number of VLANs the specified port-channel is associated with.
`Switchport priority`	Switchport priority of the specified port-channel.

Parameter	Description
Last clearing of “show interface counters”	Time since “show interface counters” was cleared. Below the time, all current counters related to the specified port are listed.
Port-channel 0 is...	Whether or not this port-channel is trusted.

```
#show interface port-channel 0 access-group

Port-Channel 0:

Port-Vlan Session ACL
---------------------
SessionACL            Vlan     Status
----------            ----     ------
```

The output of this command includes the following parameters:

Parameter	Description
SessionACL	Session ACL name.
Vlan	VLAN number.
Status	ACL status.

```
#show interface port-channel 0 counters

Port          InOctets     InUcastPkts     InMcastPkts     InBcastPkts
PC 0:                0               0               0               0

Port         OutOctets    OutUcastPkts    OutMcastPkts    OutBcastPkts
```

The output of this command includes the following parameters:

Parameter	Description
PC	Port number.
InOctets	Number of octets received through the port.
InUcastPkts	Number of unicast packets received through the port.
InMcastPkts	Number of multicast packets received through the port.
InBcastPkts	Number of broadcast packets received through the port.
OutOctets	Number of octets sent through the port.
OutUcastPkts	Number of unicast packets sent through the port.
OutMcastPkts	Number of multicast packets sent through the port.
OutBcastPkts	Number of broadcast packets sent through the port.

```
#show interface port-channel 0 untrusted-vlan

Name:  FE1/0
Untrusted Vlan(s)
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the specified port.
`Untrusted Vlan(s)`	List of untrusted VLANs.

```
#show interface port-channel 0 xsec
xsec vlan 7 is ACTIVE
```

The output of this command includes the following parameters:

Parameter	Description
`xsec vlan 7 is ACTIVE`	This states that xsec is active on the specified port as well as the associated VLAN.

Command History

Release	Modification
ArubaOS 3.4.1	Modified to display LACP when applicable.
ArubaOS 3.0.	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show interface tunnel

```
show interface tunnel
```

Description

Displays information about tunnel interfaces.

Syntax

No parameters

Example

The example below shows the output of **show interface tunnel**.

```
#show interface tunnel 2000

Tunnel 2000 is up line protocol is up
Description: Tunnel Interface
Internet address is 3.3.3.1 255.255.255.0
Source  192.168.203.1
Destination 192.168.202.1
Tunnel mtu is set to 1100
Tunnel is an IP GRE TUNNEL
```

he output of this command includes the following parameters:

Parameter	Description
`Tunnel 2000 is...`	Status of the specified tunnel.
`line protocol is...`	Displays the status of the line protocol on the specified tunnel.
`Description`	Description of the specified interface.
`Internet address is...`	IP address and subnet mask of the specified interface.
`Source`	IP address of the tunnel's source.
`Destination`	IP address of the tunnel's source.
`Tunnel mtu is set to...`	Size of the specified tunnel's MTU.
`Tunnel is an...`	Description of the specified tunnel.
`Tunnel is...`	Whether or not the specified tunnel is trusted.
`Inter tunnel flooding is...`	Status of inter tunnel flooding on the specified tunnel.
`Tunnel keepalive is...`	Status of tunnel keepalive on the specified tunnel.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show interface vlan

```
show interface vlan
```

Description

Displays information about a specified VLAN interface.

Syntax

No parameters

Example

The example below shows the output of **show interface vlan 1**on a W-600 Series Controller controller.

```
#show interface vlan 1

VLAN1 is up line protocol is up
Hardware is CPU Interface, Interface address is 00:0B:86:51:14:D0 (bia
00:0B:86:51:14:D0)
Description: 802.1Q VLAN
Internet address is 10.3.49.50  255.255.255.0
Routing interface is enable, Forwarding mode is enable
Directed broadcast is disabled
Encapsulation 802, loopback not set
MTU 1500 bytes
```

The output of this command includes the following parameters:

Parameter	Description
`VLAN1 is...`	Status of the specified VLAN
`line protocol is...`	Displays the status of the line protocol on the specified port
`Hardware is...`	Describes the hardware interface type
`Interface address is...`	Displays the MAC address of the hardware interface
`Description`	Description of the specified VLAN
`Internet address is...`	IP address and subnet mask of the specified VLAN
`Routing interface is...`	Status of the routing interface
`Forwarding mode is...`	Status of the forwarding mode
`Directed broadcast is...`	Displays whether or not directed broadcast is enabled
`Encapsulation`	Encapsulation type
`loopback...`	Loopback status
`MTU`	MTU size of the specified port in bytes
`Last clearing of “show interface counters”`	Time since “show interface counters” was cleared
`link status last changed`	Time since link status last changed
`Proxy ARP is...`	Status of proxy ARP on the specified interface

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show inventory

```
show inventory
```

Description

Displays hardware inventory of the controller.

Syntax

No parameters

Example

Issue this command to display the hardware component inventory of the controller.

```
Supervisor Card slot              : 1
Mobility Processor                : FPGA Rev 0x30030920
Mobility Processor Assembly#      : 2010027B
Mobility Processor Serial#        : F00488202
SC      Assembly#                 : 2010032B (Rev:02.00)
SC      Serial#                   : FP0001470 (Date:07/01/24)
SC      Model#                    : M3mk1
Mgmt Port HW MAC Addr             : 00:0B:86:F0:23:02
HW MAC Addr                       : 00:0B:86:01:C5:00 to 00:0B:86:01:C5:7
FXPLD Version                     : (Rev: 20)
PEER Supervisor Card              : Absent
Line Card 0                       : Absent
Line Card 1                       : Not accessible from this SC
Line Card 2                       : Present
Line Card 2 FPGA                  : LCCI Rev 0x6
Line Card 2 Switch Chip           : Broadcom 56308 Rev 0x3
Line Card 2 Mez Card              : Present
Line Card 2 SPOE                  : Present
Line Card 2 Sup Card 0            : Absent
Line Card 2 Sup Card 1            : Present ( Active )
Line Card 2 Assembly#             : 2000001C (Rev:03.00) (24FE+2GE)
Line Card 2 Serial#               : C00000277 (Date:02/22/05)
Line Card 2 SPOE Assembly#        : 2000020B (Rev:01.00) (SPOE-2)
Line Card 2 SPOE Serial#          : FP0000100
Line Card 2 MEZZ Assembly#        : 2000002A (Rev:01.00)
Line Card 2 MEZZ Serial#          : S00000540
Line Card 3                       : Present
Line Card 3 FPGA                  : LCCI Rev 0x6
Line Card 3 Switch Chip           : Broadcom 56308 Rev 0x3
Line Card 3 Mez Card              : Present
Line Card 3 SPOE                  : Present
Line Card 3 Sup Card 0            : Absent
Line Card 3 Sup Card 1            : Present ( Active )
Line Card 3 Assembly#             : 2000001C (Rev:03.00) (24FE+2GE)
Line Card 3 Serial#               : C00007293 (Date:09/27/05)
Line Card 3 SPOE Assembly#        : 2000003B (Rev:02.00) (SPOE-1)
Line Card 3 SPOE Serial#          : S00001750
Line Card 3 MEZZ Assembly#        : 2000002A (Rev:01.00)
Line Card 3 MEZZ Serial#          : C00007172
FAN 0                             : OK, Speed High
FAN 1                             : OK, Speed High
FAN 2                             : OK, Speed High
Fan Tray Assembly#                : 2000007C (Rev:01.00)
Fan Tray Serial#                  : C00013879 (Date:12/18/04)
```

The output includes the following parameters:

Note: The output of this command will vary between controllers

Parameter	Description
`Supervisor Card Slot`	Supervisor card slot number
`Mobility Processor`	Revision of the image downloaded to the FPGA. This can change if a newer image is included in a newer release.
`SC Assembly#`	Assembly number of the supervisor card.
`SC Serial#`	Serial number of the supervisor card.
`SC Model#`	Model number of the supervisor card.
`Mgmt Port HW MAC Address`	MAC address of the mgmt port
`HW MAC Address`	MAC address
`FXPLD Version`	Revision of programmable logic device on supervisor card.
`PEER Supervisor Card`	States whether or not a PEER supervisor card is present.
`Line Card <slot number>`	States whether or not a line card is present in the specified slot
`Line Card <slot number> FPGA`	Name/type of FPGA associated with the specified line card slot
`Line Card <slot number> Switch Chip`	Name/type of switch card associated with the specified line card slot
`Line Card <slot number> Mez Card`	States whether or not a mezzanine card is present in the specified slot
`Line Card <slot number> SPOE`	States whether or not a SPOE card is present in the specified slot
`Line Card <slot number> Sup Card 0`	States whether or not a supervisor card 0 is present in the specified slot
`Line Card <slot number> Sup Card 1`	States whether or not a supervisor card 1 is present in the specified slot
`Line Card <slot number> Assembly#`	Assembly number of the line card in the specified slot
`Line Card <slot number> Serial#`	Serial number of the line card in the specified slot
`Line Card <slot number> SPOE Assembly#`	Assembly number of SPOE line card in the specified slot
`Line Card <slot number> SPOE Serial#`	Serial number of SPOE line card in the specified slot
`Line Card <slot number> MEZZ Assembly#`	Assembly number of the mezzanine card in the specified slot
`Line Card <slot number> MEZZ Serial#`	Serial number of the mezzanine card in the specified slot

Parameter	Description
FAN *<Fan number>*	Status of the specified fan
Fan Tray Assembly#	Assembly number of the fan tray
Fan Tray Serial#	Serial number of fan tray
Back Plane Assembly#	Assembly number of the back plane
Back Plane Serial#	Serial number of the back plane
Power Supply Type	Power supply type
Power Supply *<power supply number>*	Power supply status
M3mk1 Card Temperatures • M3mk1 card • CPU	• The temperature from the sensor on the supervisor card • The temperature from the CPU die
AMP Card Temperatures • Processor Card • Mobility Processor	• The temperature from the sensor on the Mobility Processor card • The temperature from the FPGA die
M3mk1 Card Voltages	This parameter displays to columns of voltages for many components displayed previously by this command. The voltage displayed in the right column should match the corresponding value in the left column, generally with +/- 5%.

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show ip access-group

```
show ip access-group
```

Description

Display access control lists (ACLs) configured for each port on the controller.

Syntax

No parameters.

Examples

The example below shows part of the output of this command. If a port does not have a defined session ACL, the *Port-Vlan Session ACL* table will be blank.

```
(host) # show ip access-group
FE 1/0:
Rx access list 200 is applied
session access list User14 is applied

Port-Vlan Session ACL
---------------------
SessionACL            Vlan     Status
----------            ----     ------
coltrane              22       configured
```

The output of this command includes the following parameters:

Parameter	Description
`Session ACL`	Name of the ACL applied to the interface.
`VLAN`	If the ACL was applied to a VLAN associated with this port, this column will show the VLAN ID.
`Status`	Shows whether or not the session ACL is configured.

Related Commands

Command	Description
`interface fastethernet | gigabitethernet ip access-group`.	Configure an access group for an interface.

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4	The VLAN output parameters was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on master or local controllers

show ip access-list

```
show ip access-list {brief|<string>}
```

Description

Display a table of all configured access control lists (ACLs), or show details for a specific ACL.

Syntax

Parameter	Description
`brief`	Display a table of information for all ACLs.
`<string>`	Specify the name of a single ACL to display detailed information on that ACL.

Examples

The example below shows general information for all ACLs in the Access List table.

```
(Host) #show ip access-list brief

Access list table
-----------------
Name               Type      Use Count  Roles
----               ----      ---------  -----
200                eth
33                 standard
allowall           session   2          trusted-ap default-vpn-role
ap-acl             session   2          rap_role ap-role
captiveportal      session   4          coltrane-logon wizardtest-logon test-logon logon
control            session   7          ap-role coltrane-logon wizardtest-logon guest stateful test-logc
cplogout           session   1          guest
default            session
guest              session
log-https          session
srcnat             session
stateful-dot1x     session   2          stateful-dot1x logon
stateful-kerberos  session
validuser          session   1          test-24325
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of an access-control list (ACL).
Type	Shows that the ACL is one of the following ACL policy types: • Ethertype • Standard • Session • MAC • Extended
Use Count	Number of rules defined in the ACL.
Roles	Names of user roles associated with the ACL.

Include the name of a specific ACL to show detailed configuration information for that ACL.

```
(Host)# show ip access-list stateful-dot1x

ip access-list session stateful-dot1x
stateful-dot1x
--------------
Priority  Source  Destination  Service   Action    TimeRange  Log  Expired  Queue  TOS  8021P  Blacklist  Mirror  DisScan
--------  ------  -----------  -------   ------    ---------- ---  -------  -----  ---  -----  ---------  -------  -------
1         any     any          svc-dns   permit                            Low
2         any     any          svc-dhcp  permit                            Low
3         any     127.0.0.1    udp 1812  redirect                          Low
```

The output of this command may include some or all of the following parameters:

Parameter	Description
Priority	Name of an access-control list (ACL).
Source	The traffic source, which can be one of the following: • **alias**: The network resource (use the netdestination command to configure aliases; use the show netdestination command to see configured aliases) • **any**: Matches any traffic. • **host**: A single host IP address. • **network**: The IP address and netmask. • **user**: The IP address of the user. • **localip**: The set of all local IP addresses on the system, on which the ACL is applied.
Destination	The traffic destination, which can be one of the following: • **alias**: The network resource (use the netdestination command to configure aliases; use the show netdestination command to see configured aliases) • **any**: Matches any traffic. • **host**: A single host IP address. • **network**: An IP address and netmask. • **user**: The IP address of the user. • **localip**: The set of all local IP addresses on the system, on which the ACL is applied.
Service	Network service, which can be one of the following: • An IP protocol number (0-255). • The name of a network service (use the show netservice command to see configured services). • **any**: Matches any traffic. • **tcp**: A TCP port number (0-65535). • **udp**: A UDP port number (0-65535).
Action	Action if rule is applied, which can be one of the following: **deny**: Reject packets. **dst-nat**: Perform destination NAT on packets. **dual-nat**: Perform both source and destination NAT on packets. **permit:** Forward packets. **redirect**: Specify the location to which packets are redirected, which can be one of the following: • Datapath destination ID (**0-65535**). • **esi-group**: Specify the ESI server group configured with the esi group command • **opcode**: Specify the datapath destination ID (0x33, 0x34, or 0x82). Do not use this parameter without proper guidance from Dell PowerConnect **tunnel:** Specify the ID of the tunnel configured with the interface tunnel command. **src-nat**: Perform source NAT on packets.
Timerange	Any defined time range for this rule.
Log	Shows if the rule was configured to generate a log message when the rule is applied.
Expired	Shows if the rule has expired.

Parameter	Description
Queue	Shows if the rule assigns a matching flow to a priority queue (high/low).
Tos	Specifies the configured ToS value (0-63)
8021.p	802.11p priority level applied by the rule (0-7).
Blacklist	Shows if the rule should blacklist any matching user.
Mirror	Shows if the rule was configured to mirror all session packets to datapath or remote destination.
DisScan	Shows if the rule was configured to pause ARM scanning while traffic is present.

Related Commands

Command	Description
`ip access-list session`	Configure an access list for an interface.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on master or local controllers

show ip cp-redirect-address

```
show ip cp-redirect-address
```

Description

Show the captive portal automatic redirect IP address.

Syntax

No parameters.

Examples

The example below shows the IP address to which captive portal users are automatically directed.

```
(host) # show ip cp-redirect-address

Captive Portal redirect Address... 10.3.63.11
```

Related Commands

Command	Description
ip cp-redirect-address	This command configures a redirect address for captive portal.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on master or local controllers

show ip dhcp

```
show ip dhcp {binding|database|statistics}
```

Description

Show DHCP Server Settings.

Syntax

Parameter	Description
`binding`	Show DHCP server bindings.
`database`	Show DHCP server settings.
`statistics`	Show DHCP pool statistics.

Examples

The example below shows DHCP statistics for two configured networks.

```
(host) # show ip dhcp statistics

Network Name         172.19.42.0/24
   Free leases       137
   Active leases     115
   Expired leases    0
   Abandoned leases  0

Network Name         10.14.86.0/24
   Free leases       126
   Active leases     126
   Expired leases    0
   Abandoned leases  0
```

The output of this command includes the following parameters:

Parameter	Description
Network Name	Range of addresses that the DHCP server may assign to clients.
Free leases	Number of available DHCP leases.
Expired leases	Number of leases that have expired because they have extended past their valid lease period.
Abandoned leases	Number of abandoned leases. Abandoned leases will not be reassigned unless there are no free leases available.

Related Commands

Command	Description
`ip dhcp pool`	This command configures a DHCP pool on the controller.

Command History

Introduced in ArubaOS 3.0.

show ip domain-name

```
show ip domain-name
```

Description

Show the full domain name and server.

Syntax

No parameters.

Examples

The example below shows that the IP domain lookup feature is enabled, but that no DNS server has been configured on the controller.

```
(host) #show ip domain-name

IP domain lookup:       Enabled
IP Host.Domain name:    MyCompany2400.

No DNS server configured
```

Related Commands

Command	Description
`ip domain lookup`	This command enables Domain Name System (DNS) hostname to address translation.
`ip domain-name`	This command configures the default domain name.
`ip dhcp pool`	This command configures a DHCP pool on the controller.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on master or local controllers

show ip igmp

```
show ip igmp config|counters|{group maddr <maddr>}|{interface [vlan <vlan>]}|{proxy-
group vlan <vlan>}|{proxy-mobility-group maddr <maddr>}|proxy-mobiity-stats|proxy-stats
```

Description

Display Internet Group Management Protocol (IGMP) timers and counters.

Syntax

Parameter	Description
`config`	Show the current IGMP configuration
`counters`	Display a list counters for the following IGMP queries: • received-total • received-queries • received-v1-reports • received-v2-reports • received-leaves • received-unknown-types • len-errors • checksum-errors • not-vlan-dr • transmitted-queries • forwarded
`group maddr <maddr>`	Show IGMP group information
`interface vlan <vlan>`	Show IGMP interface information
`proxy-group vlan <vlan>`	Show IGMP proxy group information for a specific interface.
`proxy-mobility-group maddr <maddr>`	Display the IGMP proxy group information stored for mobile clients which are away from the controller.
`proxy-mobiity-stats`	Display the most important messages exchanged between the mobility process and the IGMP proxy.
`proxy-stats`	Display the number of messages transmitted and received by the IGMP proxy on the upstream interface

Examples

The example below displays the IGMP interface table for all VLANs on the controller.

```
(host) # show ip igmp interface vlan 2
IGMP Interface Table
--------------------
VLAN  Addr        Netmask        MAC Address        IGMP      Snooping  Querier     Destination IGMP Proxy
----  ----        -------        -----------        ----      --------  -------     ----------- -----------
64    10.6.4.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled  10.6.4.252  CP           disabled
65    10.6.5.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled  10.6.5.252  CP           disabled
1     10.6.2.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled  10.6.2.252  CP           disabled
66    10.6.6.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled  10.6.6.252  CP           disabled
63    10.6.3.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled  10.6.3.252  CP           disabled
```

The output of this command includes the following parameters:

Parameter	Description
VLAN	A VLAN ID number.
Addr	IP address of a VLAN router.
Netmask	Subnet mask for the IP address.
MAC Address	MAC destination address.
IGMP	Shows if IGMP proxy is enabled or disabled.
Snooping	Shows if IGMP snooping is enabled or disabled.
Querier	IP address of an IGMP querier.
Destination	Traffic destination.
IGMP Proxy	Shows if IGMP proxy.

The following example displays the current IGMP configuration settings for the controller.

```
(host) #show ip igmp config

IGMP Config
-----------
Name                              Value
----                              -----
robustness-variable               2
query-interval                    125
query-response-interval           100
startup-query-interval            31
startup-query-count               2
last-member-query-interval        10
last-member-query-count           2
version-1-router-present-timeout  400
```

The output of this command includes the following parameters:

Parameter	Description
robustness-variable	This variable is increased from its default level of 2 to allow for expected packet loss on a subnetwork.
query-interval	Interval, in seconds, at which the controller sends host-query messages to the multicast group address 224.0.0.1 to solicit group membership information.
query-response-interval	Maximum time, in .1 second intervals, that can elapse between when the controller sends a host-query message and when it receives a response. This must be less than the **query-interval**.
startup-query-count	Number of queries that the controller sends out on startup, separated by startup-query-interval. The default setting is the value of the **robustness-variable** parameter.
startup-query-interval	Interval, in seconds, at which the controller sends general queries on startup. The default value of this parameter is 1/4 of the **query-interval**.
last-member-query-count	Number of group-specific queries that the controller sends before assuming that there are no local group members.
last-member-query-interval	Maximum time, in seconds, that can elapse between group-specific query messages.

Parameter	Description
`version-1-router-present-timeout`	Timeout, in seconds, if the controller detects a version 1 IGM router.

Related Commands

Command	Description
`ip igmp`	This command configures Internet Group Management Protocol (IGMP) timers and counters.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on master controllers.

show ip mobile

```
show ip mobile
   active-domains
   binding [<host-ip>|<host-macaddr>|brief]
   domain [<name>]
   global
   hat
   host [<host-ip>|<host-macaddr>|brief]
   packet-trace [<count>]
   remote <host-ip>|<host-macaddr>
   trace <ip-addr>|<mac-addr>|{force <ip-addr>|<mac-addr>}
   traffic dropped|foreign-agent|home-agent|proxy|proxy-dhcp
   trail <host-ip>|<host-macaddr>
   tunnel
   visitor [<host-ip>|<host-macaddr>|brief]
```

Description

Display statistics and configuration information for the mobile protocol.

Syntax

Parameter	Description
`active domains`	IP mobility domains active on this switch
`binding`	Display a list of Home Agent Bindings
`[<host-ip>]`	Filter the Home Agent Bindings list to display data for a specific host IP address.
`[<host-macaddr>]`	Filter the Home Agent Bindings list to display data for a specific host MAC address.
`[brief]`	Limit the output of this command to show just two lines of data.
`domain [<name>]`	Display subnet, VLAN and home agent information for all mobility domains, or specify a mobility domain name to view data for that domain only.
`global`	View the current Mobility Agents global configuration
`hat`	Display the Active Home Agent table.
`host`	Display a list of Mobile IP hosts.
`[<host-ip>]`	Filter the Mobile Host List to display data for a specific host IP address.
`[<host-macaddr>]`	Filter the Mobile Host List to display data for a specific host MAC address.
`[brief]`	Limit the output of this command to show just two lines of data.
`packet-trace [<count>]`	Packet trace between Datapath-Mobility
`remote <host-ip>|<host-macaddr>`	Display Mobile IP remote host(s)
`trace`	Show if the Mobile IP feature will poll remote controllers for mobility status of station
`<ip-addr>`	Host IP address
`<mac-addr>`	Host MAC address
`force <ip-addr>|<mac-addr>`	Show if the Mobile IP feature will poll remote controllers for mobility status of station.
`traffic`	Display mobile IP protocol statistics for: • Proxy DHCP • Proxy Mobile IP • Home Agent Registrations • Foreign Agent Registrations • Registration Revocations
`dropped`	Show only counters for dropped mobility traffic.
`foreign-agent`	Show only mobile IP foreign agent statistics. A foreign agent is the controller which handles all mobile IP communication with a home agent on behalf of a roaming client.
`home-agent`	Show only mobile IP home agent statistics. A home agent for a mobile client is the controller where the client first appears when it joins the mobility domain.
`proxy`	Show only counters for mobile IP proxy traffic.
`proxy-dhcp`	Show only counters for mobile IP proxy DHCP traffic.
`trail <host-ip>|<host-macaddr>`	Show the mobile IP roaming trail by entering a host's IP or MAC address.
`tunnel`	Show the Mobile Tunnel Table for IPIP Tunnels.

Parameter	Description
visitor	Display a list of mobile nodes visiting a foreign agent.
[<host-ip>]	Filter the Foreign Agent Visitor list to display data for a specific host IP adddress.
[<host-macaddr>]	Filter the Foreign Agent Visitor list to display data for a specific host MAC adddress.
[brief]	Limit the output of this command to show just two lines of data.

Examples

The example below lists mobility domains configured on the controller, and shows information for any subnets defined on these domains.

```
(host) #show ip mobile domain
Mobility Domains:, 2 domain(s)
------------------------------

Domain name default
   Home Agent Table, 0 subnet(s)

Domain name newdomain
   Home Agent Table, 2 subnet(s)
   subnet          mask            VlanId Home Agent         Description
   --------------- --------------- ------ ---------------    ----------------------
   10.2.124.76     255.255.255.255 1      10.4.62.2          Corporate mobility entry
   172.21.5.50     255.255.255.255 1      10.4.62.2          Reserved entries
```

The output of this command includes the following parameters:

Parameter	Description
subnet	Subnet configured for the IP mobility service.
mask	Subnet mask
VLAN ID	VLAN ID of the VLAN used by the subnet.
Home Agent	IP address of the home agent or mobility agent.
Description	Description of the HAT entry.

Use the **show ip mobile host** command to track mobile users.

```
(host) #show ip mobile host

Mobile Host List, 1 host(s)

--------------------------

00:40:96:a6:a1:a4  10.0.100.194
   Roaming Status: Home Switch/Home VLAN, Service time 0 days 00:06:47
   Home VLAN 100 on network 10.0.100.0/24
   DHCP lease for corporate-240 at Thu Sep 21 15:11:44 2006 for 7200 secs from 10.3.26.1
```

The output of this command includes the following parameters:

Parameter	Description
<mac-addr> <ip-addr>	MAC and IP addresses of the host
Roaming Status	Displays how long the host has used its current controller and VLAN.
Home VLAN	VLAN ID, IP address and subnet of the home VLAN.

Parameter	Description
`DHCP lease`	Displays the amount of time the station has had its current DHCP lease.

Related Commands

Command	Description
`ip mobile active-domain`	This command configures the mobility domain that is active on the controller.
`ip mobile domain`	This command configures the mobility domain on the controller.
`ip mobile foreign-agent`	This command configures the foreign agent for IP mobility.
`ip mobile home-agent`	This command configures the home agent for IP mobility.
`ip mobile proxy`	This command configures the proxy mobile IP module in a mobility-enabled controller.
`ip mobile revocation`	This command configures the frequency at which registration revocation messages are sent.
`ip mobile trail`	This command configures the capture of association trail for all devices.

Command History

Command introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on master or local controllers

show ip nat pool

```
show ip nat pool
```

Description

Display pools of IP addresses for network address translation (NAT.

Syntax

No parameters

Examples

The example below shows the current NAT pool configuration on the controller.

```
(host) # show ip nat pools
NAT Pools
---------
Name  Start IP  End IP      DNAT IP
----  --------  ---------   -------
2net   2.1.1.1   2.1.1.125
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the NAT pool.
`Start IP`	IP address that defines the beginning of the range of source NAT addresses in the pool.
`End IP`	IP address that defines the end of the range of source NAT addresses in the pool.
`DNAT IP`	Destination NAT IP address, if defined.

Related Commands

Command	Description
`ip nat`	This command configures a pool of IP addresses for network address translation (NAT).

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Though this command is available in the operating system, you must have a PEFNG license to configure a NAT pool.	Available in Config or Enable mode on master or local controllers

show ip ospf

```
show ip ospf [database]|[debug route]|[interface tunnel|vlan <id>]|[neighbor]|
[redistribute]|[subnet]
```

Description

Display statistics and configuration information for the Open Shortest Path First (OSPF) routing protocol.

Syntax

Parameter	Description
`database`	Show database information for the OSPF protocol.
`debug route`	Show debugging information for OSPF routes.
`interface tunnel|vlan <id>`	Display the status of OSPF on an individual interface by specifying a tunnel or VLAN ID number.
`neighbor`	Display data for OSPF neighboring routers.
`redistribute`	Display OSPF route distribution information.
`subnet`	Display the subnets manually added to the Subnet Exclude List via the **`router ospf subnet exclude <addr> <mask>`** command.

Example

If you issue this command without any of the optional parameters described in the table above, the **show ip ospf** command will display general router and area settings for the OSPF.

```
(host) (config-subif)# show ip ospf
OSPF is currently running with Router ID 123.45.110.200
Number of areas in this router is 1
Area 10.1.1.0
   Number of interfaces in this area is 2
   Area is totally stub area
   SPF algorithm executed 0 times
```

The output of this command includes the following parameters.

Parameter	Description
OSPF Router ID	Verifies that OSPF is running and the router ID that OSPF is running on.
Number of areas	List the number of areas configured in the router.
Area	Displays the Area ID followed by: • number of interfaces in the area • indicates if the area is a totally stub area • number of times the SPF algorithm has been executed

To display OSPF settings for an individual interface, you must specify a VLAN or tunnel ID number. The example below displays part of the output of the **show ip ospf interface vlan** command.

```
(host) # show ip ospf interface vlan 10
Vlan 3 is up, line protocol is up
Internet Address 3.3.3.1, Mask 255.255.255.0, Area 10.1.1.1
Router ID 10.4.131.227, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAIT, Priority 1
Designated Router id 0.0.0.0, Interface Address 3.3.3.1
Backup designated Router id 0.0.0.0, Interface Address 3.3.3.1
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Neighbor Count is 0
Tx Stat: Hellos 1 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 1
Rx Stat: Hellos 0 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 0
         DisCd 0 BadVer 0 BadNet 0 BadArea 0 BadDstAdr 0 BadAuType 0
         BadAuth 0 BadNeigh 0 BadPckType 0 BadVirtLink 0
...
```

The output may include some or all of the following parameters.

Parameter	Description
Vlan <number>	Identifies that the interface type and ID are up and functional.
Internet Address	Internet address, network mask, and area assigned to the interface.
Router ID	Displays the router ID, that the network type is Broadcast, and the cost value.
Transmit Delay	Details of the transmit delay, state, and priority.
Designated Router	Details of the designated router ID and interface address.
Backup Designated Router ID	Details of the backup router ID and interface address.
Timer intervals configured	Details of elapse time intervals for Hello, Dead, Transmit (wait), and retransmit.
Neighbor Count	Details the number of neighbors and adjacent neighbors.
Tx Stat	Counters and statistics for transmitted data. • **Hellos**: Number of transmitted hello packets. These packets are sent every hello interval. • **DbDescr**: Number of transmitted database description packets. • **LsReq**: Number of transmitted link state request packets. • **LsUpdate**: Number of transmitted link state update packets. • **LsAck**: Number of transmitted link state acknowledgment packets • **Pkts**: Total number of transmitted packets.
Rx Stat	Counters and statistics for received data. • **Hellos**: Number of received hello packets. These packets are sent every hello interval. • **DbDescr**: Number of received database description packets. • **LsReq**: Number of received link state request packets. • **LsUpdate**: Number of received link state update packets. • **LsAck**: Number of received link state acknowledgment packets • **Pkts**: Total number of received packets.
DisCd	Number of received packets that are discarded.
BadVer	Number of received packets that have bad OSPF version number.
BadNet	Number of received packets that belong to different network than the local interface.
BadArea	Number of received packets that belong to different area than the local interface.
BadDstAdr	Number of received packets that have wrong destination address.

Parameter	Description
BadAuType	Number of received packets that have different authentication type than the local interface.
BadAuth	Number of received packets where authentication failed.
BadNeigh	Number of received packets which didn't have a valid neighbor.
BadPckType	Number of received packets that have wrong OSPF packet type.
BadVirtLink	Number of received packets that didn't match have a valid virtual link.

Related Commands

Command	Description
`ip ospf`	Configure OSPF on the interface
`router ospf`	Configure OSPF on the router

Command History

Introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on master or local controllers

show ip pppoe-info

```
show ip pppoe-info
```

Description

Display configuration settings for Point-to-Point Protocol over Ethernet (PPPoE).

Syntax

No parameters.

Examples

The example below shows the current PPPoE configuration.

```
(host) #show ip pppoe-info

PPPoE username: rudolph123
PPPoE password: <HIDDEN>
PPPoE service name: ppp2056
PPPoE VLAN: 22
```

The output of this command includes the following parameters:

Parameter	Description
`PPPoE username`	PAP username configured on the PPPoE access concentrator.
`PPPoE password`	If this parameter displays the word **<HIDDEN>**, a PAP password is configured on the PPPoE access concentrator. If this parameter is **<NONE>**, there is no PPOE password configured.
`PPPoE service name`	PPPoE service name.
`PPPoE VLAN`	VLAN configured to use PPPoE to obtain an IP address via the command **interface vlan <id> ip address pppoe.**

Related Commands

Command	Description
`ip pppoe-password`	This command configures the PPP over Ethernet (PPPoE) password.
`ip pppoe-service-name`	This command configures the PPP over Ethernet (PPPoE) service name.
`ip pppoe-username`	This command configures the PPP over Ethernet (PPPoE) username.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on master or local controllers

show ip radius

```
show ip radius nas-ip|source-interface
```

Description

Display global parameters for configured RADIUS servers.

Syntax

Command	Description
`nas-ip`	Show the Network Access Server (NAS) IP address attribute sent in outgoing RADIUS requests
`source-interface`	Show the source address of outgoing RADIUS requests

Examples

The example below shows the RADIUS client NAS IP address.

```
(host) #show ip radius nas-ip

RADIUS client NAS IP address = 10.168.254.221
```

Related Commands

Command	Description
`ip radius`	This command configures global parameters for configured RADIUS servers.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on master or local controllers

show ip route

```
show ip route [static]
```

Description

View the Dell controller routing table.

Syntax

Command	Description
`static`	Include this optional parameter to display only static routes.

Usage Guidelines

This command displays static routes configured on the controller via the ip route command. Use the ip default-gateway command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect the controller.

Examples

The example below shows the ip address of routers and the VLANs to which they are connected.

```
(host) #show ip route

Codes: C - connected, O - OSPF, R - RIP, S - static
       M - mgmt, U - route usable, * - candidate default

Gateway of last resort is 10.6.2.254 to network 0.0.0.0

S*    0.0.0.0/0  [1/0] via 10.6.2.254*
C    10.9.2.0 is directly connected, VLAN1
C    10.9.3.0 is directly connected, VLAN63
C    10.9.4.0 is directly connected, VLAN64
C    10.9.5.0 is directly connected, VLAN65
C    10.9.6.0 is directly connected, VLAN66
C    0.0.0.0 is directly connected, Tunnel 1
C    10.100.103.253 is an ipsec map default-local-master-ipsecmap
```

Related Commands

Command	Description
`ip radius`	This command configures global parameters for configured RADIUS servers.

Command History

Introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on master or local controllers

show ipc statistics app-ap

```
show ipc statistics app-ap {am|sapd|sta} {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr
<ip-addr>}
```

Description

Display Inter Process Communication (IPC) statistics for a specific AP or BSSID.

Syntax

Parameter	Description
`am`	Show IPC statistics for an air monitor.
`sapd`	Show IPC statistics for the SAPD process.
`stm`	Show IPC statistics for station management communications.
`ap-name <ap-name>`	Show IPC statistics for an AP with a specific name.
`bssid <bssid>`	Show IPC statistics for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show IPC statistics for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Usage Guidelines

Issue this command at the request of Dell support to troubleshoot application errors.

Example

The following example shows IPC statistics for the SAPD process on an AP named **mpp125**.

```
(host) #show ipc statistics app-ap sapd ap-name mpp125
Local Statistics
To application      Tx Msg   Tx Blk   Tx Ret  Tx Fail   Rx Ack   Rx Msg  Rx Drop   Rx Err   Tx Ack
MESH                     3        0        1        0        3        1        1        0        1
RF Client                1        0        0        0        1        1        0        0        1
STM                      1        0        0        0        1        0        0        0        0
Nanny                    1        0        0        0        1        0        0        0        0

Remote Statistics
To application      Tx Msg   Tx Blk   Tx Ret  Tx Fail   Rx Ack   Rx Msg  Rx Drop   Rx Err   Tx Ack
AMAPI CLI Client         0        0        0        0        0        1        0        0        1
STM                    248        0        0        0        0      248        0        0        0

Allocated Buffers   0
Static Buffers      1
Static Buffer Size  1444
```

The output of this command includes the following data columns:

Parameter	Description
Tx Msg	Number of transmitted messages.
Tx Blk	Number of blocking messages transmitted.
Tx Ret	Number of transmitted messages that were returned.
Tx Fail	Number of failure messages that were transmitted.
Rx Ack	Number of received acknowledgements.

Parameter	Description
Rx Msg	Number of received messages.
Rx Drop	Number of received messages that were dropped.
Rx Err	Number of received messages with errors.
Tx Ack	Number of transmitted acknowledgements.
Allocated Buffers	Number of allocated buffers for IPC messages.
Static Buffers	Number of static buffers for IPC messages.
Static Buffer Size	Size of the static buffer.

Command History

This command was available in ArubaOS 1.0.

Command Informationh

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show ipc statistics app-id

```
show ipc statistics app-id <app-id>
```

Description

Display Inter Process Communication (IPC) statistics for a specific AP or BSSID.

Syntax

Parameter	Description
`<app-id>`	Application ID number. This number must be obtained from Dell support.

Usage Guidelines

Issue this command at the request of Dell support to troubleshoot application errors.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show ipc statistics app-name

```
show ipc statistics app-name <name>
```

Description

Display Inter Process Communication (IPC) statistics for a specific application.

Syntax

Parameter	Description	
<name>	One of the following application names: • **aaa**: Administrator Authentication • **ads**: Anomaly Detection • **authmgr**: User Authentication • **certmgr**: Certificate Manager • **cfgm**: Config Manager • **cts**: Transport Service • **dbsync**: Database Synchronization • **dhcp**: DHCP Server • **esi**: Server Load Balancing • **fpapps**: Layer 2,3 control • **httpd**: HTTPD • **ike**: IKE Daemon	• **l2tp**: L2TP • **licensemgr**: License Manager • **mobileip**: Mobile IP • **ntp**: NTP Daemon • **pim**: Protocol Independent Multicast • **pktfilter**: Packet Filter • **pptp**: PPTP • **profmgr**: Profile Manager • **publisher**: Publish subscribe service • **resolver**: Resolver • **snmp**: SNMP agent • **stm**: Station Management

Example

The following example shows IPC statistics for the **STM** process.

```
(host) #show ipc statistics app-name stm

Local Statistics
To application      Tx Msg   Tx Blk   Tx Ret  Tx Fail   Rx Ack   Rx Msg  Rx Drop   Rx Err   Tx Ack
AMAPI Web Client         0        0        0        0        0    34405        0        0    34405
Layer2/3            233098        1        0        0   233095       12        0        0       12
Authentication Se  1076236        0        0        0  1076236        0        0        0        0
Authentication       54494     7448       54        1    54050   468811        0        0        0
Publisher                4        0        0        0        4        2       52        0        2
AMAPI CLI Client         1        0        0        0        1      702        0        0      702
Profile Manager          1        1        0        0        1        0        0        0        0
Mobile IP          1120303        0        0        0  1076236        1        0        0        0
Syslog Manager           2        2        0        0        2        0        0        0        0
WMS                      0        0        0        0        0       19        0        0       19
PIM                      2        1        0        0        2        1        1        0        1
Configuration Man        2        1        0        0        2       13        0        0       12
License Manager          1        1        0        0        1        0        0        0        0
Datapath           3281237    66425        1        0  1907552  1382289      104        6        0
Nanny                    1        0        0        0        0        0        0        0        0

Remote Statistics
To application      Tx Msg   Tx Blk   Tx Ret  Tx Fail   Rx Ack   Rx Msg  Rx Drop   Rx Err   Tx Ack
WMS                      59        0        0        0       59        0        0        0        0
STM                   54983        0        0        0        0  1527435        0        0        0

Allocated Buffers   0
Static Buffers      4
Static Buffer Size  1400
```

The output of this command includes the following data columns:

Parameter	Description
Tx Msg	Number of transmitted messages.
Tx Blk	Number of blocking messages transmitted.
Tx Ret	Number of transmitted messages that were returned.
Tx Fail	Number of failure messages that were transmitted.
Rx Ack	Number of received acknowledgements.
Rx Msg	Number of received messages.
Rx Drop	Number of received messages that were dropped.
Rx Err	Number of received messages with errors.
Tx Ack	Number of transmitted acknowledgements.
Allocated Buffers	Number of allocated buffers for IPC messages.
Static Buffers	Number of static buffers for IPC messages.
Static Buffer Size	Size of the static buffer.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

show ipv6 access-list

```
show ipv6 access-list [<string> | brief]
```

Description

Displays IPv6 access list configured in the controller.

Syntax

Parameter	Description
`string`	To view details of a specific ACL.
`brief`	To view a summary of all IPv6 ACLs.

Example

This example displays the session access control list details.

```
(host) #show ipv6 access-list brief

Access list table
-----------------
Name              Type     Use Count  Roles
----              ----     ---------  -----
v6-allowall       session  2          default-vpn-role authenticated
v6-dhcp-acl       session  1          guest
v6-dns-acl        session  1          guest
v6-http-acl       session  1          guest
v6-https-acl      session  1          guest
v6-icmp-acl       session  1          guest
v6-logon-control  session  1          logon


(host) #show ipv6 access-list v6-allowall

ipv6 access-list session v6-allowall
v6-allowall
-----------
Priority  Source  Destination  Service  Action  TimeRange  Log  Expired  Queue  TOS  8021P  Blacklist
Mirror  DisScan
--------  ------  -----------  -------  ------  ---------  ---  -------  -----  ---  -----  ---------
----  -------
1         any     any          any      permit                           Low
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the IPv6 ACL.
`Type`	Type of ACL rule.
`Use Count`	Number of times impacted.
`Roles`	Roles using the ACL.

Command History

This command was available in ArubaOS 3.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show ipv6 datapath session counters

```
show ipv6 datapath session counters
```

Description

Displays datapath session table statistics.

Example

This example displays the session counter statistics.

```
(host) #show datapath session counters

Datapath Session Table Statistics
---------------------------------
Current Entries      7
High Water Mark      167
Maximum Entries      65535
Total Entries        37287
Allocation Failures  0
Duplicate Entries    0
Cross linked Entries 0
No Reverse Entries   0
Max link length      2
```

The output of this command includes the following parameters:

Parameter	Description
`Current Entries`	Number of session entries in the datapath table.
`High Water Mark`	The maximum number of session since the controller uptime.
`Maximum Entries`	The maximum limit for session entries.
`Total Entries`	The total number of session entries.
`Allocation Failures`	The number of datapath sessions that could not be established.
`Duplicate Entries`	The total number of duplicate session entries.
`No Reverse Entries`	The total number of sessions that does not have reverse entries.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show ipv6 datapath session table

```
show ipv6 datapath session table <IPv6 Address>
```

Description

Displays current IPv6 session on the controller.

Syntax

Parameter	Description
<IPv6 IP Address>	Optional parameter. If specified, displays IPv6 datapath session table for that IP address. By defaults, displays session table for all IPv6 addresses.

Example

This example displays the session access control list details.

```
(host) #show ipv6 datapath session

Datapath Session Table Statistics
---------------------------------
Current Entries      45
High Water Mark      47
Maximum Entries      524287
Total Entries        9098
Allocation Failures  0
Duplicate Entries    0
Cross linked Entries 0
No Reverse Entries   0
Max link length      0

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

Source IP                              Destination IP          Prot SPort DPort  Cntr Prio ToS Age Destination Flags
---------                              --------------          ---- ----- -----  ---- ---- --- --- ----------- -----
2003:d81f:f9f0:1001:617c:9151:6d25:f754  2003:d81f:f9f0:1001::3  58   3951  32768  0    0    0   1   tunnel 13   FYCI
2003:d81f:f9f0:1001:617c:9151:6d25:f754  2003:d81f:f9f0:1001::3  58   3950  32768  0    0    0   1   tunnel 13   FYCI
```

The output of this command includes the following parameters:

Parameter	Description
Source IP	The source IP address of the datapath.
Destination IP	The destination IP address of the datapath.
Prot	Denotes the protocol number.
SPort	Source port of the datapath.
DPort	Destination port of the datapath.
ToS	Specifies the type of service.

Parameter	Description
Age	Age of the session in seconds.
Destination	Destination slot of the controller.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show ipv6 datapath user counters

```
show ipv6 datapath user counters
```

Description

Displays datapath user table statistics.

Example

This example displays the user table statistics for IPv6 users.

```
(host) #show ipv6 datapath user counters

Datapath User Table Statistics
------------------------------
Current Entries      0
Pending Deletes      0
High Water Mark      0
Maximum Entries      2047
Total Entries        0
Allocation Failures  0
Invalid Users        0
Max link length      0
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show ipv6 datapath user table

```
show ipv6 datapath user table
```

Description

Displays ipv6 datapath user table entries.

Example

This example displays the user table entries in the datapath.

```
(host) #show ipv6 datapath user table

Datapath User Table Entries
---------------------------

Flags: P - Permanent, W - WEP, T- TKIP, V - ProxyArp for User, A - ProxyARP to User, N - VPN

IP                                      MAC               ACLs  Contract   Location  Age  Sessions   Flags
--                                      ---               ----  --------   --------  ---  ---------  -----
fe80::216:ceff:fe2c:b485                00:16:CE:2C:B4:85  1/0   0/0        1         28     0/65535  W
2003:d81f:f9f0:1001:617c:9151:6d25:f754 00:16:CE:2C:B4:85  1/0   0/0        1         0      0/65535  W
```

The output of this command includes the following parameters:

Parameter	Description
IP	IP address of the user (client).
MAC	MAC address of the user (client).
ACLs	The access control list assigned to the user.
Contract	Bandwidth contract.
Location	This value refers to the AP-group of the IPv6 client. Use the `show aaa state ap-group` to get the AP group and the location ID mapping.
Age	Total time connected to the controller.
Sessions	Number of active sessions.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show ipv6 firewall

```
show ipv6 firewall
```

Example

This example displays the status of all firewall configurations.

```
(host) #show ipv6 firewall

Global IPv6 firewall policies
-----------------------------
Policy                                    Action    Rate  Slot/Port
------                                    ------    ----  ---------
Monitor ping attack                       Disabled
Monitor TCP SYN attack                    Disabled
Monitor IPv6 sessions attack              Disabled
Deny inter user bridging                  Disabled
Deny all IPv6 fragments                   Disabled
Per-packet logging                        Disabled
Enforce TCP handshake before allowing data  Disabled
Prohibit RST replay attack                Disabled
Session Idle Timeout                      Disabled
Session mirror destination                Disabled
Prohibit IPv6 Spoofing                    Disabled
Enable IPv6 Stateful Firewall             Disabled
```

The output of this command includes the following parameters:

Parameter	Description
`Monitor ping attack`	Displays status on monitoring ICMP pings, frequency (in seconds) at which the attacks are monitored and the port on which the monitoring is configured.
`Monitor TCP SYN attack`	Status on monitoring TCP SYN messages, frequency (in seconds) at which the attacks are monitored and the port on which the monitoring is configured.
`Monitor IPv6 sessions attack`	Status on TCP and UDP connection requests, in seconds) at which the attacks are monitored and the port on which the monitoring is configured.
`Deny inter user bridging`	Status on Layer-2 traffic forwarding between wired and wireless users, frequency (in seconds) at which the messages are monitored and the port on which the monitoring is configured.
`Deny all IPv6 fragments`	Status on IPv6 fragments to be dropped.
`Per-packet logging`	Status on packet logging for the corresponding session rule.
`Enforce TCP handshake before allowing data`	Status on TCP handshake between two clients.
`Prohibit RST replay attack`	Status on a TCP connections in both directions.
`Session Idle Timeout`	Status on TCP session idle timeout.
`Session mirror destination`	Status on mirrored session packet traffic.
`Prohibit IPv6 Spoofing`	Status on IP spoofing. When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.
`Enable IPv6 Stateful Firewall`	Status of IPv6 firewall.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show ipv6 mld config

```
show ipv6 mld config
```

Description

Displays Multicast Listener Discover (MLD) configuration details.

Example

This example displays the current MLD configuration values.

```
(host) #show ipv6 mld config

MLD Config
----------
Name                        Value
----                        -----
robustness-variable         2
query-interval              125
query-response-interval     100
startup-query-interval      31
startup-query-count         2
last-member-query-interval  10
last-member-query-count     2
```

The output of this command includes the following parameters:

Parameter	Description
`robustness-variable`	Denotes the value that is used to calculate the timeout value of a MLD client.
`query-interval`	Denotes the time interval at which the MLD query is sent.
`query-response-interval`	Denotes the time interval during the MLD query response should be received.
`startup-query-interval`	Denotes the time interval between successive MLD queries during startup.
`startup-query-count`	Number of times queries are sent during startup.
`last-member-query-interval`	Denotes the time interval between successive MLD queries after the last member has left the MLD group.
`last-member-query-count`	Number of times queries are sent after the last member has left the MLD group.

Command History

This command was available in ArubaOS 3.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show ipv6 mld counters

```
show ipv6 mld counters
```

Description

Displays the statistics of MLD.

Example

This example displays the MLD statistics for the following values.

```
(host) #show ipv6 mld counters

MLD Statistics
--------------
Name                    Value
----                    -----
received-total          0
received-queries        0
received-v1-reports     0
received-leaves         0
received-unknown-types  0
len-errors              0
checksum-errors         0
not-vlan-dr             0
transmitted-queries     0
forwarded               0
```

The output of this command includes the following parameters:

Parameter	Description
`received-total`	The total number of MLD messages.
`received-queries`	The total number of MLD queries.
`received-v1-reports`	The total number of MLD v1 reports received.
`received-leaves`	The total number of MLD v1 leave messages received.
`received-unknown-types`	The total number of unrecognized messages received.
`len-errors`	The total number of error message where the length check has failed.
`checksum-errors`	The total number of error message where the checksum has failed.
`not-vlan-dr`	The number of messages received for which the current controller is not the designated router.
`transmitted-queries`	The total number of transmitted MLD queries.
`forwarded`	The total number of MLD messages forwarded.

Command History

This command was available in ArubaOS 3.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show ipv6 mld group

```
show ipv6 mld group
```

Example

This example displays MLD group details.

```
(host) #show ipv6 mld group

MLD Group Table
---------------
Group  Members
-----  -------
```

The output of this command includes the following parameters:

Parameter	Description
`Group`	Name of MLD groups.
`Members`	Number of members in an MLD group.

Command History

This command was available in ArubaOS 3.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show ipv6 mld interface

```
show ipv6 mld interface
```

Example

This example displays MLD status on VLANs. To view details for a specific VLAN, you can specify the VLAN ID.

```
(host) #show ipv6 mld interface

MLD Interface Table
-------------------
VLAN  Addr          Netmask        MAC Address        MLD       Snooping  Querier  Destination
----  ----          -------        -----------        ---       --------  -------  -----------
224   10.224.224.1  255.255.255.0  00:0b:86:f0:20:20  disabled  disabled  ::       CP
1     10.15.44.10   255.255.255.0  00:0b:86:f0:20:20  disabled  disabled  ::       CP
50    156.1.50.1    255.255.255.0  00:0b:86:f0:20:20  disabled  disabled  ::       CP
211   211.1.1.1     255.255.255.0  00:0b:86:f0:20:20  disabled  disabled  ::       CP
51    156.1.51.1    255.255.255.0  00:0b:86:f0:20:20  disabled  disabled  ::       CP
999   99.1.1.2      255.255.255.0  00:0b:86:f0:20:20  disabled  disabled  ::       CP
7     7.7.7.1       255.255.255.0  00:0b:86:f0:20:20  disabled  disabled  ::       CP
170   192.170.1.1   255.255.255.0  00:0b:86:f0:20:20  disabled  disabled  ::       CP
```

The output of this command includes the following parameters:

Parameter	Description
VLAN	Denotes the VLAN ID.
Addr	IP address of the VLAN interface.
Netmask	Network mask of the VLAN interface IP address.
MAC Address	MAC address of VLAN interface.
MLD	Status of MLD.
Snooping	Status of MLD snooping.
Querier	IPv6 address of the MLD querier for the VLAN.
Destination	Denotes the destination of the MLD messages.

Command History

This command was available in ArubaOS 3.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show ipv6 user-table

```
show ipv6 user-table [authentication-method {dot1x | mac | stateful-dot1x | vpn | web} |
   bssid <bssid> |
   debug {rows | unique} |
   essid <essid-name> |
   internal {rows} |
   ip <IPv6-address> |
   location <ap-group-name> |
   mac <mac-address> |
   mobile {bindings | rows | unique | visitors} |
   name <user-name> |
   phy-type {a | b} |
   role <role-name> |
   rows |
   station |
   verbose ]
```

Description

Displays IPv6 user table entries. You can filter the output based on various parameters are described in table.

Syntax

Parameter	Description
`authentication-method`	Displays entries in the IPv6 user-table that matches the following authentication methods: • dot1x • mac • stateful-mac • vpn • web
`bssid`	Displays entries in the IPv6 user-table that are associated to the specified BSSID.
`debug`	Displays entries in the IPv6 user-table that are in debug mode.
`essid`	Displays entries in the IPv6 user-table that are associated to the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
`internal`	Displays internal IPv6 users.
`ip`	Displays IPv6 users that match the specified IPv6 IP address.
`location`	This value refers to the AP-group of the IPv6 client. Use the `show aaa state ap-group` to get the AP group and the location ID mapping.
`mac`	Displays users with the specified MAC address.
`mobile`	Displays list of mobile users in the IPv6 user table. The following filters are available for this parameter: • **bindings**—list of users that have moved away from the current controller. • **rows**—displays entries that match the specified row number. • **unique**—displays unique entries in the IPv6 user-table. • **visitors**—displays users that have associated with the current controller.
`name`	Displays IPv6 user table entries that match the specified name.
`phy-type`	Displays IPv6 user table entries that match **a** or **b** phy-type.
`role`	Displays IPv6 user table entries that match the specified role.
`rows`	Displays specific rows in the IPv6 user table. Enter the starting row number and the number of rows to be displayed.
`station`	Displays the station table information for the IPv6 user table entries.
`verbose`	Displays the complete IPv6 user table with all details.

Example

This example displays dot1x authenticate users in IPv6 user table.

```
(host) show ipv6 user-table authentication-method dot1x

Users
-----
   IP                                   MAC           Name     Role     Age(d:h:m)  Auth    VPN link  AP name
Roaming   Essid/Bssid/Phy                  Profile
----------                               ------------       ------    ----      ----------  ----    --------  ------
-           -------   ---------------                 -------
fe80::216:ceff:fe2c:b485                 00:16:ce:2c:b4:85  Wing-A   logon     00:00:06    802.1x
00:0b:86:c1:0e:8c  Wireless  Wing-A/00:0b:86:90:e8:c0/g  default-dot1x
2003:d81f:f9f0:1001:617c:9151:6d25:f754  00:16:ce:2c:b4:85  Wing-A   logon     00:00:06    802.1x
00:0b:86:c1:0e:8c  Wireless  Wing-A/00:0b:86:90:e8:c0/g  default-dot1x
```

The output of this command includes the following parameters:

Parameter	Description
IP	IP address of the client in that row that authenticating using dot1x
MAC	MAC address of the client.
Name	Name of the client.
Role	The role assigned to the client.
Age (d:h:m)	Total time that client is connected to controller.
Auth	Authentication type.
AP name	Name of the AP associated with the client.
Roaming	Current roaming status of the client.
Essid/Bssid/Phy	ESSID/BSSID/Phy to which the client is associated.
Profile	Displays the AAA profile.

Command History

This command was available in ArubaOS 3.3.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master and local controllers

show keys

```
show keys [all]
```

Description

Show whether optional keys and features are enabled or disabled on the controller.

Syntax

Parameter	Description
`all`	Include this optional parameter to display the status of all optional keys and features. If this parameter is omitted, the output displays the status of the most commonly used features and keys.

Example

The following example displays the status of the most commonly used keys and features on the controller.

```
(host) #show keys
Licensed Features
-----------------
Feature                                          Status
-------                                          ------
Access Points                                    128
Remote Access Points                             128
Ortronics Access Points                          128
Outdoor Mesh Access Points                       128
RF Protect                                       128
Voice Service Module                             Unlimited
VPN Server Module                                2048
xSec Module                                      4096
Indoor Mesh Access Points                        128
120abg Upgrade                                   128
121abg Upgrade                                   128
124abg Upgrade                                   128
125abg Upgrade                                   128
Next Generation Policy Enforcement Firewall Module  128
RF Protect                                       ENABLED
Policy Enforcement Firewall                      ENABLED
Remote APs                                       ENABLED
External Services Interface                      ENABLED
Client Integrity Module                          ENABLED
VPN Server                                       ENABLED
xSec Module                                      ENABLED
MMC AP                                           DISABLED
Netgear AP                                       DISABLED
Voice Services Module                            ENABLED
Ortronics AP                                     ENABLED
Mesh Point APs                                   ENABLED
AP Developers Module                             DISABLED
Internal Test Functions                          DISABLED
Public Access                                    DISABLED
Policy Enforcement Firewall for VPN users        ENABLED
Content Security                                 DISABLED
```

Related Commands

To view the license usage database (including the license key strings) use the command show license.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show lacp

```
show lacp <group_number> {counters | internal | neighbor}
```

Description

View the LACP configuration status.

Syntax

Parameter	Description
`<group_number>`	Enter the Link aggregation group number. Range: 0-7
`counters`	Enter the keyword **counters** to view the LACP traffic.
`internal`	Enter the keyword **internal** to view the LACP internal information.
`neighbor`	Enter the keyword **neighbor** to view the LACP neighbor information.

Example

The port uses the group number +1 as its "actor admin key". By default, all the ports use the long timeout value (90 seconds).

```
(Host)#show lacp 0 neighbor
Flags: S - Device is requesting Slow LACPDUs
   F - Device is requesting fast LACPDUs
   A - Device is in active mode P - Device is in passive mode
Partner's information
---------------------
Port    Flags  Pri  OperKey  State Num  Dev Id
----    -----  ---- -------  ----- ---- ----------------
FE 1/1  SA     1    0x10     0x45  0x5  00:0b:86:51:1e:70
```

When a port, in a LAG, is misconnected (that is, the partner device is different than the other ports or the neighborship times out or can not exchange LACPDUs with the partner), the port status is displayed as "DOWN" (see the following example).

```
(Host)#show lacp 0 internal
Flags: S - Device is requesting Slow LACPDUs
   F - Device is requesting fast LACPDUs
   A - Device is in active mode P - Device is in passive mode

Port    Flags  Pri  AdminKey  OperKey  State Num  Status
----    -----  ---- --------  -------- ----- ---- -------
```

The "counters" option allows you to view LACP received (Rx) traffic, transmitting (Tx) traffic, data units (DU) received and transmitted by port.

```
(Host)#show lacp 0 counters
Port    LACPDUTx  LACPDURx  MarkrTx  MarkrRx  MrkrRspTx MrkrRspRx
----    --------  --------  -------  -------- --------- ---------
FE 1/1  10        10        0        0        0         0
FE 1/2  12        12        0        0        0         0
```

Related Command

Command	Description
`lacp group`	Enable LACP and configure on the interface
`show interface port-channel`	View information on a specified port-channel interface
`show lacp sys-id`	View the LACP system ID information

Command History

Release	Modification
ArubaOS 3.4.1	Command introduced

Command Information

Platform	Licensing	Command Mode
All Platforms	Base operating system	Enable and Configuration modes for Master and Local controllers

show lacp sys-id

```
show lacp sys-id
```

Description

View the LACP system MAC address and port priority.

Example

This command returns the port priority and the MAC address (comma separated). In the example below, the port priority is the default value 32768 followed by the MAC address 00:0B:86:40:37:C0

```
(Host)#show lacp sys-id
32768,00:0B:86:40:37:C0
```

Related Command

Command	Description
`lacp group`	Enable LACP and configure on the interface
`lacp port-priority`	Configure the LACP port priority
`show lacp`	View the LACP configuration status
`show interface port-channel`	View information on a specified port channel interface

Command History

Release	Modification
ArubaOS 3.4.1	Command introduced

Command Information

Platform	Licensing	Command Mode
All Platforms	Base operating system	Enable and Configuration modes (config) for Master and Local controller

show license

```
show license [limits]
```

Description

Displays the license table.

Syntax

Parameter	Description
limits	Enter the keyword **limit** to display the current license limits.

Example

An example output of the **show license** command.

```
(host) # show license

License Table
-------------
Key                                          Installed   Expires  Flags  Service Type
---                                          ---------   -------  -----  ------- -----
yKrTGQaj-JxrMimpT-VOvoA1MQ-hfHABSZe-+RnWQFe6-rbQ  2010-01-21  Never     E     Ortronics Access Points: 1
                                             20:59:09
x7kbiBm5-3jI5MiBY-HVTAH/ci-llxPiKBV-dY8QGBMg-240  2010-01-21  Never           Access Points: 1024
                                             21:00:22
itY24Hca-HSQlvJhi-yZtW6RB7-HGuBXzIq-N6hd6TNV-nZk  2010-01-21  Never     E     120abg Upgrade: 128
                                             21:01:03
oqdLOxZ6-+FS5DT2P-iNmtvc3o-NFyasYrO-ixGUrszE-4uo  2010-01-21  Never     E     121abg Upgrade: 128
                                             21:01:13
GIleLrCX-d8lxt3z5-vQC50n60-f31amOxu-Rf0uEoTn-qXQ  2010-01-21  Never     E     124abg Upgrade: 128
                                             21:01:22
ldsXG7ik-pj/HVm4t-Qt3541UC-3wzC+Efj-yn08g/HF-/Dg  2010-01-21  Never     E     125abg Upgrade: 128
                                             21:01:3
sJvaPL88-gWDdlMpj-LZMZ2YKK-2fU8NV6l-XIH4wRk8-44I  2010-05-05  Never     E     RF Protect: 512
                                             08:51:57
QtemJpLj-Qm5D9WvK-8c9lbaL6-t2nU6/Pj-LSNd00FZ-tJo  2010-05-05  Never     E     RF Protect: 1024
                                             08:52:07
                                             21:18:55
WNx6RasB-Qn9YVZ+5-giraq0Uy-aoIqS3as-FXmFh5dY-cSs  2010-01-21  Never     E     xSec Module: 1024
                                             21:20:56
u/GdQHWa-m4bzUCMC-ydMsWTif-hDMDajyB-qAlIMwnN-pGM  2010-01-25  Never     E     Policy Enforcement Firewall for VPN users
                                             18:44:19
F9dGNdjV-EmwLhqlI-oKMQQepZ-b9Jl3OB2-HQjwmc+r-vhI  2010-01-25  Never     E     Next Generation Policy Enforcement
Firewall Module: 128
```

The output of this command includes the following data columns:

Parameter	Description
Key	The license key.
Installed	The license installation date and time.
Expires	The date that your evaluation license expires is listed in this column. Permanent license will always have a “Never” in this column. Expired evaluation licenses will also be indicated in this column.

Parameter	Description
Flags	This column displays some status about your license. The legend for this column appears at the bottom of the display output. They are: **A**: The license is auto-generated. **E**: The license if fully enabled. **R**: You must reboot your controller to fully enable this license.
Service Type	The license name (feature).

Related Commands

To view additional statistics for license key usage, use the command show keys.

Command History

Release	Modification
ArubaOS1.0	Command introduced.
ArubaOS 3.4	Verbose parameter was deprecated. This command now displays the entire license key by default.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on local and master controllers

show license-usage

```
show license-usage ap|user|xsec
```

Description

Display license usage information.

Syntax

Parameter	Description
ap	Show AP license usage information.
user	Show Policy Enforcement Firewall (PEF) user license usage.
vpn	Deprecated
xsec	Show Extreme Security (xSec) user and tunnel license usage.

Example

The following example displays the AP license usage.

```
(host) #show license-usage ap

Total AP Licenses                     : 128
AP Licenses Used                      : 1
Unused AP Licenses                    : 127
Licenses used for Campus AP's         : 1
Available Campus AP's                 : 31
Licenses used for Remote AP's         : 0
Available Remote AP's                 : 127
Total Ortronics AP Licenses           : 128
Ortronics AP Licenses Used            : 0
Total Indoor Mesh AP's Supported      : 128
Indoor Mesh AP's Active               : 0
Total Outdoor Mesh AP's supported     : 128
Outdoor Mesh AP's Active              : 0
Total RF Protect Licenses : 128
RF Protect Licenses Used : 1
Total PEF Licenses                    : 128
PEF Licenses Used                     : 1
Total 802.11n-120abg Licenses   : 128
802.11n-120abg Licenses Used    : 0
Total 802.11n-121abg Licenses   : 128
802.11n-121abg Licenses Used    : 0
Total 802.11n-124abg Licenses   : 128
802.11n-124abg Licenses Used    : 0
Total 802.11n-125abg Licenses   : 128
802.11n-125abg Licenses Used    : 0
```

Command History

Release	Modification
ArubaOS 3.0	Command Introduced.
ArubaOS 3.3	The following parameters were introduced in the output of **show license-usage ap**. • Total 802.11n-120abg Licenses • 802.11n-120abg Licenses Used • Total 802.11n-121abg Licenses • 802.11n-121abg Licenses Used • Total 802.11n-124abg Licenses • 802.11n-124abg Licenses Used • Total 802.11n-125abg Licenses • 802.11n-125abg Licenses Used
ArubaOS 5.0	Deprecated the option “vpn”

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system. The output of this command varies, according to the licenses currently installed on the controller.	Enable or Config mode on master controllers

show localip

```
show localip
```

Description

Displays the IP address and VPN shared key between master and local.

Syntax

No parameters.

Example

The output of this command shows the controller's IP address and shared key between master and local controllers.

```
(host) # show localip


Local Switches configured by Local Switch IP
--------------------------------------------
Switch IP address of the Local  Key
------------------------------  ---
0.0.0.0                         ********
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show local-userdb

```
show local-userdb {[maximum-expiration][start <offset> page <page_size]}
```

Description

Shows information about user's accounts in the local user database.

Syntax

Parameter	Description
`maximum-expiration`	How long the account is valid, in minutes, in the internal database.
`<offset>`	The user account record's location (by number) as it is listed in the database.
`<page_size>`	The number of user account records that display on one page.

Usage Guidelines

Issue this command without any parameters to display a general overview of user's accounts in the database. Use the **maximum-expiration** parameter to show how long the account is valid for in minutes. Use the **start <offset> page <page_size>** parameters to control which user account records in the database display initially and the number of account records displayed on a page.

Example

This example shows the basic summary of a user accounts in the database.

```
(host) #show local-userdb maximum-expiration start 5 page 4

local-userdb maximum-expiration 90

User Summary
------------
Name           Password  Role   E-Mail  Enabled  Expiry  Status  Sponsor-Name  Grantor-Name
----           --------  ----   ------  -------  ------  ------  ------------  ------------
guest-0657984  ********  guest          Yes              Active                admin
guest-8330301  ********  guest          Yes              Active                admin
guest-5433352  ********  guest          Yes              Active                admin
guest-3469360  ********  guest          Yes              Active                admin

User Entries: 11
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the user.
`Password`	The user's password.
`Role`	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.
`E-mail`	Shows the email address of the user account.
`Enabled`	Shows whether the account is enabled or disabled.
`Expiry`	Shows the expiration date for the user account. If this is not set, the account does not expire.

Parameter	Description
`Status`	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.
`Sponsor-Name`	Shows the sponsor's name.
`Grantor-Name`	Shows the grantor's name.
`User Entries`	Shows the number of user accounts in the database.

Related Commands

Command	Description	Mode
`local-userdb add`	Use **`this command`** to configure the parameters displayed in the output of this show command.	Enable and Config modes
`local-userdb-guest add`	Use this command to configure parameters for a guest user account.	Enable and Config modes

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4	The **Expiry**, **Status**, **Sponsor-name** and **Grantor-name** were introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master and local controllers

show local-userdb username

```
show local-userdb username <name>
```

Description

Shows information about specific user account in the internal controller database.

Usage Guidelines

Issue this command to display an overview of a particular user account in the database.

Example

This example shows the basic summary of a user account **Paula** in the database.

```
(host) #show local-userdb username Paula

User Summary
------------
Name   Password  Role   E-Mail  Enabled  Expiry  Status    Sponsor-Name  Grantor-Name
----   --------  ----   ------  -------  ------  ------    ------------  ------------
paula  ********  guest          Yes              Inactive                admin

User Entries: 1
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master and local controllers

show local-userdb-remote-node

```
show local-userdb-remote-node mac-address <mac-addr> start <offset>
```

Description

The output of this command lists the MAC address and assigned Remote Node profile for of each Remote Node Controller associated with that Remote Node Controller master.

Syntax

Parameter	Description
`mac-address <mac-addr>`	How long the account is valid, in minutes, in the internal database.
`start`	The user account record's location (by number) as it is listed in the database.
`<page_size>`	The number of user account records that display on one page.

Usage Guidelines

If your network incudes multiple Remote Node Controller-masters under a single master controller the output of this command shows all Remote Node Controllers and Remote Node Controller-masters on the network.By default, this command displays all entries in the whitelist. To display only part of the Remote Node Controller whitelist, include the **start <offset>** parameters to start displaying the Remote Node Controller whitelist at the specified entry value. You can also include the optional **mac-address <mac-addr>** parameters to display values for a single Remote Node Controller entry.

Example

This example shows the basic summary of a user accounts in the database.

```
(host) #show  local-userdb-remote-node mac-address 00:16:CF:AF:3E:E1


Remote-Node-entry Details
-----------------
Name               Remote-Node-Profile
----               -----------
00:16:cf:af:3e:e1  Myremotenode

Remote-Node Entries: 1
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Mac address of the Remote Node Controller.
`remote-node profile`	Name of the Remote Node Controller profile
`Remote Node Controller Entries`	Number of Remote Node Controller entries on this controller.

Related Commands

Command	Description	Mode
`remote-node-profile`	The remote-node-profile command lets you create a Remote Node Controller profile.	Config mode

Command History

Release	Modification
ArubaOS 6.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master and local controllers

show log all

```
show log all [<number>]
```

Description

Show the controller's full log.

Syntax

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.

Example

This example shows the most ten recent log entries for the controller.

```
(host) #show log all 10

Mar  3 13:26:20  localdb[567]: <133006> <ERRS> |localdb|  User admin Failed Authentication
Mar  3 13:26:20  localdb[567]: <133006> <ERRS> |localdb|  User admin Failed Authentication
Mar  3 13:26:20  localdb[567]: <133019> <ERRS> |localdb|  User admin was not found in the database
Mar  3 13:26:20  localdb[567]: <133019> <ERRS> |localdb|  User admin was not found in the database
Mar  3 13:46:54  fpcli: USER: admin connected from 10.100.100.66 has logged out.
Mar  3 13:57:53  fpcli: USER: admin has logged in from 10.100.100.66.
Mar  3 13:57:53  localdb[567]: <133006> <ERRS> |localdb|  User admin Failed Authentication
Mar  3 13:57:53  localdb[567]: <133006> <ERRS> |localdb|  User admin Failed Authentication
Mar  3 13:57:53  localdb[567]: <133019> <ERRS> |localdb|  User admin was not found in the database
Mar  3 13:57:53  localdb[567]: <133019> <ERRS> |localdb|  User admin was not found in the database
```

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show log ap-debug

```
show log ap-debug{[<number>][all]}
```

Description

Show the controller's AP debug logs.

Syntax

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the AP debug logs for the controller.

Example

This example shows the ten most recent AP debug logs for the controller.

```
(host) #show log ap-debug 10

Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): Copyright (c) 2005-2006 Atheros Communications, Inc. All Rights
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): wifi0: Base BSSID 00:1a:1e:25:97:d0, 16 available BSSID(s)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): edev->dev_addr=00:1a:1e:ca:59:7c
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): wifi0: AP type AP-125, radio 0, max_bssids 16
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): wifi1: Base BSSID 00:1a:1e:25:97:c0, 16 available BSSID(s)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): edev->dev_addr=00:1a:1e:ca:59:7c
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): wifi1: AP type AP-125, radio 1, max_bssids 16
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21):  ^H<6>Ethernet Channel Bonding Driver: v3.0.1 (January 9, 2006)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): secure_jack_link_state_change: Error finding device eth0
Nov 24 20:54:25  KERNEL(AP39@10.6.1.21): Kernel watchdog refresh ended.
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show log bssid-debug

```
show log bssid-debug{[<number>][all]}
```

Description

A Basic Service Set Identifier (BSSID) uniquely defines each wireless client and Wireless Broadband Router. This command shows the controller's BSSID debug logs.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the BSSID debug logs for the controller.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes

show log errorlog

```
show log errorlog{[<number>][all]}
```

Description

Show the controller's system errors and other critical information.

Syntax

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the error logs for the controller.

Example

This example shows the ten most recent system log errors.

```
(host) #show log errorlog 10

Mar 5 10:30:34 <sapd 106007>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Rogue AP detecte
dnh-blah, BSSID 00:0b:86:b5:86:c0, Wired MAC 00:0b:86:02:ee:00, and IP 10.3.49.254
Mar 5 10:31:39 <sapd 404080>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: ADHOC network de
00:13:ce:45:91:a0, BSSID 02:13:ce:2d:37:50, ESSID adhoc_ap70 Channel 11 and RSSI 22
Mar 5 10:32:12 <sapd 106007>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Rogue AP detecte
dnh-blah, BSSID 00:0b:86:b5:86:c0, Wired MAC 00:0b:86:02:ee:00, and IP 10.3.49.254
Mar 5 10:32:46 <sapd 106007>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Rogue AP detecte
dnh-blah, BSSID 00:0b:86:b5:86:c0, Wired MAC 00:0b:86:02:ee:00, and IP 10.3.49.254
Mar 5 10:40:32 <localdb 133019>  <ERRS> |localdb|  User admin was not found in the database
Mar 5 10:40:32 <localdb 133006>  <ERRS> |localdb|  User admin Failed Authentication
Mar 5 10:41:10 <sapd 106007>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Rogue AP detecte
rlo-open, BSSID 00:0b:86:c9:9e:20, Wired MAC 00:00:00:00:00:00, and IP 0.0.0.0
Mar 5 10:41:31 <sapd 106007>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Rogue AP detecte
QA_MARORA_VOCERA, BSSID 00:0b:86:c9:9e:21, Wired MAC 00:0b:86:02:ee:00, and IP 10.3.49.254
Mar 5 10:48:01 <sapd 404080>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: ADHOC network de
00:13:ce:45:d9:4d, BSSID 02:13:ce:28:40:48, ESSID adhoc_ap70 Channel 11 and RSSI 8
Mar 5 11:04:21 <sapd 404080>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: ADHOC network de
00:13:ce:45:d9:4d, BSSID 02:13:ce:2d:37:50, ESSID adhoc_ap70 Channel 11 and RSSI 9
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show log essid-debug

```
show log essid-debug{[<number>][all]}
```

Description

Show the controller's ESSID debug logs.

An Extended Service Set Identifier (ESSID) is used to identify the wireless clients and Wireless Broadband Routers in a WLAN. All wireless clients and Wireless Broadband Routers in the WLAN must use the same ESSID.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the ESSID debug logs for the controller.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show log network

```
show log network{[<number>][all]}
```

Description

Show the controller's system network errors.

Syntax

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the network logs for the controller.

Example

This example shows the controller's recent network log errors.

```
(host) #show log network all

Feb 17 14:47:14 :209801:  <WARN> |fpapps|  Physical link down: port 1/1
Feb 17 14:48:04 :209801:  <WARN> |fpapps|  Physical link down: port 1/1
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show log security

```
show log security{[<number>][all]}
```

Description

Show the controller's security logs.

Syntax

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the security logs for the controller.

Example

This example shows the controller's last seven security logs.

```
(host) #show log security 7

Mar 5 11:53:43 :124004:  <DBUG> |authmgr|  Local DB auth failed for user admin, error (User not found in
Mar 5 11:53:43 :124003:  <INFO> |authmgr|  Authentication result=Authentication failed(1), method=Manage
server=Internal, user=10.100.100.66
Mar 5 11:53:43 :124004:  <DBUG> |authmgr|  Auth server 'Internal' response=1
Mar 5 11:53:43 :125027:  <DBUG> |aaa|  mgmt-auth: admin, failure, , 0
Mar 5 11:53:43 :125024:  <NOTI> |aaa|  Authentication Succeeded for User admin, Logged in from 10.100.10(
Connecting to 10.3.49.100 port 22 connection type SSH
Mar 5 11:53:58 :103060:  <DBUG> |ike|  ipc.c:ipc_get_cfgm_role:2826 Sending REQUEST for CFGM Role
Mar 5 11:53:58 :103060:  <DBUG> |ike|  ipc.c:get_local_cfg_trigger_ike:2653 IKE got trigger from CFGM :
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show log system

```
show log system{[<number>][all]}
```

Description

Show the controller's system logs.

Syntax

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the system logs for the controller.

Example

This example shows the controller's last ten system logs.

```
(host) #show log system 10

Mar 5 11:55:59 :316073:  <DBUG> |wms|  Received New AP Message: AP 00:0b:86:b5:87:c2 Status 1 Num-WM 0
Mar 5 11:55:59 :316083:  <DBUG> |wms|  mysql: UPDATE ap_table SET ssid='qa-abu-customerissue', current_c
type='generic-ap', ibss='no', phy_type='80211g', rap_type='interfering', match_mac='00:00:00:00:00:00',
power_level='255', status='up' WHERE id='71575' ;
Mar 5 11:55:59 :316029:  <DBUG> |wms|  Sending message to Probe: IP:10.3.49.253 Msg-Type:PROBE_RAP_TYPE
00:0b:86:b5:87:c2 Type:1
Mar 5 11:55:59 :316036:  <DBUG> |wms|  Received New STA Message: MAC 00:0b:86:b5:87:c2 Status 0
Mar 5 11:55:59 :316032:  <DBUG> |wms|  STA Probe: ADD Probe 00:0b:86:a2:e7:40 for STA 00:0b:86:b5:87:c2
Mar 5 11:56:00 :399814:  <DBUG> |fpapps|  PoE: RAN THRU ITERATION 2
Mar 5 11:56:00 :326001:  <DBUG> |AP 1.1.1@10.3.49.253 sapd|  AM: am_read_bss_data_stats: radio 0: pktsIn
bytesIn 0 bytesOut 0
Mar 5 11:56:00 :326001:  <DBUG> |AP 1.1.1@10.3.49.253 sapd|  AM: am_read_bss_data_stats: radio 0: pktsIn
bytesIn 0 bytesOut 18143486
Mar 5 11:56:01 :326001:  <DBUG> |AP 1.1.1@10.3.49.253 sapd|  AM: MPPS 2722 CPPS 338 PKTS 452036609 BYTES
334327351
Mar 5 11:56:02 :399814:  <DBUG> |fpapps|  PoE: Evaluating port 1/5 rv is 0 and crv is 1
state :3
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show log user

```
show log user{[<number>][all]}
```

Description

Show the controller's user logs.

Syntax

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the user logs for the controller.

Example

This example shows the controller's last ten user logs.

```
(host) #show log user 10

Mar 5 13:29:57 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC address from
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:32:08 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC address from
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:36:41 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC address from
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:38:42 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC address from
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:40:41 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC address from
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:42:51 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC address from
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:47:03 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC address from
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:49:07 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC address from
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:53:08 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC address from
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:55:14 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC address from
00:0b:86:a2:e7:40-1.1.1
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show log user-debug

```
show log user-debug{[<number>][all]}
```

Description

Show the controller's user debug logs.

Syntax

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the user debug logs for the controller.

Example

This example shows the controller's last ten user debug logs.

```
(host) #show log user-debug 10

Mar 5 13:57:24 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-00:0b:86:a2:e7:
Mar 5 13:57:24 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-00:0b:86:a2:e7:
Mar 5 13:58:26 :501082:  <DBUG> |stm|  Probe request: 00:18:f8:ab:77:a4: AP 10.3.49.253-00:0b:86:a2:e7:4
Mar 5 13:58:26 :501085:  <DBUG> |stm|  Probe request: 00:18:f8:ab:77:a4: AP 10.3.49.253-00:0b:86:a2:e7:4
Mar 5 13:58:26 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-00:0b:86:a2:e7:
Mar 5 13:58:26 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-00:0b:86:a2:e7:
Mar 5 13:58:27 :501082:  <DBUG> |stm|  Probe request: 00:18:f8:ab:77:a4: AP 10.3.49.253-00:0b:86:a2:e7:4
Mar 5 13:58:27 :501085:  <DBUG> |stm|  Probe request: 00:18:f8:ab:77:a4: AP 10.3.49.253-00:0b:86:a2:e7:4
Mar 5 13:58:27 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-00:0b:86:a2:e7:
Mar 5 13:58:27 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-00:0b:86:a2:e7:
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show log wireless

```
show log wireless{[<number>][all]}
```

Description

Show the controller's wireless logs.

Syntax

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the wireless logs for the controller.

Example

This example shows the controller's last ten wireless logs.

```
(host) #show log wireless 10

Mar 5 13:59:31 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering AP detecte
cp-psk and BSSID 00:0b:86:8b:70:20
Mar 5 13:59:35 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering AP detected
BSSID 00:0b:86:c0:06:83
Mar 5 13:59:38 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering AP detected
BSSID 00:0b:86:c0:06:85
Mar 5 13:59:41 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering AP detected
BSSID 00:0b:86:89:f9:42
Mar 5 13:59:41 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering AP detecte
SANJAY-OSUWIRELESS and BSSID 00:0b:86:89:f9:40
Mar 5 13:59:44 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering AP detecte
SANJAY-OSUVOICE and BSSID 00:0b:86:8c:fb:c0
Mar 5 13:59:44 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering AP detecte
Google and BSSID 00:0b:86:4f:82:c0
Mar 5 13:59:47 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering AP detecte
SANJAY-OSUVOICE and BSSID 00:0b:86:89:f9:41
Mar 5 13:59:50 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering AP detected
BSSID 00:0b:86:c0:06:86
Mar 5 13:59:50 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering AP detecte
dnh-blah and BSSID 00:0b:86:60:b8:80
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show logging

```
show logging facility|server|{level [verbose]}
```

Description

the IP address of the remote logging server, as well as facility log types and their associated facility levels.

Syntax

Parameter	Description
`facility`	View the facility used when logging messages into the remote syslog server.
`server`	Show the IP address of a remote logging server.
`level [verbose]`	Show logging levels at which the messages are logged. Include the optional verbose parameter to display additional data for logging subcategories and processes.

Usage Guidelines

The ArubaOS logging levels follow syslog convention:

- level 7: Emergency
- level 6: Alert
- level 5: Critical
- level 4: Errors.
- level 3: Warning
- level 2:Notices
- level 1:Informational
- level 0: Debug

The default logging level is **level 1**. You can change this setting via the **logging** command.

Example

This example below displays defined logging levels for each logging facility.

```
(host) #show logging level

LOGGING LEVELS
--------------
Facility  Level
--------  -----
network   warnings
security  warnings
system    warnings
user      warnings
wireless  warnings
```

This example below displays the IP address of a remote log server. If a remote log server has not yet been defined, this command will not display any output.

```
(host) #show logging server

Remote Server: 1.1.1.1

FACILITY MAPPING TABLE
----------------------
local-facility  severity   remote-facility
--------------  --------   ---------------
user            debugging  local1
```

Related Commands

Command	Description	Mode
logging	Use this command to specify the IP address of the remote logging server, as well as facility log types and their associated facility levels.	Config mode on master and local controllers

Command History

This command was introduced in ArubaOS 2.5.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers

show loginsessions

```
show loginsessions
```

Description

Displays the current administrator login sessions statistics.

Syntax

No parameters.

Example

Issue this command to display the admin login session statistics.

```
Session Table
-------------
ID  User Name  User Role  Connection From  Idle Time  Session Time
--  ---------  ---------  ---------------  ---------  ------------
```

The output includes the following parameters:

Parameter	Description
`ID`	Sessions identification number
`User Name`	Administrator's user name
`User Role`	Administrator's role
`Connection From`	The IP address from which the administrator is connecting
`Idle Time`	Amount of time the user has been idle
`Session Time`	Total time the session has been open

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show mac-address-table

```
show mac-address-table
```

Description

Displays a MAC forwarding table.

Syntax

No parameters.

Example

Issue this command to display the MAC forwarding table.

```
Dynamic Address Count:           0
Static Address (User-defined) Count:             0
System Self Address Count:               0
Total MAC  Addresses :           6
Maximum MAC addresses :                  6
MAC Address Table
------------------
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  ----------------
00:0b:86:00:00:00    Mgmt          1     vlan 1
```

The output includes the following parameters:

Parameter	Description
`Dynamic Address Count`	Count of dynamic addresses currently associated with the controller
`Static Address (User-defined) Count`	Count of static, user-defined addresses associated with the controller
`System Self Address Count`	Number of self system addresses
`Total MAC Addresses`	Total number of MAC addresses associated with the controller
`Maximum MAC Addresses`	Maximum number of MAC addresses
`Destination Address`	Destination MAC address
`Address Type`	Destination address type
`VLAN`	Associated VLAN
`Destination Port`	Destination port

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show master-configpending

```
show master-configpending
```

Description

Displays the list of global commands which are not saved and are not sent to the local controller.

Syntax

No parameters.

Example

This example below displays the commands which are not saved and are not sent to the local controller.

```
(host) #show master-configpending

aaa profile "default-xml-api"
aaa xml-api server "10.17.93.2"
aaa xml-api server "10.17.93.2"
aaa xml-api server "10.17.93.2" key "12345678"
aaa profile "default-xml-api"
aaa profile "default-xml-api" xml-api-server "10.17.93.2"
user-role "logon"
user-role "logon" captive-portal "default"
user-role "logon"
user-role "logon" no captive-portal "default"
user-role "logon"
user-role "logon" captive-portal "default"
voice rtp-analysis-config
voice rtp-analysis-config rtp-analysis
voice rtp-analysis-config rtp-analysis
voice rtp-analysis-config no rtp-analysis
voice rtp-analysis-config rtp-analysis
```

Related Commands

Command	Description
master-redundancy	This command associates a VRRP instance with master controller redundancy.
master-local	This command displays the statistics between the local and the master controllers.
switches	This command provides the details on the switches connected to the master controller, including the master controller itself.

Command History

This command was introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers.

show master-local stats

```
show master-local stats [<ip-addr>] [<page>]
```

Description

Display statistics for communication between master and local controllers.

Syntax

Parameter	Description
<ip-addr>	Include the IP address of a controller to display statistics that controller only.
<page>	Start displaying the output of this command at the specified page number.

Usage Guidelines

By default, master and Local controllers exchange heartbeat messages every 10 seconds. These "Heartbeats" a include configuration timestamp. If a master controller has later timestamp than the local controller, the state of the local controller changes from 'Update Successful' to 'Update Required'.

Example

This example below shows statistics for all communications between the master and local controller.

```
(host) #show master-local stats

Missed -> HB Resp from Master
-----------------------------
IP Address  HB Req      HB Resp     Total Missed  Last Sent Missed  Peer Reset  Cfg Terminate  Last Synced
----------  ------      -------     ------------  ----------------  ----------  -------------  -----------
10.6.2.252  194721      194208      926           0                 105         1              Thu Feb 26 21:12:04 2009
```

The output of this command includes the following data columns:

Parameter	Description
IP Address	IP address of the local controller.
HB Req	Heartbeat requests sent from the local controller.
HB Resp	Heartbeat responses sent from the master controller.
Total Missed	Total number of heartbeats that were not received by the local controller.
Last Sent Missed	This counter will increment if controller misses the last heartbeat from the peer controller. This counter will keep on incrementing until the heartbeat message is received from peer.
Peer Reset	The number of times the connection to peer is been reset. The connection could reset due to network connectivity problems or when the peer switch reboots.
Cfg Terminate	Number of times the controller has failed to upgrade to a new configuration
Last Synced	Timestamp showing the last time the local controller synched its configuration from the master controller.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show master-redundancy

```
show master-redundancy
```

Description

Display the master controller redundancy configuration.

Syntax

No parameters.

Example

This example below shows the current master redundancy configuration, including the ID number of the master VRRP virtual router and the IP address of the peer controller for master redundancy.

```
(host) #show master-redundancy
Master redundancy configuration:
    VRRP Id 2 current state is MASTER
    Peer's IP Address is 2.1.1.4
```

Related Commands

Command	Description
master-redundancy	This command associates a VRRP instance with master controller redundancy.
vrrp	This command configures the Virtual Router Redundancy Protocol (VRRP).

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master controllers.

show memory

```
show memory [ap {meshd|rfd|sapd} {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-
addr>}]
   |[auth | cfgm |debug [[verbose]]|dbsync |fpapps | fpcli| isakmpd | l2tpd | mobileip |
   ospf | pim | pptpd | profmgr | slb| snmpd | stm | udbserver |wms]
```

Description

Show the amounts of free and available memory on the controller, or include a process name to show memory information for a process on the AP or controller.

Syntax

Parameter	Description
ap	Show memory information for a process running on a specific AP.
meshd	Display memory information for the meshd process on the specified AP.
rfd	Display memory information for the rfd process on the specified AP.
sapd	Display memory information for the rfd process on the specified AP.
ap-name <ap-name>	Display memory information for an AP with the specified AP name.
bssid <bssid>	Display memory information for an AP with the specified BSSID.
ip-addr <ip-addr>	Display memory information for an AP with the specified IP address.
auth	Display memory information for the **auth** process on the controller.
cfgm	Display memory information for the **cfgm** process on the controller.
debug [verbose]	Display detailed memory information to debug memory errors the controller. This command should only be used under the supervision of Dell Technical Support.
dbsync	Display memory information for the **dbsync** process on the controller.
fpapps	Display memory information for the **fpapps** process on the controller.
fpcli	Display memory information for the **fpcli** process on the controller.
isakmpd	Display memory information for the **isakmpd** process on the controller.
l2tpd	Display memory information for the **l2tpd** process on the controller.
mobileip	Display memory information for the **mobileip** process on the controller.
ospf	Display memory information for the **ospf** process on the controller.
pim	Display memory information for the **pim** process on the controller.
pptpd	Display memory information for the **pptpd** process on the controller.
profmgr	Display memory information for the **profmgr** process on the controller.
slb	Display memory information for the **slb** process on the controller.
apsnmpd	Display memory information for the **apsnmpd** process on the controller.
stm	Display memory information for the **auth** process on the controller.
udbserver	Display memory information for the **udbserver** process on the controller.
wms	Display memory information for the **wms** process on the controller.

Usage Guidelines

Include the name of a process to show memory information for that process. Use this command under the supervision of Dell technical support to help debug process errors.

Example

The command **show memory** displays, in Kilobytes, the total memory on the controller, the amount of memory currently being used, and the amount of free memory.

```
(host) # show memory

Memory (Kb): total: 256128, used: 162757, free: 93371
```

Include the name of a process to show memory statistics for that process. The example below shows memory statistics for **mobileip**.

```
(host) # show memory mobileip
Type     Num Allocs     Size Allocs     Total Allocs     Total Size
default  92             145622          441              241087

           PC                Allocs           Size
          0x1000be14              1             64
          0x10016cb0              1          41000
          0x10021604              1             80
          0x10032e34              1             24
          0x30019a24              1           2200
          0x30019bd8              1          41000
          0x30019bf0              1          41000
          0x30019c28              1          11263
          0x3001b134              2           1967
          0x300326b8              9             72
          0x30032738              4             64
          0x3019dfdc              1             44
          0x3019ee60              3             48
          0x3019ef18              1            784
          0x301b63bc             13            312
          0x301b6470             10            200
          0x301b648c             10            920
          0x301b7614              3             36
          0x301b7770              8            128
          0x301bd460              3             60
```

The output of this command includes the following columns:

Column	Description
Type	The **show memory** command currently shows information for predefined processes only, so this column always displays the parameter **default**.
Num Alloc	Current number of memory allocations.
Size Allocs	Total size of all memory allocations, in bytes.
Total Allocs	Maximum number of allocations used throughout in the life of the process.
Total Size	Maximum size of allocations used throughout in the life of the process, in bytes.
PC	Program counter: the address of a memory allocation. (For internal use only.)
Allocs	Number of memory allocations at that program counter. (For internal use only.)
Size	Size of all memory allocations at that program counter. (For internal use only.)

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show mgmt-role

```
show mgmt-role
```

Description

This command allows the user to view a list of management role configurations.

Syntax

No parameters.

Example

Issue this command to display a list of management user roles.

```
Management User Roles
---------------------
ROLE                 DESCRIPTION
----                 -----------
root                 Super user role
read-only            Read only commands
network-operations   network-operations
guest-provisioning   guest-provisioning
```

The output includes the following parameters:

Parameter	Description
ROLE	Name of the management user role
DESCRIPTION	Description of the management user role

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master controllers

show mgmt-users

```
show mgmt-users [ <username> |
   local-authentication-mode <username> |
   ssh-pubkey <username> |
   webui-cacert <username> ]
```

Description

Displays list of management users on the controller and also details of each management users.

Syntax

Parameter	Description
`username`	To view details of a specific management user.
`local-authentication-mode`	Status of local-authentication mode.
`ssh-pubkey`	Number of management users using the ssh-pubkey.
`webui-cacert`	Number of management users using web CA certificates.

Example

The output of this command shows the number of management users in the controller.

```
(host) # show mgmt-user

Management User Table
---------------------
USER    PASSWD  ROLE   STATUS
----    ------  ----   ------
admin   *****   root   ACTIVE
```

Command History

This command was available in ArubaOS 3.3.2

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show netdestination

```
show netdestination <netdestination name>
```

Description

Displays network destination information.

Syntax

No parameters.

Example

Issue this command to display all netdestination configured on this controller. The output shown displays information for all configuration netdestinations. To display additional detailed information for an individual netdestinations, include the name of the netdestination at the end of the command.

```
(host) #show destination
Controller
----------
Position  Type  IP addr      Mask/Range
--------  ----  -------      ----------
1         host  10.16.15.1

user
----
Position  Type     IP addr           Mask/Range
--------  ----     -------           ----------
1         network  255.255.255.255   0.0.0.0

mswitch
-------
Position  Type  IP addr      Mask/Range
--------  ----  -------      ----------
1         host  10.16.15.1

any
---
Position  Type     IP addr   Mask/Range
--------  ----     -------   ----------
1           network  0.0.0.0   0.0.0.0
```

The output includes the following parameters:

Parameter	Description
Position	Network destination position
Type	Network destination type
IP addr	IP address of the network destination
Mask/Range	Network destination subnet mask and range

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	You must have a PEFNG license to configure or view a netdestination.	Enable or config mode on master controllers

show netservice

```
show netservice [<string>]
```

Description

Show network services

Syntax

Parameter	Description
<string>	Name of a network service.

Usage guidelines

Issue this command without the optional **<string>** parameter to view a complete table of network services on the controller. Include the **<string>** parameter to display settings for a single network service only.

Example

The following example shows the protocol type, ports and application-level gateway (ALG) for the DHCP service.

```
(host) #show netservice svc-dhcp
Services
--------
Name      Protocol  Ports  ALG
----      --------  -----  ---
svc-dhcp  udp       67     68
```

Related Commands

To configure an alias for network protocols, use the command netservice.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show netstat

```
show netstat [stats]
```

Description

Show current active network connections.

Syntax

Parameter	Description
<string>	Show network statistics, filtered by protocol type.

Usage guidelines

Issue this command without the optional **stats** parameter to view a complete table of active network connections. Include the **stats** parameter to display aggregate statistics for IP, ICMP, TCP and UDP protocols.

Example

The following example shows incoming and outgoing packet statistics for the controller.

```
(host) #show netstat stats

Ip:
    1084012095 total packets received
    2 with invalid headers
    3 forwarded
    426940 incoming packets discarded
    932097114 incoming packets delivered
    1004595164 requests sent out
    52847 fragments dropped after timeout
    201323411 reassemblies required
    50179757 packets reassembled ok
    53204 packet reassembles failed
    136827034 fragments created
Icmp:
    1969625 ICMP messages received
    5 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 1752058
        timeout in transit: 1684
        redirects: 70805
        echo requests: 145073
        echo replies: 5
    249806 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 51944
        time exceeded: 52796
        redirect: 2
        echo replies: 145064
Tcp:
    3 active connections openings
    0 passive connection openings
    0 failed connection attempts
    0 connection resets received
    2 connections established
    1006383 segments received
    1147229 segments send out
    9603 segments retransmitted
    0 bad segments received.
    2568 resets sent
Udp:
    928478757 packets received
    40767 packets to unknown port received.
    426937 packet receive errors
    910267627 packets sent
```

Related Commands

To configure an alias for network protocols, use the command netservice.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on local and master controllers

show network-printer

```
show network-printer [config | job <printer-name> | status]
```

Description

Displays configuration, job status details, and printer status of USB printers connected to a Aruba 600 series controller.

Syntax

Parameter	Description
`config`	Displays the configuration details of the printer service on the controller.
`job`	Displays the list of job in queue in all printers connected to the controller.
`status`	Displays the status of all printers connected to the controller.

Example

The output of this command shows the status of all printers connected to the controller.

```
(host) #show network-printer status

Networked Printer Status
------------------------
Printer Name                                              Printer Alias  Status  Comment
------------                                              -------------  ------  -------
usblp_Hewlett-Packard_HP_Color_LaserJet_CP3505_CNBJ8B1003  HPLJ_P3005     idle    enabled
usblp_HP_Officejet_Pro_L7500_MY872231FX                   HPOJ_L7500     idle    enabled
```

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
Aruba 600 series controller	Base operating system	Enable mode

show network-storage

```
show network-storage [ files opened |
   shares {<file-system-path> | disk |
   status |
   users {disk <disk-name>} ]
```

Description

Displays details about the USB storage device connect to a Aruba 600 series controller.

Syntax

Parameter	Description
`files opened`	Displays the list of opened files in the USB storage device connected to the controller.
`shares`	Displays the list of shares that are created in the USB storage device. This option provides the following details: • name of the share • name of the disk by alias. • the folder associated with the share, • the access mode
`status`	Displays the status of the storage service on the controller.
`users`	Displays the list of users by IP address, connected share name and connection time.

Example

The output of this command shows the status of all printers connected to the controller.

```
(host) #show network-storage users

NAS Users
---------
Share Name  Machine      Connected at
----------  -------      ------------
```

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
Aruba 600 series controller	Base operating system	Enable mode

show ntp peer

```
show ntp peer <a.b.c.d>
```

Description

Show NTP peer information.

Syntax

Parameter	Description
<a.b.c.d>	IP address of an NTP peer

Usage guidelines

The **show ntp peer** command is used for NTP server troubleshooting, and should only be used under the supervision of Dell technical support. Issue the show ntp servers command to view basic settings for currently configured NTP servers.

Related Commands

To configure an NTP server, use the command ntp server.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show ntp servers

```
show rft servers [brief]
```

Description

Show information for Network TIme Protocol (NTP) servers.

Syntax

Parameter	Description
`brief`	Display only the IP address of the defined NTP servers.

Example

The following example shows values for the primary and backup NTP servers. The primary server is marked with an asterisk (*) and the backup server is marked with an equals sign (=). Note that a backup server will not display delay, offset or dispersion data, as it is not currently in use.

```
(host) #show ntp servers

     remote           local      st poll reach  delay   offset    disp
==============================================================================
=10.4.0.21       10.6.2.253      16 1024    0 0.00000  0.000000 0.00000
*10.1.1.250      10.6.2.253       2 1024  377 0.00081 -0.010376 0.03040
```

The output of this command includes the following parameters:

Parameter	Description
remote	IP address of the remote NTP server defined using the cli command ntp server.
local	IP address of the local clock.
st	NTP uses hierarchical levels of clock sources, or strata, and assigns each layer a number starting with zero at the root. The **st** column in the output of this command represents the number of servers between the configured NTP server and the root reference clock.
poll	Interval, in seconds, between the local NTP server's attempt to poll the remote NTP server.
reach	An index that measures whether or not the remote NTP server could be reached at eight most recent polling intervals. If the NTP server has just been configured and hasn't yet been polled successfully, the value will be zero (0). A value of 377 indicates that the last eight poll queries were successful.
delay	Delay, in seconds, between the time that the local clock polls the NTP server and the NTP server returns a reply.
offset	The difference in time, in seconds, between the local clock and the NTP server.
disp	Dispersion represents the maximum error of the local clock relative to the reference clock, and is a measurement of the time server and network quality. Lower dispersion values are preferred over higher dispersion values.

Related Commands

To configure an NTP server, use the command ntp server.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show ntp status

```
show ntp status
```

Description

Show information for a NTP server.

Syntax

No parameters.

Example

The following example shows values for the primary NTP server.

```
(host) #show ntp status

system uptime:          7594
time since reset:       7594
bad stratum in packet:  0
old version packets:    113
new version packets:    0
unknown version number: 0
bad packet format:      0
packets processed:      110
bad authentication:     0
packets rejected:       0
system peer:            10.1.1.250
system peer mode:       client
leap indicator:         00
stratum:                3
precision:              -18
root distance:          0.03236 s
root dispersion:        0.06728 s
reference ID:           [10.1.1.250]
reference time:         cd45b701.bcbc05d5  Tue, Feb 17 2009 14:21:53.737
system flags:           auth monitor ntp kernel stats
jitter:                 0.005020 s
stability:              0.866 ppm
broadcastdelay:         0.003998 s
authdelay:              0.000000 s
```

The output of this command includes the following parameters:

Parameter	Description
system uptime	The number of seconds the local NTP server has been associated with the switch.
time since reset	The number of seconds since the last time the local NTP server was restarted.
bad stratum in packet	The number of NTP packets with a corrupted stratum bit.
old version packets	Number of packets that match the previous NTP version. A version number is in every NTP packet.
new version packets	Number of packets that match the current NTP version.
unknown version number	Number of packets with an unknown NTP version.
bad packet format	Number of NTP packets dropped due to an invalid packet format.
packets processed	Number of NTP packets received and processed by the controller.
bad authentication	Number of NTP packets that failed to be authenticated.

Parameter	Description
packets rejected	Number of NTP packets rejected because they had an invalid format.
system peer	The IP address of the peer NTP server.
system peer mode	The peer mode of this remote association: • Symmetric Active • Symmetric Passive • Client • Server • Broadcast
leap indicator	This parameter indicates whether or not a leap-second should be inserted or removed at the end of the last day of the current month. • 00 no warning • 01 +1 second (following minute has 61 seconds) • 10 -1 second (following minute has 59 seconds)
stratum	The stratum level of the peer
precision	The advertised precision of the switch. This value can range from -4 and -20, inclusive.
root distance	Total round trip delay to the stratum 1 reference clock.
root dispersion	Total dispersion to the stratum 1 reference clock. This value is a cumulative measure of all errors associated with the network hops and servers between the NTP server and its stratum 1 server.
reference ID	IP address of the remote NTP server
reference time	Time when the local system clock was last set or corrected, in NTP timestamp format.
system flags	This parameter displays any flags configured for this NTP entity.
jitter	The average magnitude of jitter between several time queries.
stability	The average magnitude of offset between several time queries
broadcastdelay	The broadcast delay of this NTP server association, in seconds.
authdelay	The authentication delay of this NTP server association, in seconds.

Related Commands

To configure an NTP server, use the command ntp server.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show packet-capture

```
show packet-capture
```

Description

Displays packet capture status on the controller.

Syntax

No parameters.

Example

The output of this command shows the packet capture configuration details.

```
(host) # show packet-capture

Current Active Packet Capture Actions(current switch)
=====================================================
Packet filtering TCP with 1 port(s) enabled:
  2
Packet filtering UDP with 1 port(s) enabled:
  5
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets enabled.


Packet Capture Defaults(across switches and reboots if saved)
=============================================================
Packet filtering TCP with 1 port(s) enabled:
  2
Packet filtering UDP with 1 port(s) enabled:
  5
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets enabled.
```

Command History

This command was available in ArubaOS 3.3.2

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show packet-capture-defaults

```
show packet-capture-defaults
```

Description

Displays the status of default packet capture options.

Syntax

No parameters.

Example

The output of this command shows packet capture status.

```
(host) # show packet-capture-defaults

Current Active Packet Capture Actions(current switch)
=====================================================
Packet filtering for TCP ports disabled.
Packet filtering for UDP ports disabled.
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.


Packet Capture Defaults(across switches and reboots if saved)
=============================================================
Packet filtering for TCP ports disabled.
Packet filtering for UDP ports disabled.
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.
```

Command History

This command was available in ArubaOS 3.3.2

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show papi-security

```
show papi-security
```

Description

This command shows a configured papi-security profile.

Syntax

Parameter	Description	Range	Default
`PAPI Key`	The key string. The key authenticates the messages between systems.	Range: 10–64 characters	—
`Enhanced security mode`	Indicates if the enhanced security mode is enabled or disabled. This mode causes the system to reject messages when an incorrect key is used.	—	disabled

Usage Guidelines

Issue this command to show the selected papi-security profile configuration. The **papi-security** command is used to enforce advanced security options and provides an enhanced level of security.

The **Parameter** column displays the PAPI Key and Enhanced security mode parameters. The **Value** column displays a Papi key value (encrypted) and indicates whether the Enhanced security mode is enabled or disabled. If an AP cannot be authenticated because it has the wrong key, the show ap database command displays a "Bad key" status.

.

```
(host) #show papi-security

PAPI Security Profile
---------------------
Parameter               Value
---------               -----
PAPI Key                ********
Enhanced security mode  Enabled
```

Related Commands

Use the command papi-security to configure a papi-security profile.

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master or local controllers

show phonehome

```
show phonehome
   global
   history
   report-status
   stats
```

Description

Use this command to view current configuration settings and debugging statistics for the phonehome automatic reporting feature.

Syntax

Parameter	Description
`global`	Show whether the phonehome service and auto-reporting is enabled or disabled, and display current SMTP settings for this feature.
`history`	Issue this command under the guidance of Dell support troubleshoot phonehome automatic reporting.
`report-status`	Issue this command under the guidance of Dell support troubleshoot phonehome automatic reporting.
`status`	Include this parameter to show the number of reports successfully sent to the SMTP server, the number of times the controller attempted to retry sending a report to the SMTP server and the number of reports that failed to reach the SMTP server after one or more retry attempts, and

Usage Guidelines

The automatic reporting feature, also known as *PhoneHome*, allows a controller to securely contact Dell support servers over the Internet to report events such as hardware failures, software malfunctions, and other critical events. When the PhoneHome automatic reporting feature is enabled, the controller sends Dell support weekly reports about the controller's configuration, licenses, software and hardware versions, and any software malfunctions via a secure email.

This feature requires that your network has a local SMTP server capable of relaying email. When the controller generates the report email with the phonehome data file attachment, it forwards the email to the SMTP server configured on your local network, which then delivers the message to Dell. If your email server requires the sender to be authenticated before message delivery, the controller can connect to the SMTP by supplying the sender's user name and password.

Each PhoneHome report attachment is encrypted before it is transmitted to the SMTP server, and is decrypted by Dell support when it is received. If the PhoneHome status report email is larger than the maximum email size supported by your SMTP server, the controller will divide the PhoneHome attachment into multiple smaller attachments and send the report to Dell in multiple emails.

In the event that you need to contact Dell support with a question about your controller, you can use the **phonehome now** command in enable mode to generate and immediately send a status report, so that Dell support can diagnose the issue with the most current controller data.

Example

The following command turns on the PhoneHome feature, enables weekly auto-reports, and identifies the SMTP server to be used by this feature:

```
(host) #show phonehome global

PhoneHome information:
PhoneHome Service:      Disabled
PhoneHome Auto-Report:  Disabled
Local SMTP server:      172.21.18.170:25
SMTP From Email:        admin@mycorp.com
Max Attachment Size:    10 MB
```

Command History

This command was introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers.

show poe

```
show poe [slot/port]
```

Description

Displays the PoE status of all or a specific port on the controller.

Syntax

No parameters.

Example

The output of this command shows the PoE status of port 10 in slot 1.

```
(host) # show poe 1/10

PoE Status
----------
Port     Status  Voltage(mV)  Current(mA)  Power (mW)
----     ------  -----------  -----------  ----------
FE 1/10  Off     N/A          N/A          N/A
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show port link-event

```
show port link-event
```

Description

Displays the link status on each of the port on the controller.

Syntax

No parameters.

Example

The output of this command shows the link status on all ports in the controller.

```
(host) # show port link-event

Slot/Port   UP     DOWN             Slot/Port   UP     DOWN
---------   --     ----             ---------   --     ----
  2 /  0    0      0                  2 /  1    0      0
  2 /  2    0      0                  2 /  3    1      1
  2 /  4    0      0                  2 /  5    0      0
  2 /  6    0      0                  2 /  7    1      1
  2 /  8    0      0                  2 /  9    0      0
  2 / 10    10     9                  2 / 11    2      1
  2 / 12    1      0                  2 / 13    0      0
  2 / 14    1      0                  2 / 15    6      5
  2 / 16    5      4                  2 / 17    9      8
  2 / 18    1      0                  2 / 19    5      4
  2 / 20    0      0                  2 / 21    4      4
  2 / 22    2      2                  2 / 23    9      9
  2 / 24    0      0                  2 / 25    0      0
  3 /  0    24     23                 3 /  1    0      0
  3 /  2    0      0                  3 /  3    0      0
  3 /  4    1      0                  3 /  5    1      0
  3 /  6    0      0                  3 /  7    0      0
  3 /  8    94     94                 3 /  9    0      0
  3 / 10    0      0                  3 / 11    5886   5886
  3 / 12    49751   49750            3 / 13    50     49
  3 / 14    2589   2588               3 / 15    228    227
  3 / 16    2      1                  3 / 17    2423   2423
  3 / 18    8245   8244               3 / 19    5098   5098
  3 / 20    74     73                 3 / 21    2      2
  3 / 22    1      0                  3 / 23    0      0
  3 / 24    0      0                  3 / 25    0      0
```

Command History

This command was available in ArubaOS 3.3.2

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show port monitor

```
show port monitor
```

Description

Displays the list of ports that are configured to be monitored.

Syntax

No parameters.

Example

The output of this command shows the link status on all ports in the controller.

```
(host) # show port monitor


Monitor Port  Port being Monitored
------------  --------------------
FE 1/10       FE 1/20
```

Command History

This command was available in ArubaOS 3.3.2

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show port stats

```
show port status
```

Description

Displays the activity statistics on each of the port on the controller.

Syntax

No parameters.

Example

The output of this command shows the link status on all ports in the controller.

```
(host) # #show port stats

Port Statistics
---------------
Port     PacketsIn  PacketsOut  BytesIn    BytesOut   InputErrorBytes  OutputErrorBytes  CRCErrors
----     ---------  ----------  -------    --------   ---------------  ----------------  ---------
...
    ...
FE1/4    0          0           0          0          0                0                 0
FE1/5    0          0           0          0          0                0                 0
FE1/6    0          0           0          0          0                0                 0
FE1/7    0          0           0          0          0                0                 0
FE1/8    0          0           0          0          0                0                 0
FE1/9    0          0           0          0          0                0                 0
FE1/10   0          2041530     0          296644355  0                0                 0
FE1/11   0          0           0          0          0                0                 0
FE1/12   0          0           0          0          0                0                 0
FE1/13   0          0           0          0          0                0                 0
FE1/14   0          3           0          138        0                0                 0
FE1/15   0          0           0          0          0                0                 0
FE1/16   2937495    1861880     582814945  244607030  32               0                 2
FE1/17   0          0           0          0          0                0                 0
FE1/18   591066     1220117     67049881   143261677  0                0                 0
FE1/19   0          0           0          0          0                0                 0
FE1/20   1205264    836266      211330696  85313659   80               0                 5
FE1/21   0          0           0          0          0                0                 0
FE1/22   0          0           0          0          0                0                 0
...
    ...
```

Command History

This command was available in ArubaOS 3.3.2

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show port status

```
show port status
```

Description

Displays the status of all ports on the controller.

Syntax

No parameters.

Example

The output of this command shows the status of all ports in the controller.

```
(host) # show port status

Port Status
-----------
Slot-Port  PortType  adminstate  operstate  poe       Trusted  SpanningTree  PortMode
---------  --------  ----------  ---------  ---       -------  ------------  --------
1/0        FE        Enabled     Up         Enabled   Yes      Forwarding    Access
1/1        FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/2        FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/3        FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/4        FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/5        FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/6        FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/7        FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/8        FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/9        FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/10       FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/11       FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/12       FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/13       FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/14       FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/15       FE        Enabled     Down       Enabled   Yes      Disabled      Access
1/16       FE        Enabled     Up         Enabled   Yes      Forwarding    Access
...
   ...
   ...
```

Command History

This command was available in ArubaOS 3.3.2

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show port trusted

```
show port trusted
```

Description

Displays the list of ports configured with trusted profiles.

Syntax

No parameters.

Example

The output of this command shows the list of ports with trusted profile.

```
(host) # show port trusted

FE 1/0
FE 1/1
FE 1/2
FE 1/3
FE 1/4
FE 1/5
FE 1/6
FE 1/7
FE 1/8
FE 1/9
FE 1/10
FE 1/11
FE 1/12
FE 1/13
FE 1/14
FE 1/15
FE 1/16
FE 1/17
FE 1/18
FE 1/19
FE 1/20
FE 1/21
FE 1/22
FE 1/23
GE 1/24
GE 1/25
```

Command History

This command was available in ArubaOS 3.3.2

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show port xsec

```
show port xsec
```

Description

Displays the list of xSec enabled ports.

Syntax

No parameters.

Example

The output of this command shows the list of xSec enabled ports.

```
(host) # #show port xsec

Xsec Ports
----------
Interface  xsec vlan  state
---------  ---------  -----
```

Command History

This command was available in ArubaOS 3.3.2

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show priority-map

```
show priority-map
```

Description

Displays the list of priority maps on a interface.

Syntax

No parameters.

Example

The output of this command shows the priority maps configured on all interfaces.

```
(host) # show priority-map

Priority Map
------------
ID  Name    DSCP-TOS  DOT1P-COS
--  ----    --------  ---------
1   my-map  4-20,60      4-7
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show processes

```
show processes [sort-by {cpu | memory}]
```

Description

Displays the list of all process running on the controller. You can sort the list either by CPU intensive or memory intensive processes.

Syntax

Parameter	Description
`sort-by`	To add sort filter to the output
`cpu`	This will sort output based on CPU usage.
`memory`	This will sort output based on memory usage.

Example

The output of this command shows list of processes sorted by CPU usage.

```
(host) # show priority-map

%CPU S   PID  PPID   VSZ  RSS   F  NI START     TIME      EIP CMD
 3.7 S   595   517 20908 12184 040  0 Apr24 03:39:04 303a4fa8 /mswitch/bin/fpapps
 0.2 S 12354   410  1028  296 000   0 02:13 00:00:00 30087fa8 sleep 10
 0.1 S   536   441 12012 7264 040   0 Apr24 00:09:08 100e4a74 /mswitch/mysql/libexec/mysqld --basedir=/m
datadir=/var/
 0.0 S     2     1     0    0 040   0 Apr24 00:00:00 00000000 [keventd]
 0.0 S     4     0     0    0 040   0 Apr24 00:00:00 00000000 [kswapd]
 0.0 S     6     0     0    0 040   0 Apr24 00:00:00 00000000 [kupdated]
 0.0 S    57     1     0    0 040   0 Apr24 00:00:00 00000000 [kjournald]
 0.0 S    67     1  1036  424 000   0 Apr24 00:00:00 30087fa8 /bin/sh /mswitch/bin/syslogd_start
 0.0 S     1     0  1028  384 100   0 Apr24 00:00:12 30087fa8 init
 0.0 S   397     1  1732  804 100   0 Apr24 00:00:00 30152fa8 /mswitch/bin/nanny /mswitch/bin/nanny_list
 0.0 S   399   397 14140 10172 100  0 Apr24 00:00:16 303c8fa8 /mswitch/bin/arci-cli-helper
 0.0 S   402     1   768  268 040   0 Apr24 00:00:00 30060fa8 /sbin/tftpd -s -l -u nobody /mswitch/sap
 0.0 S    69    67  1404  752 100   0 Apr24 00:01:27 300d3fa8 /mswitch/bin/syslogd -x -r -n -m 0 -f /msw
syslog.conf
 0.0 S   407   397  3100 1028 100   0 Apr24 00:00:00 302a0fa8 /mswitch/bin/packet_filter
 0.0 S   408   397  4296 1340 100   0 Apr24 00:00:00 30339fa8 /mswitch/bin/certmgr
 0.0 R     3     0     0    0 040  19 Apr24 00:00:01 00000000 [ksoftirqd_CPU0]
 0.0 S   453   397   700  284 000   0 Apr24 00:01:20 30087fa8 /mswitch/bin/msgHandler -g
 0.0 S   468   397  1236  492 100   0 Apr24 00:00:00 300f8fa8 /mswitch/bin/pubsub
 0.0 S   484   397 18456 14064 100  0 Apr24 00:00:19 303c8fa8 /mswitch/bin/cfgm
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show profile-errors

```
show profile-errors
```

Description

Displays the list of invalid user-created profiles.

Syntax

No parameters.

Example

The output of this command shows list of profiles that are invalid and also displays the error in those profiles. In this example, the VLAN 1000 that is mapped to virtual-ap *test-vap* does not exist.

```
(host) #show profile-errors

Invalid Profiles
----------------
Profile                     Error
-------                     -----
wlan virtual-ap "test-vap"  VLAN 1000 does not exist
```

The following are the list of some profile errors:

Error	Description
Named VLAN [named_VLAN] is removed	These errors are displayed if a virtual AP profile is configure with a VLAN that does not exist.
Named VLAN [named_VLAN] is not mapped	
Named VLAN [named_VLAN] is invalid	
VLAN [x] does not exist	
Server group is invalid	This error is displayed if an AAA profile is configured an invalid server group.
User derivation rule is invalid	This error is displayed if a user role in an AAA profile is invalid.
User role is invalid	
Controller country code is undefined	These errors are displayed, if your controller is not set to the correct country code or if the country code specified in a WLAN profile does not match the controller's country code.
Country [country_name] does not match controller country [country_name]	
Opmode requires WPA key	This message is displayed if a SSID profile is configured without a WPA key.
WARNING: if weptxkey = [x], wepkey[x] must be set in order to use static WEP	This message is displayed if a SSID profile is configured to use a static WEP and the WEP is not configured.

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show profile-hierarchy

```
show profile-hierarchy
```

Description

Displays the profile hierarchy template.

Syntax

No parameters.

Example

The output of this command shows how profiles relate to each other, and how some higher-level profiles reference other lower-level profiles.

```
(host) # show profile-hierarchy

ap-group
    wlan virtual-ap
        aaa profile
            aaa authentication mac
            aaa server-group
            aaa authentication dot1x
            aaa xml-api server
            aaa rfc-3576-server
        wlan ssid-profile
            wlan edca-parameters-profile station
            wlan edca-parameters-profile ap
            wlan ht-ssid-profile
    rf dot11a-radio-profile
        rf arm-profile
        rf ht-radio-profile
    rf dot11g-radio-profile
        rf arm-profile
        rf ht-radio-profile
    ap wired-ap-profile
    ap enet-link-profile
    ap system-profile
    wlan voip-cac-profile
    wlan traffic-management-profile
    ap regulatory-domain-profile
    ap snmp-profile
        ap snmp-user-profile
    rf optimization-profile
    rf event-thresholds-profile
    ids profile
        ids general-profile
        ids signature-matching-profile
            ids signature-profile
        ids dos-profile
            ids rate-thresholds-profile
        ids impersonation-profile
        ids unauthorized-device-profile
    ap mesh-radio-profile
        ap mesh-ht-ssid-profile
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show provisioning-params

```
show provisioning-params
```

Description

Displays the list of parameters and the values used to provision the APs.

Syntax

No parameters.

Example

The output of this command shows list of all provisioning parameters and their values.

```
(host) # show provisioning-params
AP provisioning
---------------
Parameter                       Value
---------                       -----
AP Name                         N/A
AP Group                        default
Location name                   N/A
SNMP sysLocation                N/A
Master                          N/A
Gateway                         N/A
Netmask                         N/A
IP Addr                         N/A
DNS IP                          N/A
Domain Name                     N/A
Server Name                     N/A
Server IP                       N/A
Antenna gain for 802.11a        N/A
Antenna gain for 802.11g        N/A
Use external antenna            No
Antenna for 802.11a             both
Antenna for 802.11g             both
IKE PSK                         N/A
PAP User Name                   N/A
PAP Password                    N/A
PPPOE User Name                 N/A
PPPOE Password                  N/A
PPPOE Service Name              N/A
USB User Name                   N/A
USB Password                    N/A
USB Device Type                 any
USB Device Identifier           N/A
USB Dial String                 N/A
USB Initialization String       N/A
USB TTY device path             N/A
Mesh Role                       none
Installation                    default
Latitude                        N/A
Longitude                       N/A
Altitude                        N/A
Antenna bearing for 802.11a     N/A
Antenna bearing for 802.11g     N/A
Antenna tilt angle for 802.11a  N/A
Antenna tilt angle for 802.11g  N/A
Mesh SAE                        sae-default
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show profile-list aaa

```
show profile-list aaa [{authentication [captive-portal | dot1x | mac | stateful-ntlm |
wispr]} |{authentication-server [ldap | radius | tacacs | windows]} | {profile} | {rfc-
3576-server} | {server-group} | {xml-api}]
```

Description

Displays the list of AAA profiles.

Syntax

Parameter	Description
`authentication`	List of aaa authentication profiles.
`captive-portal`	Captive portal authentication profiles.
`dot1x`	802.1x authentication profiles.
`mac`	MAC authentication profiles.
`stateful-ntlm`	Stateful-NTLM authentication profiles.
`wispr`	WISPr authentication profiles.
`authentication-server`	List of aaa authentication servers
`ldap`	List of servers using LDAP for AAA authentication.
`radius`	List of servers using RADIUS for AAA authentication.
`tacacs`	List of servers using TACACS+ for AAA authentication.
`windows`	List of Windows servers used for AAA authentication.
`profile`	Displays the AAA profile details.
`rfc-3576-server`	Displays IP address of RADIUS servers that use RFC 3576 specification to exchange authorization messages.
`server-group`	List of server group used for RADIUS accounting.
`xml-api`	List of servers configured in an external XML API server.

Example

The output of this command shows list of AAA profiles that use captive-portal authentication.

```
(host) # show profile-list aaa authentication captive-portal

Captive Portal Authentication Profile List
------------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  1
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show profile-list ap

```
show profile-list ap [ enet-link-profile | mesh-cluster-profile |
   mesh-ht-ssid-profile | mesh-radio-profile | regulatory-domain-profile |
   snmp-profile | snmp-user-profile | system-profile | wired-ap-profile ]
```

Description

Displays the list of AP profiles.

Syntax

Parameter	Description
`enet-link-profile`	Display a list of AP ethernet link profiles.
`mesh-cluster-profile`	Display a list of mesh cluster profiles used by mesh nodes.
`mesh-ht-ssid-profile`	Display a list of mesh high-throughput SSID profiles used by mesh nodes.
`mesh-radio-profile`	Display a list of mesh radio profiles used by mesh nodes.
`regulatory-domain-profile`	Display a list of AP regulatory profiles.
`snmp-profile`	Display a list of SNMP profiles.
`snmp-user-profile`	Display a list of SNMPv3 user profiles.
`system-profile`	Display a list of AP system profiles.
`wired-ap-profile`	Display a list of wired AP profiles.

Example

The output of this command shows list of profiles that are invalid and also displays the error in those profiles.

```
(host) # show profile-list aaa authentication captive-portal

Captive Portal Authentication Profile List
------------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  1
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show profile-list ap-group

```
show profile-list ap-group
```

Description

Displays the status of AP groups profiles in the controller.

Syntax

No parameters.

Example

The output of this command shows the status of AP group profiles in the controller.

```
(host) # show profile-list ap-group

AP group List
-------------
Name     Profile Status
----     --------------
default

Total:1
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show profile-list ap-name

```
show profile-list ap-name
```

Description

Displays the status of AP profiles in the controller.

Syntax

No parameters.

Example

The output of this command shows status of AP profiles in the controller.

```
(host) # show profile-list ap-name

AP name List
------------
Name  Profile Status
----  --------------

Total:0
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show profile-list ids

```
show profile-list ids [dos-profile | general-profile | impersonation-profile |
   profile | rate-thresholds-profile | signature-matching-profile |
   signature-profile | unauthorized-device-profile ]
```

Description

Displays the status of all IDS profiles in the controller.

Syntax

Parameter	Description
`dos-profile`	Display a list of IDS DoS profiles.
`general-profile`	Display a list of IDS generate profiles.
`impersonation-profile`	Display a list IDS impersonation profile.
`profile`	Display a list of IDS profiles.
`rate-thresholds-profile`	Display a list of IDS rate threshold profiles.
`signature-matching-profile`	Display a list of IDS signature-matching profiles.
`signature-profile`	Display a list of IDS signature profiles.
`unauthorized-device-profile`	Display a list of IDS unauthorized device profiles.

Example

The output of this command shows a list of all IDS DoS profiles.

```
(host) # show profile-list ids dos-profile

IDS Denial Of Service Profile List
----------------------------------
Name                    References  Profile Status
----                    ----------  --------------
default                 1
ids-dos-disabled        1           Predefined
ids-dos-high-setting    1           Predefined
ids-dos-low-setting     1           Predefined
ids-dos-medium-setting  1           Predefined

Total:5
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show profile-list rf

```
show profile-list rf [ arm-profile | dot11a-radio-profile | dot11g-radio-profile |
   event-thresholds-profile | ht-radio-profile | optimization-profile ]
```

Description

Displays the status of all radio profiles.

Syntax

Parameter	Description
`arm-profile`	Details of Adaptive Radio Management (ARM) Profile.
`dot11a-radio-profile`	Details of AP radio settings for the 5GHz frequency band, including the ARM profile and the high-throughput (802.11n) radio profile.
`dot11g-radio-profile`	Details of AP radio settings for the 2.4 GHz frequency band, including the ARM profile and the high-throughput (802.11n) radio profile.
`event-thresholds-profile`	Details of events thresholds profile.
`ht-radio-profile`	Details of high-throughput AP radio settings
`optimization-profile`	Details of the RF optimization profile

Example

The output of this command shows status of ARM profile.

```
(host) # show profile-list rf arm-profile

Adaptive Radio Management (ARM) profile List
--------------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  2

Total:1
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show profile-list wlan

```
show profile-list wlan [ dotllk-profile | edca-parameters-profile | ht-ssid-profile |
   ssid-profile | traffic-management-profile | virtual-ap | voip-cac-profile | wmm-
   traffic-management-profile]
```

Description

Displays the status of WLAN profiles on the controller.

Syntax

Parameter	Description
`dot11k-profile`	Show a list of all 802.11K Profiles
`edca-parameters-profile`	Show a list of all enhanced distributed channel access (EDCA) profile for APs or for clients (stations)
`ht-ssid-profile`	Show a list of all high-throughput SSID profile.s
`traffic-management-profile`	Show a list of all traffic management profiles.
`virtual-ap`	Show a list of all the virtual AP profiles.
`voip-cac-profile`	Show a list of all voice over IP (VoIP) call admission control (CAC) profiles
`wmm-traffic-management-profile`	Show a list of all WMM traffic management profiles.

Example

The output of this command shows that the controller has a single ARM profile, “default”.

```
(host) # show profile-list rf arm-profile

Adaptive Radio Management (ARM) profile List
--------------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  2

Total:1
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show provisioning-ap-list

```
show provisioning-ap-list
```

Description

Displays the list of all APs that are in queue to be provisioned by the admin.

Syntax

No parameters.

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show rap-wml

```
show rap-wml [cache <server-name> | server | wired-mac <bssid-of-AP>]
```

Description

Displays the name and attributes of a MySQL database or a MySQL server.

Syntax

Parameter	Description
`cache`	Displays the cache of all lookups for a database server.
`servers`	Displays the database server state.
`wired-mac`	Displays the wired MAC discovered on traffic through the AP.

Example

The output of this command shows status of all database servers.

```
(host) # #show rap-wml servers

WML DB Servers
--------------
name  ip  type  user  password  db-name  cache  ageout(sec)  in-service
----  --  ----  ----  --------  -------  -----  -----------  ----------
WML DB Tables
-------------
server  db  table  column  timestamp-column  lookup-time(sec)  delimiter  query-count
------  --  -----  ------  ----------------  ----------------  ---------  -----------
Mesh SAE                    sae-default
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show references aaa authentication

crypto-local

```
show references aaa authentication {captive-portal <profile-name>}|{dot1x <profile-
name>}|{mac <profile-name>}|mgmt|stateful-dot1x|{stateful-ntlm <profile-
name>}|vpn|wired|{wispr {profile-name>} [page <number>] [start <number>]
```

Description

Show AAA profile references.

Syntax

Parameter	Description
`captive-portal <profile-name>`	Show the number of references to a captive-portal profile.
`dot1x <profile-name>`	Show the number of references to a 802.1x authentication profile.
`mac <profile-name>`	Show the number of references to a MAC authentication profile.
`mgmt <profile-name>`	Show the number of references to a management authentication profile.
`stateful-dot1x`	Show the number of references to the stateful 802.1X authentication profile.
`stateful-ntlm <profile-name>`	Show the number of references to the specified stateful NTLM authentication profile.
`vpn`	Show the number of references to VPN authentication.
`wired`	Show the number of references to wired authentication.
`wired`	Show the number of references to a wispr authentication.
`wispr <profile-name>`	Show the number of references to the specified WISPr authentication profile.
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

Use this command to show where a specified AAA profile has been applied. The output of the example shown below indicates that the aaa profile **default-dot1x** contains a single reference to the 802.1x authentication profile **default**.

```
(host) #show references aaa authentication dot1x default

References to 802.1X Authentication Profile "default"
-----------------------------------------------------
Referrer                                        Count
--------                                        -----
aaa profile "default-dot1x" authentication-dot1x  1
Total References:1
```

Command History.

Version	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4.1	The **stateful-ntlm** and **wispr** parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references aaa authentication-server

crypto-local
show references aaa authentication-server {ldap <ldap-server-name>}|{radius <radius-server-name>}|{tacacs <tacacs-server-name>} [page <number>] [start <number>]

Description

Display information about AAA authentication servers.

Syntax

Parameter	Description
ldap <ldap-server-name>	Show the number of server groups that include references to the specified LDAP server.
radius <radius-server-name>	Show the number of server groups that include references to the specified RADIUS server.
tacacs <radius-server-name>	Show the number of server groups that include references to the specified TACACS server.
page <number>	Include this optional parameter to limit output of this command to the specified number of items.
start <number>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

Issue this command to show the AAA server groups that include references to the specified server. The example below shows that two server groups, **default** and **rad,** each include a single reference to the radius server **rad01**.

```
(host) #show references aaa authentication-server radius rad01

References to RADIUS Server "rad01"
-----------------------------------
Referrer                                Count
--------                                -----
aaa server-group "default" server_group  1
aaa server-group "rad" server_group      1
Total References:2
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references aaa profile

```
crypto-local
show references aaa profile <profile-name>
```

Description

Show references to an AAA Profile.

Syntax

Parameter	Description
`profile <profile-name>`	Name of an AAA profile for which you want to view references.

Example

Issue this command to show the wlan virtual AP profiles that include references to the specified AAA profile. The example below shows that seven different virtual AP profiles include a single reference to the AAA profile **default**.

```
(host) #References to AAA Profile "default"
-----------------------------------
Referrer                                              Count
--------                                              -----
wlan virtual-ap "1.0.0_corporateHQ-wpa2" aaa-profile   1
wlan virtual-ap "110.0.corporateHQ-wpa2" aaa-profile   1
wlan virtual-ap "default" aaa-profile                  1
wlan virtual-ap "corporateHQ-vocera" aaa-profile       1
wlan virtual-ap "corporateHQ-voip-wpa2" aaa-profile    1
wlan virtual-ap "Test123" aaa-profile                  1
wlan virtual-ap "branch12" aaa-profile                 1
Total References:7
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references aaa server-group

```
crypto-local
show references aaa server-group <sg-name> [page] [start]}
```

Description

Show references to a server group.

Syntax

Parameter	Description
`server-group <sg-name>`	Name of the server group for which you want to show references
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

.Issue this command to display a list of AAA profiles that include references to the specified server group.

```
(host) #show references aaa server-group default

References to Server Group "default"
------------------------------------
Referrer                                                Count
--------                                                -----
aaa profile "aircorp-office-ssid" mac-server-group      1
aaa profile "amigopod-guest" mac-server-group           1
aaa profile "default" mac-server-group                  1
aaa profile "default-airwave-office" mac-server-group   1
aaa profile "defaultcorporate" mac-server-group         1
aaa profile "defaultcorporate-no-okc" mac-server-group  1
aaa profile "defaultcorporate-okc" mac-server-group     1
aaa profile "default-dot1x" mac-server-group            1
aaa profile "default-India" mac-server-group            1
aaa profile "default-india-hotel" mac-server-group      1
aaa profile "default-India-split" mac-server-group      1
aaa profile "voip-psk" mac-server-group                 1
aaa profile "default-dot1x-psk" mac-server-group        1
aaa profile "default-mac-auth" mac-server-group         1
aaa profile "default-open" mac-server-group             1
aaa profile "default-xml-api" mac-server-group          1
Total References:16
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references ap

```
crypto-local
show references ap
   enet-link-profile <profile-name>
   mesh-cluster-profile <profile-name>
   mesh-ht-ssid-profile <profile-name>
   mesh-radio-profile <profile-name>
   regulatory-domain-profile <profile-name>
   system-profile <profile-name>
   wired-ap-profile <profile-name>
   page <number>
   start <number>
```

Description

Show the number of references to a specific AP profile.

Syntax

Parameter	Description
`enet-link-profile <profile-name>`	Show AP groups that include a references to this ethernet link profile.
`mesh-cluster-profile <profile-name>`	Show AP groups that include a references to this mesh cluster profile.
`mesh-ht-ssid-profile <profile-name>`	Show AP groups that include a references to this mesh high-throughput SSID profile.
`mesh-radio-profile <profile-name>`	Show AP groups that include a references to this mesh radio profile.
`regulatory-domain-profile <profile-name>`	Show AP groups that include a references to this regulatory domain profile.
`system-profile <profile-name>`	Show AP groups that include a references to this system profile.
`wired-ap-profile <profile-name>`	Show AP groups that include a references to this wired AP profile.
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

The example below shows that 10 different AP groups include links to the AP ethernet link profile **Default**. These 10 AP groups reference the **Default** ethernet link profile for both their ethernet 0 and ethernet 1 interfaces, for a total of 20 references altogether.

```
(host)#show references ap enet-link-profile default

References to AP Ethernet Link profile "default"
------------------------------------------------
Referrer                                    Count
--------                                    -----
ap-group "10.0.0" enet0-profile             1
ap-group "10.0.0" enet1-profile             1
ap-group "corp" enet0-profile               1
ap-group "corp" enet1-profile               1
ap-group "Corp_AM_Ch1" enet0-profile        1
ap-group "Corp_AM_Ch1" enet1-profile        1
ap-group "Corp_AM_Ch6" enet0-profile        1
ap-group "Corp_AM_Ch6" enet1-profile        1
ap-group "corpTest" enet0-profile           1
ap-group "corpTest" enet1-profile           1
ap-group "default" enet0-profile            1
ap-group "default" enet1-profile            1
ap-group "India_Local" enet0-profile        1
ap-group "India_Local" enet1-profile        1
ap-group "ops" enet0-profile                1
ap-group "ops" enet1-profile                1
ap-group "voip-test" enet0-profile          1
ap-group "voip-test" enet1-profile          1
ap-group "voip-test-nokia" enet0-profile    1
ap-group "voip-test-nokia" enet1-profile    1
Total References:20
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references guest-access-email

```
crypto-local
show references guest-access-email [page <number>] [start <number>]
```

Description

Show references to the global guest access email profile.

Syntax

Parameter	Description
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host) #show references guest-access-email

References to Guest-access Email Profile
----------------------------------------
Referrer  Count
--------  -----
Total References:0
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references ids

```
crypto-local
show references ids
   dos-profilegeneral-profile
   general-profile
   impersonation-profile
   profile
   rate-thresholds-profile
   signature-matching-profile
   signature-profile
   unauthorized-device-profile
```

Description

Displays IDS profile references.

Syntax

Parameter	Description
`dos-profilegeneral-profile`	Show references to an IDS Denial Of Service Profile
`general-profile`	Show references to an IDS General Profile
`impersonation-profile`	Show references to an IDS Impersonation Profile
`profile`	Show references to an IDS Profile
`rate-thresholds-profile`	Show references to an IDS Rate Thresholds Profile
`signature-matching-profile`	Show references to an IDS Signature Matching Profile
`signature-profile`	Show references to an IDS Signature Profile
`unauthorized-device-profile`	Show references to an IDS Signature Profile

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references papi-security

```
crypto-local
show references papi-security [page <number>] [start <number>]
```

Description

Show references to a PAPI security profile.

Syntax

Parameter	Description
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host) #show references papi-security

References to PAPI Security Profile
-----------------------------------
Referrer  Count
--------  -----
Total References:0
```

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references rf

```
crypto-local
show references rf
   dot11a-radio-profile <profile-name>
   dot11g-radio-profile <profile-name>
   event-thresholds-prof <profile-name>
   ht-radio-profile <profile-name>
   optimization-profile <profile-name>
```

Description

Show RF profile references.

Syntax

Parameter	Description
`dot11a-radio-profile`	Show references to a 802.11a radio profile
`dot11g-radio-profile`	Show references to a 802.11g radio profile
`event-thresholds-prof`	Show references to an RF Event Thresholds Profile
`ht-radio-profile`	Show references to a High-throughput radio profile
`optimization-profile`	Show references to an RF Optimization Profile

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references user-role

```
crypto-local
show references user-role <role_name>
```

Description

Show access rights for user role.

Syntax

Parameter	Description
<role_name>	The role name assigned to a user.

Example

```
(host) #show references user-role guest

References to User Role "guest"
-------------------------------
aaa profile "airwave-office-ssid" mac-default-role
aaa profile "amigopod-guest" mac-default-role
aaa profile "corp1344-voip" mac-default-role
aaa profile "default" mac-default-role
aaa profile "default-airwave-office" mac-default-role
aaa profile "default-corp1344" mac-default-role
aaa profile "default-corp1344-no-okc" mac-default-role
aaa profile "default-corp1344-okc" mac-default-role
aaa profile "default-dot1x" mac-default-role
aaa profile "default-dot1x-psk" mac-default-role
aaa profile "default-dot1x-psk" dot1x-default-role
aaa profile "default-India" mac-default-role
aaa profile "default-india-hotel" mac-default-role
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references web-server

```
crypto-local
show references web-server [page <number>] [start <number>]
```

Description

Show the Web server configuration references.

Syntax

Parameter	Description
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host) #show references web-server

References to Web Server Configuration
--------------------------------------
Referrer  Count
--------  -----
Total References:0
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show references wlan

```
crypto-local
show references wlan
   dot11k-profile <profile-name>
   edca-parameters-profile <profile-name>
   ht-ssid-profile <profile-name>
   ssid-profile <profile-name>
   traffic-management-pr <profile-name>
   virtual-ap <profile-name>
   voip-cac-profile <profile-name>
```

Description

Shows WLAN profile references.

Syntax

Parameter	Description
`dot11k-profile <profile-name>`	Shows references to a 802.11K profile.
`edca-parameters-profile <profile-name>`	Shows references to an EDCA parameters profile.
`ht-ssid-profile <profile-name>`	Shows references to a high-throughput SSID profile.
`ssid-profile <profile-name>`	Shows references to an SSID management profile.
`traffic-management-pr <profile-name>`	Shows references to a traffic management profile.
`virtual-ap <profile-name>`	Shows references to a virtual AP profile.
`voip-cac-profile <profile-name>`	Shows references to a VOIP Call Admission Control profile.

Example

```
(host) #show references web-server

References to Web Server Configuration
--------------------------------------
Referrer  Count
--------  -----
Total References:0
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master and local controllers

show remote-node

Description

Shows configuration and other information about the remote node.

Syntax

Parameter	Description
`config <mac-address>`	Shows configuration information for the remote node.
`dhcp-instance <mac-address>`	Shows the remote node address pool information including pool name, DHCP pool start IP address, DHCP pool mask, DHCP pool broadcast IP address, and the DHCP pool gateway IP address.
`license-usage`	Shows the remote node AP license usage information including the remote node MAC address, IP address and the AP, PEF and RF Protect licenses along with the last time the licenses were updated.
`running-config <mac-address>`	Shows the running configuration for this remote node

Usage Guidelines

Issue this command to display configuration, DHCP pool information license usage information and running configuration information for a remote node.

Examples

This example shows a remote node configuration.

```
(host) #show remote-node config 00:0b:86:f0:26:e0

controller-ip vlan 2
vlan 2
vlan 3
interface fastethernet "1/7"
  interface fastethernet "1/7" switchport access vlan 3
  interface fastethernet "1/7" trusted
interface fastethernet "1/2"
  interface fastethernet "1/2" switchport access vlan 2
  interface fastethernet "1/2" trusted
interface fastethernet "1/3"
  interface fastethernet "1/3" switchport access vlan 2
  interface fastethernet "1/3" trusted
interface fastethernet "1/1"
  interface fastethernet "1/1" switchport access vlan 2
  interface fastethernet "1/1" trusted
interface vlan 3
  interface vlan 3 ip address 10.3.29.79 255.255.255.0
interface vlan 2
  interface vlan 2 ip address 192.167.1.1 255.255.255.240
uplink wired vlan 4
interface tunnel 1
  interface tunnel 1 tunnel destination remote-node-master-ip
ip route 10.100.102.217 255.255.255.255 10.3.29.254
ip route 10.100.102.173 255.255.255.255 10.3.29.254
ip route 10.1.1.41 255.255.255.255 10.3.29.254
mgmt-user "admin" "root" "ade8c0d3890aa97914d926120279aef2"
service dhcp
ip dhcp pool vlanx domain-name mycorp.com
ip dhcp pool vlanx
ip dhcp pool vlanx default-router 192.167.1.1
ip dhcp pool vlanx dns-server 192.167.1.1
ip dhcp pool vlanx network 192.167.1.0 255.255.255.240
remote-node config-id 32
```

This example shows remote node AP license usage information.

```
(host) #show remote-node license-usage

Remote Node AP License Usage (license limit: 65)
------------------------------------------------
MAC Address        IP Address   AP Lic. Used  PEF Lic. Used  RF Protect Lic. Used  Last update (secs. ago)
-----------        ----------   ------------  -------------  --------------------  ----------------------
00:0b:86:f0:26:e0  192.167.1.1  0             0              0                     2
```

Related Commands

Command	Description	Mode
`remote-node-profile`	Use this command to create a Remote Node profile.	Enable and Config modes
`remote-node-localip`	Use this command to configure the switch-IP address and preshared key for the local Remote Node on a master Remote Node.	Enable and Config modes
`remote-node-masterip`	Use this command to configure the IP address and preshared key for the master Remote Node on a local Remote Node.	Enable and Config modes

Command History

Release	Modification
ArubaOS 6.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master and local controllers

show remote-node-dhcp-pool

```
show remote-node-dhcp-pool <remote-node-profile-name>
```

Description

The output of this command lists shows Remote Node DHCP pool summary information.

Syntax

Parameter	Description
`remote-node-profile-name`	Name of the Remote Node profile

Usage Guidelines

Each Remote Node profile contains a Remote Node DHCP address pool, which defines a range of IP addresses allocated for Remote Node controllers at a remote site, and the VLAN to be associated with those addresses. A remote-node dhcp pool is configured in the remote-note mode.

Use the show **remote-node-dhcp-pool** command to view a summary of Remote Node address pool information.

Example

This example shows a summary of Remote Node DHCP address pool information.

```
(host) #show remote-node-dhcp-pool pool1

Remote Node Address Pools
-------------------------------------
Pool Name  Type    Start IP Address  End IP Address  Domain Name  Num Hosts
---------  ----    ----------------  --------------  -----------  ---------
```

The output of this command includes the following parameters:

Parameter	Description
`Pool Name`	Name of the new DHCP pool.
`Type`	Type of pool. This can be tunnel or vlan.
`Start IP Address`	IP addresses at the start and end of the Remote Node's address range, in dotted-decimal format.
`End IP Address`	IP address at the end of the Remote Node's address range, in dotted-decimal format.
`Domain Name`	The DHCP domain name.
`Num Hosts`	Maximum number of hosts supported by a Remote Node using this pool.

Related Commands

Command	Description	Mode
`remote-node-profile`	The remote-node-profile command lets you create a Remote Node profile.	Config mode

Command History

Release	Modification
ArubaOS 6.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master and local controllers

show remote-node-profile

```
show remote-node-profile
```

Description

The output of this command shows Remote Node profile configuration information.

Syntax

Parameter	Description
`remote-node-profile-name`	Name of the Remote Node profile

Usage Guidelines

This **show remote-node-profile** command shows the configuration status of a Remote Node profile. To create a Remote Node profile, use the **remote-node-profile** command to create a Remote Node profile.

Example

This example shows the configuration status of Remote Node profile named “test.”

```
(host) #show remote-node-profile ?
<remote-node-profile-name>      Profile name
|                       Output Modifiers
<cr>

(host) #show remote-node-profile test

.......Vlan interface not configured for the controller-ip vlan.
.......No uplink information has been configured.


remote-node-profile test
  remote-node-dhcp-pool newpool
    pool-type tunnel 0
    domain-name mycorp.com
    range startip 0.0.0.0 endip 0.0.0.0 hosts 1
  !
!
```

Related Commands

Command	Description	Mode
`remote-node-profile`	The remote-node-profile command lets you create a Remote Node profile.	Config mode

Command History

Release	Modification
ArubaOS 6.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master and local controllers

show rf arm-profile

```
show rf arm-profile [<profile>]
```

Description

Show an Adaptive Radio Management (ARM) profile.

Syntax

Parameter	Description
<profile>	Name of an ARM profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire ARM profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has five configured ARM profiles. The **References** column lists the number of other profiles with references to the ARM profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) # show rf arm-profile
Adaptive Radio Management (ARM) profile List
--------------------------------------------
Name                   References  Profile Status
----                   ----------  --------------
airwave                2
default                4
default-AP85           2
no-scanning            1
Wireless-rf-profile    1

Total:5
```

This example displays the configuration settings for the profile **Wireless_rf_profile.**

```
(host) #show rf arm-profile default
Adaptive Radio Management (ARM) profile "test"
----------------------------------------------
Parameter                         Value
---------                         -----
Assignment                        disable
Allowed bands for 40MHz channels  a-only
Client Aware                      Enabled
Max Tx Power                      30 dBm
Min Tx Power                      9 dBm
Multi Band Scan                   Enabled
Rogue AP Aware                    Disabled
Scan Interval                     10 sec
Active Scan                       Disabled
Scanning                          Enabled
Scan Time                         110 msec
VoIP Aware Scan                   Disabled
Video Aware Scan                  Enabled
Power Save Aware Scan             Enabled
Ideal Coverage Index              10
Acceptable Coverage Index         4
Free Channel Index                25
Backoff Time                      240 sec
Error Rate Threshold              50 %
Error Rate Wait Time              30 sec
Noise Threshold                   75 -dBm
Noise Wait Time                   120 sec
Minimum Scan Time                 8 sec
Load aware Scan Threshold         1250000 Bps
Mode Aware Arm                    Disabled
Scan Mode                         all-reg-domain
```

The output of this command includes the following parameters:

Parameter	Description
Assignment	Displays the current ARM channel/power assignment mode.
Allowed bands for 40MHz channels	Shows if 40 MHz mode of operation is allowed on the 5 GHz (802.11a) or 2.4 GHz (802.11b/g) frequency band only, on all frequency bands, or on neither frequency band.
Client Aware	Shows if the client aware feature is enabled or disabled. When enabled, the AP does not change channels when there are active clients.
Max Tx Power	The highest transmit power levels for the AP, from 0-30 dBm in 3 dBm increments. Higher power level settings may be constrained by local regulatory requirements and AP capabilities. In the event that an AP is configured for a Max Tx Power setting it cannot support, this value will be reduced to the highest supported power setting.
Min Tx Power	The lowest transmit power levels for the AP, from 0-30 dBm, in 3 dBm increments. Note that power settings will not change if the Assignment option is set to disabled or maintain.
Multi Band Scan	If enabled, single-radio APs will try to scan across bands for rogue AP detection.
Rogue AP Aware	If enabled, Dell APs may change channels to contain off-channel rogue APs with active clients. This security features allows APs to change channels even if the Client Aware setting is disabled. This setting is disabled by default, and should only be enabled in high-security environments where security requirements are allowed to consume higher levels of network resources. You may prefer to receive Rogue AP alerts via SNMP traps or syslog events.

Parameter	Description
Scan Interval	If Scanning is enabled, the Scan Interval defines how often the AP will leave its current channel to scan other channels in the band. Off-channel scanning can impact client performance. Typically, the shorter the scan interval, the higher the impact on performance. If you are deploying a large number of new APs on the network, you may want to lower the Scan Interval to help those APs find their optimal settings more quickly. Raise the Scan Interval back to its default setting after the APs are functioning as desired.
Active Scan	If enabled, the AP initiates active scanning via probe request. This option elicits more information from nearby APs, but also creates additional management traffic on the network. Active Scan is disabled by default, and should not be enabled except under the direct supervision of Dell Support.
Scanning	Shows if the AP has enabled or disabled AP scanning of other channels.
Scan Time	The amount of time, in milliseconds, an AP will drift out of the current channel to scan another channel.
VoIP Aware Scan	Shows if Dell's VoIP Call Admission Control (CAC) prevents any single AP from becoming congested with voice calls. If CAC is enabled, you should also enable VoIP Aware Scan in the ARM profile, so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call.
Power Save Aware Scan	When enabled, the AP will not scan if Power Save is active.
Video Aware Scan	If Video Aware Scan is enabled in the ARM profile, the AP will not attempt to scan a different channel if one of its clients has an active video session.
Ideal Coverage Index	The coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be.
Acceptable Coverage Index	The minimal coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be.
Free Channel Index	The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel.
Backoff Time	Time, in seconds, an AP backs off after requesting a new channel or power level.
Error Rate Threshold	The percentage of errors in the channel that triggers a channel change.
Error Rate Wait Time	Time, in seconds, that the error rate has to maintain or surpass the error rate threshold before it triggers a channel change.
Noise Threshold	Maximum level of noise (in -dBm) in a channel that triggers a channel change.
Noise Wait Time	Time, in seconds, the noise has to be high to trigger a channel change.
Minimum Scan Time	Time, in seconds, that a channel must be scanned before it is considered for assignment.
Load aware Scan Threshold	The traffic throughput level an AP must reach before it stops scanning, in bytes/second. A value of 0 to disables this feature.
Mode Aware Arm	If enabled, ARM will turn APs into Air Monitors (AMs) if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (e.g. less than 60 feet apart).
Scan Mode	This parameter defines the scan mode for the AP. • all-reg-domain: The AP scans channels within all regulatory domains. This is the default setting. • reg-domain:Limit the AP scans to just the regulatory domain for that AP.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show rf dot11a-radio-profile

```
show rf dot11a-radio-profile [<profile>]
```

Description

Show an 802.11a Radio profile.

Syntax

Parameter	Description
<profile>	Name of an 802.11a profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire 802.11a Radio profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured 802.11a Radio profiles. The **References** column lists the number of other profiles with references to the 802.11a Radio profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) # show rf dot11a-radio-profile
802.11a radio profile List
--------------------------
Name          References  Profile Status
----          ----------  --------------
default       18
default-AP85  1
test          1

Total:3
```

This example displays the configuration settings for the profile **default**.

```
(host) # show rf dot11a-radio-profile default
Parameter                                    Value
---------                                    -----
Radio enable                                 Enabled
Mode                                         ap-mode
High throughput enable (radio)               Enabled
Channel                                      N/A
Beacon Period                                100 msec
Beacon Regulate                              Disabled
Transmit EIRP                                15 dBm
Advertise 802.11d and 802.11h Capabilities   Disabled
TPC Power                                    15 dBm
Spectrum load balancing                      Disabled
Spectrum Load balancing mode                 channel
Spectrum load balancing update interval (sec) 2147483647 secon
Advertized regulatory max EIRP               99999
Spectrum Load Balancing domain               N/A
RX Sensitivity Tuning Based Channel Reuse    disable
RX Sensitivity Threshold                     0 -dBm
Enable CSA                                   Disabled
CSA Count                                    4
Management Frame Throttle interval           1 sec
Management Frame Throttle Limit              20
ARM/WIDS Override                            Disabled
Adaptive Radio Management (ARM) Profile      default
High-throughput Radio Profile                default-a
Maximum Distance                             0 meters
```

The output of this command includes the following parameters:

Parameter	Description
Radio enable	Shows if the AP has enabled or disabled transmissions on this radio band.
Mode	Access Point operating mode. Available options are: • am-mode: Air Monitor mode • ap-mode: Access Point mode • apm-mode: Access Point Monitor mode • sensor-mode: RFprotect sensor mode
High throughput enable (radio)	Name of a high-throughput profile referenced by this 802.11a radio profile. A high-throughput profile manages 40 Mhz tolerance settings, and controls whether or not APs using this profile will advertise intolerance of 40 MHz operation. (This option is disabled by default, allowing 40 MHz operation.) A high-throughput profile also determines whether an AP radio using the profile will stop using the 40 MHz channels surrounding APs or stations advertise 40 Mhz intolerance. This option is enabled by default.
Channel	Channel number for the AP 802.11a/802.11n physical layer.
Beacon Period	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Beacon Regulate	If enabled, this option introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air. This option is disabled by default.
Transmit EIRP	Maximum transmit power (EIRP) in dBm from 0 to 51 in .5 dBm increments. Further limited by regulatory domain constraints and AP capabilities.
Advertise 802.11d and 802.11h Capabilities	If enabled, the radio advertises its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities.
TPC Power	The transmit power advertised in the TPC IE of beacons and probe responses.

Parameter	Description
Spectrum Load balancing mode	SLB Mode allows control over how to balance clients. Channel-based load-balancing balances clients across channels. Radio-based load-balancing distributes clients across radios on the same band, independent of channels.
Spectrum Load balancing mode update interval	This parameter specifies how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.
Spectrum load balancing	The Spectrum load balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests. If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Dell AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.
RX Sensitivity Tuning Based Channel Reuse	Shows if the channel reuse feature's current operating mode, static, dynamic or disable. • **Static**: This mode of operation is a coverage-based adaptation of the Clear Channel Assessment (CCA) thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. • **Dynamic**: In this mode, the Clear Channel Assessment (CCA) thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. • **Disable**: This mode does not support the tuning of the CCA Detect Threshold.
RX Sensitivity Threshold	If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (-dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. For example, if the RX sensitivity threshold was set to -65 dBm, the AP would ignore signals with a strength from -1 dBM to -64 dBm. If the value is set to zero, the feature will automatically determine an appropriate threshold.
Enable CSA	Shows if Channel Switch Announcements (CSAs) are enabled or disabled. CSAs, as defined by IEEE 802.11h, enable an AP to announce that it is switching to a new channel before it begins transmitting on that channel. This allows clients that support CSA to transition to the new channel with minimal downtime.
CSA Count	Number of channel switch announcements that must be sent prior to switching to a new channel. The default CSA count is 4 announcements.
Management Frame Throttle Interval	Averaging interval for rate limiting mgmt frames from this radio, in seconds. A management frame throttle interval of 0 seconds disables rate limiting.
Management Frame Throttle Limit	Maximum number of management frames that can come in from this radio in each throttle interval.
ARM/WIDS Override	If enabled, this option disables Adaptive Radio Management (ARM) and Wireless IDS functions and slightly increases packet processing performance. If a radio is configured to operate in Air Monitor mode, then the ARM/WIDS override functions are always enabled, regardless of whether or not this check box is selected.
Adaptive Radio Management (ARM) Profile	Name of an Adaptive Radio Management profile associated with this 802.11a profile.
Maximum Distance	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km.

Command History

Release	Modification
ArubaOS 3.0	Command introduced.
ArubaOS 3.3.2	Introduced support for the high-throughput IEEE 802.11n standard.
ArubaOS 3.4.0	Support for the following parameters: • Spectrum load balancing • RX Sensitivity Tuning Based Channel Reuse • RX Sensitivity Threshold • ARM/WIDS Override
ArubaOS 3.4.2	Support for the **Beacon Regulate** parameter

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show rf dot11g-radio-profile

```
show rf dot11g-radio-profile [<profile>]
```

Description

Show an 802.11g Radio profile.

Syntax

Parameter	Description
<profile>	Name of a 802.11g profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire 802.11g profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has four configured 802.11g profiles. The **References** column lists the number of other profiles with references to the 802.11g profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) # show rf arm-profile
Adaptive Radio Management (ARM) profile List
--------------------------------------------
Name                   References  Profile Status
----                   ----------  --------------
airwave                4
default                4
no-scanning            1
nokia-rf-profile       1

Total:4
```

This example displays the configuration settings for the profile **airwave**.

```
(host) # show rf dot11g-radio-profile default

802.11g radio profile "default"
-------------------------------
Parameter                                   Value
---------                                   -----
Radio enable                                Enabled
Mode                                        ap-mode
High throughput enable (radio)              Enabled
Channel                                     N/A
Beacon Period                               100 msec
Beacon Regulate                             Disabled
Transmit EIRP                               15 dBm
Advertise 802.11d and 802.11h Capabilities  Disabled
TPC Power                                   15 dBm
Spectrum load balancing                     Disabled
Spectrum Load balancing mode                channel
Spectrum load balancing update interval (sec)  30 seconds
Advertized regulatory max EIRP              0
Spectrum Load Balancing domain              N/A
RX Sensitivity Tuning Based Channel Reuse   disable
RX Sensitivity Threshold                    0 -dBm
Non 802.11 Interference Immunity            Level-2
Enable CSA                                  Disabled
CSA Count                                   4
Management Frame Throttle interval          1 sec
Management Frame Throttle Limit             20
ARM/WIDS Override                           Disabled
Protection for 802.11b Clients              Enabled
Adaptive Radio Management (ARM) Profile     default
High-throughput Radio Profile               default-g
Maximum Distance                            0 meters
```

The output of this command includes the following parameters:

Parameter	Description
Radio enable	Shows if the AP has enabled or disabled transmissions on this radio band.
Mode	Access Point operating mode. Available options are: • am-mode: Air Monitor mode • ap-mode: Access Point mode • apm-mode: Access Point Monitor mode • sensor-mode: RFprotect sensor mode
High throughput enable (radio)	Name of a high-throughput profile referenced by this 802.11a radio profile. A high-throughput profile manages 40 Mhz tolerance settings, and controls whether or not APs using this profile will advertise intolerance of 40 MHz operation. (This option is disabled by default, allowing 40 MHz operation.) A high-throughput profile also determines whether an AP radio using the profile will stop using the 40 MHz channels surrounding APs or stations advertise 40 Mhz intolerance. This option is enabled by default.
Channel	Channel number for the AP 802.11a/802.11n physical layer.
Beacon Period	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Beacon Regulate	If enabled, this option introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air. This option is disabled by default.
Transmit EIRP	Maximum transmit power (EIRP) in dBm from 0 to 51 in .5 dBm increments. Further limited by regulatory domain constraints and AP capabilities.

Parameter	Description
Advertise 802.11d and 802.11h Capabilities	If enabled, the radio advertises its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities.
TPC Power	The transmit power advertised in the TPC IE of beacons and probe responses.
Spectrum Load balancing mode	SLB Mode allows control over how to balance clients. Channel-based load-balancing balances clients across channels. Radio-based load-balancing distributes clients across radios on the same band, independent of channels.
Spectrum Load balancing mode update interval	This parameter specifies how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.
Spectrum load balancing	The Spectrum load balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests. If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Dell AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.
RX Sensitivity Tuning Based Channel Reuse	Shows if the channel reuse feature's current operating mode, static, dynamic or disable. • **Static**: This mode of operation is a coverage-based adaptation of the Clear Channel Assessment (CCA) thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. • **Dynamic**: In this mode, the Clear Channel Assessment (CCA) thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. • **Disable**: This mode does not support the tuning of the CCA Detect Threshold.
RX Sensitivity Threshold	If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (-dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. For example, if the RX sensitivity threshold was set to -65 dBm, the AP would ignore signals with a strength from -1 dBM to -64 dBm. If the value is set to zero, the feature will automatically determine an appropriate threshold.
Non 802.11 Interference Immunity	Show the current value for 802.11 Interference Immunity on the 2.4 Ghz band. The default setting for this parameter is level 2. When performance drops due to interference from non-802.11 interferers (such as DECT or Bluetooth devices), the level can be increased up to level 5 for improved performance. However, increasing the level makes the AP slightly "deaf" to its surroundings, causing the AP to lose a small amount of range. The levels for this parameter are: • Level-0: no ANI adaptation. • Level-1: noise immunity only. • Level-2: noise and spur immunity. • Level-3: level 2 and weak OFDM immunity. • Level-4: level 3 and FIR immunity. • Level-5: disable PHY reporting.
Enable CSA	Shows if Channel Switch Announcements (CSAs) are enabled or disabled. CSAs, as defined by IEEE 802.11h, enable an AP to announce that it is switching to a new channel before it begins transmitting on that channel. This allows clients that support CSA to transition to the new channel with minimal downtime.
CSA Count	Number of channel switch announcements that must be sent prior to switching to a new channel. The default CSA count is 4 announcements.
Management Frame Throttle Interval	Averaging interval for rate limiting mgmt frames from this radio, in seconds. A management frame throttle interval of 0 seconds disables rate limiting.

Parameter	Description
Management Frame Throttle Limit	Maximum number of management frames that can come in from this radio in each throttle interval.
ARM/WIDS Override	If enabled, this option disables Adaptive Radio Management (ARM) and Wireless IDS functions and slightly increases packet processing performance. If a radio is configured to operate in Air Monitor mode, then the ARM/WIDS override functions are always enabled, regardless of whether or not this check box is selected.
Protection for 802.11b Clients	Shows if the profile has enabled or disabled protection for 802.11b clients.
Adaptive Radio Management (ARM) Profile	Name of an Adaptive Radio Management profile associated with this 802.11a profile.
High-throughput Radio Profile	Name of a High Throughput Radio profile associated with this 802.11a profile.
Maximum Distance	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km.

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3.2	Introduced protection for 802.11b clients and support for the high-throughput IEEE 802.11n standard
ArubaOS 3.4	Support for the following parameters: • Spectrum load balancing • RX Sensitivity Tuning Based Channel Reuse • RX Sensitivity Threshold • ARM/WIDS Override
ArubaOS 3.4.2	Support for the **Beacon Regulate** parameter

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show rf event-thresholds-profile

```
show rf event-thresholds-profile [<profile>]
```

Description

Show an Event Thresholds profile.

Syntax

Parameter	Description
<profile>	name of an Event Thresholds profile

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire Event Thresholds profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured Event Thresholds profiles. The **References** column lists the number of other profiles with references to the Event Thresholds profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) # show rf event-thresholds-profile

RF Event Thresholds Profile List
--------------------------------
Name     References  Profile Status
----     ----------  --------------
default  6
event1   2

Total: 2
```

This example displays the configuration settings for the profile **default**.

```
(host) # show rf event-thresholds-profile default
RF Event Thresholds Profile "default"
-------------------------------------
Parameter                                Value
---------                                -----
Detect Frame Rate Anomalies              Disabled
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  16 %
Frame Fragmentation Rate Low Watermark   8 %
Frame Low Speed Rate High Watermark      16 %
Frame Low Speed Rate Low Watermark       8 %
Frame Non Unicast Rate High Watermark    0 %
Frame Non Unicast Rate Low Watermark     0 %
Frame Receive Error Rate High Watermark  16 %
Frame Receive Error Rate Low Watermark   8 %
Frame Retry Rate High Watermark          16 %
Frame Retry Rate Low Watermark           8 %
```

The output of this command includes the following parameters:

Parameter	Description
Detect Frame Rate Anomalies	Shows of the profile enables or disables detection of frame rate anomalies.
Bandwidth Rate High Watermark	If bandwidth in an AP exceeds this value, it triggers a **bandwidth exceeded condition**. The value represents the percentage of maximum for a given radio. (For 802.11b, the maximum bandwidth is 7 Mbps. For 802.11 a and g, the maximum is 30 Mbps.) The recommended value is 85%.
Bandwidth Rate Low Watermark	If an AP triggers a **bandwidth exceeded** condition, the condition persists until bandwidth drops below this value.
Frame Error Rate High Watermark	If the frame error rate (as a percentage of total frames in an AP) exceeds this value, it triggers a **frame error rate exceeded** condition.
Frame Error Rate Low Watermark	If an AP triggers a **frame error rate exceeded** condition, the condition persists until the frame error rate drops below this value.
Frame Fragmentation Rate High Watermark	If the frame fragmentation rate (as a percentage of total frames in an AP) exceeds this value, it triggers a **frame fragmentation rate exceeded** condition.
Frame Fragmentation Rate Low Watermark	If an AP triggers a **frame fragmentation rate exceeded** condition, the condition persists until the frame fragmentation rate drops below this value.
Frame Low Speed Rate High Watermark	If the rate of low-speed frames (as a percentage of total frames in an AP) exceeds this value, it triggers a **low-speed rate exceeded** condition.
Frame Low Speed Rate Low Watermark	After a **low-speed rate exceeded condition** exists, the condition persists until the percentage of low-speed frames drops below this value.
Frame Non Unicast Rate High Watermark	If the non-unicast rate (as a percentage of total frames in an AP) exceeds this value, it triggers a **non-unicast rate exceeded** condition. This value depends upon the applications used on the network.
Frame Non Unicast Rate Low Watermark	If an AP triggers a **non-unicast rate exceeded** condition, the condition persists until the non-unicast rate drops below this value.
Frame Receive Error Rate High Watermark	If the frame receive error rate (as a percentage of total frames in an AP) exceeds this value, it triggers a **frame receive error rate exceeded** condition.
Frame Receive Error Rate Low Watermark	If an AP triggers a **frame receive error rate exceeded** condition, the condition persists until the frame receive error rate drops below this value.
Frame Retry Rate High Watermark	If the frame retry rate (as a percentage of total frames in an AP) exceeds this value, it triggers a **frame retry rate exceeded** condition.
Frame Retry Rate Low Watermark	If an AP triggers a **frame retry rate exceeded** condition exists, the condition persists until the frame retry rate drops below this value.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show rf ht-radio-profile

```
show rf ht-radio-profile [<profile>]
```

Description

Show a High-throughput Radio profile.

Syntax

Parameter	Description
<profile>	Name of a High-throughput Radio profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire High-throughput Radio profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has five configured High-throughput Radio profiles. The **References** column lists the number of other profiles with references to the High-throughput Radio profile, and the **Profile Status** column indicates whether the profile is predefined and editable, and if that predefined profile has been changed from its default settings. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) # show rf ht-radio-profile
High-throughput radio profile List
----------------------------------
Name           References  Profile Status
----           ----------  --------------
default        0
default-a      8           Predefined (editable)
default-g      3           Predefined (changed)
legacystation  1
test           1

Total:5
```

This example displays the configuration settings for the predefined profile **default-a**.

```
(host) #show rf ht-radio-profile default-a
High-throughput radio profile "default-a" (Predefined (editable))
-----------------------------------------------------------------
Parameter                 Value
---------                 -----
40 MHz intolerance        Disabled
Honor 40 MHz intolerance  Enabled
Legacy station workaround  Disabled
```

The output of this command includes the following parameters:

Parameter	Description
40 MHz intolerance	Shows whether or not APs using this radio profile will advertise intolerance of 40 MHz operation. By default, 40 MHz operation is allowed.
Honor 40 MHz intolerance	If this parameter is enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.

Parameter	Description
Legacy station workaround	Shows if the profile enables interoperability for misbehaving legacy stations. This parameter is disabled by default.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show rf optimization-profile

```
show rf optimization-profile [<profile>]
```

Description

Show an Optimization profile.

Syntax

Parameter	Description
<profile>	name of an ARM profile

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire Optimization profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured Optimization profiles. The **References** column lists the number of other profiles with references to the Optimization profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) # show rf optimization-profile
RF Optimization Profile List
----------------------------
Name     References  Profile Status
----     ----------  --------------
default  6
profile2 1

Total:2
```

This example displays the configuration settings for the profile **profile2**.

```
(host) #show rf optimization-profile profile2
RF Optimization Profile "profile2"
----------------------------------
Parameter                           Value
---------                           -----
Station Handoff Assist              Disabled
Detect Association Failure          Disabled
Coverage Hole Detection             Disabled
Hole Good RSSI Threshold            20
Hole Good Station Ageout            30 sec
Hole Detection Interval             180 sec
Hole Idle Station Ageout            90 sec
Hole Poor RSSI Threshold            10
Detect interference                 Disabled
Interference Threshold              90 %
Interference Threshold Exceed Time  25 sec
Interference Baseline Time          25 sec
RSSI Falloff Wait Time              0 sec
Low RSSI Threshold                  0
RSSI Check Frequency                0 sec
```

The output of this command includes the following parameters:

Parameter	Description
Station Handoff Assist	If enabled, this parameter allows the controller to force a client off an AP when the RSSI drops below a defined minimum threshold.
Detect Association Failure	Shows if the profile enables or disables STA association failure detection.
Coverage Hole Detection	Shows if the profile enables or disables coverage hole detection.
Hole Good RSSI Threshold	Time, in seconds, after a coverage hole is detected until a coverage hole event notification is generated. This parameter requires the RF Protect license.
Hole Good Station Ageout	Stations with signal strength above this value are considered to have good coverage. This parameter requires the RF Protect license.
Hole Detection Interval	Time, in seconds, after which a station with good coverage is aged out. This parameter requires the RF Protect license.
Hole Idle Station Ageout	Time, in seconds, after which a station in a poor coverage area is aged out. This parameter requires the RF Protect license.
Hole Poor RSSI Threshold	Stations with signal strength below this value will trigger detection of a coverage hole. This parameter requires the RF Protect license.
Detect interference	Enables or disables interference detection.
Interference Threshold	Percentage increase in the frame retry rate (FRR) or frame receive error rate (FRER) before interference monitoring begins on a given channel.
Interference Threshold Exceed Time	Time, in seconds, the FRR or FRER exceeds the threshold before interference is reported.
Interference Baseline Time	Time, in seconds, the air monitor should learn the state of the link between the AP and client to create frame retry rate (FRR) and frame receive error rate (FRER) baselines.
RSSI Falloff Wait Time	Time, in seconds, to wait with decreasing RSSI before a deauthorization message is sent to the client. The maximum value is 8 seconds.
Low RSSI Threshold	Minimum RSSI above which deauthorization messages should never be sent.
RSSI Check Frequency	Interval, in seconds, to sample RSSI.

Command History

Version	Modification
ArubaOS 3.0	Base operating system
ArubaOS 3.4	Output parameters displaying load balancing status were removed. You can now view the status of the load balancing feature via the commands show rf dot11a-radio-profile and show rf dot11g-radio-profile.

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show rf spectrum-profile

```
rf spectrum-profile <profile-name>
```

Description

Show a spectrum profile used by the spectrum analysis feature.

Syntax

Parameter	Description
<profile>	Name of a spectrum profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire spectrum profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured spectrum profiles. The **References** column lists the number of other profiles with references to the spectrum profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show rf spectrum-profile

Spectrum profile List
---------------------
Name       References  Profile Status
----       ----------  --------------
spectrum5  1
default-a  2           Predefined (editable)
default-g  2           Predefined (editable)
```

This example displays the configuration settings for the profile **spectrum5**.

```
(host) #show rf spectrum-profile default

Spectrum profile "default"
--------------------------
Parameter                                  Value
---------                                  -----
Spectrum Band                              5ghz-upper
Age Out: WIFI                              600 sec
Age Out: Unknown                           600 sec
Age Out: Microwave                         15 sec
Age Out: Microwave (Inverter type)         15 sec
Age Out: Video Device                      10 sec
Age Out: Audio Device                      10 sec
Age Out: Cordless Phone Fixed Frequency    10 sec
Age Out: Generic Fixed Frequency           10 sec
Age Out: Bluetooth                         25 sec
Age Out: Xbox                              25 sec
Age Out: Cordless Network Frequency Hopper 25 sec
Age Out: Cordless Base Frequency Hopper    25 sec
Age Out: Generic Frequency Hopper          25 sec
```

The output of this command includes the following information:

Parameter	Description
`spectrum-band`	Radio band or portion a radio band monitored by a spectrum monitor radio using that profile.
`Age Out: WIFI`	The number of seconds for which a wifi device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 600 seconds.
`Age Out: Unknown`	The number of seconds for which an unknown device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 600 seconds.
`Age Out: Microwave`	The number of seconds for which a microwave device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 15 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.
`Age Out: Microwave (inverter type)`	The number of seconds for which an inverter microwave must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 15 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.
`Age Out: Video Device`	The number of seconds for which a video device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 10 seconds.
`Age Out: Audio Device`	The number of seconds for which an audio device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 10 seconds.
`Age Out: Cordless Phone Fixed Frequency`	The number of seconds for which a fixed frequency cordless phone must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 10 seconds.
`Age Out: Generic Fixed Frequency`	The number of seconds for which a generic fixed frequency device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 10 seconds.
`Age Out: Bluetooth`	The number of seconds for which a bluetooth device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.
`Age Out: Cordless Network Frequency Hopper`	The number of seconds for which a frequency-hopping cordless network device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds.
`Age Out: Cordless Base Frequency Hopper`	The number of seconds for which a frequency-hopping cordless phone base must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds.
`Age Out: Generic Frequency Hopper`	The number of seconds for which a generic frequency-hopping device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds.
`Age Out: Xbox`	The number of seconds for which an Xbox device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.

Related Commands

`rf spectrum-profile`

Command History

Introduced in ArubaOS 6.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on master and local controllers

show rft profile

```
show rft profile {all|antenna-connectivity|link-quality|raw}
```

Description

Show parameters for the predefined RF test profiles.

Syntax

Parameter	Description
`all`	Show all predefined profiles.
`antenna-connectivity`	Show configured parameters for the predefined **Antenna Connectivity** test profile.
`link-quality`	Show configured parameters for the predefined **Link Quality** test profile.
`raw`	Show configured parameters for the predefined **RAW** test profile.

Usage guidelines

The rft command is used for RF troubleshooting, and should only be used under the supervision of Dell technical support. Issue the **show rft profile** command to view the profiles used for these RF tests.

Example

The following example shows the testing parameters for the predefined link-quality RF test profile.

```
(host) #show rft profile link-quality

Profile LinkQuality: Built-in profile
-------------------------------------
Parameter    Value
---------    -----
Antenna      1 and/or 2
Frame Type   Null Data
Num Packets  100 for each data-rate
Packet Size  1500
Num Retries  0
Data Rate    All rates are tried
```

Related Commands

To view the results of an RF test, use the command show rft result.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show rft result

```
show rft result all|{trans-id <trans-id>}
```

Description

Show the results of an RF test.

Syntax

Parameter	Description
`all`	Show the most recent test result for each test type (antenna-connectivity, link-quality or raw).
`trans-id <trans-id>`	Each RF test is assigned a transaction ID. Include the **trans-id <trans-id>** parameters to show the test result for a specific transaction ID.

Usage guidelines

The rft command is used for RF troubleshooting, and should only be used under the supervision of Dell technical support.

Related Commands

To view a list of the most recent transaction IDs for each test type, use the command show rft transactions.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show rft transactions

```
show rft transactions
```

Description

Show transaction IDs of RF tests.

Syntax

No parameters.

Usage guidelines

The rft command is used for RF troubleshooting, and should only be used under the supervision of Dell technical support. Issue the **show rft transaction** command to view the transaction IDs for the most recent test of each test type.

Example

The following example shows the transaction IDs for the latest RAW, link-quality and antenna-connectivity tests.

```
(host) #show rft transactions

RF troubleshooting transactions
-------------------------------
Profile              Transaction ID
-------              --------------
RAW                  2001
LinkQuality          2101
AntennaConnectivity  1801
```

Related Commands

Use transaction IDs with the command show rft result to view results for individual RF tests.

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show rights

```
show rights [<name-of-a-role>]
```

Description

Displays the list of user roles in the roles table with high level details of role policies. To view role policies of a specific role specify the role name.

Syntax

Parameter	Description
`name-of-a-role`	Enter the role name to view its policy details.

Example

The output of this command shows the list of roles in the role table.

```
(host) # show rights

RoleTable
---------
Name              ACL  Bandwidth                 ACL List                                  Type
----              ---  ---------                 --------                                  ----
ap-role           4    Up: No Limit,Dn: No Limit control/,ap-acl/                          System
authenticated     39   Up: No Limit,Dn: No Limit allowall/,v6-allowall/                    User
default-vpn-role  37   Up: No Limit,Dn: No Limit allowall/,v6-allowall/                    User
guest             3    Up: No Limit,Dn: No Limit http-acl/,https-acl/,dhcp-acl/User
guest-logon       6    Up: No Limit,Dn: No Limit logon-control/,captiveportal/             User
logon             1    Up: No Limit,Dn: No Limit logon-control/,captiveportal/             User
stateful-dot1x    5    Up: No Limit,Dn: No Limit                                         System
voice             38   Up: No Limit,Dn: No Limit sip-acl/,noe-acl/,svp-acl/,vocera-acl/  User
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show roleinfo

```
show roleinfo
```

Description

Displays the role of the controller.

Syntax

No parameters.

Example

The output of this command shows the role of the controller.

```
(host) # show roleinfo

switchrole:master
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show rrm dot11k admission-capacity

```
show rrm dot11k admission-capacity
```

Description

Displays the available admission capacity for voice traffic on an AP.

Syntax

No parameters.

Example

The output of this command shows the available admission capacity for voice traffic on all APs.

```
(host) # show rrm dot11k admission-capacity

802.11K Available Admission Capacity for Voice
----------------------------------------------

Flags: B: Bandwidth based CAC, C: Call-count based CAC
       D: CAC Disabled,        E: CAC Enabled

AP Name    IP Address    Freq Band  Chan  Total  Available  Flags
-------    ----------    ---------  ----  -----  ---------  -----
r-wing-94  10.16.12.247  5 GHz      40    31250  0          EC
r-wing-94  10.16.12.247  2.4 GHz    11    31250  0          EC

Num APs:2
```

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show rrm dot11k ap-channel-report

```
show rrm dot11k ap-channel-report [ap-name <name-of-an-ap> |
   bssid <bssid-of-an-ap> | ip-addr <ip-address-of-an-ap>]
```

Description

Displays the channel information gathered by the AP. You can either specify an ap-name, bssid or ip-address of an AP to see more details.

Syntax

Parameter	Description
`ap-name`	Enter the name of the AP.
`bssid`	Enter the BSSID address of the AP.
`ip-addr`	Enter the IP address of the AP.

Example

The output of this command shows the channel information for r-wing-94:94.

```
(host) # show rrm dot11k ap-channel-report ap-name r-wing-94

802.11K AP Channel Report Details
---------------------------------
Freq Band  Channel List
---------  ------------
2.4 GHz    11,
5 GHz      36, 40, 157, 161, 165,

Num Entries:2
```

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show rrm dot11k beacon-report

```
show rrm dot11k beacon-report
```

Description

Displays the beacon report information sent by a client to its AP.

Syntax

No parameters.

Example

The output of this command shows the beacon report for the client 00:1f:6c:7a:d4:fd.

```
(host) # show rrm dot11k beacon-report station-mac 00:1f:6c:7a:d4:fd

802.11K Beacon Report Details

-------------------------------------------------

Channel     BSSID              Reg Class     Antenna ID      Meas. Mode
----------  -------            ------------  -------------   ----------------
1           00:0b:86:6d:3e:40  0             1               Bcn Table

Num Elements:1
```

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show rrm dot11k neighbor-report

```
show rrm dot11k neighbor-report [ap-name |
   bssid <bssid-of-an-ap> | ip-addr <ip-address-of-an-ap>]
```

Description

Displays the neighbor information for a particular AP. If the AP name or the AP's IP address is specified, the user should specify the ESSID to get the neighbor information. If the ESSID is not specified, the command will display the neighbor information for all the Virtual AP's configured on the AP.

Syntax

Parameter	Description
`ap-name`	Identify the AP for which you want to view information.
`<name-of-an-ap>`	Name of an AP.
`<essid>`	ESSID of the AP. If the ESSID includes spaces, you must enclose it in quotation marks.
`bssid`	Enter the BSSID address of the AP.
`ip-addr`	Enter the IP address of the AP.

Example

The output of this command shows the neighbor information for r-wing-94**.**

```
(host) # show rrm dot11k neighbor-report ap-name r-wing-94

802.11K Neighbor Report Details
-------------------------------

Flags: S: Spectrum Management, Q: QoS, A: APSD, R: Radio Measurement

ESSID         BSSID              Channel  Reachability  Security  Authenticator  Preference  Flags
-----         -----              -------  ------------  --------  -------------  ----------  -----
r-wing-voice  00:0b:86:6d:3e:30  165      Reachable     Same      Same           1           SR
r-wing-voice  00:0b:86:6d:3e:20  1        Reachable     Same      Same           1           SR
r-wing-data   00:0b:86:6d:3e:40  6        Reachable     Same      Same           1           SR
r-wing-data   00:0b:86:6d:4e:41  153      Reachable     Same      Same           1           SR

Num Entries:4
```

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show rrm dot11k transmit-stream-report station-mac

```
show rrm dot11k transmit-stream-report station-mac <mac-addr>
```

Description

This is a diagnostic option for quick verification of received transmit stream measurement reports. Displays the contents of the transmit stream measurement reports received from a client.

Syntax

Parameter	Description
`mac-addr`	MAC address of the client.

Command History

This command is introduced in ArubaOS 5.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show running-config

```
show running-config
```

Description

Displays the current controller configuration, including all pending changes which are yet to be saved.

Syntax

No parameters.

Example

The output of this command shows the running configuration on the controller.

```
(host) # show running-config

version 5.0
enable secret "******"
telnet soe
loginsession timeout 0
hostname "vjoshi-2400"
clock timezone PST -8
location "Building1.floor1"
mms config 0
controller config 986
ip access-list eth validuserethacl
  permit any
!
netservice svc-netbios-dgm udp 138
netservice svc-snmp-trap udp 162
netservice svc-https tcp 443
netservice svc-dhcp udp 67 68 alg dhcp
netservice svc-smb-tcp tcp 445
netservice svc-ike udp 500
netservice svc-l2tp udp 1701
...
   ...
   ...
netservice svc-bootp udp 67 69
netservice svc-snmp udp 161
netservice svc-v6-dhcp udp 546 547
netservice svc-icmp 1
--More-- (q) quit (u) pageup (/) search (n) repeat
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show session-acl-list

```
show session-acl-list
```

Description

Displays the list of configured session ACLs in the controller.

Syntax

No parameters.

Example

The output of this command shows the session ACLs in the controller.

```
(host) # show session-access-list

v6-icmp-acl
allow-diskservices
control
validuser
v6-https-acl
vocera-acl
icmp-acl
v6-dhcp-acl
captiveportal
v6-dns-acl
allowall
test
sip-acl
https-acl
...
   ...
   ...
v6-http-acl
dhcp-acl
http-acl
stateful-dot1x
ap-acl
svp-acl
noe-acl
stateful-kerberos
v6-logon-control
h323-acl
```

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show slots

```
show slots
```

Description

Displays the list of slots in the controller, including the status and card type.

Syntax

No parameters.

Example

The output of this command shows slot details on the controller.

```
(host) # show slots

Slots
------
Slot  Status   Card Type
----  ------   ---------
1     Present  A2400
```

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show snmp community

```
show snmp community
```

Description

Displays the SNMP community string details.

Syntax

No parameters.

Example

The output of this command shows slot details on the controller.

```
(host) # show snmp community

SNMP COMMUNITIES
----------------
COMMUNITY  ACCESS     VERSION
---------  ------     -------
 public    READ_ONLY  V1, V2c
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show snmp inform

```
show snmp inform
```

Description

Displays the length of SNMP inform queue.

Syntax

No parameters.

Example

The output of this command shows slot details on the controller.

```
(host) # show snmp inform stats

Inform queue size is 100

SNMP INFORM STATS
-----------------
HOST  PORT  INFORMS-INQUEUE  OVERFLOW  TOTAL INFORMS
----  ----  ---------------  --------  -------------
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show snmp trap-host

```
show snmp trap-host
```

Description

Displays the configured SNMP trap hosts.

Syntax

No parameters.

Example

The output of this command shows details of a SNMP trap host.

```
(host) # show snmp trap-hosts

SNMP TRAP HOSTS
---------------
HOST          VERSION    SECURITY NAME  PORT   TYPE  TIMEOUT  RETRY
----          -------    -------------  ----   ----  -------  -----
 10.16.14.1    SNMPv2c    public         162    Trap  N/A      N/A
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show snmp trap-list

```
show snmp trap-list
```

Description

Displays the list of SNMP traps.

Syntax

No parameters.

Example

The output of this command shows the list of SNMP traps and the status.

```
(host) # show snmp trap-list

SNMP TRAP LIST
--------------
TRAP-NAME                                 CONFIGURABLE  ENABLE-STATE
---------                                 ------------  ------------
authenticationFailure                     Yes           Enabled
coldStart                                 Yes           Enabled
linkDown                                  Yes           Enabled
linkUp                                    Yes           Enabled
warmStart                                 Yes           Enabled
wlsxAPBssidEntryChanged                   Yes           Enabled
wlsxAPEntryChanged                        Yes           Enabled
wlsxAPImpersonation                       Yes           Enabled
wlsxAPInterferenceCleared                 Yes           Enabled
wlsxAPInterferenceDetected                Yes           Enabled
wlsxAPRadioAttributesChanged              Yes           Enabled
wlsxAPRadioEntryChanged                   Yes           Enabled
wlsxAccessPointIsDown                     Yes           Enabled
wlsxAccessPointIsUp                       Yes           Enabled
wlsxAdhocNetwork                          Yes           Enabled
wlsxAdhocNetworkBridgeDetected            Yes           Enabled
wlsxAdhocNetworkBridgeDetectedAP          Yes           Enabled
...
...
   ...
   ...
wlsxFanOK                                 Yes           Enabled
wlsxFanTrayInserted                       Yes           Enabled
--More-- (q) quit (u) pageup (/) search (n) repeat
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show snmp trap-queue

```
show snmp trap-queue
```

Description

Displays the list of SNMP traps in queue.

Syntax

No parameters.

Example

The output of this command shows the list of SNMP traps sent to host.

```
(host) # show snmp trap-queue

2009-04-29 00:47:40 An AP/AM 00:0b:86:cd:cc:14, radio 2 at Location 00:0b:86:cd:cc:14 and channel 1, det
interfering access point (BSSID 00:e0:fc:18:b5:35, SSID WA1003A). More information can be obtained from
10.16.15.1/screens/wmsi/reports.html?mode=ap&bssid=00:e0:fc:18:b5:35.

2009-04-29 00:49:01 An AP/AM 00:0b:86:cd:cc:14, radio 2 at Location 00:0b:86:cd:cc:14 and channel 10, de
interfering access point (BSSID 00:1a:1e:a8:2d:a0, SSID l-wing-94). More information can be obtained fro
10.16.15.1/screens/wmsi/reports.html?mode=ap&bssid=00:1a:1e:a8:2d:a0.

2009-04-29 00:49:19 An AP/AM 00:0b:86:cd:cc:14, radio 2 at Location 00:0b:86:cd:cc:14 and channel 1, det
interfering access point (BSSID 00:e0:fc:18:b5:35, SSID WA1003A). More information can be obtained from
10.16.15.1/screens/wmsi/reports.html?mode=ap&bssid=00:e0:fc:18:b5:35.

2009-04-29 00:49:20 An AP/AM 00:0b:86:cd:cc:14, radio 2 at Location 00:0b:86:cd:cc:14 and channel 1, det
interfering access point (BSSID 00:0b:86:5c:d8:e0, SSID r-wing-94). More information can be obtained fro
10.16.15.1/screens/wmsi/reports.html?mode=ap&bssid=00:0b:86:5c:d8:e0.

2009-04-29 00:49:31 An AP/AM 00:0b:86:cd:cc:14, radio 1 at Location 00:0b:86:cd:cc:14 and channel 36, de
interfering access point (BSSID 00:1a:1e:8d:dc:20, SSID ). More information can be obtained from http://
screens/wmsi/reports.html?mode=ap&bssid=00:1a:1e:8d:dc:20.

2009-04-29 00:50:15 An AP/AM 00:0b:86:cd:cc:14, radio 2 at Location 00:0b:86:cd:cc:14 and channel 1, det
interfering access point (BSSID 00:e0:fc:18:b5:35, SSID WA1003A). More information can be obtained from
10.16.15.1/screens/wmsi/reports.html?mode=ap&bssid=00:e0:fc:18:b5:35.

--More-- (q) quit (u) pageup (/) search (n) repeat
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show snmp user-table

```
show snmp user-table [user <username> auth-prot [sha | md5] <value> priv-prot [aes | des] <value>]
```

Description

Displays the list of SNMP user profile for a specified username.

Syntax

Parameter	Description
`auth-prot`	Authentication protocol for the user, either HMAC-MD5-98 Digest Authentication Protocol (MD5) or HMAC-SHA-98 Digest Authentication Protocol (SHA), and the password for use with the designated protocol.
`priv-prot`	Privacy protocol for the user, either Advanced Encryption Standard (AES) or CBC-DES Symmetric Encryption Protocol (DES), and the password for use with the designated protocol.

Example

The output of this command shows the list of SNMP traps sent to host.

```
(host) # show snmp user-table

SNMP USER TABLE
---------------
USER    AUTHPROTOCOL  PRIVACYPROTOCOL  FLAGS
----    ------------  ---------------  -----
 Sam    SHA           AES
 fire   SHA           AES
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show spanning-tree

```
show spanning-tree
   <interface [fastethernet slot/port | gigabitethernet slot/port | port-channel id]
   <vlan vlan-id>
```

Description

View the RSTP and PVST+ configuration.

Syntax

Parameter	Description
interface	Enter the keyword **interface** followed by the interface and slot/port or port-channel id: • for Fast Ethernet enter the keyword **fastethernet** followed by the slot/port • For Gigabit Ethernet enter the keyword **gigabitethernet** followed by the slot/port • For Port Channel enter the keyword **port-channel** followed by an id number Range: 0 to 7
vlan	Enter the keyword **vlan** follow by the VLAN ID. Range: 1 to 4094 Default: 1

Example—show spanning-tree

```
(host) # show spanning-tree

Spanning tree instance for vlan 10
Spanning Tree is executing the IEEE compatible Rapid Spanning Tree protocol
Bridge Identifier has priority 32768, address 00:0b:86:f0:20:00
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag is not set, detected flag not set, changes 1
Times: hold 1, topology change 35 hello 2, max age 20, forward delay 15
Timers: hello 0, notification 0
Last topology change: 2 days, 0 hours, 31 mins, 21 secs

Spanning tree instance for vlan 20
Spanning Tree is executing the IEEE compatible Rapid Spanning Tree protocol
Bridge Identifier has priority 32768, address 00:0b:86:f0:20:00
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag is not set, detected flag not set, changes 1
Times: hold 1, topology change 3 hello 2, max age 20, forward delay 15
Timers: hello 0, notification 0
Last topology change: 1 days, 0 hours, 3 mins, 2 secs
```

Example—show spanning-tree vlan

```
(host) # show spanning-tree vlan 2
Spanning Tree is executing the IEEE compatible Rapid Spanning Tree protocol
Bridge Identifier has priority 32768, address 00:0b:86:f0:20:00
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag is not set, detected flag not set, changes 1
Times: hold 1, topology change 35 hello 2, max age 20, forward delay 15
Timers: hello 0, notification 0
Last topology change: 2 days, 0 hours, 31 mins, 21 secs
```

Command History

Release	Modification
6.0	PVST+ added
3.4	Upgraded STP to RSTP with full backward compatibility.

Command Information

Platform	Licensing	Command Mode
All platforms	Base operating system	Enable mode and Configuration mode (config) on master controllers

show spantree

```
show spantree
   <blocking> | <enable> | <forwarding> | <off> | <vlan>
```

Description

View the global RSTP and PVST+ topology.

Syntax

Parameter	Description
blocking	View the spanning tree ports in the Blocking state.
enable	View the spanning tree ports in the Enable state.
forwarding	View the spanning tree ports in the Forwarding state.
off	View the ports with spanning tree disabled
vlan	View the spanning tree instance for the VLAN.

Example

```
(host) # show spantree

Spanning tree instance    vlan 10

Designated Root MAC       00:0b:86:f0:20:00

Designated Root Priority  32768

This bridge is the root

Root Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Bridge MAC                00:0b:86:f0:20:00

Bridge Priority           32768

Configured Max Age 20 sec   Hello Time 2 sec   Forward Delay 15

Interface        Role       State       Cost      Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

eth1/3           Root       Forwarding   2         128.131  P2p Peer

eth1/1           Designated Forwarding   2         128.129  Edge P2p


Rapid Spanning Tree port configuration

--------------------------------------

Port    State       Cost  Prio  PortFast  P-to-P  Role

----    -----       ----  ----  --------  ------  ----

FE 1/3  Discarding  0     128   Disable   Enable  Disabled

FE 1/1  Forwarding  4     128   Disable   Enable  Designated


Spanning tree instance    vlan 20
```

```
Designated Root MAC       00:0b:86:f0:20:20
Designated Root Priority  32768
Root Cost  11
Root Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Bridge MAC                00:0b:86:f0:20:30
Bridge Priority           32768
Configured Max Age 20 sec   Hello Time 2 sec   Forward Delay 15

Rapid Spanning Tree port configuration
--------------------------------------
Port    State       Cost  Prio  PortFast  P-to-P  Role
----    -----       ----  ----  --------  ------  ----
FE 1/3  Discarding  0     128   Disable   Enable  Disabled
FE 1/1  Forwarding  4     128   Disable   Enable  Designated
```

Command History

Release	Modification
6.0	PVST+ added
3.4	Upgraded STP to RSTP with full backward compatibility.

Command Information

Platform	Licensing	Command Mode
All platforms	Base operating system	Enable mode and Configuration mode (config) on master controllers

show ssh

```
show ssh
```

Description

Displays the SSH configuration details.

Syntax

No parameters.

Example

The output of this command shows SSH configuration details.

```
(host) # show ssh

SSH Settings:
-------------
DSA                                 Enabled
Mgmt User Authentication Method     username/password
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show startup-config

```
show startup-config
```

Description

Displays the configuration which will be used the next time the controller is rebooted. It contains all the options last saved using the write memory command. Any unsaved changes are not included.

Syntax

No parameters.

Example

The output of this command shows slot details on the controller.

```
(host) # show startup-config

version 3.4
enable secret "608265290155fb924578f15b12670a75a37045cbdf62fb0d3a"
telnet cli
telnet soe
loginsession timeout 30
hostname "FirstFloor2400"
clock timezone PST -8
location "Building1.floor1"
mms config 0
controller config 22

ip access-list eth validuserethacl
  permit any
!
netservice svc-snmp-trap udp 162
netservice svc-dhcp udp 67 68
netservice svc-smb-tcp tcp 445
netservice svc-https tcp 443
netservice svc-ike udp 500
netservice svc-l2tp udp 1701
netservice svc-syslog udp 514
...
   ...
   ...
netservice svc-msrpc-udp udp 135 139
netservice svc-ssh tcp 22
netservice svc-http-proxy1 tcp 3128
--More-- (q) quit (u) pageup (/) search (n) repeat
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show station-table

```
show station-table [mac <mac_address>]
```

Description

Displays the internal station table entries and also details of a station table entry.

Syntax

No parameters.

Example

The output of this command shows details of an entry in the station table.

```
(host) # show station-table mac 00:1f:6c:7a:d4:fd

Association Table
-----------------
     BSSID              IP        Essid   AP name  Phy  Age
---------------    -----------   -------  -------  ---  ---
00:0b:86:6d:3e:30  10.15.20.252  sam      -        a    01:03:41
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show storage

```
show storage
```

Description

Displays the storage information on the controller.

Syntax

No parameters.

Example

The output of this command shows the storage details on the controller.

```
(host) # show storage
Filesystem               Size      Used Available Use% Mounted on
/dev/root               57.0M     54.6M      2.3M  96% /
none                    70.0M      2.0M     68.0M   3% /tmp
/dev/hda3              149.7M      9.3M    132.6M   7% /flash
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show switch ip

```
show switch ip
```

Description

Displays the IP address of the controller and VLAN ID.

Syntax

No parameters.

Example

The output of this command shows the IP address and VLAN ID of the controller.

```
(host) # show switch ip

Switch IP Address: 10.16.15.1

Switch IP is from Vlan Interface: 1
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show switch software

```
show switch software
```

Description

Displays the details of the software running in the controller.

Syntax

No parameters.

Example

The output of this command shows the details of software running in the controller.

```
(host) # show switch software
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show switches

```
show switches [all | state {complete | incomplete | inprogress | required} | summary ]
```

Description

Displays the details of switches connected to the master controller, including the master controller itself.

Syntax

Parameter	Description
`all`	List of all switches.
`state`	Configuration status of all switches.
`summary`	Status of all switches connected to the master.

Example

The output of this command shows that there is a single local controller connected to the master controller.

```
(host) # show switches all

All Switches
------------
IP Address  Name         Location          Type    Version        Status  Configuration State  Config Sync Time (sec)
----------  ----         --------          ----    -------        ------  -------------------  ----------------------
10.16.12.1  r-wing-94    Building1.floor1  master  6.0.0.0_13782  up      UPDATE SUCCESSFUL    0
192.0.2.12  CorpA2400    Building1.floor1  master  6.0.0.0_13782  up      UPDATE SUCCESSFUL    0
```

Command History

Version	Description
ArubaOS 3.0	Command introduced.
ArubaOS 6.0	The **version** column in the output of this command was expanded to include both the version and the build number for controllers running ArubaOS 6.0 and later releases.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show switchinfo

```
show switchinfo
```

Description

Displays the latest and complete summary of controller details including role, last configuration change, hostname, reason for last reboot.

Syntax

No parameters.

Example

The output of this command lists all controllers connected to the master controller including the master controller.

```
(host) # show switchinfo
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show syscontact

```
show syscontact
```

Description

Displays the contact information for support.

Syntax

No parameters.

Example

The output of this command shows the contact information for technical support.

```
(host) # show syscontact

admin@mycompany.com
```

Command History

This command was available in ArubaOS 3.1

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show syslocation

```
show syslocation
```

Description

Displays the location details of the controller.

Syntax

No parameters.

Example

The output of this command location of the controller.

```
(host) # show syslocation

Building 1, Floor 1
```

Command History

This command was available in ArubaOS 3.1

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show tech-support

```
show tech-support
```

Description

Displays all information about the controller required for technical support purposes.

Syntax

No parameters.

Command History

This command was available in ArubaOS 3.1

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show telnet

```
show telnet
```

Description

Displays the status of telnet access using command line interface (CLI) or serial over ethernet (SOE) to the controller.

Syntax

No parameters.

Example

The output of this command shows the status of CLI and SOE access to the controller.

```
(host) # show telnet

telnet cli is enabled
telnet soe is enabled
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show time-range

```
show time-range [<string>|summary]
```

Description

Displays the list of time range configured in the system and rules affected by the time range.

Syntax

No parameters.

Example

The output of this command shows the absolute time range details

```
(host) # show time-range

Time-Range monitoring, Absolute
-------------------------------
StartDate  Start-time  EndDate    End-time  Applied
---------  ----------  -------    --------  -------
4/29/2009  23:00       4/30/2009  12:00     No
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show tpm cert-info

```
show tpm cert-info
```

Description

Displays the TPM and Factory Certificate information on MIPS controllers (W-3000, W-600 Series Controller).

Syntax

No parameters.

Usage Guidelines

Use this command to verify that TPM and factory certificates are installed as expected. This command should be executed *before* enabling CPSec on MIPS controllers (W-3000, W-600 Series Controller).

Example

In the example below, the TPM and certificates are installed.

```
(host)#show tpm cert-info

subject= /CN=AF0000168::00:0b:86:f0:33:e0
issuer= /DC=com/DC=arubanetworks/DC=ca/CN=DEVICE-CA2
serial=1F023F05000000015087
notBefore=Jan 30 01:38:57 2009 GMT
notAfter=Jan 25 01:38:57 2029 GMT
```

In the example below, the controller is not able to verify the TPM or Factory Certificate information.

```
(host)#show tpm cert-info

Cannot get TPM and Factory Certificate Info
TPM and/or Factory Certificates might be missing.
```

Command History

Release	Modification
ArubaOS 5.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
MIPS controllers (W-3000, W-600 Series Controller)	Base operating system	Enable Mode

show trunk

```
show trunk
```

Description

Displays the list of trunk ports on the controller.

Syntax

No parameters.

Example

The output of this command shows details of a trunk port.

```
(host) # show trunk

Trunk Port Table
-----------------
Port    Vlans Allowed                          Vlans Active                           Native Vlan
----    -------------                          ------------                           -----------
FE2/12  1,613,615-617,632-633,636-640,667-668  1,613,615-617,632-633,636-640,667-668  1
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show uplink

```
crypto-local
show uplink [config|{connection <link_id>}|signal|{stats <link_id}]
```

Description

Displays uplink configuration details on an Aruba 600 series controller.

Syntax

Parameter	Description
`config`	Enter the keyword **config** to display the uplink manager, the default wired priority and default cellular priority
`connection`	Enter the keyword **connection** followed by the uplink ID number to display the connection details.
`signal`	Enter the keyword **signal** to display the cellular uplink signal strength.
`stats`	Enter the keyword **stats** followed by the uplink ID number to display the statistical information on the designated uplink.

Example

The output of this command displays the controller uplink status .

```
(host) ##show uplink
Uplink Manager: Enabled

Uplink Management Table
-----------------------
Id  Uplink Type  Properties  Priority  State         Status
--  -----------  ----------  -------  -----         ------
1   Wired        vlan 1      200      Initializing  Waiting for link
2   Cellular Novatel_U727 100 Standby Ready
```

Command History

Introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
Aruba 600 controllers	Base operating system	Config mode on master and local controllers

show usb

```
crypto-local
   show usb [cellular|ports|test|verbose]
```

Description

Display detailed USB device information.

Syntax

Parameter	Description
`cellular`	Enter the keyword **cellular** to display cellular devices.
`ports`	Enter the keyword **ports** to display detailed TTY port information such as signal strength.
`test`	Enter the keyword **test** to test the USB TTY ports. **NOTE:** Testing an invalid modem port may cause the controller to "hang". To resolve this, unplug and re-plug the modem.
`verbose`	Enter the keyword **verbose** to display detailed USB information including serial number and USB type.

Examples

The USB Device table, in the example below, displays the USB port is in the 'Device Ready' state, meaning that the port has passed the diagnostic test and is ready to send and receive data.

```
(host) (config-cellular new_modem)# show usb
USB Device Table
----------------
Address  Product                Vendor  ProdID  Serial           Type      Profile    State
-------  -------                ------  ------  ------           ----      -------    -----
18       Novatel Wireless CDMA  1410    4100    091087843891000  Cellular  new_modem  Device ready
```

Below is an example of the **show usb verbose** display output (partial).

```
(host) #show usb verbose
...
T: Bus=01 Lev=02 Prnt=02 Port=00 Cnt=01 Dev#= 3 Spd=12 MxCh= 0
D: Ver= 1.10 Cls=00(>ifc ) Sub=00 Prot=00 MxPS=64 #Cfgs= 1
P: Vendor=1410 ProdID=4100 Rev= 0.00
S: Manufacturer=Novatel Wireless Inc.
S: Product=Novatel Wireless CDMA
S: SerialNumber=091087843891000
C:* #Ifs= 5 Cfg#= 1 Atr=a0 MxPwr=500mA
...
```

Command History

Introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
Aruba 600 controllers	Base operating system	Config mode on master and local controllers

show user

```
show user
   authentication-method {[dot1x][mac][stateful-dot1x][vpn][web]}[rows <NUMBER>
   <NUMBER>]
   bssid <A:B:C:D:E:F> rows <NUMBER> <NUMBER>
   essid <STRING> rows <NUMBER> <NUMBER>
   internal rows <NUMBER> <NUMBER>
   ip <A.B.C.D> rows <NUMBER> <NUMBER>
   location b.f.l rows <NUMBER> <NUMBER>
   mac <A:B:C:D:E:F>
   mobile {[bindings][visitors]} [rows <NUMBER> <NUMBER>]
   name <STRING>
   phy-type {[a]|[b]}[rows <NUMBER> <NUMBER>]
   role <STRING> rows <NUMBER> <NUMBER>
   rows <NUMBER> <NUMBER>
```

Description

Displays detailed information about the controller's connection in regards to mobility state and statistics, authentication statistics, VLAN assignment method, AP datapath tunnel info, radius accounting statistics, user name, user-role derivation method, datapath session flow entries, and 802.11 association state and statistics. The **show user** command allows you to filter specific information by parameter.

Syntax

Parameter	Description
`authentication-method`	Authentication method used for the device.
`dot1x`	Number of users to create starting with <ipaddr>.
`mac`	Authentication method.
`stateful-dot1x`	802.1x authentication.
`vpn`	MAC authentication.
`web`	Stateful 802.1x authentication.
`rows <NUMBER> <NUMBER>`	Displays the log output from the specified number of rows from the end of the log and the total number of rows to display.
`bssid <A:B:C:D:E:F>`	BSSID address of the device.
`essid <STRING>`	ESSID of the device. If the ESSID includes spaces, you must enclose it in quotation marks.
`internal rows <NUMBER> <NUMBER>`	Displays the log output from the specified number of rows from the end of the log and the total number of rows to display
`ip <A.B.C.D>`	IP address of user.
`location b.f.l`	Displays the building, floor and location of the device.
`mac <A:B:C:D:E:F>`	MAC address .
`mobile`	Mobile users.
`bindings`	Users that have moved away.
`visitors`	Users that are visitors.
`name <STRING>`	User's name.
`phy-type`	801.11 type
`a`	Matches PHY type a.
`g`	Matches PHY type b or g.
`role <STRING>`	User role such as employee, visitor and so on.
`rows <NUMBER> <NUMBER>`	Displays the output from the specified number of rows from the end of the log and the total number of rows to display
`rows <NUMBER> <NUMBER>`	Displays the output from the specified number of rows from the end of the log and the total number of rows to display

Usage Guidelines

Use the **show user** command to show detailed output (which matches the controller output of user statistics) and includes the entire output of show user-table, mobility state and statics, authentication statistics, VLAN assignment method, AP datapath tunnel information, radius accounting statistics, user-role derivation method, datapath session flow entries and 802.11 association state and statistics.

Example

This example displays users currently in the **employee** role. The output of this command is split into two tables in this document, however it appears in one table in the CLI.

```
(host) (config) show user role employee
Users
-----
    IP              MAC            Name           Role      Age(d:h:m)  Auth    VPN link  AP name
----------      ------------       ------         ----      ----------  ----    --------  -------
192.168.160.1   00:23:6c:80:3d:bc  madisonl       employee  01:05:50    802.1x            1263
10.100.105.100  00:05:4e:45:5e:c8  CORP1NETWORKS  employee  00:02:22    802.1x            wlan-qa-cage
10.100.105.102  00:14:a5:30:c2:7f  pdedhia        employee  01:20:09    802.1x            2198
10.100.105.97   00:1b:77:c4:a2:fa  CORP1NETWORKS  employee  00:02:18    802.1x            2198
10.100.105.109  00:21:5c:02:16:bb  myao           employee  00:05:40    802.1x            1109



Users
-----
Roaming     Essid/Bssid/Phy                          Profile
 -------     ---------------                          -------
Associated  ethersphere-wpa2/00:1a:1e:85:d3:b1/a-HT  default
Associated  ethersphere-wpa2/00:1a:1e:6f:e5:51/a     default
Associated  ethersphere-wpa2/00:1a:1e:87:ef:f1/a     default
Associated  ethersphere-wpa2/00:1a:1e:87:ef:f1/a     default
Associated  ethersphere-wpa2/00:1a:1e:85:c2:11/a-HT  default
```

The output of this command includes the following information:

Column	Description
IP	IP address of the device.
MAC	MAC address of the device.
Name	User's name of the device.
Role	User's assigned role.
Age(d:h:m)	Age of the user's current session, in the format *days:hours:minutes*.
Auth	Authentication method.
VPN link	Shows if the user is connected via a VPN link.
AP name	Name of the AP.
Roaming	Roaming type.
Essid/Bssid/Phy	The Extended Service Set Identifier (ESSID), unique hard-wireless MAC address of the AP (BSSID), and the 802.11 (PHY) type.
Profile	Profile assigned to the device.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes.

show user_session_count (deprecated)

```
show user_session_count
```

Description

Show the number of users using an ESSID for different time intervals.

Syntax

No parameters

Command History

Version	Modification
ArubaOS 3.0	Command introduced
ArubaOS 6.0	Command deprecated

show util_proc

```
show util_proc guest-email counters
```

Description

Show counters for the guest email process.

Syntax

No parameters.

Usage Guidelines

As part of guest provisioning, the guest access email feature allows you to define the SMTP port and server that processes guest provisioning email. This server sends email to the guest or the sponsor when a guest user manually sends email from the Guest Provisioning page, or when a user creates a guest account.

Example

The output of this command shows the numbers of guest emails received, sent and dropped since the controller was last reset.

```
(host) #show util_proc guest-email counters

Guest Email Counters
--------------------
Name            Value
----            -----
Email Received  14
Email Sent      3
Email Dropped   0
```

Related Commands

To configure SMTP servers and server ports for guest email, use the command guest-access-email.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show valid-network-oui-profile

```
show valid-network-oui-profile
```

Description

This command displays the Valid Equipment OUI Profile table

Syntax

No parameters

Usage Guidelines

If you used the valid-networkoui-profile to add a new OUI to the controller, issue the show valid-network-oui-profile command to see a list of current OUIs.

Example

```
(Host) (config) #show valid-network-oui-profile

Valid Equipment OUI profile
---------------------------
Parameter  Value
---------  -----
OUI        00:1A:1E
```

Command History

Release	Modification
ArubaOS 5.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master controllers

show version

```
show version
```

Description

Show the system software version.

Syntax

No parameters.

Example

The output of this command in this example shows that the controller is an W-3200 model running ArubaOS version 6.0.0.

```
(host) #show version
Aruba Operating System Software.
ArubaOS (MODEL: Aruba3200-US), Version 6.0.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2010, Aruba Networks, Inc.
Compiled on 2010-09-19 at 20:59:26 PDT (build 25423) by p4build

ROM: System Bootstrap, Version CPBoot 1.2.0.0 (build 20527)
Built: 2009-01-20 18:56:10
Built by: p4build@re_client_20527

Switch uptime is 1 days 45 minutes 25 seconds
Reboot Cause: User reboot.
Supervisor Card
Processor XLR 508 (revision C4) with 842M bytes of memory.
32K bytes of non-volatile configuration memory.
512M bytes of Supervisor Card System flash (model=CF 512MB).
```

The output of this command includes the following information

Parameter	Description
Model	Controller model type.
Version	Version of ArubaOS software.
ROM	System bootstrap version.
Switch Uptime	Switch uptime (time elapsed since the last controller reset.
Reboot Cause	Reason the controller was last rebooted.
Supervisor Card	Details for the controller's internal supervisor card.

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on local and master controllers

show vlan

```
show vlan <id>
```

Description

This command shows a configured VLAN interface number, description and associated ports.

Syntax

Parameter	Description	Range	Default
<id>	Identification number for the VLAN.	1-4094	1

Usage Guidelines

Issue this command to show the selected VLAN configuration. The **VLAN** column lists the VLAN ID. The **Description** column provides the VLAN name or number and the **Ports** column shows the VLAN's associated ports. The **AAA Profile column** shows if a wired AAA profile has been assigned to a VLAN, enabling role-based access for wired clients connected to an untrusted VLAN or port on the controller.

```
(host) #show vlan

VLAN CONFIGURATION
------------------
VLAN  Description     Ports                          AAA Profile
----  -----------     -----                          -----------
1     Default         GE0/3-7 GE0/9 XG0/10-11 Pc0-7  N/A
10    VLAN0010        GE0/8                          N/A
20    RAP_VLAN                                       N/A
25    VLAN0025        GE0/0                          mac-auth-aaa-prof
30    VLAN0030                                       N/A
56    VLAN0056                                       default
57    VLAN0057                                       default
58    VLAN0058                                       default
128   120_128_to_159  GE0/8                          N/A
129   120_160_to_191  GE0/1 GE0/8                     N/A
201   VLAN0201                                       mac-auth-aaa-prof
```

Related Commands

```
(host) (config) #vlan
(host) (config) #vlan-name
```

Command History

Release	Modification
ArubaOS 3.0	Command available.
ArubaOS 6.0	The output of this command was modified to include the **AAA Profile** column.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master or local controllers

show vlan mapping

```
show vlan mapping
```

Description

This command shows a configured VLAN name, its pool status and the VLAN IDs assigned to the pool.

Syntax

Parameter	Description	Range	Default
<id>	Identification number for the VLAN.	1-4094	1

Usage Guidelines

Issue this command to show the selected VLAN configuration. The **VLAN Name** column displays the name of the VLAN pool. The **Pool Status** column indicates if the pool is enabled or disabled. The **VLAN IDs** column lists the VLANs that are part of the pool. .

```
(host) #show vlan mapping

VLAN Name   Pool Status  VLAN IDs
---------   -----------  --------
mypool      Enabled      65,210
mypool2     Enabled      212,256
```

Related Commands

```
(host) (config) #vlan
(host) (config) #vlan-name
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master or local controllers

show vlan status

```
show vlan status <id>
```

Description

This command shows the current status of all VLANs on the controller.

Syntax

No parameters.

Usage Guidelines

Issue this command to show the status of VLANs on the controller.The **VLAN ID** column displays the VLAN ID name or number. The **IP Address** column provides the VLAN's IP address. The **Adminstate** column indicates if the VLAN is enabled or disabled. The **Operstate** column indicates if the VLAN is currently up and running. The **PortCount** column shows how many ports are associated with the VLAN. The **Nat Inside** column displays whether source Nat is enabled for the VLAN interface. If Nat is enabled, all the traffic passing through this VLAN interface is the source natted to the outgoing interface's IP address..

```
(host) #show vlan status

Vlan Status
-----------
VlanId  IPAddress                       Adminstate  Operstate  PortCount  Nat Inside
------  ---------                       ----------  ---------  ---------  ----------
1       10.168.254.221/255.255.255.252  Enabled     Up         5          Disabled
2       unassigned/unassigned           Enabled     Down       2          Disabled
4       unassigned/unassigned           Enabled     Down       1          Disabled
25      unassigned/unassigned           Enabled     Down       1          Disabled
212     10.168.212.2/255.255.255.0      Enabled     Down       2          Disabled
213     10.168.213.2/255.255.255.0      Enabled     Down       2          Disabled
1170    10.3.132.14/255.255.255.0       Enabled     Up         2          Disabled
```

Related Commands

```
(host) (config) #vlan
(host) (config) #vlan-name
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master or local controllers

show vlan summary

```
show vlan summary
```

Description

This command shows the number of existing VLANs.

Syntax

Parameter	Description
`Number of existing VLANs`	The number of existing VLANs on the controller.

Usage Guidelines

Issue this command to show the number of existing VLANs on the controller.

```
(host) #show vlan summary

Number of existing VLANs               :13
```

Related Commands

```
(host) (config) #vlan
(host) (config) #vlan-name
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on master or local controllers

show vlan-bwcontract-explist

```
show vlan-bwcontract-explist [internal]
```

Description

Show entries in the VLAN bandwidth contracts MAC exception lists.

Syntax

Parameter	Description
`internal`	Include the optional **internal** parameter to display the MAC addresses in the internal, preconfigured VLAN bandwidth contracts MAC exception list.

Example

The following command displays the MAC addresses in the internal MAC exception list.

```
(host) (config) #show vlan-bwcontract-explist internal

VLAN BW Contracts Internal MAC Exception List
---------------------------------------------
MAC address
-----------
01:80:C2:00:00:00
01:00:0C:CC:CC:CD
01:80:C2:00:00:02
01:00:5E:00:82:11
```

Related Commands

Command	Description
vlan-bwcontract-explist	Add or remove MAC addresses from the VLAN bandwidth contract MAC exception list.

Command History

Command introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on master or local controllers

tar

```
tar clean {crash|flash|logs}| crash | flash | logs [tech-support]
```

Description

This command archives a directory.

Syntax

Parameter	Description
`clean`	Removes a tar file
`crash`	Removes crash.tar
`flash`	Removes flash.tar.gz
`logs`	Removes logs.tar
`crash`	Archives the crash directory to crash.tar. A crash directory must exist.
`flash`	Archives and compresses the /flash directory to flash.tar.gz.
`logs`	Archives the logs directory to log.tar. Optionally, technical support information can be included.

Usage Guidelines

This command creates archive files in Unix tar file format.

Example

The following command creates the log.tar file with technical support information:

```
tar logs tech-support
```

Command History

The command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

show voice call-cdrs

```
show voice call-cdrs [bssid <value> | cid <value> | count <number> | detail | essid
<value> | extn <value> | ip <ip-address> | proto {sip | svp | noe | sccp | vocera |
h323} | rtpa | sta <mac-address>]
```

Description

Displays detailed call records of voice client.

Syntax

Parameter	Description
`bssid`	Filter records based on BSSID of voice clients.
`cid`	View the detailed records filtered on the CDR Id.
`count`	Specify the number of records to be displayed by entering a number.
`detail`	Include this parameter to view the following additional information for each call record. • Reason • Codec • Band • Setup Time (sec) • Re-Assoc • Initial-BSSID • Initial-ESSID • Initial-AP Name
`essid`	Filter records based on ESSID of voice clients.
`extn`	View detailed records for a particular extension number.
`ip`	View detailed records of voice client using its IP address.
`proto`	View detailed records filtered on protocol.
`rtpa`	Include this parameter to view the voice call quality reports based on the call quality analysis from the RTP media streams. **NOTE:** This parameter is applicable only if Real Time Call Quality Analysis is enabled on the voice calls.
`sta`	View the detailed records filtered on the MAC address of a voice client.

Example

The output of this command shows detailed call records filtered by SIP protocol and limited to 5 entries.

```
(host) #show voice call-cdrs proto sip count 5 detail

Voice Client(s) CDRs (Detail)
-----------------------------
CDR Id  Client IP    Client Name  ALG  Dir  Called/Calling Party  Status    Dur(sec)  Orig time       R-value  Reason
Codec   Band    Setup Time(sec)  Re-Assoc  Initial-BSSID      Initial-ESSID  Initial-AP Name
------  ---------    -----------  ---  ---  -------------------  ------     --------  ---------        -------  -----
-       -----  ----    ---------------  --------  -------------      -------------  ---------------
NA      10.15.20.74  6202        sip  IC   6203                 CONNECTED  2773      Aug 19 13:39:09  82
G729    GREEN   0               0         00:1a:1e:a8:2d:80  legap          AP-65-2
NA      10.15.20.75  6203        sip  OG   6202                 CONNECTED  2774      Aug 19 13:39:08  65
G729    YELLOW  3               0         NA                 NA             NA
56      10.15.20.74  6202        sip  IC   6203                 SUCC       390       Aug 19 13:20:03  60       Terminated
G729    YELLOW  0               0         00:1a:1e:a8:2d:80  legap          AP-65-2
55      10.15.20.75  6203        sip  OG   6202                 SUCC       390       Aug 19 13:20:03  61       Terminated
G729    YELLOW  3               0         00:1a:1e:a8:2d:80  legap          AP-65-2
54      10.15.20.75  6203        sip  OG   6203                 FAIL       0         Aug 19 13:19:57  NA
NA      NA      0               0         00:1a:1e:a8:2d:80  legap          AP-65-2
Num CDRS:5
```

Command History

Version	Description
ArubaOS 3.3.1	Command introduced.
ArubaOS 6.0	The cid and rtpa parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice call-counters

```
show voice call-counters
```

Description

Displays outgoing, incoming and terminated call counter details. The total calls equals the sum of the calls originated and terminated. It also equals the sum of the active, success, failed, blocked, aborted, and forwarded calls.

Syntax

No parameters.

Example

The output of this command shows call counter statitics.

```
(host) # show voice call-counters

System Wide Voice Call Counters
-------------------------------
Total  Call Originated  Call Terminated  Active  Success  Failed  Blocked  Aborted  Forwarded
-----  ---------------  ---------------  ------  -------  ------  -------  -------  ---------
31     16               15               0       29       0       0        2        0
```

Command History

Version	Description
ArubaOS 3.3.1	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice call-density

```
show voice call-density [bssid <value> | essid <value> | extn <value> |
   ip <ip-address> | proto <protocol>]
```

Description

Displays call density report for voice calls.

Syntax

Parameter	Description
`bssid`	Filter records based on BSSID of voice clients.
`essid`	Filter records based on ESSID of voice clients.
`extn`	Filter records based on the extension of a voice client.
`ip <ip-address>`	Filter records based on the IP address of an AP.
`proto <protocol>`	Filter records based on a VOIP protocol. Supported values are: • SIP • SVP • NOE • SCCP • VOCERA • H323

Example

The output of this command shows call density report for extension 3015.

```
(host) # show voice call-density extn 3015

VoIP Call Density Report for Client '3015'
------------------------------------------
Sample Time      Orig  Term  Active  Succ  Fail  Blocked  Aborted  Forwarded  R-Value
-----------      ----  ----  ------  ----  ----  -------  -------  ---------  -------
Jan 31 16:01:42  0     0     0       0     0     0        0        0          NA
Jan 31 16:00:00  0     0     0       0     0     0        0        0          NA
Jan 31 15:50:00  0     0     0       0     0     0        0        0          NA
Jan 31 15:40:00  0     0     0       0     0     0        0        0          NA
Jan 31 15:30:00  0     0     0       0     0     0        0        0          NA
Jan 31 15:20:00  0     1     1       1     0     0        0        0          73.000000
Jan 31 15:10:00  0     2     3       2     0     0        0        0          84.000000
Jan 31 15:00:00  0     1     1       0     0     0        1        0          80.000000
Jan 31 14:50:00  0     0     0       0     0     0        0        0          NA
Jan 31 14:40:00  0     0     0       0     0     0        0        0          NA
Jan 31 14:30:00  0     0     0       0     0     0        0        0          NA
Jan 31 14:20:00  0     0     0       0     0     0        0        0          NA
Jan 31 14:10:00  0     0     0       0     0     0        0        0          NA
...
...
...
```

Command History

Version	Description
ArubaOS 3.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice call-perf

```
show voice call-perf [bssid <value> | essid <value> | extn <value> |
   ip <ip_address> | proto <value>
```

Description

Displays the performance of voice calls of all clients connected to the controller. You can filter the report based on BSSID, ESSID, extension, IP address or the VOIP protocol type.

Syntax

Parameter	Description
`bssid`	Filter records based on BSSID of voice clients.
`essid`	Filter records based on ESSID of voice clients.
`extn`	Filter records based on the extension of a voice client.
`ip <ip-address>`	Filter records based on the IP address of an AP.
`proto <protocol>`	Filter records based on a VOIP protocol. Supported values are: • SIP • NOE • SCCP • VOCERA • H323

Example

The output of this command shows call performance report for extension 3015.

```
(host) # show voice call-perf extn 3015
VoIP Call Performance Report for Client '3015'
-----------------------------------------------
Sample Time      Delay(ms)  AP-Switch Delay(ms)  Jitter  Packet Loss  R-Value  MOS   Band
-----------      ---------  -------------------  ------  -----------  -------  ---   ----
Jan 31 15:54:46  0.00       0.00                 0.000   0.00         0.00     NA    NA
Jan 31 15:50:00  0.00       0.00                 0.000   0.00         0.00     NA    NA
Jan 31 15:40:00  0.00       0.00                 0.000   0.00         0.00     NA    NA
Jan 31 15:30:00  0.00       0.00                 0.000   0.00         0.00     NA    NA
Jan 31 15:20:00  108.24     0.00                 7.793   8.81         73.00    3.60  YELLOW
Jan 31 15:10:00  106.67     0.00                 12.500  4.44         84.00    4.02  GREEN
Jan 31 15:00:00  0.00       0.00                 0.000   0.00         0.00     NA    NA
Jan 31 14:50:00  0.00       0.00                 0.000   0.00         0.00     NA    NA
Jan 31 14:40:00  0.00       0.00                 0.000   0.00         0.00     NA    NA
Jan 31 14:30:00  0.00       0.00                 0.000   0.00         0.00     NA    NA
...
...
...
```

Command History

Version	Description
ArubaOS 3.3.1	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice call-quality

```
show voice call-quality [bssid <value> | essid <value> | extn <value> |
ip <ip_address> | proto <value> | rtpa | sta <mac-address>
```

Description

Displays voice call quality for each call over a period of time.

Syntax

Parameter	Description
`bssid`	Filter records based on BSSID of voice clients.
`essid`	Filter records based on ESSID of voice clients.
`extn`	Filter records based on the extension of a voice client.
`ip <ip-address>`	Filter records based on the IP address of a voice client.
`proto <protocol>`	Filter records based on a VOIP protocol. Supported values are: • SIP • NOE • SCCP • VOCERA • H323
`rtpa`	Include this parameter to view the voice call quality reports based on the call quality analysis from the RTP media streams. **NOTE:** This parameter is applicable only if Real Time Call Quality Analysis is enabled on the voice calls.
`sta`	Filter records based on the MAC address of a voice client.

Example

The output of this command shows call quality report for calls made by extension 3015.

```
(host) # show voice call-quality extn 3015

Voice Client(s) Call Quality Reports
------------------------------------
Client(IP)    Client(MAC)       Client(Name)  ALG   Orig Time       Direction  Called/Calling Party  Duration  Codec
Delay    Jitter  Pkt Loss  R-Value  Band    BSSID              ESSID  AP Name
----------    -----------       ------------  ---   ---------       ---------  --------------------  --------  ----
-  -----    ------  --------  -------  ----    -----              -----  -------

10.100.1.10  00:11:22:33:bc:bd  3015          sccp  Jan 31 15:10:44  IC         3042                 141
108.241  7.793   8.809     73       YELLOW  00:0b:86:5c:d6:08  nkrtp  voice-a
10.100.1.10  00:11:22:33:bc:bd  3015          sccp  Jan 31 15:07:48  IC         3042                 119
115.333  13.000  8.480     78       YELLOW  00:0b:86:5c:d6:08  nkrtp  voice-a
10.100.1.10  00:11:22:33:bc:bd  3015          sccp  Jan 31 15:01:22  IC         3042                 35
98.000   12.000  0.391     90       GREEN   00:0b:86:5c:d6:08  nkrtp  voice-a
10.100.1.10  00:11:22:33:bc:bd  3015          sccp  Jan 31 14:58:58  IC         3042                 100       G711
103.528  6.056   4.622     80       GREEN   00:0b:86:5c:d6:08  nkrtp  voice-a
Num Records:4
```

Command History

Version	Description
ArubaOS 3.3.1	Command introduced.
ArubaOS 6.0	The rtpa and sta parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice call-stats

```
show voice call-stats [bssid <value> | cip <client-ip-address> | essid <value> |
   extn <value> | ip <ip_address> | proto <value> | sta <value>]
```

Description

Displays voice call statistics for each client.

Syntax

Parameter	Description
`bssid`	Filter records based on BSSID of a voice client.
`cip`	Filter records based on a client's IP address.
`essid`	Filter records based on ESSID of a voice client.
`extn`	Filter records based on the extension of a voice client.
`ip <ip-address>`	Filter records based on the IP address of an AP.
`proto <protocol>`	Filter records based on a VOIP protocol. Supported values are: • SIP • NOE • SCCP • VOCERA • H323
`sta`	Filter records based on the MAC address of a voice client.

Example

The output of this command shows call quality report for calls made by extension 6210.

```
(host) # show voice call-stats

Voice Client(s) Call Statistics
-------------------------------
Client IP     Client MAC        Client Name  ALG   Originated  Terminated  Active  Failed  Success  Blocked  Aborted
Duration             R-Value            Band
---------     ----------        -----------  ---   ----------  ----------  ------  ------  -------  -------  -------
--------             -------           ----
10.15.86.248  00:1f:6c:7a:d4:fd  6005         sccp  3           2           0       0       5        0        0
20489.0/2.0/4173.0   93.00/79.00/89.00  GREEN
10.15.86.247  00:1f:6c:7a:d5:f8  6002         sccp  2           3           0       0       4        0        1
57709.0/2.0/11616.8  93.00/71.00/87.00  GREEN
Num Clients:2
```

Command History

Version	Description
ArubaOS 3.3.1	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice client-status

```
show voice client-status [active-only | bssid | essid <value> |
   extn <value> | ip <ip_address> | proto <value> | sta <value>]
```

Description

Displays list of voice clients and their status. You can also view details of a specifc voice client.

Syntax

Parameter	Description
`active-only`	Filter records based on active voice clients
`bssid`	Filter records based on BSSID of a voice client.
`essid`	Filter records based on ESSID of a voice client.
`extn`	Filter records based on the extension of a voice client.
`ip <ip-address>`	Filter records based on the IP address of a voice client.
`proto <protocol>`	Filter records based on a VOIP protocol. Supported values are: • SIP • SVP • NOE • SCCP • VOCERA • H323
`sta`	Filter records based on the MAC address of a voice client.

Example

The output of this command shows details about all the voice clients on a controller.

```
(host) #show voice client-status

Voice Client(s) Status
----------------------
Client(IP)  Client(MAC)     Client Name  ALG  Server(IP)  Registration State  Call Status  BSSID
ESSID         AP Name   Flags
----------  -----------     -----------  ---  ----------  ------------------  -----------  -----
-----         -------   -----
10.15.22.32  00:1f:6c:7a:d5:30  6001         sccp  10.15.32.20  REGISTERED          Idle
00:1a:1e:80:bb:10  keepwalking1  AP-L-125
Num Clients:1
Flags: V - Visitor, W - Wired, R - Remote
```

Command History

Version	Description
ArubaOS 3.3.1	Command introduced.
ArubaOS 6.0	The sta parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice configurations

```
show voice configurations
```

Description

Displays the details of the voice related configurations on your controller.

Syntax

No parameters.

Example

The output of this command shows details about all voice configurations on a controller.

```
(host) #show voice configurations
Voice firewall policies
-----------------------
Policy                      Action
------                      ------
Stateful SIP Processing     Enabled
Broadcast-filter ARP        Disabled

SSID Profiles
-------------
Profile Name            WMM       WMM-UAPSD  TSPEC Min Inactivity(msec)  ...  EDCA STA prof  EDCA AP prof  Strict SVP
------------            ---       ---------  --------------------------  ...  -------------  ------------  ----------
default                 Enabled   Enabled    100000                      ...  default        default       Disabled
qa-ma-vocera            Enabled   Enabled    0                                default        default       Disabled

AP Group Profiles
-----------------
Profile Name   VoIP CAC Profile
------------   ----------------
default        default
local          default

Virtual AP Group Profiles
-------------------------
Profile Name           802.11K Profile  HA Discovery on-assoc.  Drop Broadcast/Multicast  Broadcast ARP to Unicast
------------           ---------------  ----------------------  ------------------------  ----------------------
abcd                   default          Disabled                Disabled                  Disabled

VoIP Call Admission Control Profiles
------------------------------------
Profile Name  VoIP CAC
------------  ---------
default       Disabled

802.11K Profiles
----------------
Profile Name  Advertise 802.11K Capability
------------  ----------------------------
default       Disabled

SIP settings
------------
Parameter         Value
---------         -----
Session Timer     Disabled
Session Expiry    300 sec
Dialplan Profile  N/A

Voice rtcp-inactivity:disable
Voice sip-midcall-req-timeout:disable
```

Command History

Version	Description
ArubaOS 6.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice dialplan-profile

```
show voice dialplan-profile <profile>
```

Description

Displays list of SIP voice dialplan. You can also specify a dialplan to view configuration.

Syntax

No parameter.

Example

The output of this command shows list of all dialplans and the configuration of long distance dialplan.

```
(host) (config) #show voice dialplan-profile
Dialplan Profile List
---------------------
Name          References  Profile Status
----          ----------  --------------
default       1
extenstion    0
local         0
longDistance  0
Total:4

(host) (config) #show voice dialplan-profile longDistance
Dialplan Profile "longDistance"
-------------------------------
Parameter  Value
---------  -----
dialplan   102 +1XXXXXXXXXX 9%e
```

Command History

Version	Description
ArubaOS 5.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice logging

```
show voice logging
```

Description

Displays the MAC address of the voice client that has logging enabled.

Syntax

No parameters.

Example

The output of this command shows the MAC address of the voice client that has logging enabled.

```
(host) #show voice logging

VoIP Logging
------------
Parameter                        Value
---------                        -----
Client's MAC Address for Logging  11:22:33:44:55:67
```

Command History

Version	Description
ArubaOS 6.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice msg-stats

```
show voice msg-stats
   [sccp { bssid <value> | cip <client-ip-address> | essid <value> | ip <ip_address> |
   sta <client-MAC-address> } ]
   [sip { bssid <value> | cip <client-ip-address> | essid <value> | ip <ip_address> |
   sta <client-MAC-address> } ]
```

Description

Displays voice message counters for each call using either the SCCP or SIP protocol.

Syntax

Parameter	Description
bssid	Filter records based on BSSID of a voice client.
cip	Filter records based on a client's IP address.
essid	Filter records based on ESSID of a voice client.
ip	Filter records based on the IP address of an AP.
sta	Filter records based on the MAC address of a voice client.

Example

The output of this command shows voice message statistics for essid sam filtered on SCCP protocol.

```
(host) # show voice msg-stats sccp essid sam

SCCP Voice Client(s) Msg Statistics
-----------------------------------
Client Name  Client IP     AP Name    BSSID             ESSID  Register  Register Ack  Unregister  Unregister Ack
Keepalive  Keepalive Ack  OpenRecvChannel  OpenRecvChannel Ack  StartMedia  CloseRecvChannel  StopMedia  OffHook
OnHook  Ringing  Connected  Busy  Hold  Transfer  Invalid
-----------  ---------     -------    -----              -----  --------  ------------  ----------  --------------  -
--------  -------------  ---------------  ------------------  ----------  ----------------  ---------  -------  ----
--  -------  ---------  ----  ----  --------  -------
6005        10.15.86.248  AP-70-862  00:0b:86:6d:3e:30 sam 43       5           1          2            5950
6185          7             4                  6          7              6         5       17     2       8
0     0     0         0
6002        10.15.86.247  AP-70-862  00:0b:86:6d:3e:30  sam 39       6           2          2            5936
6048          4             4                  4          7              6         4       18     3       4
0     0     0         0
Num Clients:2
```

Command History

Version	Description
ArubaOS 3.3.1	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice real-time-analysis

```
show voice real-time-analysis [sta <client MAC address>]
```

Description

Displays the call quality parameters based on the call quality analysis on the RTP media streams for voice calls.

Syntax

Parameter	Description
sta	View the detailed Real Time Call Quality analysis report for a voice client based on the MAC address. You can also view the average call quality values for all the clients without passing the MAC address.

Example

The output of this command shows the detailed call quality parameters based on the RTP media stream for a specific voice client.

```
#show voice real-time-analysis sta 00:1f:6c:7a:d5:30

Real-Time Analysis detail report
--------------------------------
Time              Jitter(U)(msec)  Pkt-loss(U)(%)  Delay(U)(usec)  rvalue(U)  Jitter(D)(msec)  Pkt-loss(D)(%)
Delay(D)(usec)  rvalue(D)
---------------  ---------------  --------------  --------------  ---------  ---------------  --------------  ------
--------  ---------
Aug 17 11:55:18   71.000          0.000           0.000           93.360     0.000            0.000           0.000
NA
Aug 17 11:55:13   76.000          0.000           0.000           93.360     0.000            0.000           0.000
NA
Aug 17 11:55:08   69.000          0.000           0.000           93.360     0.000            0.000           0.000
NA
Aug 17 11:55:03   71.000          0.000           0.000           93.360     0.000            0.000           0.000
NA
...
...
...
```

Command History

Version	Description
ArubaOS 6.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice real-time-analysis-config

```
show voice real-time-analysis-config
```

Description

Displays the status of Real Time Call Quality Analysis configuration.

Syntax

No parameters.

Example

The output of this command shows the status of Real Time Call Quality Analysis configuration on a controller.

```
(host) #show voice real-time-config

Configure Real-Time Analysis
----------------------------
Parameter                         Value
---------                         -----
Real-Time Analysis of voice calls  Enabled
```

Command History

Version	Description
ArubaOS 6.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice rtcp-inactivity

```
show voice rtcp-inactivity
```

Description

Displays the status of RTCP protocol.

Syntax

No parameters.

Example

The output of this command shows the status of RTCP protocol.

```
(host) #show voice rtcp-inactivity

Voice rtcp-inactivity:disable
```

Command History

Version	Description
ArubaOS 3.3.1	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice sip

```
show voice sip
```

Description

Displays the SIP settings on the controller.

Syntax

No parameters.

Example

The output of this command shows the SIP settings on a controller.

```
(host) #show voice sip

SIP settings
------------
Parameter         Value
---------         -----
Session Timer     Enabled
Session Expiry    300 sec
Dialplan Profile  N/A
```

Command History

Version	Description
ArubaOS 6.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice sip-midcall-req-timeout

```
show voice sip-midcall-req-timeout
```

Description

Displays the status of the SIP mid-call request timeout configuration on the controller.

Syntax

No parameters.

Example

The output of this command shows the status of the SIP mid-call request timeout configuration on a controller.

```
(host) #show voice sip-midcall-req-timeout

Voice sip-midcall-req-timeout:disable
```

Command History

Version	Description
ArubaOS 6.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice statistics

```
show voice statistics [ cac | sip-dialplan-hits | tspec-enforcement ]
```

Description

Displays the CAC, UDP SIP dial plan hits, and TSPEC enforced voice statistics.

Syntax

Parameter	Description
`cac`	Displays the dropped SIP Invites and SIP Status Code for both server and the client side. **Note**: This filter supports only the SIP protocol and will work only if CAC is enabled for the parameters.
`sip-dialplan-hits`	Displays the statistics of SIP dialplan hits.
`tspec-enforcement`	Displays the statistics of the number of TSPEC requests accepted, rejected, or denied.

Example

The output of this command shows statistics for TSPEC enforced calls.

```
(host) # show voice statistics tspec-enforcement

TSPEC Enforcement statistics
----------------------------
Name                                        Value
----                                        -----
TSPEC ADDTS Request                         16
TSPEC accepted                              16
TSPEC denied due to CAC                     0
TSPEC enforcement timer events              2
Calls established within enforcement period 0
TSPEC deleted after enforcement period      1
```

Command History

Version	Description
ArubaOS 3.3.1	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show voice trace

```
show voice trace
   [ sccp {count <value> | ip <ip_address> | mac <mac_address>} ]
   [ sip {count <value> | ip <ip_address> | mac <mac_address>} ]
```

Description

Displays the signalling message trace details for all clients.

Syntax

Parameter	Description
count	View the specified number of the latest SIP or SCCP voice client messages. Specify an integer value.
ip	Specify the IP address of a client to display its SIP or SCCP voice client messages.
mac	Specify the IP address of a client to display its SIP or SCCP voice client messages.

Example

The output of this command shows signalling message trace.

```
(host) #show voice trace sip count 4

SIP Voice Client(s) Message Trace
---------------------------------
ALG  Client Name  Client(MAC)       Client(IP)   Event Time      Direction        Msg
BSSID
---  -----------  -----------       ----------   ----------      ---------        ---                -
----
SIP  6201        00:24:7d:99:49:01  10.15.20.59  Aug 17 10:21:22  Server-To-Client  200_OK
00:1a:1e:a8:2d:80
SIP  6201        00:24:7d:99:49:01  10.15.20.59  Aug 17 10:21:22  Client-To-Server  REGISTER
00:1a:1e:a8:2d:80
SIP  6201       00:24:7d:99:49:01  10.15.20.59  Aug 17 10:21:22  Server-To-Client  4XX_REQUEST_FAILURE
00:1a:1e:a8:2d:80
SIP  6201        00:24:7d:99:49:01  10.15.20.59  Aug 17 10:21:22  Client-To-Server  REGISTER
00:1a:1e:a8:2d:80
Num of Rows:4
```

Command History

Version	Description
ArubaOS 3.3.1	Command introduced.
ArubaOS 6.0	The trace output included the BSSID parameter.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on master or local controllers

show vpdn l2tp configuration

```
show vpdn l2tp configuration
```

Description

Displays the VPN L2TP tunnel configuration.

Syntax

No parameters.

Example

The output of this command shows the L2TP tunnel configuration.

```
(host) # show vpdn l2tp configuration

Enabled
Hello timeout: 30 seconds
DNS primary server: 10.16.15.1
DNS secondary server: 10.16.14.1
WINS primary server: 0.0.0.0
WINS secondary server: 0.0.0.0
PPP client authentication methods:
         PAP
IP LOCAL POOLS:
         vpnpool: 10.16.15.150 - 10.16.15.160
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show vpdn pptp configuration

```
show vpdn pptp configuration
```

Description

Displays the PPTP configuration on the controller.

Syntax

No parameters.

Example

The output of this command shows the L2TP tunnel configuration.

```
(host) # show vpdn pptp configuration

Enabled
Hello timeout: 30 seconds
DNS primary server: 10.15.1.1
DNS secondary server: 10.15.1.200
WINS primary server: 0.0.0.0
WINS secondary server: 0.0.0.0
PPP client authentication methods:
         MSCHAP
         MSCHAPv2
MPPE Configuration
         128 bit encryption enabled
IP LOCAL POOLS
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show vpdn pptp local pool

```
show vpdn pptp local pool <pool_name>
```

Description

Displays the IP address pool for VPN users using Point-to-Point Tunneling Protocol.

Syntax

No parameters.

Example

The output of this command shows the all IP address pools for VPN users.

```
(host) # show vpdn pptp local pool

IP addresses used in pool localgroup
0 IPs used - 11 IPs free - 11 IPs configured
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show via

```
show via
   version
   websessions
```

Description

Displays VIA version and web session details.

Syntax

Parameter	Description	Range	Default
`version`	Displays the version of VIA client available on the controller.	—	—
`websessions`	Displays the list of users connected to the VIA controller using the VIA client.	—	—

Example

The following example displays the version of VIA client available on the controller.

```
(host) # show via version
(host) (VIA Client WLAN Profile "example") #show  via version
Default VIA Installer:
----------------------
<aruba>
        <via>
                <platform>win32</platform>
                <version>1.0.0.23373</version>
        </via>
</aruba>
```

Command History

This command was available in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show vpn-dialer

```
show vpn-dialer <dialer_name>
```

Description

Displays the VPN dialer configuration for users using VPN dialers.

Syntax

No parameters.

Example

The output of this command shows the VPN dialer configuration for remoteUsers.

```
(host) # show vpn-dialer remoteUser

remoteUser
----------
Attribute           Value
---------           -----
PPTP                disabled
L2TP                enabled
DNETCLEAR           disabled
WIREDNOWIFI         disabled
PAP                 enabled
CHAP                enabled
MSCHAP              enabled
MSCHAPV2            enabled
CACHE-SECURID       disabled
IKESECS             4000
IKEENC              3DES
IKEGROUP            ONE
IKEHASH             MD5
IKEAUTH             PRE-SHARE
IKEPASSWD           ********
IPSECSECS           4000
IPSECGROUP          GROUP1
IPSECENC            ESP-3DES
IPSECAUTH           ESP-MD5-HMAC
SECURID_NEWPINMODE  disabled
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show vrrp

```
show vrrp <vrid>
```

Description

Displays the list of all VRRP configuration on the controller. To view a specific VRRP configuration, specify the VRID number.

Syntax

No parameters.

Example

The output of this command shows the VRRP configuration enabled in one of the floors of the building.

```
(host) # show vrrp


Virtual Router 2:
    Description Floor-1 Settings
    Admin State DOWN, VR State INIT
    IP Address 10.15.1.10, MAC Address 00:00:5e:00:01:02, vlan 1
    Priority 2, Advertisement 10 sec, Preemption Enable
    Auth type PASSWORD, Auth data: 123456
    tracking type is master-up-time, duration 500 minutes, value 3
    tracking type is vrrp-master-state, vrid 10, value 1
    tracking type is vlan, vlanid 1, subtract value 3
    tracking type is interface, fastethernet 1/1, subtract value 3
    tracked priority 2
```

Command History

Version	Modification
ArubaOS 1.0	Command introduced
ArubaOS 3.3	The **tracking interface** and **tracking vlan** parameters were introduced.
ArubaOS 3.3.2	The **add** option was removed from the **tracking interface** and **tracking vlan** parameters.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show web-server

```
show web-server
```

Description

Displays the configuration of the controller's web server.

Syntax

No parameters.

Example

The output of this command shows the web-server configuration.

```
(host) # show web-server

Web Server Configuration
------------------------
Parameter                                    Value
---------                                    -----
Cipher Suite Strength                        high
SSL/TLS Protocol Config                      sslv3 tlsv1
Switch Certificate                           default
Captive Portal Certificate                   default
Management user's WebUI access method        username/password
User session timeout <30-3600> (seconds)     900
Maximum supported concurrent clients <25-400>  25
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on master or local controllers

show wlan dot11k-profile

```
show wlan dot11k-profile [<profile>]
```

Description

Show a list of all 802.11k profiles, or display detailed configuration information for a specific 802.11k profile.

Syntax

Parameter	Description
<profile>	Name of an 802.11k profile.

Usage Guidelines

Issue this command without the <profile> parameter to display the 802.11k profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured 802.11k profiles. The **References** column lists the number of other profiles with references to the 802.11k profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host) #show wlan dot11k-profile

802.11K Profile List
--------------------
Name         References  Profile Status
----         ----------  --------------
default      8
11kprofile2  1

Total: 2
```

The following example shows configuration settings defined for the profile **default**.

```
(host) #show wlan dot11k-profile default

802.11K Profile "default"
-------------------------
Parameter                                                    Value
---------                                                    -----
Advertise 802.11K Capability                                 Disabled
Forcefully disassociate on-hook voice clients                Disabled
Measurement Mode for Beacon Reports                          beacon-table
Configure specific channel for Beacon Requests               Disabled
Channel requested for Beacon Reports in 'A' band             36
Channel requested for Beacon Reports in 'BG' band            1
Time duration between consecutive Beacon Requests            60 sec
Time duration between consecutive Link Measurement Requests  60 sec
Time duration between consecutive Transmit Stream Measurement Requests  90 sec
```

The output of this command includes the following data columns:

Parameter	Description
Advertise 802.11K Capability	Shows if the profile has enabled or disabled the 802.11K feature.
Forcefully disassociate on-hook voice clients	If enabled, the AP may forcefully disassociate clients that reach the maximum CAC peak capacity or call handoff reservation.

Parameter	Description
Measurement Mode for Beacon Reports	Shows the profile's beacon measurement mode: • **active**: In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. • **beacon-table**: In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. This is the default beacon measurement mode. • **passive**: In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show wlan edca-parameters-profile

```
show wlan edca-parameters-profile ap|station [<profile>]
```

Description

Display an Enhanced Distributed Channel Access (EDCA) profile for APs or for clients (stations). EDCA profiles are specific either to APs or clients.

Syntax

Parameter	Description
<profile>	Name of a EDCA Parameters profile.

Usage Guidelines

Issue this command without the <profile> parameter to display a EDCA Parameters profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three EDCA Parameters profiles configured for stations. The **References** column lists the number of other profiles with references to the EDCA Parameters profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host) #show wlan edca-parameters-profile station
EDCA Parameters profile (Station) List
---------------------------------
Name           References  Profile Status
----           ----------  --------------
station-corp1  3
station-corp2  1
testprofile    0

Total:3
```

The following example shows configuration settings defined for the profile **station-corp1**.

```
(host) #show wlan edca-parameters-profile ap station-corp1
EDCA Parameters
---------------
AC           ECWmin  ECWmax  AIFSN  TXOP  ACM
--           ------  ------  -----  ----  ---
Best-effort  4       6       3      0     0
Background   4       10      7      0     0
Video        3       4       1      94    0
Voice        2       3       1      47    0
```

The output of this command includes the following data columns:

Parameter	Description
AC	Name of an Access channel queue (**Best-effort**, **Background**, **Video** or **Voice**).
ECWmin	The exponential (n) value of the minimum contention window size, as expressed by 2^n-1. A value of 4 computes to 2^4-1 = 15.
ECWmax	The exponential (n) value of the maximum contention window size, as expressed by 2^n-1. A value of 4 computes to 2^4-1 = 15.

Parameter	Description
AIFSN	Arbitrary inter-frame space number.
TXOP	Transmission opportunity, in units of 32 microseconds.
ACM	If this column displays a 1, the profile has enabled mandatory admission control. If this column displays a 0, the profile has disabled this feature.

Command History

This command was introduced in ArubaOS 3.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system, but the controller must have the PEFNG license in order to configure EDCA Parameter Profiles.	Enable and Config mode on master or local controllers

show wlan ht-ssid-profile

```
show wlan ht-ssid-profile [<profile>]
```

Description

Show a list of all High-throughput SSID profiles, or display detailed configuration information for a specific High-throughput SSID profile.

Syntax

Parameter	Description
<profile>	Name of a High-throughput SSID profile.

Usage Guidelines

Issue this command without the <profile> parameter to display the entire High-throughput SSID profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured High-throughput SSID profiles. The **References** column lists the number of other profiles with references to the High-throughput SSID profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host) #show wlan ht-ssid-profile
High-throughput SSID profile List
---------------------------------
Name         References  Profile Status
----         ----------  --------------
HT-profile1  16
default2     1

Total:2
```

The following example shows configuration settings defined for the profile **default2**.

```
(host) #show wlan ht-ssid-profile default
High-throughput SSID profile "default"
--------------------------------------
Parameter                           Value
---------                           -----
High throughput enable (SSID)       Enabled
40 MHz channel usage                Enabled
MPDU Aggregation                    Enabled
Max transmitted A-MPDU size         65535 bytes
Max received A-MPDU size            65535 bytes
Min MPDU start spacing              0 usec
Supported MCS set                   0-15
Short guard interval in 40 MHz mode Enabled
Legacy stations                     Allowed
Allow weak encryption               Disabled
```

The output of this command includes the following data columns:

Parameter	Description
`High throughput enable (SSID)`	Shows if the profile enables or disables high-throughput (802.11n) features.
`40 MHz channel usage`	Shows if the profile enables or disables the use of 40 MHz channels.

Parameter	Description
`MPDU Aggregation`	Shows if the profile enables or disables MAC protocol data unit (MPDU) aggregation.
`Max transmitted A-MPDU size`	Configured maximum size of a transmitted aggregate MPDU, in bytes.
`Max received A-MPDU size`	Configured maximum size of a received aggregate MPDU, in bytes.
`Min MPDU start spacing`	Configured minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds.
`Supported MCS set`	Displays a list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20MHz vs. 40MHz) and the number of spatial streams used by the mesh node.
`Short guard interval in 40 MHz mode`	Shows if the profile enables or disables use of short (400ns) guard interval in 40 MHz mode.
`Legacy stations`	Allow or disallow associations from legacy (non-HT) stations. By default, this parameter is enabled (legacy stations are allowed).
`Allow weak encryption`	Shows if the profile enables or disables the use of TKIP or WEP for unicast traffic.

Command History

Version	Description
ArubaOS 3.3	Command introduced
ArubaOS 3.3.1	The **legacy-stations** parameter was introduced
ArubaOS 3.3.2	De-aggregation of MAC Service Data Units (A-MSDUs) was introduced

Command Information

Platforms	Licensing	Command Mode
All platforms but operates with IEEE 802.11n compliant devices only	Base operating system	Config mode on master controllers

show wlan ssid-profile

```
show wlan ssid-profile [<profile>]
```

Description

Show a list of all SSID profiles, or display detailed configuration information for a specific SSID profile.

Syntax

Parameter	Description
<profile>	Name of an SSID profile.

Usage Guidelines

Issue this command without the <profile> parameter to display the entire SSID profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has six configured SSID profiles. The **References** column lists the number of other profiles with references to the SSIDs profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host) #show wlan ssid-profile
SSID Profile List
-----------------
Name                              References  Profile Status
----                              ----------  --------------
coltrane-ssid-profile             1
corp1-ssid-profile                3
Remote                            1
Secure-Profile2                   0
test-ssid-profile                 1
wizardtest-ssid-profile           1

Total:6
```

The following example shows configuration settings defined for the SSID Profile **Remote**.

```
(host) #show wlan ssid-profile remote

SSID Profile "Remote"
---------------------
Parameter                                       Value
---------                                       -----
SSID enable                                     Enabled
ESSID                                           remoteoffice
Encryption                                      opensystem
DTIM Interval                                   1 beacon periods
802.11a Basic Rates                             6 12 24
802.11a Transmit Rates                          6 9 12 18 24 36 48 54
802.11g Basic Rates                             1 2
802.11g Transmit Rates                          1 2 5 6 9 11 12 18 24 36 48 54
Station Ageout Time                             1000 sec
Max Transmit Attempts                           8
RTS Threshold                                   2333 bytes
Short Preamble                                  Enabled
Max Associations                                64
Wireless Multimedia (WMM)                       Disabled
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave  Enabled
WMM TSPEC Min Inactivity Interval               0 msec
DSCP mapping for WMM voice AC                   56
DSCP mapping for WMM video AC                   40
DSCP mapping for WMM best-effort AC             24
DSCP mapping for WMM background AC              8
902il Compatibility Mode                        Disabled
Hide SSID                                       Disabled
Deny_Broadcast Probes                           Disabled
Local Probe Response                            Enabled
Disable Probe Retry                             Enabled
Battery Boost                                   Disabled
WEP Key 1                                       N/A
WEP Key 2                                       N/A
WEP Key 3                                       N/A
WEP Key 4                                       N/A
WEP Transmit Key Index                          1
WPA Hexkey                                      N/A
WPA Passphrase                                  N/A
Maximum Transmit Failures                       0
EDCA Parameters Station profile                 N/A
EDCA Parameters AP profile                      N/A
BC/MC Rate Optimization                         Disabled
Strict Spectralink Voice Protocol (SVP)         Disabled
High-throughput SSID Profile                    default
```

The output of this command includes the following data columns:

Parameter	Description
SSID	Shows of the profile has enabled or disabled this SSID
ESSID	Name that uniquely identifies a wireless network. If the ESSID includes spaces, you must enclose it in quotation marks.
Encryption	The layer-2 authentication and encryption type used on this ESSID.
DTIM Interval	The interval, in milliseconds, between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon.
802.11a Basic Rates	List of supported 802.11a rates, in Mbps, that are advertised in beacon frames and probe responses.
802.11a Transmit Rates	Set of 802.11a rates at which the AP is allowed to send data.

Parameter	Description
802.11g Basic Rates	List of supported 802.11b/g rates, in Mbps, that are advertised in beacon frames and probe responses.
802.11g Transmit Rates	Set of 802.11b/g rates at which the AP is allowed to send data.
Station Ageout Time	Time, in seconds, that a client is allowed to remain idle before being aged out.
Max Transmit Attempts	Maximum transmission failures allowed before the client gives up.
RTS Threshold	Wireless clients transmitting frames larger than this defined threshold must issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS).
Short Preamble	Shows if the profile enables or disables short preamble for 802.11b/g radios
Max Associations	Maximum number of wireless clients for the AP
Wireless Multimedia (WMM)	Shows if the profile enables or disables WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF)
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave	Shows if the profile enables or disables Wireless Multimedia (WMM) UAPSD powersave.
WMM TSPEC Min Inactivity Interval	Specifies the minimum inactivity time-out threshold of WMM traffic.
DSCP mapping for WMM voice AC	DSCP value used to map WMM voice traffic.
DSCP mapping for WMM video AC	DSCP value used to map WMM video traffic.
DSCP mapping for WMM best-effort AC	DSCP value used to map WMM best-effort traffic.
DSCP mapping for WMM background AC	DSCP value used to map WMM background traffic.
902il Compatibility Mode	(For clients using NTT DoCoMo 902iL phones only) When enabled, the controller does not drop packets from the client if a small or old initialization vector value is received.
Hide SSID	Shows if the profile enables or disables hiding of the SSID name in beacon frames.
Deny_Broadcast Probes	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID
Local Probe Response	Shows if the profile enables or disables local probe response on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients' probe requests. If this option is disabled, then the controller sends the 802.11 probe responses
Disable Probe Retry	Shows if the profile enables or disables battery MAC level retries for probe response frames.
Battery Boost	If enabled, this feature converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval.
WEP Key 1	Displays the Static WEP key associated with this key index.
WEP Key 2	Displays the Static WEP key associated with this key index.
WEP Key 3	Displays the Static WEP key associated with this key index.
WEP Key 4	Displays the Static WEP key associated with this key index.
WEP Transmit Key Index	Show the key index that specifies which static WEP key is to be used

Parameter	Description
WPA Hexkey	WPA pre-shared key (PSK).
WPA Passphrase	WPA passphrase used to generate a pre-shared key (PSK).
Maximum Transmit Failures	Maximum transmission failures allowed before the client gives up.
EDCA Parameters Station profile	Name of the enhanced distributed channel access (EDCA) Station profile that applies to this SSID.
EDCA Parameters AP profile	Name of the enhanced distributed channel access (EDCA) AP profile that applies to this SSID.
BC/MC Rate Optimization	Shows if the profile enables or disables scanning of all active stations currently associated to an AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate
Strict Spectralink Voice Protocol (SVP)	Shows if the profile enables or disables strict Spectralink Voice Protocol (SVP).
High-throughput SSID Profile	Name of the high-throughput SSID profile associated with this SSID profile.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show wlan traffic-management-profile

```
show wlan traffic-management-profile [<profile>]
```

Description

Show a list of all traffic management profiles, or display detailed configuration information for a specific traffic management profile.

Syntax

Parameter	Description
<profile>	Name of a Traffic Management profile.

Usage Guidelines

Issue this command without the <profile> parameter to display the entire Traffic Management profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured Traffic Management profiles. The **References** column lists the number of other profiles with references to the Traffic Management profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host) #show wlan
Traffic management profile List
-------------------------------
Name     References  Profile Status
----     ----------  --------------
mgmt1     1
mgmt3     0
mgmt4     2

Total: 3
```

The following example shows configuration settings defined for the profile **mgmt1**.

```
(host) #show wlan traffic-management-profile mgmt1
Traffic management profile "default"
------------------------------------
Parameter                   Value
---------                   -----
Proportional BW Allocation  N/A
Report interval             5 min
Station Shaping Policy      default-access
```

The output of this command includes the following data columns:

Parameter	Description
`Proportional BW Allocation`	Minimum bandwidth, as a percentage of available bandwidth, allocated to an SSID when there is congestion on the wireless network. An SSID can use all available bandwidth if no other SSIDs are active.
`Report interval`	Number of minutes between bandwidth usage reports.

Parameter	Description
`Station Shaping Policy`	Shows which of three possible Station Shaping policies is configured on the profile. • **default-access**: Traffic shaping is disabled, and client performance is dependent on MAC contention resolution. This is the default traffic shaping setting. • **fair-access**: Each client gets the same airtime, regardless of client capability and capacity. This option is useful in environments like a training facility or exam hall, where a mix of 802.11a/g, 802.11g and 802.11n clients need equal to network resources, regardless of their capabilities. The **bw-alloc** parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network.You must set traffic shaping to f**air-access** to use this bandwidth allocation value for an individual virtual AP. • **preferred-access**: High-throughput (802.11n) clients do not get penalized because of slower 802.11a/g or 802.11b transmissions that take more air time due to lower rates. Similarly, faster 802.11a/g clients get more access than 802.11b clients.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show wlan virtual-ap

```
show wlan virtual-ap [<profile>]
```

Description

Show a list of all Virtual AP profiles, or display detailed configuration information for a specific Virtual AP profile.

Syntax

Parameter	Description
<profile>	Name of a Virtual AP profile

Usage Guidelines

Issue this command without the <profile> parameter to display the entire Virtual AP profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has six configured Virtual AP profiles. The **References** column lists the number of other profiles with references to the Virtual AP profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host) #show wlan virtual-ap

Virtual AP profile List
-----------------------
Name                            References  Profile Status
----                            ----------  --------------
coltrane-vap-profile            1
default                         2
MegTest                         1
Remote     1
test-vap-profile                1
wizardtest-vap-profile          1

Total: 6
```

The following example shows configuration settings defined for the profile **wizardtest-vap-profile**.

```
(host) #show wlan virtual-ap test-vap-profile
Virtual AP profile "wizardtest-vap-profile"
---------------------------
Parameter                                   Value
---------                                   -----
Virtual AP enable                           Enabled
Allowed band                                all
AAA Profile                                 default
802.11K Profile                             default
SSID Profile                                default
VLAN                                        N/A
Forward mode                                tunnel
Deny time range                             N/A
Mobile IP                                   Enabled
HA Discovery on-association                 Disabled
DoS Prevention                              Enabled
Station Blacklisting                        Enabled
Blacklist Time                              3600 sec
Dynamic Multicast Optimization (DMO)             Disabled
Dynamic Multicast Optimization (DMO) Threshold  6
Authentication Failure Blacklist Time       3600 sec
Fast Roaming                                Disabled
Strict Compliance                           Enabled
VLAN Mobility                               Disabled
Remote-AP Operation                         standard
Drop Broadcast and Multicast                Disabled
Convert Broadcast ARP requests to unicast   Enabled
Band Steering                               Disabled
```

The output of this command includes the following data columns:

Parameter	Description
`Virtual AP enable`	Shows if the profile enables or disables the virtual AP.
`Allowed band`	The band(s) on which to use the virtual AP: • **a**—802.11a band only (5 GHz) • **g**—802.11b/g band only (2.4 GHz) • **all**—both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz)
`AAA Profile`	Name of the AAA profile associated with this virtual AP.
`802.11K Profile`	Name of an 802.11k profile associated with this virtual AP.
`SSID Profile`	Name of an SSID profile associated with this virtual AP.
`VLAN`	The VLAN(s) into which users are placed in order to obtain an IP address.
`Forward mode`	Forwarding mode defined on the profile: • tunnel mode • bridge mode • **split-tunnel mode** • decrypt-tunnel mode The forwarding mode controls whether data is tunneled to the controller using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the controller, and Internet access remains local). When an AP is configured to use the decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to to the controller, which then applies firewall policies to the user traffic. When the controller sends traffic to a client, the controller sends 802.3 traffic through the GRE tunnel to the AP, which then converts it to encrypted 802.11 and forwards to the client.
`Deny time range`	Time range for which the AP will deny access.

Parameter	Description
Mobile IP	Shows if the profile has enabled or disabled IP mobility.
HA Discovery on-association	If enabled, all clients of a virtual-ap will received mobility service on association.
DoS Prevention	If enabled, APs ignore deauthentication frames from clients. This prevents a successful deauth attack from being carried out against the AP. This does not affect third-party APs.
Station Blacklisting	Shows if the profile has enabled or disabled detection of denial of service (DoS) attacks, such as ping or SYN floods, that are not spoofed deauth attacks.
Dynamic Multicast Optimization (DMO)	If enabled DMO techniques will be used to reliably transmit video data.
Dynamic Multicast Optimization (DMO) Threshold	Maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops
Blacklist Time	Number of seconds that a client is quarantined from the network after being blacklisted.
Authentication Failure Blacklist Time	Time, in seconds, a client is blocked if it fails repeated authentication. An authentication failure blacklist time of 0 blocks failed users indefinitely.
Multi Association	If enabled, this feature allows a station to be associated to multiple APs. If this feature is disabled, when a station moves to new AP it will be de authorized by the AP to which it was previously connected, deleting station context and flushing key caching information
Fast Roaming	Shows if the AP has enabled or disabled fast roaming.
Strict Compliance	If enabled, the AP denies client association requests if the AP and client station have no common rates defined. Some legacy client stations which are not fully 802.11-compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.
VLAN Mobility	Shows if the AP has enabled or disabled VLAN (Layer-2) mobility.
Remote-AP Operation	Shows how the virtual AP operates on a remote AP: • **always**: Permanently enables the virtual AP. • **backup**: Enables the virtual AP if the remote AP cannot connect to the controller. • **persistent**: Permanently enables the virtual AP after the remote AP initially connects to the controller. • **standard**: Enables the virtual AP when the remote AP connects to the controller.
Drop Broadcast and Multicast	If enabled, the virtual AP will filter out broadcast and multicast traffic in the air.
Convert Broadcast ARP requests to unicast	If enabled, all broadcast ARP requests are converted to unicast and sent directly to the client
Band Steering	If enabled, ARM's band steering feature encourages dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4GHz band for single band clients like VoIP phones.

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show wlan voip-cac-profile

```
show wlan voip-cac-profile [<profile>]
```

Description

Show a list of all VoIP Call Admission Control profiles, or display detailed configuration information for a specific VoIP Call Admission Control profile.

Syntax

Parameter	Description
<profile>	Name of a VoIP Call Admission Control profile

Usage Guidelines

Issue this command without the <profile> parameter to display the entire VoIP Call Admission Control profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured VoIP Call Admission Control profiles. The **References** column lists the number of other profiles with references to the VoIP Call Admission Control profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host) #show wlan voip-cac-profile
VoIP Call Admission Control profile List
----------------------------------------
Name        References  Profile Status
----        ----------  --------------
corp-voip   6
kgtest      0
QAlab-voip  1

Total:3
```

The following example shows configuration settings defined for the profile **QAlab-voip**.

```
(host) #show wlan voip-cac-profile
VoIP Call Admission Control profile "QAlab-voip"
------------------------------------------------
Parameter                                       Value
---------                                       -----
VoIP Call Admission Control                     Disabled
VoIP Bandwidth based CAC                        Disabled
VoIP Call Capacity                              10
VoIP Bandwidth Capacity (kbps)                  2000
VoIP Call Handoff Reservation                   20 %
VoIP Send SIP 100 Trying                        Enabled
VoIP Disconnect Extra Call                      Disabled
VOIP TSPEC Enforcement                          Disabled
VOIP TSPEC Enforcement Period                   1 sec
VoIP Drop SIP Invite and send status code (client)  486
VoIP Drop SIP Invite and send status code (server)  486
```

The output of this command includes the following data columns:

Parameter	Description
`VoIP Call Admission Control`	Shows if the profile enables or disables WiFi VoIP Call Admission Control features.
`VoIP Bandwidth based CAC`	Shows the desired call admission control (CAC) Mechanism: • Disable - CAC is based on Call Counts • Enable - CAC should be based on Bandwidth.
`VoIP Call Capacity`	Number of simultaneous calls that can be handled by one radio.
`VoIP Bandwidth Capacity (kbps)`	The maximum bandwidth that can be handled by one radio, in kbps.
`VoIP Call Handoff Reservation`	Percentage of call capacity reserved for mobile VoIP clients on call.
`VoIP Send SIP 100 Trying`	Shows if the profile enables or disables sending of *SIP 100 - trying* messages to a call originator to indicate that the call is proceeding.
`VoIP Disconnect Extra Call`	If enabled, the controller disconnects calls that exceed the high capacity threshold by sending a deauthentication frame.
`VOIP TSPEC Enforcement`	Shows if the profile enables or disables validation of TSPEC requests for CAC.
`VOIP TSPEC Enforcement Period`	Maximum time for the station to start the call after the TSPEC request
`VoIP Drop SIP Invite and send status code (client)`	Display the status code sent back to the client if the profile is configured to drop a SIP Invite: • **480**: Temporary Unavailable • **486**: Busy Here • **503**: Ser vice Unavailable • **none**: Don't send SIP status code
`VoIP Drop SIP Invite and send status code (server)`	Display the status code sent back to the server if the profile is configured to drop a SIP Invite: • **480**: Temporary Unavailable • **486**: Busy Here • **503**: Ser vice Unavailable • **none**: Don't send SIP status code

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on master or local controllers.

show wms ap

```
show wms ap {<bssid>}|{list [mon-mac <mon-mac> bssid <bssid>}|{stats [mon-mac <mon-mac>
bssid <bssid>}
```

Description

Display information for APs currently monitored by the ArubaOS Wireless Management System (WMS).

Syntax

Parameter	Description
<bssid>	Enter the AP's BSSID number in hexadecimal format (XX:XX:XX:XX:XX:XX).
list	Show the AP Tree Table for all APs.
mon-mac <mon-mac>	Show the AP Tree Table for an AP with the specified MAC address.
bssid <bssid>	Show the AP Tree Table for an AP with the specified BSSID.
stats	Show the AP Tree Table for all APs.
mon-mac <mon-mac>	Show the AP Tree Table for an AP with the specified MAC address.
bssid <bssid>	Show the AP Tree Table for an AP with the specified BSSID.

Usage Guidelines

The WMS feature periodically sends statistics that it has collected for APs and Probes to the WMS process. When WMS receives an event message from an AM, it will save the event information along with the BSSID of the AP that generated the event in the WMS database. When WMS receives statistics from the AM, it updates its state, and the database.

Examples

The command **show wms ap <bssid>** displays a list of AP MAC addresses and the BSSIDs seen by each AP.

```
(host)# show wms ap 00:1a:1e:88:01:e0

AP Info
-------
BSSID              SSID   Channel  Type     RAP_Type  Status  Match MAC          Ageout  HT-Type   HT-Sec-Chan
-----              ----   -------  ----     --------  ------  ---------          ------  -------   -----------
00:1a:1e:88:01:e0  sw-ad  11       soft-ap  valid     up      00:00:00:00:00:00  -1

Probe Info
----------
MAC                IP           Name         Type     Status  AP Type
---                --           ----         ----     ------  -------
00:1a:1e:88:02:80  10.3.129.94  ad-ap125-13  soft-ap  up      125
00:1a:1e:88:01:e0  10.3.129.96  mp3          soft-ap  up      125
00:1a:1e:81:c6:00  10.3.129.99  ad-ap124-11  soft-ap  down    124
00:0b:86:8a:15:20  10.3.129.93  sap61-1-6    soft-ap  down    65
```

The output of this command includes the following information:

Column	Description
BSSID	Basic Service Set Identifier for the AP. This is usually the AP's MAC address.
SSID	The Service Set Identifier that identifies a wireless network.
Channel	Channel used by the AP's radio.

Column	Description
Type	A WMS AP type can be one of the following: • **soft-ap**: an Dell Access Point (AP). • **air-monitor**: An Dell Air Monitor (AM).
RAP_Type	Indicates one of the following Rogue AP types: • Valid (not a rogue AP) • Interfering • Rogue • Suspected Rogue • Disabled Rogue • Unclassified • Known Interfering
Status	If **up**, the AP is active. If **down** (or no information is shown) the AP is inactive.
Match MAC	MAC address of a wired device that helped identify the AP as a rogue. If the AP has not been identified as a rogue, this column will display the MAC address 00:00:00:00:00:00.
Ageout	An ageout time is the time, in minutes, that the client must remain unseen by any probes before it is eliminated from the database. If this column displays a **-1**, the client has not yet aged out. Any other number indicates the number of minutes since the client has passed its ageout interval.
HT-type	The type of high-throughput traffic sent by the AP: • **HT-20mhz**: The AP radio uses a single 20 mHz channel • **HT-40mhz:** The AP radio uses a 40 MHz channel pair comprised of two adjacent 20 MHz channels.
HT-Sec-Chan	Secondary channel used for 40 MHz high-throughput transmissions.
MAC	MAC address of a probe that can see the specified AP.
IP	IP address of a probe that can see the specified AP.
Name	Name of the probe.
Type	Displays the probe type: A WMS probe can be one of the following: • **soft-ap**: an Dell Access Point (AP). • **air-monitor**: An Dell Air Monitor (AM).
Status	If **up**, the AP is active. If **down** (or no information is shown) the AP is inactive.
AP Type	AP model type.

The example below shows received and transmitted data statistics for each BSSID seen by a monitoring AP.

```
(host)# show wms ap stats
AP Stats Table
---------------
Monitor-MAC        BSSID              RSSI  TxPkt    RxPkt   TxByte     RxByte    HTRates-Rx
-----------        -----              ----  -----    -----   ------     ------    ----------
00:0b:86:c1:af:20  00:0b:86:9a:f2:00  12    1575675  65      173239998  9340      0
00:0b:86:c1:af:20  00:0b:86:9a:f2:08  12    1560559  0       162297938  0         0
00:0b:86:c1:be:56  00:0b:86:9b:e5:60  12    1683013  4188    184400159  257583    0
00:0b:86:c1:be:56  00:0b:86:9b:e5:68  12    1580152  105     164216336  1470      0
00:0b:86:c2:0a:98  00:0b:86:a0:a9:80  48    1608023  40596   166962148  568386    0
00:0b:86:c2:1c:08  00:0b:86:a1:c0:80  42    1587097  26236   164904668  453196    0
00:0b:86:c2:1c:38  00:0b:86:a1:c3:80  42    1573040  20511   174536514  654024    0
00:0b:86:c2:3e:a9  00:0b:86:a3:ea:90  48    1588204  34179   165017293  897431    0
00:0b:86:c4:0f:3c  00:0b:86:c0:f3:d0  48    1571202  14258   174338376  351148    0
00:0b:86:c4:4d:06  00:0b:86:c4:d0:70  48    1598423  56198   182267018  3805826   0
00:1a:1e:c0:88:82  00:1a:1e:88:88:30  18    1717310  247532  394461405  14998234  8
00:1a:1e:c0:88:82  00:1a:1e:88:88:20  18    1092023  114722  242006054  2442917   10
00:1a:1e:c0:88:88  00:1a:1e:88:88:90  36    1783226  485620  460219125  27781583  16
```

The output of this command includes the following information:

Column	Description
Monitor-MAC	MAC address of an AP.
BSSID	Basic Service Set Identifier of a station.
RSSI	Received Signal Strength Indicator for the station, as seen by the AP.
txPkt	Number of transmitted packets.
RxPkt	Number of received packets.
TxByte	Number of transmitted bytes.
RxByte	Number of received bytes.
HTRates-Rx	Number of bytes received at high-throughput rates.

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show wms channel

```
show wms channel stats
```

Description

Display per-channel statistics for monitored APs.

Syntax

No parameters.

Example

This example shows per-channel statistics for monitored APs.

```
(host) #show wms channel stats

 Channel Stats Table
---------------------
Monitor-MAC        Channel  NumAP  NumSta  TotalPkt  TotalByte   Noise
-----------        -------  -----  ------  --------  ---------   -----
00:0b:86:c1:af:20  1        1      0       5228276   613640650   97
00:0b:86:c1:af:20  6        1      0       1355      168764      0
00:0b:86:c1:af:20  11       8      0       5880      1040338     0
00:0b:86:c1:af:20  36       0      0       2         28          0
00:0b:86:c1:af:20  40       0      0       2         112         0
00:0b:86:c1:af:20  44       0      0       50        903         0
00:0b:86:c1:af:20  48       0      0       23        544         0
00:0b:86:c1:af:20  149      1      0       27094     557579      0
00:0b:86:c1:af:20  153      3      0       4648662   544817261   99
00:0b:86:c1:af:20  165      1      0       1655      200349      0
00:0b:86:c1:be:56  1        43     4       14446324  1959058619  0
00:0b:86:c1:be:56  6        8      1       14168505  1955474600  96
00:0b:86:c1:be:56  11       72     1       180553    23987119    0
00:0b:86:c1:be:56  36       53     0       14716     1022825     0
00:0b:86:c1:be:56  40       8      0       3033      501568      0
00:0b:86:c1:be:56  44       3      0       1453      217596      0
00:0b:86:c1:be:56  48       4      0       5330      1067660     0
00:0b:86:c1:be:56  149      0      0       609279    72205247    105
00:0b:86:c1:be:56  153      1      0       7615369   779579648   0
00:0b:86:c1:be:56  165      1      0       4238      486121      0
00:0b:86:c2:0a:98  40       4      0       4247      434512      0
00:0b:86:c2:0a:98  48       5      0       4052      420436      0
00:0b:86:c2:0a:98  149      4      0       6548323   732910481   104
00:0b:86:c2:1c:08  40       3      0       4613      478188      0
00:0b:86:c2:1c:08  48       4      0       6235436   658263321   103
00:0b:86:c2:1c:08  149      5      0       18904     803078      0
```

The output of this command includes the following information:

Column	Description
`Monitor-MAC`	MAC address of an AP.
`Channel`	802.11 radio channel.
`NumAP`	Number of other APs seen on the specified channel.
`NumSta`	Number stations seen on the specified channel.
`TotalPkt`	Number of received packets.
`TotalByte`	Number of received bytes.
`Noise`	Current noise level.

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show wms client

```
show wms client <mac>|{list}|{probe <mac>}|{stats [mon-mac <mon-mac> mac <mac>]}
```

Description

Display a list of client information for the clients that can be seen by monitoring APs.

Syntax

Parameter	Description
<mac>	Show statistics for a client with the specified MAC address, including the BSSID of the AP to which that client is currently associated, and the MAC addresses of other monitoring APs that can see that client.
list	Show statistics for all monitored clients.
probe <mac>	Specify a client's MAC address to show the BSSIDs of all probes that can see that client.
stats	Show the STA stats table, which displays data for all clients seen by each monitoring AP.
mon-mac <mon-mac> mac <mac>	Enter a monitoring AP's MAC address (<mon-mac>) and the MAC address of a client (<mac>) to show data for traffic received from and sent to a specific client as seen by a specific AP.

Example

The AP Info table in the example below shows that the client is associated to an AP with the BSSID **00:0b:86:cd:86:a0**. The Probe info table shows the MAC addresses of three other APs that can see the client.

```
(host) #show wms client 00:0e:35:29:9b:28

STA Info
--------
MAC               Type   Status  Ageout
---               ----   ------  ------
00:0e:35:29:9b:28 valid  up      -1


AP Info
-------
BSSID             SSID    Channel  Type     RAP_Type  Status  Match MAC          Ageout
-----             ----    -------  ----     --------  ------  ---------          ------
00:0b:86:cd:86:a0 MySSiD  11       soft-ap  valid     up      00:00:00:00:00:00  -1


Probe Info
----------
MAC               IP            Name  Type     Status  Name    AP Type
---               --            ----  ----     ------  ----    -------
00:0b:86:a2:2b:50 192.168.2.10  0     soft-ap  up      LeftAP  61
00:0b:86:ad:94:40 192.168.2.5   0     soft-ap  up      1.1.1   61
00:0b:86:cd:86:a0 192.168.2.4   0     soft-ap  up      CEO     70
```

The output of this command includes the following information:

Column	Description
MAC	MAC address of the client
Type	Station type (**valid**, interfering, or **disabled rogue client**)
Status	If **up**, the client is active. If **down** (or no information is shown) the client is inactive.

Column	Description
ageout	An ageout time is the time, in minutes, that the client must remain unseen by any probes before it is eliminated from the database. If this column displays a **-1**, the client has not yet aged out. Any other number indicates the number of minutes since the client has passed its ageout interval.
BSSID	BSSID of the AP to which the client is associated.
SSID	Extended service set identifier (ESSID) of the BSSID.
RAP_Type	Indicates one of the following Rogue AP types: • Valid (not a rogue AP) • Interfering • Rogue • Disabled Rogue • Suspected Rogue • Unclassified • Known Interfering
Status	If **up**, the AP is active. If **down** (or no information is shown) the AP is inactive.
Match MAC	MAC address of a wired device that helped identify the AP as a rogue. If the AP has not been identified as a rogue, this column will display the MAC address 00:00:00:00:00:00.
Ageout	An ageout time is the time, in minutes, that the client must remain unseen by any probes before it is eliminated from the database. If this column displays a **-1**, the client has not yet aged out. Any other number indicates the number of minutes since the client has passed its ageout interval.
MAC	MAC address of a WMS probe.
IP	IP address of a WMS probe.
Type	A WMS AP type can be one of the following: • **soft-ap**: an Dell Access Point (AP). • **air-monitor**: An Dell Air Monitor (AM).
Status	If **up**, the probe is active. If **down** (or no information is shown) the probe is inactive.
Name	Name of the probe. If a name has not been defined for the probe, this column may display a zero (0).
AP type	Model type of the probe.

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show wms counters

```
show wms counters [debug|event]
```

Description

Show WMS event and debug counters. If you omit the optional **debug** and **events** parameters, the **show wms counters** command will display wms debug and events counters in a single table.

Syntax

Parameter	Description
debug	Show show debug counters only
events	Show events counters only. If you omit the debug and events parameters, the show wms counters will display debug and events counters in a single table.

Usage Guidelines

This command displays counters for database entries, messages and data structures. The counters displayed will vary for each controller; if the controller does not have an entry for a particular counter type, it will not appear in the output of this command

Example

This example shows part of the output of the command **show wms counters**.

```
(host) #show wms counters

Counters
--------
Name                        Value
----                        -----
DB Reads                    288268
DB Writes                   350870
Probe Table DB Reads        2477
Probe Table DB Writes       952
AP Table DB Reads           143992
AP Table DB Writes          138867
STA Table DB Reads          40404
STA Table DB Writes         99687
Probe STA Table DB Reads    101352
Probe STA Table DB Writes   117566
Probe Register              2476
Probe State Update          37077
Set RAP Type                42552
Set RAP Type Conf Level     152
...
```

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show wms general

```
show wms general
```

Description

Display general statistics for the wms configuration.

Syntax

No parameters.

Example

This example shows per-channel statistics for all monitored APs.

```
(host) #show wms general

General Attributes
------------------
Key                           Value
---                           -----
poll-interval                 176000
poll-retries                  2
ap-ageout-interval            30
sta-ageout-interval           30
learn-ap                      enable
persistent-known-interfering  disable
propagate-wired-macs          enable
stat-update                   enable
collect-stats                 enable
classification-server-ip      10.4.151.19
rtls-port                     0
wms-on-master                 disable
use-db                        disable
calc-poll-interval            176000
Switch IP                     10.6.2.253
Is Master                     enable
```

The output of this command includes the following information:

Column	Description
`poll-interval`	Interval, in milliseconds, for communication between the controller and AMs. The controller contacts the AM at this interval to download AP to station associations, update policy configuration changes, and download AP and station statistics.
`poll-retries`	Maximum number of failed polling attempts before the polled AM is considered to be down.
`ap-ageout-interval`	Time, in minutes, that an AP must remain unseen by any probes before it is deleted from the database.
`sta-ageout-interval`	Time, in minutes, that an client must unseen by any probes before it is deleted from the database.
`learn-ap`	Enables “learning” of non-Dell APs.
`persistent-known-interfering`	If enabled, APs that are marked as known interfering from being aged out.
`propagate-wired-MACs`	Shows if the controller has enabled or disabled the propagation of the gateway wired MACs.
`stat-update`	Shows if the controller has enabled or disabled WMS statistics updates in the database.
`collect-stats`	If enabled, if the master controller will collect up to 25,000 statistic entries for monitored APs and clients.

Column	Description
classification-server-ip	IP address of an AMP (Airwave Management Platform) that will perform Rogue AP classification. If there is a classification server defined, the wms-on-master and use-db parameters will be disabled.
rtls-port	Port number on the RTLS server to which WMS statistics should be sent.
wms-on-master	The WMS process is enabled on the master controller.
use-db	Shows if WMS data is updated to the database on the master controller.
calc-poll-interval	Interval (in milliseconds) specifies the frequency with which an AP sends updates about monitored APs and monitored clients to the controller. By default it uses the configured poll-interval value. If the # of deployed radios is more than 30, the **calc-poll-interval** is computed as 2000*number-of-radios.
Switch IP	IP address of the controller.
Is Master	If enabled, the controller is a master controller. Otherwise, it is defined as a local controller.

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show wms monitor-summary

```
show wms channel stats
```

Description

Display the numbers of different AP and client types monitored over the last 5 minutes, 1 hour, and since the controller was last reset.

Syntax

No parameters.

Usage Guidelines

The WLAN management system (WMS) on the controller monitors wireless traffic to detect any new AP or wireless client station that tries to connect to the network. When an AP or wireless client is detected, it is classified and its classification is used to determine the security policies which should be enforced on the AP or client. Use the **show wms monitor-summary** command to view a quick summary of each classified AP and client type currently on the network.

If AP learning is enabled (with the wms general command), non-Dell APs connected on the same wired network as Dell APs are classified as valid APs. If AP learning is disabled, a non-Dell AP is classified as an unsecure or suspect-unsecure AP.

Example

This example shows that the controller currently has 144 valid APs and 32 active valid clients, and verifies that the controller currently aware of a single disabled rogue AP.

```
(host) #show wms monitor-summary

WMS Monitor Summary
-------------------
                       Last 5 Min  Last Hour  All
-                      ----------  ---------  ---
Valid APs              0           0          144
Interfering APs        0           0          0
Rogue APs              0           0          0
Disabled Rogue APs     0           0          1
Unclassified APs       0           0          0
Known Interfering APs  0           0          0
Suspected Rogue APs    0           0          0
Valid Clients          0           0          32
Interfering Clients    0           0          0
Disabled Rogue Clients 0           0          0
```

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show wms probe

```
show wms probe
```

Description

Display detailed information for a list of WMS probes.

Syntax

No parameters.

Example

This example shows the Probe List table for WMS probes.

```
(host) #show wms probe

Probe List
----------
Monitor Eth MAC    BSSID              PHY Type        IP           LMS IP      Scan  Status  Updates  Reqs Stats  Type
---------------    -----              --------        --           ------      ----  ------  -------  ---- -----  ----
00:0b:86:cd:11:64  00:0b:86:51:16:48  80211A          10.13.11.19  10.6.2.250  No    Up      1893     0    11544  soft-
ap
00:1a:1e:c2:2c:c4  00:1a:1e:a2:cc:40  80211G          10.6.1.220   10.6.2.250  Yes   Up      940      1    40796  air-
monitor
00:0b:86:c1:be:56  00:0b:86:9b:e5:60  80211G          10.6.14.79   10.6.2.250  No    Up      927      0    30711  soft-
ap
00:0b:86:c4:4d:06  00:0b:86:c4:d0:70  80211A          10.6.14.78   10.6.2.250  No    Up      926      0    11339  soft-
ap
00:1a:1e:c2:30:80  00:1a:1e:a3:08:00  80211G          10.6.1.235   10.6.2.250  Yes   Up      1425     0    26171  air-
monitor
00:1a:1e:c2:2c:ba  00:1a:1e:a2:cb:a0  80211G          10.6.1.231   10.6.2.250  Yes   Up      971      1    21005  air-
monitor
00:1a:1e:c9:16:f0  00:1a:1e:11:6f:10  80211AHT-40mhz  10.6.1.204   10.6.2.250  No    Up      969      0    17813  soft-
```

The output of this command includes the following information:

Column	Description
Monitor Eth MAC	Ethernet MAC address of a probe.
BSSID	Probe Radio BSSID.
PHY Type	Radio PHY type: • 802.11A • 802.11AHT-40Mbps • 802.11AHT-20Mbps • 802.11G • 802,11GHT-20Mbps
IP	IP address of the AP.
LMS IP	IP address of the AP's local controller.
Scan	Shows if the Air Monitor is performing scanning.
Status	If the scan column displays a status of Up, the AP or AM is active
Updates	Number of updates the AP or AM sent to the WMS database since the controller was last reset.
Reqs	Number of database update requests that have not yet been added into the database.
Stats	Total number of statistics updates sent to the database.

Column	Description
Type	A WMS AP type can be one of the following: • **soft-ap**: an Dell Access Point (AP). • **air-monitor**: An Dell Air Monitor (AM).

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show wms rogue-ap

```
show wms rogue-ap <mac>
```

Description

Display statistics for APs classified as rogues APs.

Syntax

Parameter	Description
<mac>	MAC address of a rogue AP.

Example

The output of this command shows statistics for a suspected Rogue AP, including how it was classified as a suspected rogue.

```
(host) #show wms rogue-ap 00:0b:86:d4:ca:12

Suspect Rogue AP Info
---------------------
Key       Value
---       -----
BSSID     00:0b:86:d4:ca:12
SSID      corp1-voip
Channel   36
Type      generic-ap
RAP Type suspect-unsecure
Confidence Level 55%
Status up
Match Type Base-BSSID-Override
Match MAC 00:0b:86:c5:4c:a0
Match IP 1.1.1.249
Match AM Dell802.11n
Match Method Exact-Match
Suspect Match Types Base-BSSID-Override Base-BSSID-Override
Helper AP BSSID 00:0b:86:d4:ca:10
Match Time Sun Jul 27 13:08:16 2008

Match MAC Seen at APs
---------------------
AP-name
-------
ap-044
```

The output of this command includes the following information:

Column	Description
BSSID	BSSID of the suspected rogue AP.
SSID	The rogue AP's Extended service set identifier.
Channel	Channel used by a radio on the rogue AP.
Type	Indicates if the AP is an **Dell** AP, a **Cisco** AP, or an AP from any other manufacturer (**generic AP**).
RAP Type	Type of rogue AP, • Suspect-unsecure: AP has not been confirmed as a rogue AP. • unsecure: AP has been confirmed as a rogue AP

Column	Description
Status	Shows if the AP is active (**up**) or inactive (**down**).
Match Type	Describes how the AP was classified as a rogue. • Eth-Wired-MAC: An Dell AP or AM detected that a single MAC address was in both the Ethernet Wired-Mac table and a non-valid AP wired-Mac table. • AP-Wired-MAC: An interfering AP is marked as rogue when the Dell AP finds a MAC address in one of its valid AP wired-mac table and in an interfering AP wired-mac table. You can enable or disable the AP-Wired-MAC matching method using the CLI command **ids unauthorized-device-profile overlay-classification**. • Config-Wired-MAC: This type of classification occurs when an Dell AP or AM detects a match between a wired MAC table and a pre-defined MAC address that has manually defined via the command ids unauthorized-device-profile valid-wired-mac. • External-Wired-MAC: This type of classification occurs when an Dell AP or AM detects a match between a wired MAC table entry and a pre-defined MAC address manually defined in the rap-wml table. • Base-BSSID-Override: If an Dell AP is detected as rogue, then all virtual APs on the particular rogue are marked as rogue using Base-BSSID-Override match type. • Manual: An AP is manually defined as a rogue by via the command wms ap <bssid> mode rogue. • EMS: An AP is manually defined as a rogue by via the Element Management System
Match MAC	MAC address of a wired device that helped identify the AP as a rogue. If the AP has not been identified as a rogue, this column will display the MAC address 00:00:00:00:00:00.
Match IP	IP address of a wired device that helped identify the AP as a rogue.
Match AM	Dell Air Monitor that reporting seeing the rogue AP.
Match Method	This variable indicates the type of match.
Suspect Match Types	Describes how an AP was classified as a suspected rogue AP.
Helper Ap BSSID	BSSID of the AP or AM that helped classify a rogue AP.
AP name	Names of APs that are able to see the specified MAC address.
Match Time	Time the AP was identified as a rogue AP.

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show wms routers

```
show wms routers <mac>
```

Description

Show Learned Router Mac Information for WMS APs.

Syntax

Column	Description
<mac>	MAC address of a probe that can see the router.

Usage Guidelines

This command displays the MAC addresses of devices that have been determined to be routers by the listed APs. This output of this command will be blank if there is not any broadcast/multicast activity in an AP's subnet.

Example

In the example below, a single WMS AP has learned MAC information for four different routers.

```
(host) #show wms routers

Router Mac 00:08:00:00:11:12 is Seen by APs
-------------------------------------------
AP-Name
-------
AP32
Router Mac 00:08:00:00:11:29 is Seen by APs
-------------------------------------------
AP-Name
-------
AP32
Router Mac 00:08:00:00:11:57 is Seen by APs
-------------------------------------------
AP-Name
-------
AP32
Router Mac 00:08:00:00:11:6e is Seen by APs
-------------------------------------------
AP-Name
-------
AP32
```

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show wms system

```
show wms system
```

Description

Show the WMS system configuration and system state.

Syntax

No parameters.

Example

This example shows the WMS System Configuration and System State tables.

```
(host) #show wms system

System Configuration
--------------------
Key            Value
---            -----
max-threshold  30000

System State
-------------
Key                Value
---                -----
Max Threshold      30000
Current Threshold  28470
Total AP Count     27153
Total STA Count    3294
MAX RB-tree Count  50000
Total Tree Count   50000
Poll Count (Max)    10(365)
```

The output of this command includes the following information:

Column	Description
`Max Threshold`	The maximum number of table entries allowed. If this table displays a zero (0), there is no configured limit. **NOTE:** If a configured maximum limit has reached, the controller will not create new WMS entries for monitored APs and monitored stations. If new APs are deployed after this limit is reached, those APs will not be marked as 'valid', which will impair the effectiveness of the Adaptive Radio Management feature. If there are new Rogue APs in the network, they will not be classified as a rogue.
`Current Threshold`	Current number of table entries.
`Total AP Count`	Total number of statistics entries for monitored APs in the AP table.
`Total STA Count`	Total number of statistics entries for monitored stations in the Station table.
`MAX RB-tree Count`	Maximum number of entries allowed in the statistics.
`Total Tree Count`	Total number of entries currently in the statistics tree. If this limit has been reached, the controller will not add entries with the RSSI information for APs, monitored APs and monitored clients that are seen by them. This can negatively affect the RF Plan application.
`Poll Count (Max)`	Current and maximum poll counts.

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

show wms wired-mac

```
show wms wired-mac [{<mac>}|{ap-name <ap-name>}]
```

Description

Show a table of gateway wired addresses. This command can display a list of APs aware of a specific gateway MAC address, or list the wired MAC addresses known to a single AP.

Syntax

Column	Description
<mac>	Specify a wired MAC address to display a list of APs that are aware of this wired MAC.
ap-name <ap-name>	Specify the IP address of an AP to list the wired MAC addresses of which it is aware.

Example

This example shows that the AP Corp-AP125-AM is aware of four different gateway wired MAC addresses.

```
(host) #show wms wired-mac ap-name Corp-AP125-AM


Learned Wired Macs for AP: Corp-AP125-AM
-----------------------------------------
Wired-Mac
---------
00:0b:86:41:01:20
00:0b:86:60:2e:ac
00:0b:86:40:1e:60
00:0b:86:08:e1:00
```

Command History

This command was introduced in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

shutdown

```
shutdown all
```

Description

This command disables all interfaces on the controller.

Usage Guidelines

This command stops all traffic through the physical ports on the controller. The console port remains active. Use this command only when you have physical access to the controller, so that you can continue to manage using the console port.

To shut down an individual interface, tunnel, or VLAN, use the `shutdown` option within the `interface` command. To restore the ports, use the `no shutdown` command.

Example

The following example shuts down all physical interfaces on the controller.

```
(host) (config)#shutdown all
```

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master or local controllers

snmp-server

```
snmp-server
   community <string>
   enable trap
   engine-id
   host <ipaddr> version {1 <name> udp-port <port>}|2c|{3 <name>} [inform] [interval
     <seconds>] [retrycount <number>] [udp-port <port>]}
   inform queue-length <size>
   stats
   trap enable|disable|{source <ipaddr>}
   user <name> [auth-prot {md5|sha} <password>] [priv-prot {AES|DES} <password>]
```

Description

This command configures SNMP parameters.

Syntax

Parameter	Description	Range	Default
`community`	Sets the read-only community string.	—	—
`enable trap`	Enables sending of SNMP traps to the configured host.	—	disabled
`engine-id`	Sets the SNMP server engine ID as a hexadecimal number.	24 characters maximum	—
`host`	Configures the IP address of the host to which SNMP traps are sent. This host needs to be running a trap receiver to receive and interpret the traps sent by the controller.	—	—
`version`	Configures the SNMP version and security string for notification messages.	—	—
`inform`	Sends SNMP inform messages to the configured host.	—	disabled
`inform`	Specifies the length for the SNMP inform queue.	100-350	250
`stats`	Allows file-based statistics collection for Mobility Manager. The controller generates a file that contains statistics data used by Mobility Manager to display information in chart and graph formats. File-based statistics collection is transparent to the user and increases the efficiency of transferring information between the controller and Mobility Manager.		enabled
`trap`	Source IP address of SNMP traps.	—	disabled
`disable`	Disables an SNMP trap. You can get a list of valid trap names using the `show snmp trap-list` command.	—	—
`enable`	Enables an SNMP trap.	—	—
`source`	Enter the source IP address for sending traps.	—	—
`interval`	Estimated round trip time to this host.		60 seconds
`retrycount`	Number of times that SNMP inform messages are attempted to be sent to the host before giving up.		3
`udp-port`	The port number to which notification messages are sent.	—	162
`user`	Configures an SNMPv3 user profile for the specified username.	—	—
`auth-prot`	Authentication protocol for the user, either HMAC-MD5-98 Digest Authentication Protocol (MD5) or HMAC-SHA-98 Digest Authentication Protocol (SHA), and the password for use with the designated protocol.	MD5/SHA	SHA
`priv-prot`	Privacy protocol for the user, either Advanced Encryption Standard (AES) or CBC-DES Symmetric Encryption Protocol (DES), and the password for use with the designated protocol.	AES/DES	DES

Usage Guidelines

This command configures SNMP on the controller only. You configure SNMP-related information for APs in an SNMP profile which you apply to an AP group or to a specific AP. To configure SNMP hostname, contact, and location information for the controller, use the **hostname**, **syscontact**, and **syslocation** commands.

Example

The following command configures an SNMP trap receiver:

```
(host) (config) #snmp-server host 191.168.1.1 version 2c 12345678
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.3.1	The **stats** parameter was introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

spanning-tree (Global Configuration)

```
spanning-tree
   [forward-time <value> | hello-time <value> | max-age <value> | priority <value> |
   vlan range <WORD>
```

Note: RSTP is backward compatible with STP and is enabled by default. For ease of use, this command uses the spanning tree keyword.

Description

This command is the global configuration for the Rapid Spanning Tree Protocol (RSTP) and Per VLAN Spanning Tree (PVST+). See spanning-tree (Configuration Interface) for details on the RSTP (config-if) command.

Syntax

Parameter	Description	Range	Default
`forward-time`	Specifies the time, in seconds, the port spends in the listening and learning state. During this time, the port waits to forward data packets.	4-30	15 seconds
`hello-time`	Specifies the time, in seconds, between each bridge protocol data unit (BPDU) transmitted by the root bridge.	1-10	2 seconds
`max-age`	Specifies the time, in seconds, the root bridge waits to receive a hello packet before changing the STP topology.	6-40	20 seconds
`priority`	Set the priority of a bridge to make it more or less likely to become the root bridge. The bridge with the lowest value has the highest priority. When configuring the priority, remember the following: The highest priority bridge is the root bridge. The highest priority value is 0 (zero).	0-65535	32768
`vlan range <WORD>`	Enter the keywords **vlan range** followed by the range of VLAN iID's. Separate the VLAN IDs with a hyphen, comma or both to indicate the range. For example: 2-3 or 2,4,6 or 2-6,11	—	—

Usage Guidelines

This command configures the global RSTP settings on the controller and is backward compatible with past versions of ArubaOS using STP.

By default, all interfaces and ports on the controller run RSTP as specified in 802.1w and 802.1D. The default RSTP values can be used for most implementations.

Use the `no spanning-tree` command to disable RSTP.

Examples

The following command sets the time a port spends in the listening and learning state to 3 seconds:

```
spanning-tree forward-time 3
```

The following command sets the time the root bridge waits to transmit BPDUs to 4 seconds:

```
spanning-tree hello-time 4
```

The following command sets the time the root bridge waits to receive a hello packet to 30 seconds:

```
spanning-tree max-age 30
```

The following command sets the bridge priority to 10, making it more likely to become the root bridge:

```
spanning-tree priority 10
```

The follow command sets a spanning-tree VLAN range

```
spanning-tree vlan range 2-8,11
```

Command History

Release	Modification
ArubaOS 6.0	Added support for PVST+ and VLAN and VLAN Range
ArubaOS 3.4	Upgraded STP to RSTP with full backward compatibility
ArubaOS 1.0	Introduced the Spanning Tree Protocol (STP)

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration (config)

spanning-tree (Configuration Interface)

```
spanning-tree
   cost <value>
   point-to-point
   port-priority <value>
   portfast
   vlan <vlan-id>
      cost <value>
      port-priority <value>
   vlan range <WORD>
```

Note: RSTP is backward compatible with STP and is enabled by default. For clarity, this RSTP command uses the spanning tree keyword.

Description

Dell's RSTP implementation interoperates with both PVST (Per VLAN Spanning Tree 802.1D) and Rapid-PVST (802.1w) implementation on industry-standard router/switches. Syntax

Parameter	Description	Range	Default
`cost <value>`	Enter the spanning tree path cost. Use the cost values to determine the most favorable path to a particular destination: the lower the cost, the better the path	1 - 65535	Default: Based on Interface type: • Fast Ethernet 10Mbs—100 • Fast Ethernet 100Mbs—19 • 1Gigabit Ethernet—4 • 10 Gigabit Ethernet—2
`point-to-point`	Set the interface to a point-to-point	n/a	Enabled
`port-priority <value>`	Change the spanning tree priority.	0 - 255	128
`portfast`	Change from blocking to forwarding	n/a	Disabled
`vlan <vlan-id>`	Enter the keyword **vlan** followed by the VLAN-ID	n/a	—
`cost <value>`	Enter th keyword cost followed by the cost value to change the interface's spanning tree path cost.	1 - 65535	
`port-priority <value>`	Change the spanning tree priority.	0 - 255	128
`vlan range <WORD>`	Enter the keywords **vlan range** followed by the range of VLAN iID's. Separate the VLAN IDs with a hyphen, comma or both to indicate the range. For example: 2-3 or 2,4,6 or 2-6,11	—	—

Usage Guidelines

Dell supports global instances of RSTP and PVST+. Therefore, the ports on industry-standard routers/switches must be on the default or untagged VLAN for interoperability with controllers.

ArubaOS supports RSTP on the following interfaces:

- FastEthernet IEEE 802.3—fastethernet
- Gigabitethernet IEEE 802.3—gigabitethernet
- Port Channel ID—port-channel

In addition to port state changes, RSTP introduces port roles for all the interfaces.

RSTP (802.1w) Port Role	Description
Root	The port that receives the best BPDU on a bridge.
Designated	The port can send the best BPDU on the segment to which it is connected.
Alternate	The port offers an alternate path, in the direction of root bridge, to that provided by bridge's root port.
Backup	The port acts as a backup for the path provided by a designated port in the direction of the spanning tree.

Example

The RSTP default values are adequate for most implementation. Use caution when making changes to the spanning tree values.

```
(host) (config-if) #spanning-tree cost 345

(host) (config-if) #spanning-tree point-to-point ?

(host) (config-if) #spanning-tree portfast ?

(host) (config-if) #spanning-tree vlan range 2-8,11
```

Related Commands

spanning-tree (Global Configuration) on page 1137

Command History

Release	Modification
ArubaOS 6.0	Added support for PVST+ and VLAN and VLAN Range
ArubaOS 3.4	Upgraded STP to RSTP with full backward compatibility.
ArubaOS 1.0	Introduced the Spanning Tree Protocol (STP).

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration Interface (config-if)

spanning-tree mode

```
spanning-tree mode <rapid> | <rapid-pvst>
```

Description

Set the spanning tree mode to either Rapid Spanning Tree (802.1w) or PVST+ (Per VLAN Spanning Tree).

Syntax

Parameter	Description
rapid	Set the spanning tree mode to RSTP (Rapid Spanning Tree Protocol).
rapid-pvst	Set the spanning tree mode to PVST+ (Per VLAN Spanning Tree protocol)

Usage Guidelines

Once the spanning tree mode is set, you can configure RSTP or PVST+.

Command History

Release	Modification
6.0	PVST+ added
3.4	Upgraded STP to RSTP with full backward compatibility.

Command Information

Platform	Licensing	Command Mode
All platforms	Base operating system	Configuration mode (config) on master controllers

spanning-tree vlan (PVST+)

```
spanning-tree vlan <id>
[forward-time <value> | hello-time <value> | max-age <value> | priority <value>]
```

Note: For ease of use, this command uses the spanning tree keyword to represent PVST+

Description

Configure PVST+ on a VLAN.

Syntax

Parameter	Description	Range	Default
`forward-time`	Specifies the time, in seconds, the VLAN spends in the listening and learning state before transitions to the forward state.	4-30	15 seconds
`hello-time`	Set the time interval, in seconds, between transmission of BPDUs.	1-10	2 seconds
`max-age`	Set the time interval for the PVST+ bridge to maintain configuration information before refreshing that information.	6-40	20 seconds
`priority`	Set the priority of a bridge to make it more or less likely to become the root bridge. The bridge with the lowest value has the highest priority. When configuring the priority, remember the following: The highest priority bridge is the root bridge. The highest priority value is 0 (zero).	0-65535	32768

Example

The following command sets the time VLAN 2 spends in the listening and learning state to 3 seconds:

```
spanning-tree vlan 2 forward-time 3
```

The following command sets the time VLAN 2 waits to transmit BPDUs to 4 seconds:

```
spanning-tree vlan 2 hello-time 4
```

The following command sets the time VLAN 2 waits to receive a hello packet to 30 seconds:

```
spanning-tree vlan 2 max-age 30
```

The following command sets the VLAN 2 priority to 10, making it more likely to become the root bridge:

```
spanning-tree vlan 2 priority 10
```

Command History

Release	Modification
ArubaOS 6.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All Platforms	Base operating system	Configuration Mode (config)

spanning-tree vlan range (PVST+)

```
spanning-tree vlan range <WORD>
[forward-time <value> | hello-time <value> | max-age <value> | priority <value>]
```

Note: For ease of use, this command uses the spanning tree keyword to represent PVST+

Description

Configure PVST+ on a range of VLANs.

Syntax

Parameter	Description	Range	Default
<WORD>	Enter a string representing the VLAN range	--	--
forward-time	Specifies the time, in seconds, the VLANs spends in the listening and learning state before transition to the forward state.	4-30	15 seconds
hello-time	Set the time interval, in seconds, between transmission of BPDUs.	1-10	2 seconds
max-age	Set the time interval for the PVST+ bridge to maintain configuration information before refreshing that information.	6-40	20 seconds
priority	Set the priority of a bridge to make it more or less likely to become the root bridge. The bridge with the lowest value has the highest priority. When configuring the priority, remember the following: The highest priority bridge is the root bridge. The highest priority value is 0 (zero).	0-65535	32768

Example

The following command sets the time the VLAN range 2-3 spends in the listening and learning state to 3 seconds:

```
spanning-tree vlan range 2-3 forward-time 3
```

The following command sets the time the VLAN range 2-3 waits to transmit BPDUs to 4 seconds:

```
spanning-tree vlan range 2-3 hello-time 4
```

The following command sets the time the VLAN range 2-3 waits to receive a hello packet to 30 seconds:

```
spanning-tree vlan range 2-3 max-age 30
```

The following command sets the VLAN range 2-3 priority to 10, making it more likely to become the root bridge:

```
spanning-tree vlan range 2-3 priority 10
```

Command History

Release	Modification
ArubaOS 6.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All Platforms	Base operating system	Configuration Mode (config)

ssh

```
ssh disable_dsa | mgmt-auth {public-key [username/password] | username/password
[public-key]}
```

Description

This command configures SSH access to the controller.

Syntax

Parameter	Description	Default
`disable_dsa`	Disables DSA authentication for SSH. Only RSA authentication is used.	—
`mgmt-auth`	Configures authentication method for the management user. You can specify username/password only, public key only, or both username/password and public key.	username/password

Usage Guidelines

Public key authentication is supported using a X.509 certificate issued to the management client. If you specify public-key authentication, you need to load the client X.509 certificate into the controller and configure certificate authentication for the management user with the mgmt-user ssh-pubkey command.

Example

The following commands configure SSH access using public key authentication only:

```
(host) (config) #ssh mgmt-auth public-key
mgmt-user ssh-pubkey client-cert ssh-pubkey cli-admin root
```

Command History

Version	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.1	The **mgmt-auth** parameter was introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

stm

```
add-blacklist-client <macaddr>
kick-off-sta <macaddr> <bssid>
purge-blacklist-clients
remove-blacklist-client <macaddr>
```

Description

This command is used to manually disconnect a client from an AP or control the blacklisting of clients.

Syntax

Parameter	Description
`add-blacklist-client`	MAC address of the client to be added to the denial of service list.
`kick-off-sta`	When you use the kick-off-sta feature specify a client's MAC address and BSSID, the AP sends deauthorization frames to the station to disconnect it.
`<macaddr>`	MAC address of client to be disconnected.
`<bssid>`	The associated BSSID of the client to be disconnected.
`purge-blacklist-client`	Clear the entire client blacklist.
`remove-blacklist-client <macaddr>`	Specify the MAC address of a client to remove it from the denial of service list.

Usage Guidelines

When you blacklist a client, the client is not allowed to associate with any AP in the network. If the client is connected to the network when you blacklist it, a deauthentication message is sent to force the client to disconnect. The blacklisted client is blacklisted for the duration specified in the virtual AP profile. The client blacklist supports up to 4,000 individual client entries.

The controller retains the client blacklist in the user database, so the information is not lost if the controller reboots. When you import or export the controller's user database, the client blacklist will be exported or imported as well.

Example

The following command blacklists a client:

```
(host) #stm add-blacklist-client 00:01:6C:CC:8A:6D
```

Command History

Version	Modification
ArubaOS 1.0	Command introduced.
ArubaOS 6.0	The purge-client-blacklist parameter was introduced. The **start-trace** and **stop-trace** parameters are no longer functional.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master or local controllers

support

```
support
```

Description

This command, which should be used only in conjunction with Dell customer support, is for controller debugging purposes only.

Syntax

No parameters.

Usage Guidelines

This command is used by Dell customer support for debugging the controller. Do not use this command without the guidance of Dell customer support.

Example

The following command allows Dell customer support to debug the controller:

```
(host) #support
```

Command History

Version	Modification
ArubaOS 2.4	Command introduced as the **secret** command
ArubaOS 3.1	Command renamed to **support**

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

syscontact

```
syscontact <syscontact>
```

Description

This command configures the name of the system contact for the controller.

Syntax

Parameter	Description
`syscontact`	An alphanumeric string that specifies the name of the system contact.

Usage Guidelines

Use this command to enter the name of the person who acts as the system contact or administrator for the controller. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the alphanumeric string. For example, to create the system contact name Lab Technician 1, enter **"Lab Technician 1"** at the prompt.

To change the existing name, enter the command with a different string. The new name takes affect immediately. To unconfigure the name, enter **""** at the prompt.

Example

The following command defines **LabTechnician** as the system contact name:

```
(host) (config) #syscontact LabTechnician
```

Command History

This command was introduced in ArubaOS 3.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

syslocation

```
syslocation <syslocation>
```

Description

This command configures the name of the system location for the controller.

Syntax

Parameter	Description
`syslocation`	An alphanumeric string that specifies the name of the system location.

Usage Guidelines

Use this command to indicate the location of the controller. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the text string.

To change the existing name, enter the command with a different string. To unconfigure the location, enter `“”` at the prompt.

Example

The following command defines **SalesLab** as the location for the controller:

```
(host) # syslocation “Building 10, second floor, room 21E”
syscontact LabTechnician
```

Command History

This command was introduced in ArubaOS 3.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

telnet

```
telnet {cli|soe}
```

Description

Enable telnet to the controller or to an AP through the controller.

Syntax

Parameter	Description	Default
`cli`	Enable telnet using the CLI.	Disabled
`soe`	Enable telnet using Serial over Ethernet (SoE).	Disabled

Usage Guidelines

Use the **cli** option to enable telnet to the controller.

Use the **soe** option to enable telnet using the SoE protocol. This allows you to remotely manage an AP directly connected to the controller.

Example

The following example enables telnet to the controller using the CLI.

```
(host) (config) #telnet cli
```

Command History

The command was introduced in ArubaOS 1.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

time-range

```
time-range <name> absolute [end <mm/dd/yyyy> <hh:mm>]|[start <mm/dd/yyyy> <hh:mm>]
   time-range <name> periodic
   Daily <hh:mm> to <hh:mm>
   Friday <hh:mm> to <hh:mm>
   Monday <hh:mm> to <hh:mm>
   Saturday <hh:mm> to <hh:mm>
   Sunday <hh:mm> to <hh:mm>
   Thursday <hh:mm> to <hh:mm>
   Tuesday <hh:mm> to <hh:mm>
   Wednesday <hh:mm> to <hh:mm>
   Weekday <hh:mm> to <hh:mm>
   Weekend <hh:mm> to <hh:mm>
   no ...
```

Description

This command configures time ranges.

Syntax

Parameter	Description
`<name>`	Name of this time range. You can reference this name in other commands.
`absolute`	Specifies an absolute time range, with a specific start and/or end time and date.
`periodic`	Specifies a recurring time range. Specify the start and end time and Daily, Weekday, Weekend, or the day of the week.
`no`	Negates any configured parameter.

Usage Guidelines

You can use time ranges when configuring session ACLs. Once you configure a time range, you can use it in multiple session ACLs.

Example

The following command configures a time range for daytime working hours:

```
(host) (config) #time-range working-hours periodic
   weekday 7:30 to 18:00
```

Command History

The command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

traceroute

```
traceroute <ipaddr>
```

Description

Trace the route to the specified IP address.

Syntax

Parameter	Description
<ipaddr>	The destination IP address.

Usage Guidelines

Use this command to identify points of failure in your network.

Example

The following command traces the route to the device identified by the IP address 10.1.2.3.

```
(host) (config) #traceroute 10.1.2.3
```

Command History

The command was introduced in ArubaOS 2.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	User, Enable, and Config modes on local or master controllers

trusted

```
trusted all
```

Description

This command makes all physical interfaces on the controller trusted ports.

Syntax

Parameter	Description
`all`	Makes all ports on the controller trusted.

Usage Guidelines

Trusted ports are typically connected to internal controlled networks. Untrusted ports connect to third-party APs, public areas, or any other network to which the controller should provide access control. When APs are attached directly to the controller, set the connecting port to be trusted.

By default, all ports on the controller are treated as trusted. You can use the **interface fastethernet** or **interface gigabitethernet** commands to make individual ports trusted.

Example

The following command makes all ports trusted:

```
(host) (config) #trusted all
```

Command History

The command was introduced in ArubaOS 2.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

uplink

```
crypto-local
   uplink {cellular priority <prior>}|disable|enable|{wired priority <prior>}|{wired
   vlan <id>}
```

Description

Manage and configure the uplink network connection on the Aruba 600 controllers.

Syntax

Parameter	Description	Range
`cellular priority <prior>`	Set the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary controller link.	1-255
`enable`	Enable the uplink manager.	—
`disable`	Disable the uplink manager.	—
`wired priority <prior>`	Set the priority of the wired uplink. Each uplink type has an associated priority; wired ports having the highest priority by default.	1-255
`wired vlan <id>`	Define the VLAN identification (ID) of the uplink VLAN . A maxmim of four wired VLANs can be defined	1-4094

Usage Guidelines

The Aruba 600 controllers supports multiple 3G cellular uplinks in addition to its standard wired ports, providing redundancy in the event of a connection failure. If an Aruba 600's wired link cannot access the internet, the controller can fail over to a secondary cellular link and continue routing traffic.

Command History

Release	Modification
ArubaOS 3.4	Command introduced
ArubaOS 6.0	The **wired prority** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Aruba 600 controllers	Base operating system	Config mode on master and local controllers

usb reclassify

```
crypto-local
   usb reclassify <address>
```

Description

Disconnect and reclassify an USB device.

Syntax

Parameter	Description
<address>	USB device address from the show usb command.

Usage Guidelines

There's no way to power off an USB port on the Aruba 600 controller, but you can re-initialize the device using the usb reclassify command. This command removes the modem from the USB device list, then detects it via the USB table.

Command History

Introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
Aruba 600 controllers	Base operating system	Config mode on master and local controllers

usb-printer

```
usb-printer [printer <printer-name> alias <alias-name>]
```

Description

This command allows you to provide an alias to USB printers connected to W-600 Series Controller series controllers.

Syntax

Parameter	Description
`printer`	Enter the default printer name. To get the default printer name use the `show network-printer status` command.
`alias`	Enter a new alias name for the printer.

Example

The following command creates an alias for a printer:

```
(host) usb-printer printer usblp_HP_Officejet_Pro_L7500_MY872231FX alias HPOJ_L7500
(host) #show network-printer status

Networked Printer Status
------------------------
Printer Name                                              Printer Alias  Status  Comment
------------                                              -------------  ------  -------
usblp_Hewlett-Packard_HP_Color_LaserJet_CP3505_CNBJ8B1003  HPLJ_P3005     idle    enabled
usblp_HP_Officejet_Pro_L7500_MY872231FX                   HPOJ_L7500     idle    enabled
```

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
Aruba 600 series	Base operating system	Enable mode.

user-role

```
user-role <name>
   access-list {eth|mac|session} <acl> [ap-group <group>] [position <number>]
   bw-contract <name> [per-user] {downstream|upstream}
   captive-portal <profile>
   dialer <name>
   ipv6 session-acl <string>
   max-sessions <number>
   no ...
   pool {l2tp|pptp} <name>
   reauthentication-interval <minutes>
   session-acl <acl> [ap-group <group>] [position <number>]
   stateful-ntlm <ntlm_profile_name>
   vlan {VLAN ID|VLAN name}
   wispr <wispr_profile_name>
```

Description

This command configures a user role.

Syntax

Parameter	Description	Range	Default
<name>	Name of the user role.	—	—
access-list	Type of access control list (ACL) to be applied: **eth:** Ethertype ACL, configured with the **ip access-list eth** command. **mac:** MAC ACL, configured with the **ip access-list mac** command. **session:** Session ACL, configured with the **ip access-list session** command.	—	—
<acl>	Name of the configured ACL.		
ap-group	(Optional) AP group to which this ACL applies.	—	—
position	(Optional) Position of this ACL relative to other ACLs that you can configure for the user role. 1 is the top.	—	(last)
bandwidth-contract	Name of a bandwidth contract or rate limiting policy configured with the **aaa bandwidth-contract** command. The bandwidth contract must be applied to either downstream or upstream traffic.	—	—
downstream	Applies the bandwidth contract to traffic from the controller to the client.	—	—
per-user	Specifies that bandwidth contract is assigned on a per-user basis instead of a per-role basis. For example, if two users are active on the network and both are part of the same role with a 500 Kbps bandwidth contract, then each user is able to use up to 500 Kbps.	—	(per role)
upstream	Applies the bandwidth contract to traffic from the client to the controller.	—	—
captive-portal	Name of the captive portal profile configured with the **aaa authentication captive-portal** command.	—	—
dialer	If VPN is used as an access method, name of the VPN dialer configured with the **vpn-dialer** command. The user can login using captive portal and download the dialer. The dialer is a Windows application that configures the VPN client.	—	—
max-sessions	Maximum number of datapath sessions per user in this role.	0-65535	65535
no	Negates any configured parameter.	—	—
ipv6 session-acl <string>	Specify a session ACL for IPV6 users.		
pool	If VPN is used as an access method, specifies the IP address pool from which the user's IP address is assigned: l2tp: When a user negotiates a Layer-2 Tunneling Protocol (L2TP)/ IPsec session, specifies an address pool configured with the **ip local pool** command. pptp: When a user negotiates a Point-to-Point Tunneling Protocol (PPTP) session, specifies an address pool configured with the **pptp ip local pool** command.	—	—
<name>	Name of the L2TP or PPTP pool to be applied.	—	—
reauthentication-interval	Interval, in minutes, after which the client is required to reauthenticate.	0-4096, 0 to disable	0 (disabled)
session-acl	Session ACL configured with the **ip access-list session** command.	—	—
ap-group	(Optional) AP group to which this ACL applies.	—	—
position	(Optional) Position of this ACL relative to other ACLs that you can configure for the user role. 1 is the top.	—	(last)
stateful-ntlm	Apply stateful NTLM authentication to the specified user role		

Parameter	Description	Range	Default
`vlan`	Identifies the VLAN ID or VLAN name to which the user role is mapped. This parameters works only when using Layer-2 authentication such as 802.1x or MAC address, ESSID, or encryption type role mapping because these authentications occur before an IP address is assigned. If a user authenticates using a Layer-3 mechanism such as VPN or captive portal this parameter has no effect. **NOTE:** VLAN IDs and VLAN names cannot be listed together.	—	—
`wispr`	Apply WISPr authentication to the specified user role.		

Usage Guidelines

Every client in a user-centric network is associated with a user role. All wireless clients start in an initial role. From the initial role, clients can be placed into other user roles as they pass authentication.

Example

The following command configures a user role:

```
(host) (config) #user-role new-user
   dialer default-dialer
   pool pptp-pool-1
```

Command History

Version	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.4.1	The **stateful-ntlm** and **wispr** parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license.	Config mode on master controllers

valid-network-oui-profile

```
valid-network-oui-profile
   no
   oui <oui>
```

Description

This command allows you to add a new OUI to the controller

Syntax

Parameter	Description	Range	Default
no	Negates any configured parameter.	—	—
oui <oui>	The new OUI to be added. Use the aa:bb:cc format to input the new OUI.	—	—

Usage Guidelines

This command adds a new OUI to the controller. The new OUI must be entered in a aa:bb:cc format.

Example

The following command adds a new OUI to the controller.

```
(host) (config) #valid-network-oui-profile
(host) (Valid Equipment OUI profile) #
(host) (Valid Equipment OUI profile) #oui 00:11:22
This should only be used when adding equipment with a new OUI.  Are you sure you
want to proceed? [y/n]: y
```

Command History

Release	Modification
ArubaOS 5.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Base operating system	Config mode on master controllers

vlan

```
vlan <id> [<description>] |[<name> <vlan-ids>]|[range <range>]|[wired aaa-profile <profile>]
```

Description

This command creates a VLAN ID or a range of VLAN IDs on the controller.

Syntax

Parameter	Description	Range	Default
`<id>`	Identification number for the VLAN.	2-4094	1
`<description>`	Description of a VLAN ID.	1-32 characters; cannot begin with a numeric character	VLAN000x, where x is the ID number.
`<name>`	(Optional) Identification name of the VLAN. The VLAN name was created using the **vlan-name** command.	1-32 characters; a name cannot begin with a numeric character	VLAN<id>
`<vlan-ids>`	(Optional) List of VLAN IDs that are associated with this VLAN. If two or more IDs are listed, the VLAN needs to specified first as a VLAN pool using the **vlan-name** command.	Existing VLAN IDs	1
`range <range>`	Create a range of multiple VLAN IDs by specifying the beginning and ending VLAN ID separated by a hyphen. For example, 55-58	2-4094	—
`wired aaa-profile <profile>`	Assign an AAA profile to a VLAN to enable role-based access for wired clients connected to an untrusted VLAN or port on the controller. This parameter applies to wired clients only. Note that this profile will only take effect if the VLAN and/or the port on the controller is untrusted. If both the port and the VLAN are trusted, no AAA profile is assigned.	—	—

Usage Guidelines

Use the **`interface vlan`** command to configure the VLAN interface, including an IP address. Use the **`vlan-name`** command to create a named VLAN to set up a VLAN pool. A VLAN pool consists of a set of VLAN IDs which are grouped together to efficiently manage multi-controller networks from a single location.

To enable role-based access for wired clients connected to an untrusted VLAN and/or port on the controller, you must use the **wired aaa-profile** parameter to specify the wired AAA profile you would like to apply to that VLAN. If you do not specify a per-VLAN wired AAA profile, traffic from clients connected to an untrusted wired port or VLAN will use the global wired AAA profile, if configured.

Example

The following command creates VLAN ID 27 with the description **myvlan** on the controller.

```
(host) (config) #vlan 27 myvlan
```

The following command associates the VLAN IDs 5, 12 and 100 with VLAN guestvlan on the controller.

```
vlan guestvlan 5,12,100
```

The following command creates VLAN IDs 200-300, 302, 303-400.

```
(host) (config) #vlan range 200-300,302, 303-400
```

Related Commands

Command	Description
`show vlan`	This command shows a configured VLAN interface number, description and associated ports
`aaa authentication wired`	This command configures authentication for a client device that is directly connected to a port on the controller.

Command History

Release	Modification
ArubaOS 3.0	Command available.
ArubaOS 3.4	**vlan-ids** parameter introduced.
ArubaOS 3.4.1	**vlan range** parameter introduced.
ArubaOS 6.0	**wired aaa-profile** parameter introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

vlan-bwcontract-explist

```
vlan-bwcontract-explist mac <mac>
```

Description

Use this command to add entries to or remove entries from the MAC exception list for bandwidth contracts on broadcast/multicast traffic.

Syntax

Parameter	Description
<mac>	MAC address of a protocol that should be added to or removed from the exception list for bandwidth contracts.

Usage Guidelines

Bandwidth contracts on a VLAN can limit broadcast and multicast traffic. ArubaOS version 6.0 and later includes an internal exception list to allow broadcast and multicast traffic using the VRRP, LACP, OSPF, PVST and STP protocols. To remove per-vlan bandwidth contract limits on an additional broadcast or multicast protocol, add the MAC address for that broadcast/multicast protocol to the Vlan Bandwidth Contracts MAC Exception List.

Example

The following command adds the MAC address for CDP (Cisco Discovery Protocol) and VTP (Virtual Trunking Protocol to the list of protocols that are not limited by VLAN bandwidth contracts.

```
(host) (config) #vlan-bwcontract-explist mac 01:00:0C:CC:CC:CC
```

Related Commands

Command	Description
show vlan-bwcontract-explist [internal]	This command shows the regular or internal VLAN bandwidth contract exception list

Command History

Command introduced in ArubaOS 6.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master or local controllers

vlan-name

```
vlan-name <name> [pool]
```

Description

This command creates a named VLAN on the controller and can enable it as a pool. A named VLAN needs to be first created to assign one or a pool of VLAN IDs to that name.

Syntax

Parameter	Description	Range
<name>	Name for the VLAN.	1–32 characters
[pool]	(Optional) Sets the named VLAN to be a pool.	—

Usage Guidelines

Create a named VLAN so you can set up a VLAN pool. A VLAN pool consists of a set of VLAN IDs which are grouped together to efficiently manage multi-controller networks from a single location.

Example

The following command creates a VLAN pool named **mytest** on the controller:

```
vlan-name mytest pool
```

Related Commands

```
(host) (config) #show vlan
```

Command History

Version	Modification
ArubaOS 3.0	Command introduced.
ArubaOS 3.4	the **pool** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

voice dialplan-profile

```
voice dialplan-profile <profile>
   clone <source>
   dialplan {<sequence> <pattern> <action>}
   no...
```

Description

This command allows you to create a dial plan profile and configure dial plans to the profile.

Syntax

Parameter	Description
`<profile>`	Name of this instance of the dial plan profile.
`clone`	Name of the existing dial plan profile from which parameter values are copied.
`dialplan`	Configures a dialplan with the sequence, pattern, and action specified for the profile. You can configure upto 20 dialplans for a profile.
`<sequence>`	A number that positions the dial plan in the list of dial plans configured in the controller. The range is 100 - 65535.
`<pattern>`	A digit pattern or the number of digits that will be dialed by the user. You can specify the digit pattern using 'X', 'Z', 'N', '[ ]' and '.'. • X is a wild card that represents any character from 0 to 9. • Z is a wild card that represents any character from 1 to 9. • N is a wild card that represents any character from 2 to 9. • [ ] is a wild card that represents the number or the range specified in the brackets. • . (period) is a wild card that represents any-length digit strings.
`<action>`	A prefix code that is automatically prefixed to the dialed number. This is specified as <prefix-code>%e. Examples of dial plans are: • 9%e: The number 9 is prefixed to the dialed number. • 91%e: The number 91 is prefixed to the dialed number.

Usage Guidelines

You can configure dial plans on the controller that are required by the local EPABX system to provide outgoing PSTN call facility from a SIP device.

Note: Dial plan can be configured only for SIP over UDP.

Example

The following command creates a dial plan for the dial plan profile, *local*:

```
(host) (config) #voice dialplan-profile local
(host) (Dialplan Profile "local") #dialplan  300 Z. 91%e
```

Command History

Version	Description
ArubaOS 6.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config mode on master controller

voice logging

```
voice logging
   client mac <client mac>
   no ...
```

Description

This command allows you to enable logging for a voice client.

Syntax

Parameter	Description
`client mac`	MAC address of the voice client to be enabled for voice logging.

Usage Guidelines

You can enable voice logging for a specific voice client based on the MAC address of the client to troubleshoot any voice issues.

Example

The following command enables voice logging on the client with the MAC address 11:22:33:44:55:67:

```
(host) (config) #voice logging
(host)(VoIP Logging) #client-mac 11:22:33:44:55:67
```

Command History

Version	Description
ArubaOS 6.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config mode on master controller

voice rtcp-inactivity

```
voice rtcp-inactivity {enable | disable}
```

Description

This command enables or diables the RTCP inactivity timer.

Syntax

Parameter	Description
`enable`	Enables the RTCP inactivity timer.
`disable`	Disables the RTCP inactivity timer.

Usage Guidelines

You can enable the RTCP inactivity timer to clear a voip session if an on-hold client moves out of the coverage area.

Example

The following command enables the RTCP inactivity timer:

```
(host) (config) #voice rtcp-inactivity enable
```

Command History

Version	Description
ArubaOS 5.0	The **rtcp-inactivity** parameter was introduced to the `voip` command.
ArubaOS 6.0	This was part of the `voip` command in the earlier version. `voip` command is now deprecated.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config mode on master controller

voice real-time-config

```
voice real-time-config
   config-enable
   no...
```

Description

This command enables the controller to analyze the call quality of the voice calls based on the RTP media streams.

Syntax

Parameter	Description	Default
`config-enable`	Enables the controller to analyze the call quality of the voice calls based on the RTP media streams.	disabled

Usage Guidelines

You can enable the controller to compute and display the call quality parameters such as Jitter, delay, packet loss, and R-value directly from the RTP media stream of the voice calls. **config-enable** enables the controller to analyze the call quality of the voice calls based on the RTP media streams.

Example

The following command enables the controller to analyze the RTP media streams for call quality reports:

```
(host) (config) #voice real-time-config
(host) (Configure Real-Time Analysis) #config-enable
```

Command History

Version	Description
ArubaOS 6.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config mode on master controller

voice sip

```
voice sip
   dialplan-profile <dial-plan profile>
   no...
   session-expiry <session-expiry>
   session-timer
```

Description

This command allows you to enable SIP session timer and associate a dial plan profile to the SIP ALG.

Syntax

Parameter	Description	Default
`dial-plan profile`	Name of the existing Dial plan profile to be associated to the SIP ALG.	_
`session-expiry`	Timeout value in seconds for the session timer. The range is 240 - 1200 seconds.	300 sec
`session-timer`	If enabled, the SIP session is terminated when no session refresh request is received within the timeout value.	disabled

Usage Guidelines

You can configure the SIP settings such as enabling the session timer and associating a dial plan profile to the SIP ALG. **session-timer** acts as a keep alive mechanism for the SIP sessions using the periodic session refresh requests from the user agents. The interval for the session refresh requests is determined through a negotiation mechanism. If a session refresh request is not received within the negotiated interval, the session is terminated. **session-expiry** is the timeout interval of the session timer configured on the SIP ALG.

Example

The following command enables session timer on the SIP ALG:

```
(host) (config) #voice sip
(host)(SIP settings) #session-timer
```

The following command sets the timeout value of the session timer to 400 seconds on the SIP ALG:

```
(host)(SIP settings) #session-expiry 400
```

The following command associates the dial plan profile, *default* to the SIP ALG:

```
(host)(SIP settings) #dialplan-profile default
```

Command History

Version	Description
ArubaOS 6.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config mode on master controller

voice sip-midcall-req-timeout

```
voice sip-midcall-req-timeout {enable | disable}
```

Description

This command enables or diables the SIP mid-call request timer.

Syntax

Parameter	Description
`enable`	Enables the SIP mid-call request timer.
`disable`	Disables the timer.

Usage Guidelines

You can enable the SIP mid-call request timer on the controller to clear the voip session if there is no response to a SIP mid-call request.

Example

The following command enables the SIP mid-call request timer:

```
(host) (config) #voice sip-mid-call-req-timeout enable
```

Command History

Version	Description
ArubaOS 5.0	The **sip-midcall-req-timeout** parameter was introduced to the `voip` command.
ArubaOS 6.0	This was part of the `voip` command in the earlier version. `voip` command is now deprecated.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config mode on master controller

vpdn group l2tp

```
vpdn group l2tp
   client configuration {dns|wins} <ipaddr1> [<ipaddr2>]
   disable|enable
   l2tp tunnel hello <seconds>
   no ...
   ppp authentication {CACHE-SECURID|CHAP|EAP|MSCHAP|MSCHAPv2|PAP}
   ppp securid cache <minutes>
```

Description

This command configures an L2TP/IPsec VPN connection.

Syntax

Parameter	Description	Range	Default
`client configuration`	Configures parameters for the remote clients.	—	—
`dns`	Configures a primary and optional secondary DNS server.	—	—
`wins`	Configures a primary and optional secondary WINS server.	—	—
`disable|enable`	Disables or enables termination of L2TP clients.	—	enabled
`l2tp tunnel hello`	Configures L2TP tunneling hello timeout, in seconds.	10-1440	60 seconds
`no`	Negates any configured parameter.	—	—
`ppp authentication`	Enables the protocols for PPP authentication. This list should match the L2TP configuration configured with the **vpn-dialer** command on the controller.	—	—
`CACHE-SECUR ID`	The controller caches Secure ID tokens so that the user does not need to reauthenticate each time a network connection is lost.	—	—
`CHAP`	Use CHAP with PPP authentication.	—	—
`EAP`	Use EAP-TLS with PPP authentication. Specify this protocol for Windows IPsec VPN clients that use Common Access Card (CAC) Smart Cards that contain user information and digital certificates.	—	—
`MSCHAP`	Use MSCHAP with PPP authentication.	—	—
`MSCHAPv2`	Use MSCHAPv2 with PPP authentication. This is the default for L2TP	—	—
`PAP`	Use PAP with PPP authentication.	—	—
`ppp securid`	If CACHE-SECURID is configured for PPP authentication, this specifies the time, in minutes, that the token is cached.	15-10080	1440 minutes

Usage Guidelines

L2TP/IPsec relies on the PPP connection process to perform user authentication and protocol configuration. You specify the protocol used for PPP authentication and whether SecureID tokens are cached on the controller. Client addresses are assigned from a pool configured with the **ip local pool** command.

Example

The following command configures virtual private dial-in networking:

```
(host) (coinfig) #vpdn group l2tp
  ppp authentication PAP
  client configuration dns 10.1.1.2
  client configuration wins 10.1.1.2
```

Command History

The command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

vpdn group pptp

```
vpdn group pptp
   client configuration {dns|wins} <ipaddr1> [<ipaddr2>]
   disable|enable
   no ...
   ppp authentication {MSCHAP|MSCHAPv2}
   pptp echo <seconds>
```

Description

This command configures a PPTP VPN connection.

Syntax

Parameter	Description	Range	Default
`client configuration`	Configures parameters for the remote clients.	—	—
`dns`	Configures a primary and optional secondary DNS server.	—	—
`wins`	Configures a primary and optional secondary WINS server.	—	—
`disable|enable`	Disables or enables termination of PPTP clients.	—	enabled
`no`	Negates any configured parameter.	—	—
`ppp authentication`	Enables the protocols for PPP authentication. This list should match the PPTP configuration configured with the **vpn-dialer** command on the controller.	—	—
`MSCHAP`	Use MSCHAP with PPP authentication.	—	—
`MSCHAPv2`	Use MSCHAPv2 with PPP authentication. This is the default for L2TP	—	—
`pptp echo`	Time, in seconds, that the controller waits for a PPTP echo response from the client before considering the client to be down. The client is disconnected if it does not respond within this interval.	10-300	60 seconds

Usage Guidelines

PPTP connections require user-level authentication through a PPP authentication protocol (MSHCAPv2 is the currently-supported method.) Client addresses are assigned from a pool configured with the **pptp** command.

Example

The following command configures virtual private dial-in networking:

```
vpdn group pptp
   ppp authentication MSCHAPv2
   client configuration dns 10.1.1.2
   client configuration wins 10.1.1.2
```

Command History

The command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

vpn-dialer

```
vpn-dialer <name>
   enable dnetclear|l2tp|pptp|securid_newpinmode|wirednowifi
   ike {authentication {pre-share <key>|rsa-sig}|encryption {3des|des}|
    group {1|2}|hash {md5|sha}|lifetime [<seconds>]}
   ipsec {encryption {esp-3des|esp-des}|hash {esp-md5-hmac|esp-sha-hmac}|
    lifetime [<seconds>]|pfs {group1|group2}}
   no {enable...|ipsec...|ppp...}
   ppp authentication {cache-securid|chap|mschap|mschapv2|pap}
```

Description

This command configures the VPN dialer.

Syntax

Parameter	Description	Range	Default
<name>	Name that identifies this VPN dialer configuration.	—	—
enable	Enables dialer operations:	—	—
dnetclear	Enables "split tunneling" functionality so that traffic destined for the internal network is tunneled while traffic for the Internet is not. This option is not recommended for security reasons.	—	disabled
l2tp	Allows the dialer to negotiate a Layer-2 Tunneling Protocol (L2TP)/ IPsec tunnel with the controller.	—	enabled
pptp	Allows the dialer to negotiate a Point-to-Point Tunneling Protocol (PPTP) with the controller.	—	disabled
securid_new pinmode	Supports SecurID new and next pin mode.	—	disabled
wirednowifi	Allows the dialer to detect when a wired network connection is in use, and shuts down the wireless interface.	—	disabled
ike	Configures internet key exchange (IKE) protocol. This configuration must match the IKE policy configured with the **crypto isakmp policy** command on the controller.	—	—
authentica tion	Specifies whether preshared keys or RSA signatures are used for IKE authentication.	pre-share | rsa-sig	pre-share
encryption	Specifies the IKE encryption protocol, either DES or 3DES.	3des | des	3des
group	Specifies the Diffie-Hellman group, either 1 or 2.	1 | 2	2
hash	Specifies the HASH algorithm, ether SHA or MD5.	md5 | sha	sha
lifetime	Specifies how long an IKE security association lasts, in seconds.	300-86400	28800 seconds
ipsec	Configures IPsec. This configuration must match the IPsec parameters configured with the **crypto dynamic-map** and **crypto ipsec** commands on the controller.	—	—
encryption	Specifies the encryption type for IPsec, either DES or 3DES.	esp-3des | esp-des	esp-3des
hash	Specifies the hash algorithm used by IPsec, either MD5 or SHA.	esp-md5-hmac | esp-sha- hmac	esp-sha-hmac

Parameter	Description	Range	Default
lifetime	Specifies how long an IPsec security association lasts, in seconds.	300-86400	7200 seconds
pfs	Specifies the IPsec Perfect Forward Secrecy (PFS) mode, either group 1 or group 2.	group1 | group2	group2
no	Negates any configured parameter.	—	—
ppp authentication	Enables the protocols for PPP authentication. This list should match the L2TP or PPTP configuration configured with the **vpdn** command on the controller.	—	—
cache-security id	The controller caches Secure ID tokens so that the user does not need to reauthenticate each time a network connection is lost.	—	disabled
chap	Use CHAP with PPP authentication.	—	enabled
mschap	Use MSCHAP with PPP authentication.	—	enabled
mschapv2	Use MSCHAPv2 with PPP authentication.	—	enabled
pap	Use PAP with PPP authentication.	—	enabled

Usage Guidelines

A VPN dialer is a Windows application that configures a Windows client for use with the VPN services in the controller. When VPN is used as an access method, a user can login using captive portal and download a VPN dialer. You can customize a VPN dialer for a user role configured with the **user-role** command. After the user authenticates via captive portal, a link appears to allow download of the VPN dialer if a dialer is configured for the user role.

Example

The following command configures a VPN dialer:

```
(host) (config) #vpn-dialer default-dialer
  ike authentication pre-share f00xYz123BcA
```

Command History

The command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

vrrp

```
vrrp <id>
   advertise <interval>
   authentication <password>
   description <text>
   ip address <ipaddr>
   no...
   preempt
   priority <level>
   shutdown
   tracking interface {fastethernet <slot>/<port>|gigabitethernet <slot>/<port>}
     {sub <value>}
   tracking master-up-time <duration> add <value>
   tracking vlan <vlanid> {sub <value>}
   tracking vrrp-master-state <vrid> add <value>
   vlan <vlanid>
```

Description

This command configures the Virtual Router Redundancy Protocol (VRRP).

Syntax

Parameter	Description	Range	Default
`id`	Number that uniquely identifies the VRRP instance, also known as the VRID. This number should match the VRID on the other member of the redundant pair. For ease in administration, you should configure this with the same value as the VLAN ID. After you configure the VRID, the command platform enters VRRP mode. From here, you can access the remaining VRRP commands.	1-255	—
`advertise`	Specifies the time, in seconds, between successive VRRP advertisements sent by the current *master*. Best practices are to use the default value.	1-60 seconds	1 second (1s=1000ms)
`authentication`	Configure an optional password of up to eight characters to be used to authenticate VRRP peers in their advertisements. The password must be the same on both members of the redundant pair. The password is sent in plain-text and therefore should not be treated as a security measure. Rather, the purpose of the password is to guard against misconfigurations in the event that other VRRP devices exist on the same network.	8 characters	—
`description`	Configure an optional text string to describe the VRRP instance.	1-80 characters	—
`ip address`	Configure the virtual IP address that will be owned by the elected VRRP *master*. Use the same IP address on each member of the redundant pair. This IP address will be redundant - it will be active on the VRRP master, and will become active on the VRRP backup in the event that the VRRP master fails. The IP address must be unique; the IP address cannot be the loopback address of the controller. Only IPv4 address formats are supported.	—	—
`no`	Negates all configured VRRP parameters.	—	—
`preempt`	Preempt mode allows a controller to take over the role of master if it detects a lower priority controller currently acting as master. Best practices are to use the default value to avoid excessive interruption to users or “flapping” if a problematic controller is cycling up and down.	—	disabled
`priority`	Defines the priority level of the VRRP instance for the controller. This value is used in the election mechanism for the master. A higher number specifies a higher priority. The default priority setting is adequate for most networks.	100	1-255
`shutdown`	Administratively shutdown VRRP. When down, VRRP is not active, although the controller maintains the configuration information. To start the VRRP instance, use **no shutdown**.	—	enabled (VRRP is down)
`tracking interface`	Configures VRRP tracking based on Layer-2 interface state transitions. You can configure this on Fast Ethernet or Gigabit Ethernet interfaces. You can track a combined maximum of 16 VLAN and Layer-2 interfaces.	—	—
`<slot>`	<slot> is always 1	—	—

Parameter	Description	Range	Default
<port>	Number assigned to the network interface embedded in the controller. Port numbers start at 0 from the left-most position.	—	—
sub	Decreases the priority of the VRRP instance by the specified amount. When the interface comes up again, the value is restored to the previous priority level. The combined priority and tracking vales cannot exceed 255. If the priority value exceeds 255, the controller displays an error message.	0-255	—
tracking master-up-time duration	Monitors how long the controller has been master for the VRRP instance.	0-1440 minutes	—
tracking master-up-time add	Instructs the controller to add the specified value to the existing priority level. The combined priority and tracking values cannot exceed 255. If the priority value exceeds 255, the controller displays an error message similar to the following: Error: Vrrp 30 priority + tracking value exceeds 255	0-255	—
tracking vlan	Configures VRRP tracking based on VLAN state transitions. You can track a combined maximum of 16 VLAN and Layer-2 interfaces.	—	—
sub	Decreases the priority of the VRRP instance by the specified amount. When the VLAN comes up again, the value is restored to the previous priority level. The combined priority and tracking values cannot exceed 255. If the priority value exceeds 255, the controller displays an error message.	0-255	—
vrrp-master-state	Specifies the VRID to use for tracking the state of the VRRP master controller.	1-255	—
vrrp-master-state add	Instructs the controller to add the specified value to the existing priority level. The combined priority and tracking values cannot exceed 255. If the priority value exceeds 255, the controller displays an error message similar to the following: Error: Vrrp 30 priority + tracking value exceeds 255	0-255	—
vlan	Specifies the VLAN ID of the VLAN on which VRRP will run.	1-4094	—

Usage Guidelines

Use this command to set parameters for VRRP on the controller. The default VRRP parameters can be left for most implementations.

You can use a combination of numbers, letters, and characters to create the authentication password and the VRRP description. To include a space in the password or description, enter quotation marks around the string. For example, to create the password Floor 1, enter “Floor 1” at the prompt.

To change the existing password or description, enter the command with a different string. The new password or description takes affect immediately.

To unconfigure the existing password or description, enter “” at the prompt. If you update the password on one controller, you must update the password on the redundant member pair.

Interface Tracking

You can track multiple VRRP instances to prevent asymmetric routing and dynamically change the VRRP master to adapt to changes in the network. VRRP interface tracking can alter the priority of the VRRP instance based on

the state of a particular VLAN or Layer-2 interface. The priority of the VRRP instance can increase or decrease based on the operational state of the specified interface. For example, interface transitions (up/down events) can trigger a recomputation of the VRRP priority, which can change the VRRP master depending on the resulting priority. You can track a combined maximum of 16 interfaces.

Note: You must enable preempt mode to allow a controller to take over the role of master if it detects a lower priority controller currently acting as master

Example

The following command configures a priority of 105 for VRRP ID (VRID) 30:

```
(host) (config) #vrrp 30
  priority 105
```

The following commands configure VLAN interface tracking and assumes the following:

- You have two controllers, a primary and a backup.
- The configuration highlights the parameters for interface tracking. You may have other parameters configured for VRRP.

Primary Configuration

```
vrrp 10
  vlan 10
  ip address 10.200.22.254
  priority 105
  preempt
  tracking vlan 20 sub 10

vrrp 20
  vlan 20
  ip address 10.200.22.254
  preempt
  priority 105
  tracking vlan 10 sub 10

vrrp 30
  vlan 30
  ip address 10.200.22.254
  preempt
  priority 105
  tracking vlan 20 sub 10
```

Backup Configuration

```
vrrp 10
  vlan 10
  ip address 10.200.22.254
  priority 100
  preempt
  tracking vlan 20 sub 10

vrrp 20
  vlan 20
  ip address 10.200.22.254
  preempt
  priority 100
  tracking vlan 10 sub 10

vrrp 30
  vlan 30
  ip address 10.200.22.254
  preempt
  priority 100
  tracking vlan 20 sub 10
```

If VLAN 20 goes down, VRRP 20 automatically fails over, VRRP 10 and VRRP 30 would drop their priority to 95, causing a failover to the backup controller. Once VLAN 20 comes back up, the primary controller restores the VRRP priority to 105 for all VRRP IDs and resumes the master VRRP role.

Command History

Version	Modification
ArubaOS 1.0	Command introduced
ArubaOS 3.3	The **tracking interface** and **tracking vlan** parameters were introduced.
ArubaOS 3.3.2	The **add** option was removed from the **tracking interface** and **tracking vlan** parameters.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master and local controllers

web-server

```
web-server
   captive-portal-cert <name>
   ciphers {high|low|medium}
   mgmt-auth [certificate] [username/password]
   no ...
   ssl-protocol [sslv2] [sslv3] [tlsvl]
   session-timeout <session-timeout>
   switch-cert <name>
   web-max-clients <web-max-clients>
```

Description

This command configures the controller's web server.

Syntax

Parameter	Description	Range	Default
`captive-portal-cert`	Name of the server certificate associated with captive portal. Use the **show crypto-local pki ServerCert** command to see the server certificates installed in the controller.	—	default
`ciphers`	Configures the strength of the cipher suite: **high**: encryption keys larger than 128 bits **low**: 56 or 64 bit encryption keys **medium**: 128 bit encryption keys	high, low, medium	high
`mgmt-auth`	Authentication method for the management user; you can choose to use either username/password or certificates, or both username/password and certificates.	username/password, certificate	username/password
`no`	Negates any configured parameter.	—	—
`session-timeout <session-timeout>`	Specifies the amount of time after which the WebUI session times out and requires login for continued access.	30-3600 seconds	900 seconds
`ssl-protocol`	Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol version used for securing communication with the web server: SSLv3 TLSv1	sslv3, tlsv1	sslv3, tlsv1
`switch-cert`	Name of the server certificate associated with WebUI access. Use the **show crypto-local pki ServerCert** command to see the server certificates installed in the controller.	—	default
`web-max-clients <web-max-client>`	Configures the web server's maximum number of supported concurrent clients.	25-400	—

Usage Guidelines

There is a default server certificate installed in the controller, however this certificate does not guarantee security in production networks. Best practices are to replace the default certificate with a custom certificate issued for your site by a trusted Certificate Authority (CA). See the *ArubaOS User Guide* for more information about how to generate a Certificate Signing Request (CSR) to submit to a CA and how to import the signed certificate received from the CA into the controller. After importing the signed certificate into the controller, use the **web-server** command to specify the certificate for captive portal or WebUI access. If you need to specify a different certificate for captive portal or WebUI access, use the **no** command to revert back to the default certificate before you specify the new certificate (see the Example section).

You can use client certificates to authenticate management users. If you specify certificate authentication, you need to configure certificate authentication for the management user with the **mgmt-user webui-cacert** command.

Example

The following commands configure WebUI access with client certificates only, and specify the server certificate for the controller:

```
(host) (config) #web-server mgmt-auth certificate
   switch-cert ServerCert1
   mgmt-user webui-cacert serial 1111111 web-admin root
```

To specify a different server certificate, use the **no** command to revert back to the default certificate *before* you specify the new certificate:

```
(host) (config) #web-server mgmt-auth certificate
   switch-cert ServerCert1
   no switch-cert
   switch-cert ServerCert2
```

Command History

Version	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.1	The **mgmt-auth** parameter was introduced.
ArubaOS 3.2	The **captive-portal-cert** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	The **web-server ciphers** and **web-server ssl-protocol** commands require the PEFNG license	Config mode on master controllers

whitelist-db cpsec add

```
whitelist-db
whitelist-db cpsec
whitelist-db cpsec add mac-address <mac-address>
   state {approved-ready-for-cert|certified-factory-cert} cert-type {switch-
   cert|factory-cert}
   [description <description>]
```

Description

Add an AP entry to the campus AP whitelist.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the AP you want to enter into the cpsec whitelist database.
`state`	Select one of the following AP states: • **approved-ready-for-cert**: The AP has been approved as a valid AP and is ready to receive a certificate. • **certified-factory-cert**: The AP is already has a factory certificate. APs in this state will not be re-issued a new certificate if control plane security is reenabled.
`cert-type`	Identify the type of certificate to be used by the AP. • **switch-cert**: AP is using a certificate signed by the controller. • **factory-cert**: AP is using a factory-installed certificate. This option should only be used for AP model types W-AP105 and W-AP120 Series.
`description`	(Optional) Enter a brief description of the AP. If the description includes spaces, you must enclose the description in quotation marks.

Usage Guidelines

You can manually add entries to the campus AP whitelist to grant valid APs secure access to the network.

Example

The following command creates a new campus AP whitelist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host) (config) #whitelist-db cpsec add mac-address 00:16:CF:AF:3E:E1
   state certified-factory-cert
   cert-type factory-cert
   description "An AP-105 model, apname AP-corp22"
```

Related Commands

Command	Description	Mode
`show whitelist-db cpsec`	Show the campus AP whitelist for the control plane feature.	Enable mode

Command History

Version	Modification
ArubaOS 5.0	Command introduced
ArubaOS 6.0	The c**ontroller-cert** parameter was modified to **switch-cert**.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on master or local controllers

whitelist-db cpsec delete

```
whitelist-db cpsec delete mac-address <mac-address>
```

Description

Remove an individual AP entry to the campus AP whitelist.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the AP you want to remove from the campus AP whitelist.

Usage Guidelines

Use this command to remove an individual whitelist entries for an AP that has been either removed from the network, or is no longer a candidate for automatic certificate provisioning. If the AP whose entry you deleted is still connected to the network and the control plane security feature is configured to send certificates to all APs (or a range of addresses that include that AP), then the controller will send the AP another certificate, and the AP will reappear in the campus whitelist. To permanently revoke a certificate from an invalid or suspected rogue AP, use the command whitelist-db cpsec revoke.

Example

The following command removes an AP with the MAC address 10:14:CA:AF:3E:E1 from the campus AP whitelist.:

```
(host) (config) #whitelist-db cpsec delete mac-address 10:14:CA:AF:3E:E1
```

Related Commands

Command	Description	Mode
`show whitelist-db cpsec`	Show the campus AP whitelist for the control plane feature.	Enable mode

Command History

This command was introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on master or local controllers

whitelist-db cpsec modify

```
whitelist-db cpsec modify mac-address
   cert-type switch-cert|factory-cert
   description <description>
   mode disable|enable
   revoke-text <revoke-text>
   state approved-ready-for-cert|certified-factory-cert
```

Description

Modify an existing entry in the campus AP whitelist.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the AP you want to enter into the cpsec whitelist database.
`cert-type`	Identify the type of certificate to be used by the AP. • **switch-cert**: AP is using a certificate signed by the controller. • **factory-cert**: AP is using a factory-installed certificate. This option should only be used for AP model types W-AP105 and W-AP120 Series.
`description`	(Optional) Enter a brief description of the AP. If the description includes spaces, you must enclose the description in quotation marks.
`mode`	Select **disable** to disable an AP's entry in the campus AP whitelist. A disabled AP will not be able to contact the controller via a secure channel. Select **enable** to reenable a disabled AP.
`revoke-text`	If you disable an AP entry, the revoke-text parameter allows you to enter a brief text string describing why the AP was revoked.
`state`	Select one of the following AP states: • **approved-ready-for-cert**: AP has been approved state and is ready to receive a certificate. • **certified-factory-cert**: AP is certified and has a factory-installed certificate.

Example

The following command changes the certificate type, AP state and description of the AP with the MAC address 00:1E:37:CB:D4:52:

```
(host) (config) #whitelist-db cpsec modify mac-address 00:1E:37:CB:D4:52
   cert-type switch-cert
   state certified-factory-cert
   description "An AP-12x model, apname AP-corp16"
```

Related Commands

Command	Description	Mode
`show whitelist-db cpsec`	Show the campus AP whitelist for the control plane feature.	Enable mode

Command History

Version	Modification
ArubaOS 5.0	Command introduced
ArubaOS 6.0	The **controller-cert** parameter was modified to **switch-cert**.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on master or local controllers

whitelist-db cpsec revoke

```
whitelist-db cpsec revoke mac-address <mac-address> revoke-text <revoke-text>
```

Description

Revoke a certificate from an AP in the campus AP whitelist.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the AP you want to remove from the cpsec whitelist database.
`revoke-text <revoke-text>`	A brief description why the AP's certificate was revoked, up to 64 alphanumeric characters. If this comment includes spaces, you must enclose the comment in quotation marks.

Usage Guidelines

Use this command to revoke a certificate from a invalid or suspected rogue AP.

Example

The following command revokes a certificate from an AP. This command does not delete a whitelist entry for a revoked AP, but marks its entry with the revoked state.

```
(host) (config) #whitelist-db cpsec revoke mac-address 00:1E:37:CA:D4:51
   revoke-text "revoking cert from a rogue AP."
```

Related Commands

Command	Description	Mode
`show whitelist-db cpsec`	Show the campus AP whitelist for the control plane feature.	Enable mode

Command History

This command was introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on master or local controllers

whitelist-db cpsec purge

```
whitelist-db cpsec purge
```

Description

Clear the campus AP whitelist.

Syntax

No parameters.

Usage Guidelines

Use this command to clear all entries in the entire campus AP whitelist. If your network includes both master and local controllers, then each campus AP whitelist is synchronized across all controllers. If you purge the entire campus AP whitelist on one controller, that action will clear the campus AP whitelist on every controller in the network. To delete an individual entry in the campus AP whitelist, use the command whitelist-db cpsec delete.

Example

The following command remove all APs from the campus AP whitelist:

```
(host) (config) #whitelist-db cpsec purge
```

Related Commands

Command	Description	Mode
`show whitelist-db cpsec`	Show the campus AP whitelist for the control plane feature.	Enable mode

Command History

This command was introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on master or local controllers

whitelist-db cpsec-local-switch-list

```
whitelist-db cpsec-local-switch-list
   del mac-address <mac-address>
   purge
```

Description

Delete a local controller from the local switch whitelist.

Syntax

Parameter	Description
`del mac-address <mac-address>`	Remove a single controller from the local switch whitelist.
`purge`	Clear all entries from the local switch whitelist

Usage Guidelines

If your deployment includes both master and local controllers, then the campus AP whitelist on each controller contains an entry for every AP on the network, regardless of the controller to which it is connected. The master controller also maintains a whitelist of local controllers with APs using control plane security. When you change a campus AP whitelist on any controller, that controller contacts the master controller to check the local switch whitelist, then contacts every other controller on the local switch whitelist to notify it of the change.

If you ever remove a local controller from the network, you must also remove the local controller from the local switch whitelist. If the local switch whitelist contains entries for local controllers no longer on the network, then a campus AP whitelist entry can be marked for deletion but will not be physically deleted, as the controller will be waiting for an acknowledgement from another controller no longer on the network. Any unused local controller entries in the local switch whitelist can significantly increase network traffic and reduce controller memory resources.

Example

The following command removes a local controller from the local switch whitelist:

```
(host) (config) #whitelist-db cpsec-local-switch-list del mac-address 00:1E:33:CA:D2:51
```

Related Commands

Command	Description	Mode
`show whitelist-db cpsec-local-switch-list`	Show the local switch whitelist for the control plane feature.	Enable mode

Command History

Version	Modification
ArubaOS 5.0	Command introduced
ArubaOS 6.0	The **cpsec-local-ctlr-list** parameter was modified to **cpsec-local-switch-list**

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

whitelist-db cpsec-master-switch-list

```
whitelist-db cpsec-master-switch-list
   del mac-address <mac-address>
   purge
```

Description

Delete a master controller from the master switch whitelist.

Syntax

Parameter	Description
`del mac-address <mac-address>`	Remove a single master controller from the master switch whitelist.
`purge`	Clear all entries from the master switch whitelist

Usage Guidelines

Each local controller using the control plane security feature has a master switch whitelist which contains the IP and MAC addresses of its master controller. If your network has a redundant master controller, then this whitelist will contain more than one entry.

The master switch whitelist rarely needs to be purged. Although you can delete an entry from the master switch whitelist, you should do so only if you have removed a master switch from the network. Deleting a valid master controller from the master switch whitelist can cause errors in your network.

Example

The following command removes a master controller from the master switch whitelist

```
(host) (config) #whitelist-db cpsec-master-switch-list del mac-address
00:1E:33:CA:D2:51
```

Related Commands

Command	Description	Mode
`show whitelist-db cpsec-master-switch-list`	show the master switch whitelist for the control plane feature.	Enable mode

Command History

Version	Modification
ArubaOS 5.0	Command introduced
ArubaOS 6.0	The **cpsec-master-ctrlr-list** parameter was modified to **cpsec-master-switch-list**

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on local controllers

whoami

```
whoami
```

Description

This command displays information about the current user logged into the controller.

Syntax

No parameters.

Usage Guidelines

Use this command to display the name and role of the user who is logged into the controller for this session.

Example

The following command displays information about the user logged into the controller:

```
(host) #whoami
```

Command History

This command was available in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config modes on master and local controllers

wlan dot11k-profile

```
wlan
wlan dotllk <profile>
   bcn-measurement-mode {active|beacon-table|passive}
   clone <profile>
   dot11k-enable
   force-disassoc
   bcn-req-time
   lm-req-time
   tsm-req-time
   channel-enable
   bcn-req-chan-11a
   bcn-req-chan-11bg
   handover-threshold
   handover-trigger
   no ...
```

Description

Configure a 802.11k radio profile.

Syntax

Parameter	Description	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	“default”
`bcn-measurement-mode`	Configures an **active**, **beacon-table** or **passive** beacon measurement mode for the profile.	beacon-table
`active`	Enables **active** beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If the station doesn't support active measurement mode, it returns a Beacon Measurement Report with the *Incapable* bit set in the *Measurement Report Mode* field.	—
`beacon-table`	Enables **beacon-table** beacon measurement mode.In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. This is the default beacon measurement mode. **NOTE:** If a station doesn't support beacon-table able measurement mode, it returns a Beacon Measurement Report with the *Incapable* bit set in the *Measurement Report Mode* field.	—
`passive`	Enables **passive** beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If a station doesn't support passive measurement mode, it returns a Beacon Measurement Report with the *Incapable* bit set in the *Measurement Report Mode* field.	—
`clone <profile>`	Copy settings from another specified 802.11k profile.	—
`dot11k-enable`	Enables the 802.11K feature. This feature is disabled by default.	Disabled
`force-dissasoc`	This feature allows the AP to forcefully disassociate “on-hook” voice clients (clients that are not on a call) after period of inactivity. Without the forced disassociation feature, if an AP has reached its call admission control limits and an on-hook voice client wants to start a new call, that client may be denied. If forced disassociation is enabled, those clients can associate to a neighboring AP that can fulfil their QoS requirements. This feature is disabled by default.	Disabled
`bcn-req-time`	This option configures the time duration between two consecutive beacon requests sent to a dot11K client. By default, the beacon requests are sent to a dot11K client every 60 seconds. However, if a different value is required, the `bcn-req-time` option can be used. This permits values in the range from 10 seconds to 200 seconds.	60 seconds
`lm-req-time`	This option configures the time duration between two consecutive link measurement requests sent to an dot11K client. By default, link measurement requests are sent to a dot11K client every 61 seconds. However, you can use the `lm-req-time` option to specify different time interval. This permits values in the range from 10 seconds to 200 seconds.	61 seconds

Parameter	Description	Default
`tsm-req-time`	This option configures the time duration between two consecutive transmit stream measurement requests sent to a dot11K client. By default, the transmit stream measurement requests are sent to a dot11K client every 90 seconds. However, you can use the `tsm-req time` option to specify a different time interval. This permits values in the range from 10 seconds to 200 seconds.	90 seconds
`channel-enable`	A Beacon Request sent to a client contains a "Channel" field. By default, this field contains one of the following values: • 0: Indicates a request to make iterative measurements for all supported channels in the regulatory class where the measurement is permitted on the channel and the channel is valid for the current regulatory domain. • 255: Indicates a request to make iterative measurements for all supported channels in the current regulatory class listed in the latest AP channel Report received from the serving AP. • <any-other-value>: The channel on which the AP is currently active	
`bcn-req-chan-11a`	This value is sent in the 'Channel' field of the beacon requests on the 'A' radio. You can specify values in the range 34 to 165.	
`bcn-req-chan-11bg`	This value is sent in the 'Channel' field of the Beacon Requests on the 'BG' radio. You can specify values in the range 1 to 14.	
`handover-threshold`	The threshold value is the best signal strength (dbm) of a WiFi signal received by a voice client from all the APs. You can specify a threshold value to trigger the handover process if the signal strength is equal to or lesser than the threshold value. Threshold values can be specified in the range 20 to 70.	50
`handover-trigger`	If this parameter is enabled, the controller will initiate the handover of a voice client (for example: dual mode handsets) roaming at the edge of WiFi coverage to an alternate carrier or connection. The handover trigger is initiated if the WiFi signal strength reported by the voice client (received from all APs) is equal to or less than the threshold value. You must enable dot11k before using this command.	
no	Negates or removes any configured parameter	

Usage Guidelines

In a 802.11k network, if the AP with the strongest signal is reaches its maximum capacity, clients may connect to an under utilized AP with a weaker signal. A 802.11k profile can assigned to each virtual AP.

Example

The following command enables the 802.11k feature on the 802.11k profile and configures the beacon measurement mode and specifies the time interval for beacon, link, and transmit stream measurement requests.

```
(host) (config) #wlan dot11k-profile default
(host) (802.11K Profile "default") #dot11k-enable
(host) (802.11K Profile "default") #bcn-measurement-mode beacon-table
(host) (802.11K Profile "default") #bcn-req-time 60
(host) (802.11K Profile "default") #lm-req-time 60
(host) (802.11K Profile "default") #tsm-req-time 90
```

The following command enables the handover-trigger process if the best WiFi signal strength reported by a voice client is -60dbm or lesser.

```
(host) (802.11K Profile "default") #handover-trigger
(host) (802.11K Profile "default") #handover-threshold 60
```

Command History

This command was introduced in ArubaOS 3.4.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on master controllers

wlan client-wlan-profile

```
wlan client-wlan-profile <profile>
   auth-as-computer
   auth-as-guest
   clone
   eap-cert
   eap-cert-connect-only-to
   eap-peap
   eap-peap-connect-only-to
   eap-type
   enable-8021x
   ieap-cert-connect-only
   inner-eap
   inner-eap-type
   no
   non-broadcasting-connection
   range-connect
   ssid-profile
```

Description

You can push WLAN profiles to users computers that use the Microsoft Windows Wireless Zero Config (WZC) service to configure and maintain their wireless networks. After the WLAN profiles are pushed to user computers, they are automatically displayed as an ordered list in the preferred networks.

Syntax

Parameter	Description	Default
auth-as-computer	Authenticate with domain credentials.	
auth-as-guest	Authenticate as a guest user.	
clone	Copy settings from another WLAN client profile.	
eap-cert	If you select EAP type as certificate, you can use one of the following options: • mschapv2-use-windows-credentials • use-smartcard • simple-certificate-selection • use-different-name • validate-server-certificate	—
eap-cert-connect-only-to	Comma separated list of servers.	
eap-peap	Configure EAP-PEAP settings.	
eap-peap-connect-only-to	Comma separated list of servers.	
eap-type	Enter a EAP type used by client to connect to wireless network.	EAP-PEAP
enable-8021x	Select this option to enable 802.1x authentication for this network.	Enabled
ieap-cert-connect-only	Command separated list of servers	
inner-eap	Enter the inner EAP type.	EAP-MSCHAPv2
inner-eap-type	Specify one of the following: • mschapv2-use-windows-credentials: Automatically use the Windows logon name and password (and domain if any) • use-smartcard: Use a smart card • simple-certificate-selection: Use a certificate on the users computer or use a simple certificate selection method (recommended) • validate-server-certificate: Validate the server certificate • use-different-name: Use a different user name for the connection (and not the CN on the certificate)	
no	Negate and reset all configuration settings.	
non-broadcasting-connection	Connect even if WLAN is not broadcasting.	Disabled
range-connect	Automatically connect to this WLAN if in range.	
ssid-profile	Enter the name of the SSID profile.	

Command History

This command was introduced in ArubaOS 5.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system on master controllers	Config mode on master controllers

wlan edca-parameters-profile

```
wlan
wlan edca-parameters-profile {ap|station} <profile>
   {background | best-effort | video | voice}
   [acm][aifsn <number>] [ecw-max <exponent> [ecw-min <exponent>] [txop <number>]
   [clone <profile>
```

Description

This command configures an enhanced distributed channel access (EDCA) profile for APs or for clients (stations).

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`background`	Configures the background queue.	—	—
`best-effort`	Configures the best-effort queue.	—	—
`video`	Configures the video queue.	—	—
`voice`	Configures the voice queue.	—	—
`acm`	Specifies mandatory admission control. The client reserves the access category through traffic specification (TSPEC) signaling. Enter 1 to enable, 0 to disable.	0, 1	0 (disabled)
`aifsn`	Arbitrary inter-frame space number.	1-15	0
`ecw-max`	The exponential (n) value of the maximum contention window size, as expressed by 2^n-1. A value of 4 computes to 2^4-1 = 15.	1-15	0
`ecw-min`	The exponential (n) value of the minimum contention window size, as expressed by 2^n-1. A value of 4 computes to 2^4-1 = 15.	0-15	0
`txop`	Transmission opportunity, in units of 32 microseconds. Divide the desired transmission duration by 32 to determine the value to configure. For example, for a transmission duration of 3008 microseconds, enter 94 (3008/32).	0-2047	0
`clone`	Name of an existing EDCA profile from which parameter values are copied.	—	—

Usage Guidelines

EDCA profiles are specific either to APs or clients. You apply an EDCA profile to a specific SSID profile. use this command only under the guidance of your Dell technical support representative.

The following are the default values configured for APs:

Access Category	ecw-min	ecw-max	aifsn	txop	acm
best-effort	4	6	3	0	No
background	4	10	7	0	No
video	3	4	1	94	No
voice	2	3	1	47	No

The following are the default values configured for clients:

Access Category	ecw-min	ecw-max	aifsn	txop	acm
best-effort	4	10	3	0	No
background	4	10	7	0	No
video	3	4	2	94	No
voice	2	3	2	47	No

Example

The following command configures an EDCA profile for APs:

```
(host) (config) #wlan edca-parameters-profile ap edca1
  best-effort ecw-min 15 ecw-max 15 aifsn 15 txop 100 acm 1
```

Command History

Version	Description
ArubaOS 3.1	Command introduced.
ArubaOS 3.4.1	License requirements changed in ArubaOS 3.4.1, so the command requires the PEF license instead of the Voice Services Module license required in earlier versions.

This command was introduced in ArubaOS 3.1.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config mode on master controllers

wlan ht-ssid-profile

```
wlan ht-ssid-profile <profile>
   40MHz-enable
   allow-weak-encryption
   clone <profile>
   high-throughput-enable
   legacy-stations
   max-rx-a-mpdu-size {8191|16383|32767|65535}
   max-tx-a-mpdu-size <bytes>
   min-mpdu-start-spacing {0|.25|.5|1|2|4|8|16}
   mpdu-agg
   no...
   short-guard-intvl-40MHz
   supported-mcs-set <mcs-list>
```

Description

This command configures a high-throughput SSID profile.

Syntax

Parameter	Description	Range	Default
<profile>	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”
40MHz-enable	Enables or disables the use of this high-throughput SSID in 40 MHz mode.	—	enabled
allow-weak-encryption	Enabling the use of TKIP or WEP for unicast traffic disables A-MPDU aggregation but allows the association to proceed. Disabling this prevents stations using TKIP or WEP for unicast traffic from associating at all. It is disabled by default.	—	disabled
clone	Name of an existing high-throughput SSID profile from which parameter values are copied.	—	—
high-throughput-enable	Determines if this high-throughput SSID allows high-throughput (802.11n) stations to associate. Enabling high-throughput in an ht-ssid-profile enables Wi-Fi Multimedia (WMM) base features for the associated SSID.	—	enabled
legacy-stations	Controls whether or not legacy (non-HT) stations are allowed to associate with this SSID. By default, legacy stations are allowed to associate. This setting has no effect on a BSS in which HT support is not available.	—	enabled
max-rx-a-mpdu-size	Controls the maximum size, in bytes, of an Aggregated-MAC Packet Data Unit (A-MPDU) that can be received on this high-throughput SSID.	8191/16383/32767/65535	65535
8191	Maximum size of 8191 bytes.		
16383	Maximum size of 16383 bytes.		
32767	Maximum size of 32767 bytes.		
65535	Maximum size of 65535 bytes.		
max-tx-a-mpdu-size	Controls the maximum size, in bytes, of an A-MPDU that can be sent on this high-throughput SSID.	1576-65535	65535
min-mpdu-start-spacing	Minimum time between the start of adjacent MDPUs within an aggregate MDPU in microseconds.	0/.25/.5/1/2/4/8/16	0
0	No restriction on MDPU start spacing.		
.25	Minimum time of .25 µsec.		
.5	Minimum time of .5 µsec.		
1	Minimum time of 1 µsec.		
2	Minimum time of 2 µsec.		
4	Minimum time of 4 µsec.		
8	Minimum time of 8 µsec.		
16	Minimum time of 16 µsec.		
mpdu-agg	Enables or disables MAC protocol data unit (MDPU) aggregation.	—	enabled
no	Negates any configured parameter.	—	—
short-guard-intvl-40MHz	Enables or disables use of short guard interval in 40 MHz mode of operation.		enabled

Parameter	Description	Range	Default
`supported-mcs-set`	Comma-separated list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this high-throughput SSID.	0-15	0-15

Usage Guidelines

The ht-ssid-profile configures the high-throughput SSID.

Note: AP configuration settings related to the IEEE 802.11n standard are configurable for Dell W-AP120 series access points, which are IEEE 802.11n standard compliant devices.

De-aggregation of MAC Service Data Units (A-MSDUs) is supported on the W-3000 Controller Series controller with a maximum frame transmission size of 4k bytes; however, this feature is always enabled and is not configurable. Aggregation is not currently supported.

Example

The following command configures the maximum size of a received aggregate MDPU to be 8191 bytes for the high-throughput SSID named "htcorpnet:"

```
(host) (config) #wlan ht-ssid-profile htcorpnet
   max-rx-a-mpdu-size 8191
```

Command History

Version	Description
ArubaOS 3.3	Command introduced
ArubaOS 3.3.1	The **legacy-stations** parameter was introduced
ArubaOS 3.3.2	De-aggregation of MAC Service Data Units (A-MSDUs) was introduced

Command Information

Platforms	Licensing	Command Mode
All platforms but operates with IEEE 802.11n compliant devices only	Base operating system	Config mode on master controllers

wlan ssid-profile

```
wlan ssid-profile <profile>
   902il-compatibility-mode
   a-basic-rates <mbps>
   a-beacon-rate
   a-tx-rates <mbps>
   ageout <seconds>
   battery-boost
   clone <profile>
   deny-bcast
   disable-probe-retry
   dtim-period <milliseconds>
   edca-parameters-profile {ap|station} <profile>
   essid <name>
   g-basic-rates <mbps>
   g-beacon-rate
   g-tx-rates <mbps>
   hide-ssid
   ht-ssid-profile <profile>
   local-probe-response
   max-clients <number>
   max-retries <number>
   max-tx-fail <number>
   mcast-rate-opt
   no ...
   opmode {dynamic-wep opensystem static-wep wpa-aes wpa-psk-aes wpa-psk-tkip wpa-tkip
    wpa2-aes wpa2-psk-aes wpa2-psk-tkip wpa2-tkip xSec}
   rts-threshold <number>
   short-preamble
   ssid-enable
   strict-svp
   wepkey1 <key>
   wepkey2 <key>
   wepkey3 <key>
   wepkey4 <key>
   weptxkey <index>
   wmm
   wmm-be-dscp <best-effort>
   wmm-bk-dscp <background>
   wmm-ts-min-inact-int <milliseconds>
   wmm-vi-dscp <video>
   wmm-vo-dscp <voice>
   wpa-hexkey <psk>
   wpa-passphrase <string>
```

Description

This command configures an SSID profile.

Syntax

Parameter	Description	Range	Default
<profile>	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”

Parameter	Description	Range	Default
`902il-compatibility-mode`	(For clients using NTT DoCoMo 902iL phones only) When enabled, the controller does not drop packets from the client if a small or old initialization vector value is received. (When TKIP or AES is used for encryption and TSPEC is enabled, the phone resets the value of the initialization vector after add/delete TSPEC.) **NOTE:** This parameter requires the PEFNG license.	—	disabled
`a-basic-rates`	List of supported 802.11a rates, in Mbps, that are advertised in beacon frames and probe responses.	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 12, 24 Mbps
`a-beacon-rate`	Sets the beacon rate for 802.11a (use for Distributed Antenna System (DAS) only). Using this parameter in normal operation may cause connectivity problems.	default, 6, 9, 12, 18,24,36,48 ,54 Mbps	minimum valid rate
`a-tx-rates`	Set of 802.11a rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error/loss rate of the client.	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
`ageout`	Time, in seconds, that a client is allowed to remain idle before being aged out.		1000 seconds
`battery-boost`	Converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval. The longer interval keeps associated wireless clients from activating their radios for multicast indication and delivery, leaving them in power-save mode longer and thus lengthening battery life. **NOTE:** This parameter requires the PEFNG license.	—	disabled
`clone`	Name of an existing SSID profile from which parameter values are copied.	—	—
`deny-bcast`	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.	—	disabled
`disable-probe-retry`	Enable or disable battery MAC level retries for probe response frames. By default this parameter is enabled, which mean that MAC level retries for probe response frames is disabled.		Enabled
`dtim-period`	Specifies the interval, in milliseconds, between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that employ power management features to sleep, the client must revive at least once during the DTIM period to receive broadcasts.		1
`edca-parameters-profile`	Name of the enhanced distributed channel access (EDCA) profile that applies to this SSID. **NOTE:** This parameter requires the PEFNG license. Configure this parameter only under the guidance of your Dell representative.	—	—
`ap|sta`	Assigns the specified EDCA profile to AP or station (client).	—	—
`essid`	Name that uniquely identifies a wireless network. The ESSID can be up to 31 characters. If the ESSID includes spaces, you must enclose it in quotation marks.	—	aruba-ap
`g-basic-rates`	List of supported 802.11b/g rates that are advertised in beacon frames and probe responses.	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2 Mbps

Parameter	Description	Range	Default
g-beacon-rate	Sets the beacon rate for 802.11g (use for Distributed Antenna System (DAS) only). Using this parameter in normal operation may cause connectivity problems.	default, 1,2,5, 6 9, 11, 12, 18, 24, 36, 48, 54 Mbps	minimum valid rate
g-tx-rates	Set of 802.11b/g rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error/loss rate of the client.	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
hide-ssid	Enables or disables hiding of the SSID name in beacon frames. Note that hiding the SSID does very little to increase security.	—	disabled
ht-ssid-profile	Name of high-throughput SSID profile to use for configuring high-throughput support. See “wlan ht-ssid-profile” on page 21.	—	“default”
local-probe-response	Enable or disable local probe response on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients’ probe requests. If this option is disabled, then the controller sends the 802.11 probe responses.	—	enabled
max-clients	Maximum number of wireless clients for the AP.	0-256	64
max-retries	Maximum number of retries allowed for the AP to send a frame.	0-15	4
max-tx-fail	Maximum transmission failures allowed before the client gives up.		0
mcast-rate-opt	Enables or disables scanning of all active stations currently associated to an AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate. **NOTE:** Do not enable this parameter unless instructed to do so by your Dell technical support representative.	—	disabled
no	Negates any configured parameter.	—	—
opmode	The layer-2 authentication and encryption to be used on this ESSID to protect access and ensure the privacy of the data transmitted to and from the network.	(see following)	opensystem
dynamic-wep	WEP with dynamic keys.		
opensystem	No authentication and encryption.		
static-wep	WEP with static keys.		
wpa-aes	WPA with AES encryption and dynamic keys using 802.1x.		
wpa-psk-aes	WPA with AES encryption using a preshared key.		
wpa-psk-tkip	WPA with TKIP encryption using a preshared key.		
wpa-tkip	WPA with TKIP encryption and dynamic keys using 802.1x.		
wpa2-aes	WPA2 with AES encryption and dynamic keys using 802.1x.		
wpa2-psk-aes	WPA2 with AES encryption using a preshared key.		
wpa2-psk-tkip	WPA2 with TKIP encryption using a preshared key.		
wpa2-tkip	WPA2 with TKIP encryption and dynamic keys using 802.1x.		
wpa-psk-aes	WPA with AES encryption using a preshared key.		
wpa2-psk-tkip	WPA2 with TKIP encryption using a preshared key.		

Parameter	Description	Range	Default
wpa2-tkip	WPA2 with TKIP encryption and dynamic keys using 802.1x.		
xSec	Encryption and tunneling of Layer-2 traffic between the controller and wired or wireless clients, or between controllers. To use xSec encryption, you must use a RADIUS authentication server. For clients, you must install the Funk Odyssey client software. Requires installation of the xSec license. For xSec between controllers, you must install an xSec license in each controller.		
rts-threshold	Wireless clients transmitting frames larger than this threshold must issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS). This helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting.		2333 bytes
short-preamble	Enables or disables short preamble for 802.11b/g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble. Legacy client devices that use only long preamble generally can be updated to support short preamble.	—	enabled
ssid-enable	Enables/disables this SSID.	—	enabled
strict-svp	Enable Strict Spectralink Voice Protocol (SVP)	—	disabled
wepkey1 - wepkey4	Static WEP key associated with the key index. Can be 10 or 26 hex characters in length.	—	—
weptxkey	Key index that specifies which static WEP key is to be used. Can be 1, 2, 3, or 4.	1, 2, 3, 4	1
wmm	Enables or disables WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF). WMM provides prioritization of specific traffic relative to other traffic in the network.	—	disabled
wmm-be-dscp	DSCP value used to map WMM best-effort traffic.	0-255	24
wmm-bk-dscp	DSCP used to map WMM background traffic.	0-255	8
wmm-ts-min-inact-int	Specifies the minimum inactivity time-out threshold of WMM traffic. This setting is useful in environments where low inactivity interval time-outs are advertised, which may cause unwanted timeouts.	0-3,600,000	0 milliseconds
wmm-uapsd	Enable Wireless Multimedia (WMM) UAPSD powersave.	—	enabled
wmm-vi-dscp	DSCP used to map WMM video traffic.	0-255	40
wmm-vo-dscp	DSCP used to map WMM voice traffic.	0-255	56
wpa-hexkey	WPA pre-shared key (PSK).	—	—
wpa-passphrase	WPA passphrase with which to generate a pre-shared key (PSK).	—	—

Usage Guidelines

The SSID profile configures the SSID.

Note: AP configuration settings related to the IEEE 802.11n standard are configurable for Dell's W-AP120 series access points, which are IEEE 802.11n standard compliant devices.

Default WMM mappings exist for all SSIDs. After you customize an WMM mapping and apply it to the SSID, the controller overwrites the default mapping values and uses the user-configured values.

Multicast Rate Optimization

The Multicast Rate Optimization feature dynamically selects the rate for sending broadcast/multicast frames on any BSS. This feature determines the optimal rate for sending broadcast and multicast frames based on the lowest of the unicast rates across all associated clients.

When the Multicast Rate Optimization option (mcast-rate-opt) is enabled, the controller scans the list of all associated stations in that BSS and finds the lowest transmission rate as indicated by the rate adaptation state for each station. If there are no associated stations in the BSS, it selects the lowest configured rate as the transmission rate for broadcast and multicast frames.

This feature is disabled by default. Multicast Rate Optimization applies to broadcast and multicast frames only. 802.11 management frames are not affected by this feature and will be transmitted at the lowest configured rate.

Note: The Multicast Rate Optimization feature should only be enabled on a BSS where all associated stations are sending or receiving unicast data. If there is no unicast data to or from a particular station, then the rate adaptation state may not accurately reflect the current sustainable transmission rate for that station. This could result in a higher packet error rate for broadcast/multicast packets at that station.

Example

The following command configures an SSID for WPA2 AES authentication:

```
(host) (config) #wlan ssid-profile corpnet
   ssid Corpnet
   opmode wpa2-aes
```

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	The **wmm-ts-min-inact-int** parameter was introduced.The **wpa2-preauth** parameter was removed,
ArubaOS 3.3	Support for the high-throughput IEEE 802.11n standard was introduced including the **ht-ssid-profile** parameter and various rate changes.
ArubaOS 3.3.1	Support for configurable WMM AC mapping was introduced including the **wmm-be-dscp**, **wmm-bk-dscp**, **wmm-vi-dscp**, and **wmm-vo-dscp** parameters.
ArubaOS 3.4	The **deny-bcas**t and **disable-probe-retry** parameters were introduced. The **drop-mcast** parameter was deprecated.
ArubaOS 3.4.1	License requirements changed in ArubaOS 3.4.1, so the command required the PEF license instead of the Voice Services Module license required in earlier versions.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system except for the noted parameters	Config mode on master controllers

wlan traffic-management-profile

```
wlan traffic-management-profile <profile>
   bw-alloc virtual-ap <virtual-ap> share <percent>
   clone <profile>
   no ...
   report-interval <minutes>
   shaping-policy default-access|fair-access|preferred-access
```

Description

This command configures a traffic management profile.

Syntax

Parameter	Description	Range	Default
<profile>	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
bw-alloc	Minimum bandwidth, as a percentage of available bandwidth, allocated to an SSID when there is congestion on the wireless network. An SSID can use all available bandwidth if no other SSIDs are active.		
virtual-ap	Name of the virtual AP profile which pertains to the SSID.	—	—
share	Percentage of available bandwidth allocated to this SSID.	0-100	—
clone	Name of an existing traffic management profile from which parameter values are copied.	—	—
no	Negates any configured parameter.	—	—
report-interval	Number of minutes between bandwidth usage reports.		5 minutes
shaping-policy	Define Station Shaping Policy This feature has the following three options: • **default-access**: Traffic shaping is disabled, and client performance is dependent on MAC contention resolution. This is the default traffic shaping setting. • **fair-access**: Each client gets the same airtime, regardless of client capability and capacity. This option is useful in environments like a training facility or exam hall, where a mix of 802.11a/g, 802.11g and 802.11n clients need equal to network resources, regardless of their capabilities. The **bw-alloc** parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network.You must set traffic shaping to f**air-access** to use this bandwidth allocation value for an individual virtual AP. • **preferred-access**: High-throughput (802.11n) clients do not get penalized because of slower 802.11a/g or 802.11b transmissions that take more air time due to lower rates. Similarly, faster 802.11a/g clients get more access than 802.11b clients.	default-access fair-access preferred-access	default-access

Usage Guidelines

The traffic management profile allows you to allocate bandwidth to SSIDs. When you enable the band-steering feature, an AP keeps track of all BSSIDs active on a radio, all clients connected to the BSSID, and 802.11a/g, 802.11b, or 802.11n capabilities of each client. Every sampling period, airtime is allocated to each client, giving it

opportunity to get and receive traffic. The specific amount of airtime given to an individual client is determined by;

- Client capabilities (802.11a/g, 802.11b or 802.11n)
- Amount of time the client spent receiving data during the last sampling period
- Number of active clients in the last sampling period
- Activity of the current client in the last sampling period

The **bw-alloc** parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network.You must set traffic shaping to fair-access to use this bandwidth allocation value for an individual virtual AP.

Example

The following command configures a traffic management profile that allocates bandwidth to the corpnet virtual AP:

```
(host) (config) #wlan traffic-management-profile best
   bw-alloc virtual-ap corpnet share 75
```

Command History

This command was introduced in ArubaOS 3.0. The mode parameters were introduced in ArubaOS 3.2.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system on master controllers	Config mode on master controllers

wlan virtual-ap

```
wlan virtual-ap <profile>
   aaa-profile <profile>
   allowed-band <band>...
   auth-failure-blacklist-time <seconds>
   band-steering
   blacklist
   blacklist-time <seconds>
   broadcast-filter all|arp
   clone <profile>
   deny-time-range <range>
   dos-prevention
   dot11k-profile
   fast-roaming
   forward-mode {tunnel|bridge|split-tunnel|decrypt-tunnel}
   ha-disc-onassoc
   mobile-ip
   no ...
   rap-operation {always|backup|persistent|standard}
   ssid-profile <profile>
   steering-mode band-balancing|force-5ghz|prefer-5ghz
   strict-compliance
   vap-enable
   dynamic-mcast-optimization
   dynamic-mcast-optimization-threshold
   vlan <vlan>...
   vlan-mobility
   wmm-traffic-management-profile
```

Description

This command configures a virtual AP profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`aaa-profile`	Name of the AAA profile that applies to this virtual AP.	—	"default"
`allowed-band`	The band(s) on which to use the virtual AP: a—802.11a band only (5 GHz) g—802.11b/g band only (2.4 GHz) all—both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz)	a/g/all	all
`auth-failure-blacklist-time`	Time, in seconds, a client is blocked if it fails repeated authentication. 0 blocks indefinitely.		0
`band-steering`	ARM's band steering feature can encourage or require dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4GHz band for single band clients like VoIP phones. Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5GHz band than on the 2.4GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40MHz or 20MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile. The band steering feature supports three steering modes, which can be configured via the steering-mode parameter: Band steering can be configured on both campus APs and remote APs that have a virtual AP profile set to tunnel, decrypt-tunnel, split-tunnel or bridge forwarding mode. Note, however, that if a campus or remote APs has virtual AP profiles configured in bridge or split-tunnel forwarding mode but no virtual AP in tunnel mode, those APs will gather information about 5G-capable clients independently and will not exchange this information with other APs that also have bridge or split-tunnel virtual APs only. The Band Steering feature will not work unless the you use the enable the "Local Probe Response" parameter in the Wireless LAN SSID profile for the SSID that requires band steering. You can enable the local probe response parameter using the CLI command **wlan ssid-profile <profile> local-probe-response**.	—	disabled
`blacklist`	Enables detection of denial of service (DoS) attacks, such as ping or SYN floods, that are not spoofed deauth attacks.	—	enabled
`blacklist-time`	Number of seconds that a client is quarantined from the network after being blacklisted.		3600 seconds (1 hour)
`broadcast-filter`	Filter out broadcast and multicast traffic in the air.	—	disabled

Parameter	Description	Range	Default
`all`	Filter out broadcast and multicast traffic in the air. **NOTE:** Do not enable this option for virtual APs configured in bridge forwarding mode. This configuration parameter is only intended for use for virtual APs in tunnel mode. In tunnel mode, all packets travel to the controller, so the controller is able to drop all broadcast traffic. When a virtual AP is configured to use bridge forwarding mode, most data traffic stays local to the AP, and the controller is not able to filter out that broadcast traffic. **IMPORTANT:** If you enable this option, you must also enable the **Broadcast-Filter ARP** parameter in the stateful firewall configuration to prevent ARP requests from being dropped. Note also that although a virtual AP profile can be replicated from a master controller to local controllers, stateful firewall settings do not. If you select the **broadcast-filter all** option for a Virtual AP Profile on a master controller, you must enable the **broadcast-filter arp** setting on each individual local controller.	—	disabled
`arp`	If enabled, all broadcast ARP requests are converted to unicast and sent directly to the client. You can check the status of this option using the **show ap active** and the **show datapath tunnel** command. If enabled, the output will display the letter **a** in the flags column. Do not enable this option for virtual APs configured in bridge forwarding mode. This configuration parameter is only intended for use for virual APs in tunnel mode. In tunnel mode, all packets travel to the controller, so the controller is able to convert ARP requests directed to the broadcast address into unicast. When a virtual AP is configured to use bridge forwarding mode, most data traffic stays local to the AP, and the controller is not able to convert that broadcast traffic.	—	disabled
`clone`	Name of an existing traffic management profile from which parameter values are copied.	—	—
`deny-time-range`	Specify the name of the time range for which the AP will deny access. Time ranges can be defined using the CLI command time-range.	—	—
`dos-prevention`	If enabled, APs ignore deauthentication frames from clients. This prevents a successful deauth attack from being carried out against the AP. This does not affect third-party APs.	—	disabled
`dot11k-profile`	Name of an 802.11k profile to be associated with this VAP.	—	default
`dynamic-mcast-optimization`	Enable/Disable dynamic multicast optimization. This parameter can only be enabled on a controller with a PEFNG license.		disabled
`dynamic-mcast-optimization-threshold`	Maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops.		

Parameter	Description	Range	Default
`forward-mode`	Controls whether 802.11 frames are tunneled to the controller using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the controller, and Internet access remains local). Select one of the following forward modes: • **Tunnel**: When an AP is in tunnel forwarding mode, the AP handles all 802.11 association requests and responses. The AP sends all 802.11 data packets, action frames and EAPOL frames over a GRE tunnel to the controller for processing. The controller removes or adds the GRE headers, decrypts or encrypts 802.11 frames and applies firewall rules to the user traffic as usual. • **Bridge**: When an AP is in bridge mode, data is bridged onto the local Ethernet LAN. When in bridge mode, the AP handles all 802.11 association requests and responses, encryption/decryption processes, and firewall enforcement. 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. An AP in bridge mode supports only the 802.1x authentication type. • **Split-Tunnel**: Data frames are either tunneled or bridged, depending on the destination (corporate traffic goes to the controller, and Internet access remains local). The AP handles all 802.11 association requests and responses, encryption/decryption, and firewall enforcement. 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. An AP in split-tunnel mode supports only the 802.1x authentication type. • **Decrypt-Tunnel:** An AP in decrypt-tunnel forwarding mode decrypts and decapsulates all 802.11 frames from a station and sends the 802.3 frames through the GRE tunnel to the controller, which then applies firewall policies to the user traffic. This mode allows a network to utilize the encryption/decryption capacity the AP while reducing the demand for processing resources on the controller. APs in decrypt-tunnel forwarding mode also manage all 802.11 association requests and responses, and process all 802.11e and 802.11k action frames. **NOTE:** Virtual APs in bridge or split-tunnel mode using static WEP should use key slots 2-4 on the controller . Key slot 1 should only be used with Virtual APs in tunnel mode.	tunnel bridge split-tunnel decrypt-tunnel	tunnel
`ha-disc-onassoc`	If enabled, all clients of a virtual-ap will receive mobility service on association.	—	disabled
`mobile-ip`	Enables or disables IP mobility for this virtual AP.	—	enabled
`multi-association`	Enables or disables multi-association for this virtual AP. When enabled, this feature allows a station to be associated to multiple APs. If this feature is disabled, when a station moves to new AP it will be de authorized by the AP to which it was previously connected, deleting station context and flushing key caching information.	—	disabled
`no`	Negates any configured parameter.	—	—

Parameter	Description	Range	Default
rap-operation	Configures when the virtual AP operates on a remote AP: **always**—Permanently enables the virtual AP. **backup**—Enables the virtual AP if the remote AP cannot connect to the controller. **persistent**—Permanently enables the virtual AP after the remote AP initially connects to the controller. **standard**—Enables the virtual AP when the remote AP connects to the controller. Use **always** and **backup** for bridge SSIDs. Use **persistent** and **standard** for 802.1x, tunneled, and split-tunneled SSIDs.	always/ backup/ persistent/ standard	standard
ssid-profile	Name of the SSID profile that applies to this virtual AP.	—	"default"
steering-mode	Band steering supports three different band steering modes. • **Force-5GHz**: When the AP is configured in **force-5GHz** band steering mode, the AP will try to force 5Ghz-capable APs to use that radio band. • **Prefer-5GHz** (Default): If you configure the AP to use **prefer-5GHz** band steering mode, the AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. • **Balance-bands**: In this band steering mode, the AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5Ghz band has more channels than the 2.4 Ghz band, and that the 5Ghz channels operate in 40MHz while the 2.5Ghz band operates in 20MHz. **NOTE:** Steering modes do not take effect until the band steering feature has been enabled. The band steering feature in ArubaOS versions 3.3.2-5.0 does not support multiple band-steering modes. The band-steering feature in these versions of ArubaOS functions the same way as the default **prefer-5GHz** steering mode available in ArubaOS 6.0 and later.	Force-5GHz prefer-5ghz balance-bands	prefer-5ghz
strict-compliance	If enabled, the AP denies client association requests if the AP and client station have no common rates defined. Some legacy client stations which are not fully 802.11-compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.	—	disabled
vap-enable	Enable or disable the virtual AP.	—	enabled
vlan	The VLAN(s) into which users are placed in order to obtain an IP address. Enter VLANs as a comma-separated list of existing VLAN IDs *or* VLAN names. A mixture of names and numeric IDs are not allowed.		1
vlan-mobility	Enable or disable VLAN (Layer-2) mobility.	—	disabled
wmm-traffic-management-profile	Specify the WMM Traffic Management Profile to be associated with this Virtual AP Profile.	—	—

Usage Guidelines

Wireless LAN profiles configure WLANs in the form of virtual AP profiles. A virtual AP profile contains an SSID profile which defines the WLAN and an AAA profile which defines the authentication for the WLAN. You can configure and apply multiple instances of virtual AP profiles to an AP group or to an individual AP.

A named VLAN can be deleted although it is configured in a virtual AP profile. If this occurs the virtual AP profiles becomes invalid. If the named VLAN is added back later the virtual AP becomes valid again.

Example

The following command configures a virtual AP:

```
wlan virtual-ap corpnet
   vlan 1
   aaa-profile corpnet
```

Command History.

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 3.2	Support for the split tunneling option and the rap-operation parameter was introduced.
ArubaOS 3.3	In support of the IEEE 802.11n standard, a change to the allowed-band parameter was introduced.
ArubaOS 3.3.2	• Support for the **ha-disc-onassoc** parameter was introduced. • The **band-steering** parameter was introduced but is not a released feature in ArubaOS 3.3.2. Do not **use band-steering** without proper guidance from Dell technical support. • Support for the **voip-proxy-arp** parameter was introduced.
ArubaOS 3.4	The v**oip-proxy-arp** parameter was renamed to **broadcast-filter-arp** and i t does not require a Voice license. The **fast-roaming** parameter was renamed to **multi-association**.
ArubaOS 5.0	The **decrypt-tunnel** forwarding mode was introduced.
ArubaOS 6.0	The **steering-mode balance-bands|force-5ghz| prefer-5ghz** parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

wlan voip-cac-profile

```
wlan voip-cac-profile <profile>
   bandwidth-cac
   bandwidth-capacity <bandwidth-capacity>
   call-admission-control
   call-capacity
   call-handoff-reservation <percent>
   clone <profile>
   disconnect-extra-call
   no ...
   send-sip-100-trying
   send-sip-status-code client|server <code>
   wmm_tspec_enforcement
   wmm_tspec_enforcement_period <seconds>
```

Description

This command configures a voice over iP (VoIP) call admission control (CAC) profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`bandwidth-cac`	Select the desired call admission control (CAC) Mechanism: • Disable - CAC is based on Call Counts • Enable - CAC should be based on Bandwidth.	—	disabled
`bandwidth-capacity`	Define the maximum bandwidth that can be handled by one radio, in kbps. The default value is 2000 kbps (2 Mbps)	—	—
`<bandwidth-capacity>`	Maximum bandwidth that can be handled by one radio, in kbps. The default value is 2000 kbps (2 Mbps)	1-600000	2000
`call-admission-control`	Enables or disables WiFi VoIP Call Admission Control features.	—	disabled
`call-capacity`	Number of simultaneous calls that can be handled by one radio.	0-8000	10
`call-handoff-reservation`	Percentage of call capacity reserved for mobile VoIP clients on call.	0-100	20%
`clone`	Name of an existing VoIP CAC profile from which parameter values are copied.	—	—
`disconnect-extra-call`	Disconnects calls that exceed the high capacity threshold by sending a deauthentication frame.	—	disabled
`no`	Negates any configured parameter.	—	—
`send-sip-100-trying`	Enables sending of SIP 100 - trying messages to a call originator to indicate that the call is proceeding. This is useful when the SIP invite may be redirected through a number of servers before reaching the controller.	—	enabled

Parameter	Description	Range	Default
`send-sip-status-code client|server <code>`	Use this parameter with the **client** or **server** options to drop a SIP Invite and send status code back to the client or server. You must also include one of the following codes: • **480**: Temporary Unavailable • **486**: Busy Here • **503**: Ser vice Unavailable • **none**: Don't send SIP status code	—	486
wmm_tspec_en forcement	Enables validation of TSPEC requests for CAC.	—	disabled
wmm_tspec_en forcement_ period	Maximum time for the station to start the call after the TSPEC request.	1-100	1 second

Usage Guidelines

The VoIP CAC profile prevents any single AP from becoming congested with voice calls.

Example

The following command enables VoIP CAC:

```
(host) (config) #wlan voip-cac-profile cac1
   call-admission-control
   disconnect-extra-call
```

Command History

Version	Change
ArubaOS 3.0	Command introduced
ArubaOS 3.4	The following parameters were deprecated: • active-load-balancing • high-threshold-capacity • noe-call-capacity • sccp-call-capacity • svp-call-capacity • vocera-call-capacity The following parameters were introduced: • bandwidth-cac • bandwidth-capacity • call-capacity
ArubaOS 3.4.1	License requirements changed in ArubaOS 3.4.1, so the command required the PEF license instead of the Voice Services Module license required in earlier versions.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config mode on master controllers

wms ap

```
wms ap <bssid> mode {interfering|manually-contained|neighbor|rogue|valid}
```

Description

This command allows you to classify an AP into one of several categories.

Syntax

Parameter	Description
`<bssid>`	BSSID of the AP.
`mode`	Classify the AP into one of the following categories.
`interfering`	An AP seen in the RF environment but is not connected to the wired network.
`manually-contained`	Manually enable denial of service from this AP
`neighbor`	An neighboring AP whose BSSID is known.
`suspect-rogue`	A suspected rogue AP that is plugged into the wired side of the network but may not be an unauthorized device. Automatic shutdown of rogue APs does not apply to these devices.
`rogue`	A rogue AP that is unauthorized and is plugged into the wired side of the network. You can configure automatic shutdown of rogue APs in the IDS unauthorized device detection profile.
`valid`	An AP that is part of the enterprise providing WLAN service.

Usage Guidelines

If AP learning is enabled (with the wms general learn-ap enable command), non-Dell APs connected on the same wired network as Dell APs are classified as valid APs. If AP learning is disabled, a non-Dell AP is classified as an unsecure or suspect-unsecure AP.

Example

The following command classifies an interfering AP as a known-interfering AP:

```
(host) #wms ap 01:00:00:00:00:00 mode known-interfering
```

Command History

Release	Modification
ArubaOS 3.0.	Introduced
ArubaOS 6.0	Renamed the modes and deprecated the DoS mode.

This command was introduced in

deprecated the mode dos option

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

wms clean-db

```
wms clean-db
```

Description

This command deletes the WMS database.

Syntax

Parameter	Description
`clean-db`	Cleans the WMS database.

Usage Guidelines

This command deletes all entries from the WMS database. Do not use this command unless instructed to do so by an Dell representative.

Example

The following command cleans the WMS database:

```
(host) #wms clean-db
WMS Database will be deleted. Do you want to proceed with this action [y/n]:
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

wms client

```
wms client <macaddr> mode {dos|interfering|valid}
```

Description

This command allows you to classify a wireless client into one of several categories.

Syntax

Parameter	Description
`client`	MAC address of the client.
`mode`	Classify the client into one of the following categories:
`dos`	Enables denial of service to this client.
`neighbor`	A client seen in the RF environment that is outside of the enterprise.
`valid`	A client that is part of the enterprise.

Usage Guidelines

ArubaOS can automatically determine client classification based on client behavior, but this command allows you to explicitly classify a client. The classification of a client is used in certain policy enforcement features. For example, if **protect-valid-sta** is enabled in the IDS Unauthorized Device Profile, then clients that are classified as valid cannot connect to non-valid APs.

Example

The following command classifies a client as valid:

```
(host) #wms client 00:00:A4:34:C9:B3 mode valid
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

wms export-class

```
wms export-class <filename>
```

Description

This command exports classification information into a file.

Syntax

Parameter	Description
`<filename>`	Name of the file into which you want to export classification information

Usage Guidelines

This command writes classification data into comma separated values (CSV) files—one for APs and one for clients. You can import these files into the Dell Mobility Manager system.

Example

The following command exports classification data into an AP and a client file:

```
(host) #wms export-class class

Exported data to class_ap.csv and class_sta.csv
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

wms export-db

```
wms export-db <filename>
```

Description

This command exports the WMS database to a specified file.

Syntax

Parameter	Description
`<filename>`	Name of the file into which you want to export the database. The filename plus any extensions must be no longer than 32 characters and may contain only keyboard characters.

Usage Guidelines

The file is exported as an ASCII text file. If you have configured the controller for operation with the Dell Mobility Manager (Mobility Manager), this command will fail and an error will be returned.

Example

The following command exports the WMS database to a file:

```
(host) #wms export-db database
Exported WMS DB to database
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

wms general

```
wms general ap-ageout-interval <minutes> | collect-stats {disable|enable} |
learn-ap {enable|disable} | persistent-known-interfering {enable|disable} |
poll-interval <milliseconds> |poll-retries <number> | propagate-wired-macs
{enable|disable} | sta-ageout-interval <minutes> | stat-update
{enable|disable}
```

Description

This command configures the WLAN management system (WMS).

Syntax

Parameter	Description	Range	Default
`ap-ageout-interval`	Time, in minutes, that an AP remains unseen by any probes before it is deleted from the database.	0 to disable	30 minutes
`collect-stats`	Enables collection of statistics (up to 25,000 entries) on the master controller for monitored APs and clients. This only applies when Mobility Manager is not configured.	enable| disable	disabled
`learn-ap`	Enables "learning" of non-Dell APs.	enable| disable	disabled
`persistent-known-interfering`	Enables APs that are marked as known interfering from being aged out.	enable| disable	disabled
`poll-interval`	Interval, in milliseconds, for communication between the controller and Dell AMs. The controller contacts the AM at this interval to download AP to station associations, update policy configuration changes, and download AP and station statistics.	(any)	60000 milliseconds (1 minute)
`poll-retries`	Maximum number of failed polling attempts before the polled AM is considered to be down.	(any)	2
`propagate-wired-macs`	Enables the propagation of the gateway wired MAC information.	enable| disable	enabled
`sta-ageout-interval`	Time, in minutes, that a client remains unseen by any probes before it is deleted from the database.	0 to disable	30 minutes
`stat-update`	Enables statistics updating in the database.	enable| disable	enabled

Usage Guidelines

By default, non-Dell APs that are connected on the same wired networks as Dell APs are classified as "rogue" APs. Enabling AP learning classifies non-Dell APs as "valid" APs. Typically, you would want to enable AP learning in environments with large numbers of existing non-Dell APs and leave AP learning enabled until all APs in the network have been detected and classified as valid. Then, disable AP learning and reclassify any unknown APs as interfering.

Example

The following command enables AP learning:

```
(host) #wms general learn-ap enable
```

To disable AP learning:

```
(host) #wms general learn-ap disable
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

wms import-db

```
wms import-db <filename>
```

Description

This command imports the specified file into the WMS database.

Syntax

Parameter	Description
`<filename>`	Name of the file into which you want to import into the database. The filename plus any extensions must be no longer than 32 characters and may contain only keyboard characters.

Usage Guidelines

The imported file replaces the WMS database. The imported file must be a valid WMS database file that you previously exported using the **wms export-db** command.

Example

The following command imports the WMS database from a file:

```
(host) #wms import-db database
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

wms reinit-db

```
wms reinit-db
```

Description

This command reinitializes the WMS database to its factory defaults.

Syntax

No parameters.

Usage Guidelines

When you use this command, there is no automatic backup of the current database. If an Mobility Manager server is configured on the controller (see “mobility-manager” on page 356), this command will fail and return an error.

Example

The following command reinitializes the WMS database:

```
(host) #wms reinit-db
WMS Database will be re-initialized. Do you want to proceed with this action [y/n ]:
```

Command History

This command was introduced in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on master controllers

wms-local system

```
wms-local system max-threshold <max-threshold>
```

Description

This command defines local WMS system settings for the maximum number of APs and client stations.

Syntax

Parameter	Description
`<max-threshold>`	Set the max threshold for the total number of APs and Stations. This value can be any 32-bit number.

Usage Guidelines

Use this command with caution. Increasing the limit will cause an increase in usage in the memory by WMS. In general, each entry will consume about 500 bytes of memory. If the setting is bumped up by 2000, then it will cause an increase in WMS memory usage by 1MB

Example

The following command sets the maximum number of APs and stations at 500.

```
host) (config)# wms-local system max-threshold 500
```

Command History

This command was introduced in ArubaOS 3.3.2.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on master controllers

write

```
write {erase [all] | memory | terminal}
```

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 the controller to factory defaults.

Syntax

Parameter	Description
`erase`	Erases the running system configuration file. Rebooting the controller resets it to the factory default configuration. If you specify `all`, the configuration and all data in the controller databases (including the license, WMS, and internal databases) are erased.
`memory`	Saves the current system configuration to memory. Any configuration changes made during this session will be made permanent.
`terminal`	Displays the current system configuration.

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. To save your configuration changes, use the `write memory` command.

If you use the `write erase` command, the license key management database on the controller is not affected. If you use the `write erase all` command, all databases on the controller are deleted, including the license key management database. If you reset the controller to the factory default configuration, perform the Initial Setup as described in the *Dell Quick Start Guide*.

If you use the `write terminal` command, all of the commands used to configure the controller appear on the terminal. If paging is enabled, there is a pause mechanism that stops the output from printing continuously to the terminal. To navigate through the output, use any of the commands displayed at the bottom of the output, as described in below. If paging is disabled, the output prints continuously to the terminal. For more information about the **paging** command, see "paging" on page 370..

Key	Description
Q	Exit the display.
U	Page up through the output.
spacebar	Page down through the output.
/	Enter a text string to search for.
N	Repeat the text string to search for.

Example

The following command saves your changes so they are retained after a reboot:

```
(host) #write memory
```

The following command deletes the running configuration and databases and returns the controller to the factory default settings:

```
(host) #write erase
```

Command History

This command was introduced in ArubaOS 1.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config modes

Appendix A: Command Modes

The ArubaOS command-line interface offers different levels of user access by differentiating between different command modes.

When you first log in to the CLI, you start your session in *User mode*, which provides only limited access for basic operational testing. You must enter an additional password to access *Enable mode*, which allows you to issue show commands run certain management functions. Configuration commands can only be issued in *Config mode*. You can access Config mode by entering **configure terminal** at the command prompt. You can exit your current command mode and return to a lower-level command mode at any time by entering **exit** at the command prompt.

The following sections describes how to access each command mode, the command prompt for each mode, and links to its available commands.

User mode

You always begin a CLI session in user mode, the command mode with the lowest level of user access. The command prompt for a user mode session is a greater-than (>) symbol:

```
(host) >
```

The following commands are available in user mode.

- enable
- exit
- help
- logout
- ping
- traceroute

Enable Mode

To move from user mode to enable mode, you must enter the command **enable**, press **Enter**, then enter config mode password that was defined during the controller's initial setup process. (The default password is **enable**.) Users in enable mode may return to user mode at any time by entering the command **exit**.

The command prompt for a CLI session in enable mode is a pound (**#**) symbol:

```
(host) #
```

The following commands are available in enable mode.

- aaa authentication dot1x clear||reload-cert
- aaa authentication stateful-dot1x clear
- aaa inservice
- aaa ipv6 user add
- aaa ipv6 user clear-sessions
- aaa ipv6 user clear-sessions
- aaa ipv6 user delete
- aaa ipv6 user logout
- aaa query-server
- aaa test-server
- aaa user add
- aaa user clear-sessions
- aaa user delete
- aaa user logout
- am
- ap wipe out flash
- ap-regroup
- ap-rename
- apboot
- apdisconnect
- apflash
- audit-trail
- backup
- boot
- clock
- configure terminal
- copy
- crypto isakmp packet-dump
- crypto pki
- crypto pki-import
- database synchronize
- delete
- dir
- dynamic-ip
- encrypt
- exit
- export
- halt
- help
- license
- localuserdb
- local-userdb-guest
- packet-capture
- page
- paging
- panic
- pcap
- ping
- reload
- rename
- restore
- rft
- show
- stm
- support
- tar
- traceroute
- usb reclassify
- whoami
- wms ap
- wms clean-db
- wms client
- wms export-class
- wms export-db
- wms import-db
- wms reinit-db
- write

Config Mode

To move from enable mode to config mode, enter the command **config terminal**. Users in config mode may return to enable mode at any time by entering the command **exit**.

When you are in config mode, (**config**) appears before the # prompt:

```
(host) (config) #
```

The following commands are available in basic config mode.

- aaa authentication
- aaa bandwidth-contract
- aaa derivation-rules
- aaa inservice
- aaa ipv6 user add
- aaa derivation-rules
- aaa derivation-rules
- aaa profile
- aaa radius-attributes
- aaa rfc-3576-server
- aaa server-group
- aaa sygate-on-demand
- aaa tacacs-accounting
- aaa timers
- aaa user fast-age
- aaa xml-api
- adp
- am
- ap enet-link-profile
- ap mesh-cluster-profile
- ap mesh-ht-ssid-profile
- ap regulatory-domain-profile
- ap regulatory-domain-profile
- ap snmp-profile (deprecated)
- ap regulatory-domain-profile
- ap system-profile
- ap wipe out flash
- ap-group
- ap-regroup
- ap-rename
- apboot
- apdisconnect
- apflash
- arp
- backup
- banner motd
- boot
- cellular profile
- cfgm
- clock
- cluster-member-ip
- cluster-root-ip
- controller-ip
- control-plane-security
- crypto dynamic-map
- crypto ipsec
- crypto isakmp
- crypto map global-map
- crypto-local
- destination
- esi
- exit
- firewall
- gateway health-check disable
- guest-access-email
- help
- hostname
- ids
- interface
- ip
- ipv6 firewall
- lacp
- localuserdb
- localip
- location
- logging
- loginsession
- mac-address-table
- master-redundancy
- masterip
- mgmt-server
- mgmt-user
- mobility-manager
- netdestination
- netservice
- ntp server
- packet-capture-defaults
- papi-security
- ping
- pkt-trace
- pkt-trace-global
- pptp ip local pool
- priority-map
- process monitor
- prompt
- provision-ap
- rap-wml
- rf arm-profile
- router mobile
- service
- shutdown
- spanning-tree
- ssh
- syscontact
- syslocation
- telnet
- time-range
- traceroute
- trusted
- uplink
- user-role
- valid-network-oui-profile
- vlan
- vlan-name
- voip
- vpdn group l2tp
- vpn-dialer
- vrrp
- web-server
- whitelist-db
- whoami
- wlan
- wms general
- wms-local system

Configuration Sub-modes

Some config mode commands can enter you into a sub-mode with a limited number of available commands specific to that mode. When you are in a configuration sub-mode, the **(config)** that appears before the command prompt will change to indicate your current mode; e.g **(config-if)** for config-interface mode, and **(config-tunnel)** for config-tunnel mode.

You can exit a sub-command mode and return to the basic configuration mode at any time by entering the exit command.