ArubaOS 7.4.x Command-Line Interface

Reference Guide

aruba
a Hewlett Packard Enterprise company

Open Source Code

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

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

Revision History

The following table lists the revision history of this document.

Table 1: *Revision History*

Document Revision	Change Description
Release 01	Initial Release
Release 02	Addressed an enhancement. (ID 105150 - Dyn DNS: Unable to update IP address with myonlineportal.net as DDNS server)
Release 03	Addressed the following: 1. Customer-reported issues • Bandwidth Control in MAS • S2S VPN - multiple subnets 2. Bugs • 94980 - Sample MSTP Topology revised • 106468 - Central Activate Behavior After Leaving Factory Default • 110151 - Policer-profile sub-option per-user under user
Release 04	Addresses all enhancements from ArubaOS 7.4.0.1 through ArubaOS 7.4.1.7.
Release 05	Fixed basic typographical errors (device vs. vevice) and a few chronological ordering mistakes of commands.
Release 06	Addressed all enhancements for ArubaOS 7.4.0.5, ArubaOS 7.4.0.6, ArubaOS 7.4.1.8, and ArubaOS 7.4.1.9.

The ArubaOS 7.4.x command-line interface (CLI) allows you to configure and manage your Mobility Access Switch. The CLI is accessible from a local console connected to the serial port on the Mobility Access Switch or through a Telnet or Secure Shell (SSH) session from a remote management console or workstation.

Telnet access is disabled by default. To enable Telnet access, enter the **telnet** CLI command from a serial connection or an SSH session.

What's New in ArubaOS 7.4.x

New Commands

The following commands are introduced in the ArubaOS 7.4.x command line interface.

Command	Description
aaa auth-survivability	Use this command to enable authentication survivability in Mobility Access Switches.
arp	Use this command to add static Address Resolution Protocol (ARP) entries to the ARP table.
crypto aruba-vpn	Use this command to configure anAruba VPN tunnel.
downloadable-role-delete	Use this command to delete the downloadable roles from the ClearPass Policy Manager (CPPM) under specific conditions.
interface-profile ddns-profile	Use this command to configure a Dynamic Domain Name Server (DDNS) profile.
ip dhcp aruba-vpn-pool	Use this command to configure Distributed DHCP scope using the Aruba VPN pool profile.
ip nat pool	Use this command to create a Network Address Translation (NAT) pool.
ip tacacs source-interface	Use this command to select a specific source-interface IP address for the outgoing TACACS packets.
mode-button	Use this command to enable the **Mode** button and restore the S1500Mobility Access Switches to factory default settings.
papi-security	Use this command to enforce advanced security options and provide an enhanced level of security. You can configure a new security key if required.
pkt-trace acl	Use this command to enable or disable packet tracing in the datapath.

Command	Description
pkt-trace-global	Use this command to enable or disable global packet tracing.
probe-profile	Use this command to create a probe-profile for monitoring L3 uplink status.
rogue-ap-containment	Enable/disable and configure rogue AP containment options.
set traceflags	Use this command for setting trace flags for various packet forwarding functions.
show aaa deny-inter-user-traffic roles	Use this command to view the list of roles on which **deny-inter-user-traffic** is enabled.
show ddns-client	Use this command to view the DDNS updates that are sent to the server.
show device-group	This command displays the device-group attached interfaces.
show device-group-config	This command displays the device-group configuration parameters.
show interface-profile ddns-profile	Use this command to view the DDNS profile configuration information.
show ip dhcp aruba-vpn-pool	Use this command to view the details of the Aruba VPN pool profiles configured on the Mobility Access Switch.
show ip nat pool	Use this command to view all the NAT pools configured in the network.
show mode-button	Use this command to verify the **Mode** button configuration of S1500Mobility Access Switch.
show probe	Use this command to view the probe status of the interfaces where the probe profile is attached.
show probe-profile	Use this command to view the details of the probe profiles configured on the system.
show rogue-ap-containment	Use this command to view the rogue AP containment actions configured on the Mobility Access Switch.
show ztp-boot-info	Use this command to display the provisioning details of the Mobility Access Switch.

Modified Commands

The following commands are modified in ArubaOS 7.4.x

Command	Description
aaa authentication-server radius	A new parameter, **cppm username <username> password <password>**, to configure CPPM server credentials is introduced.
aaa authentication-server tacacs	The **source-interface** parameter and its options are introduced.
aaa profile	The **mac-limit** parameter and the **action** subparameter are introduced.
clear port-error-recovery	The **untrusted** parameter was introduced.
crypto-local ipsec-map	The **standby-interface vlan** parameter is introduced to configure a backup VPN interface.
device-group	The **auto-lacp** subcommand to enable Auto-LACP in the Mobility Access Switch is introduced.
interface gigabitethernet	Introduction of a warning message, when GVRP profile is applied on an interface without enabling the global GVRP.
interface-profile lldp-profile	The **med enable** and **med disable** commands are removed, as LLDP-MED option is set to Auto mode.
interface-profile port-security-profile	The **action** and **auto-recovery-time** sub-parameters are introduced in the sticky-mac command.
interface tunnel ethernet	The **no switching-profile** command is introduced.
interface vlan	The following new parameters are introduced: • **ddns-profile** • **ip nat outside** • **ip access-group session** • **metric** • **probe-profile** • **aruba-vpn-pool-profile**
ip-profile	The **ipsec** parameter is introduced under the **controller-ip** command.
reload	New options, **reload in** and **reload at**, are introduced
set stacking renumber	This command is modified to allow renumbering any stack member except the primary and the secondary stack members.
show datapath debug	The **trace-buffer** parameter is introduced.

Command	Description
show datapath session	The output includes **S** and **N** flags to indicate if source NAT or destination NAT is performed on the session.
show interface-config vlan	Introduced the following new parameters as part of this show command: • **Interface description** • **Interface DDNS profile** • **Probe Profile** • **metric** • **IP NAT Outside** • **Aruba VPN Pool profile** • **Egress ACL** • **Session ACL**
show interface port-channel	The **auto-lacp** parameter is introduced.
show interface brief	The **all** subparameter is introduced in the port-channel parameter.
show interface-profile port-security-profile	The **Sticky MAC Action** and **Sticky MAC Auto Recovery Time** output parameters are introduced. The status of **Proxy ARP** was also introduced in the command output .
show interface tunnel	The command output is moified to display the switching-profile as **default** when no switching profile is applied to the interface tunnel.
show interface vlan	**Metric** and **Probe profile** details are added to the output.
show ip ospf	The interface option **brief** is introduced. Also, information about autonomous system boundary router is added in the output of the **show ip ospf border-routers** command.
show ip interface brief	The output parameters are modified to include the **Probe** column indicating the probe status of all the interfaces being ping probed.
show ip pim mroute	The counters for multicast route entries are included in the output.
show ip pim-ssm mroute	The counters for multicast route entries are included in the output.
show memory	This command introduces the following changes: • The **dpa** parameter is introduced. • The output of the **show memory debug** command is enhanced to include debug information for l3m, l2m, dpa, stackmgr, cmicm, and cmica processes.
show port-error-recovery	The **untrusted** parameter was introduced.

Command	Description
show probe	**Flags**, a new column, is introduced in the output of the show probe command.
show rights	The **Deny inter-user traffic** status information is added to the output.
show running-config	The probe-profile protocol information (default value is ICMP) is displayed in the output of the show running-config command
show traceoptions	Enhancements to the output of the traceoptions command are as follows: • Filteration of OSPF and PIM traces by interface ID. • Display of actual interface number in the place of port name (for the **mstp** command's port information)
traceoptions	New options—**gigabitethernet** and **port-channel**—are introduced under **mstp** parameter.
user-role	The **deny-inter-user-traffic** parameter is introduced. Enabling this on a user-role denies the traffic between users with that role.
vlan-profile igmp-snooping-profile	The **v3** parameter is added under **snooping** and **snooping-proxy** commands.
web-server	The **ssl-protocol** parameter is modified to include only transport layer security options: tlsv1, tlsv1.1, and tlsv1.2.

Security Update

Starting from ArubaOS 7.4.1, the BASH access is disabled on Mobility Access Switch for security reasons.

About this Guide

This guide describes the ArubaOS 7.4.x 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 the command modes and platforms for which this command is applicable.

Connecting to the Mobility Access Switch

This section describes how to connect to the Mobility Access Switch to use the CLI.

Serial Port Connection

The serial port is located on the front panel of the Mobility Access Switch. Connect a terminal or PC/workstation running a terminal emulation program to the serial port on the Mobility Access Switch 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 Mobility Access Switch and connect the Mobility Access Switch to your network. This is typically performed when you run the Initial Setup on the Mobility Access Switch, as described in the *ArubaOS 7.4 Quick Start Guide*.

CLI Access

When you connect to the Mobility Access Switch 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 Mobility Access Switch. 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 (also called privileged mode password) that you entered during the Initial Setup. 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) #
```

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
exit                    Exit this session. Any unsaved changes are lost.
help                    Help on CLI command line processing and a
Description of the interactive help system
logout                  Exit this session. Any unsaved changes are lost.
ping                    Send ICMP echo packets to the specified ip address.
tracepath               Trace path to the specified IPv6 address.
traceroute              Trace route to the 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 or statistics
clock                   Configure the system clock
configure               Configuration Commands
copy                    Copy Files
crypto                  Configure IPSec, IKE, and CA
```

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 ?
dhcp-snoop-database
erase                   Erase configuration
memory                  Write to memory
terminal                Write to terminal
```

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 VLAN configuration on a user-role:

  ```
  (host) (config) #user-role <name>
  (host) (config-role) #no vlan 1
  ```

Saving Configuration Changes

Each Aruba Mobility Access Switch contains two different types of configuration images.

- The *running-config* holds the current Mobility Access Switch 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 Mobility Access Switch 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 Mobility Access Switch reboots. To save your configuration changes so they are retained in the startup configuration after the Mobility Access Switch 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.

Reloading the Mobility Access Switch

When you execute the reload command, the Mobility Access Switch prompts you to save the configuration if there are any changes in the running configuration. Reloading the Mobility Access Switch causes a momentary disruption in service as the unit resets.

Conventions

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

Table 2: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: • Sample screen output • System prompts • Filenames, software devices, and specific commands when mentioned in the text
`Commands`	In the command examples, this bold font depicts text that you must type exactly as shown.
<Arguments>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: `# send <text message>` In this example, you would type "send" at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
`[Optional]`	Command examples enclosed in brackets are optional. Do not type the brackets.
`{Item A | Item B}`	In the command examples, 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.

The following informational icons are used throughout this guide:

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

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

Indicates a risk of personal injury or death.

Command Line Editing

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

To view items in the command history, use the *up* arrow key to move back through the list and the *down* arrow key to move forward. To reissue a specific command, press **Enter** when the command appears in the command history. You can 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. Table 1 lists the editing controls. To use key shortcuts, press and hold the **Ctrl** button while you press a letter key.

Table 3: *Line Editing Keys*

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

Contacting Support

Table 4: *Contact Information*

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

aaa authentication captive-portal

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

Description

This command configures a Captive Portal authentication profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	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

Parameter	Description	Range	Default
`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
`ip-addr-in-redirection-url`	Sends IP address of one of the interface in the redirection URL when external captive portal servers are used.	—	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`	The number of authentication failures before the user is blacklisted.	0-10	0
`no`	Negates any configured parameter.	—	—

Parameter	Description	Range	Default
`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.	—	—
`show-acceptable-use-policy`	Show the acceptable use policy page before the logon page.	enabled/ disabled	disabled
`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
`single-session`	Allows only one active user session at a time.	—	disabled
`switchip-in-redirection-url`	Sends the Mobility Access Switch's IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the Mobility Access Switch from which a request originated by parsing the 'switchip' variable in the URL.	enabled/ disabled	disabled
`use-chap`	Use CHAP protocol. You should not use this option unless instructed to do so by an Aruba representative.	enabled/ disabled	disabled (PAP is used)
`user-logon`	Enables Captive Portal with authentication of user credentials.	enabled/ disabled	enabled
`user-vlan-in-redirection-url`	Sends VLAN ID of the user in the redirection URL when external captive portal servers are used.	—	—
`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

Parameter	Description	Range	Default
`white-list <white-list>`	Name of an existing white list on an IPv4 or IPv6 network destination. The white list contains authenticated websites that a guest can access.	—	—

Usage Guidelines

Use this command to create a captive portal profile on a Mobility Access Switch.

Example

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

To create a captive portal profile:

```
(host)(config)#aaa authentication captive-portal cp-profile
(host)(Captive Portal Authentication Profile "cp-profile") #default-role guest
(host)(Captive Portal Authentication Profile "cp-profile") #server-group cp-srv
```

To attach a captive portal profile to the user role:

```
(host)(config) #user-role cp-first
(host)(config-role) #captive-portal cp-profile
```

To designate the user role created as the initial role of the AAA profile:

```
(host)(config) #aaa profile cp_aaa
(host) (AAA Profile "cp_aaa") #initial-role cp-first
```

To apply the configured AAA profile to the interface:

```
(host)(config) #interface gigabitethernet 0/0/0
          aaa-profile cp_aaa      no trusted port
```

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

aaa authentication dot1x

```
aaa authentication dot1x <profile-name>
   ca-cert <certificate>
   cert-cn-lookup
   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>
   no ...
   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>}|quiet-period <seconds>}|{reauth-period <seconds>}
   tls-guest-access
   tls-guest-role <role>
```

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”
`ca-cert <certificate>`	This command creates the CA certificate. The <certificate> parameter is the name of the certificate, which must be loaded on the switch.	—	disabled
`cert-cn-lookup`	Checks certificate common name against AAA server.	—	—
`clone`	Name of existing 802.1X profile from which parameters are copied.	—	—

Parameter	Description	Range	Default
`delay-eap-success`	Introduces a delay of one second in sending the EAP Success message to the client after it completes the 802.1X authentication to ensure that the clients obtain an IP address in the correct VLAN.	—	disabled
`deny-dhcp`	Denies DHCP requests from the clients till the dot1x authentication is complete to ensure that the 802.1X clients obtain the correct IP addresses in the correct VLANs/subnets.	—	disabled
`eapol-logoff`	Enables handling of EAPOL-LOGOFF messages.	—	disabled
`framed-mtu <MTU>`	Use this command to set the framed MTU attribute that is sent to the authentication server.	500-1500	1100
`heldstate-bypass-counter <hs-counter>`	Use this command to set the maximum number of times a station can send bad user credentials and avoid going to held state by sending an EAPOL-Start.	0-3	0
`ignore-eap-id-match`	Use this command to ignore EAP ID during negotiation.	—	disabled
`ignore-eapol start-afterauthentication`	Use this command to ignore EAPOL-START messages after authentication.	—	disabled
`machine-authentication`	(For Windows environments only) These parameters set machine authentication:		
`blacklist-on-failure`	Blacklists the client if machine authentication fails.	—	disabled
`cache-timeout <hours>`	Use this command to blacklist the station if machine authentication fails.	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

Parameter	Description	Range	Default
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
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.	0-5	0 (disabled)
max-requests <number>	Sets the 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.	—	—
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>	Option to set the maximum number of authentication requests that are sent to server group.	0-3	2

Parameter	Description	Range	Default
`server-retry-period <seconds>`	Option to set the time interval, in seconds, of failed requests that are sent to a server group.	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. @@@@@ The syntax on the original doc was weird, so I just used this one. (The original was "Option to termination enable-token-caching.")	—	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-mschapv2
`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
`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)
`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.	—	guest

Usage Guidelines

The 802.1X authentication profile allows you to enable and configure machine authentication and 802.1X termination on the controller. 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
```

Command History

Version	Description
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3.1	The following parameters were added: • **delay-eap-success** • **deny-dhcp**

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system.	Configuration mode except where otherwise noted.

aaa authentication mac

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

Description

This command configures the MAC authentication profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Variable name of the mac profile.	—	"default"
`case`	The case (upper or lower) used in the MAC string sent in the authentication request.	upper|lower	lower
`clone <profile>`	Name of MAC authentication profile to copy.	—	—
`delimiter`	Use this command to specify the format of the delimiter (colon, dash, none, or oui-nic) used in the MAC string.	colon|dash|none|oui-nic	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 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa authentication mgmt

```
aaa authentication mgmt
   default-role {root | network-operations | read only | location-api-mgmt | no access |
   location-api-mgmt}
   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
`root`	Default role, super user role.		
`network-operations`	Network operator role.		
`read only`	Read-only role.		
`location-api-mgmt`	Location API management role.		
`no acesss`	None of the commands are accessible for this role.		
`enable`	Enables authentication for administrative users.	enabled| disabled	disabled
`no`	Negates any configured parameter.	—	—
`server-group <group>`	Use this command to name a server group for management authentication.	—	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.

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 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

aaa authentication wired

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

Description

This command configures authentication globally with the aaa profile.

Syntax

Parameter	Description
`no`	Negates any configured parameter.
`aaa-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.

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
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

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 <filter>
   host <ipaddr>
   key-attribute <string>
   max-connection
   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>`	Use this command for the name of the search for the LDAP server. For example: • cn=users • dc=qa • dc=domain • dc=co	—	—
`clone <server>`	Name of an existing LDAP server configuration from which parameter values are copied.	—	—

Parameter	Description	Range	Default
`enable`	Enables the LDAP server.	—	
`filter <filter>`	Use this command as the filter that should be used as a key in a search for the LDAP server. The default filter string is: (objectclass=*).	—	(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. • The value for PAP is sAMAccountName • The value for EAP-TLS is userPrincipalName	—	sAMAccountName
max-connection	The maximum number of simultaneous non-admin connections that are allowed on the LDAP server.	1-16	4
`no`	Negates any configured parameter.	—	—
`preferred-conn-type`	Preferred connection type. The default order of connection type is: • ldap-s • start-tls • 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>`	Use this command to set the timeout period for an LDAP request.	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 55).

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa authentication-server radius

```
aaa authentication-server radius <server>
   acctport <port>
   authport <port>
   clone <server>
   cppm username <username> password <password>
   enable
   host <ip-address>
   key <psk>
   nas-identifier <string>
   nas-ip <ipaddr>
   no ...
   retransmit <number>
   source-interface vlan <vlan>
   timeout <seconds>
   use-md5
```

Description

This command configures a RADIUS server.

Syntax

Parameter	Description	Range	Default
`<server>`	Name that identifies the server.	—	—
`acctport <port>`	Use this command to configure the port number for accounting.	1–65535	1813
`authport <port>`	Use this command to configure the port number for authentication.	1–65535	1812
`clone <server>`	Use this command to copy parameters from another RADIUS server.	—	—
`cppm username <username> password <password>`	Configures CPPM username and password.	—	—
`enable`	Enables the RADIUS server.	—	—
`host`	Use this command to configure IP address/Hostname of radius server..	—	—

Parameter	Description	Range	Default
`<ip-address>`	IP address of the RADIUS server.	—	—
`key <psk>`	Shared secret between the switch and the authentication server.	—	—
`nas-identifier <string>`	Use this parameter to identify the Network Access Server (NAS) 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

Parameter	Description	Range	Default
`source-interface vlan <vlan>`	Allows you to use source IP addresses to differentiate RADIUS requests. Associates a VLAN interface with the RADIUS server to allow the server-specific source interface to override the global configuration. • If you associate a Source Interface (by entering a VLAN number) with a configured server, then the source IP address of the packet will be that interface's IP address. • If you do not associate the Source Interface with a configured server (leave the field blank), then the IP address of the global Source Interface will be used.	—	—
`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).

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

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4.0.2	A new parameter, **cppm username <username> password <password>**, to configure CPPM server credentials is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa authentication-server tacacs

```
aaa authentication-server tacacs <server>
   clone <source>
   enable
   host <ip-address>
   key <psk>
   no ...
   retransmit <number>
   session-authorization
   source-interface {loopback | vlan <id> [secondary <ip>]}
   tcp-port <port>
   timeout <seconds>
```

Description

This command configures a TACACS+ server.

Syntax

Parameter	Description	Range	Default
`<server>`	Name that identifies the server.	—	—
`clone <source>`	Name of an existing TACACS server configuration from which parameter values are copied.	—	—
`enable`	Enables the TACACS server.	—	
`host <ip-address>`	Use this command to configure the IP address of the TACACS server.	—	—
`key`	Use this command to configure a preshared key to authenticate communication between the TACACS client and server.	—	—
`no`	Negates any configured parameter.	—	—
`retransmit <number>`	Use this command to set the maximum number of times a request can be retried.	0–3	3
`session-authorization`	Enables TACACS+ session authorization. Session-authorization turns on the optional authorization session for admin users.	—	disabled

Parameter	Description	Range	Default
`source-interface {loopback | vlan <id> [secondary <ip>]}`	Configures the profile-level source-interface option. The loopback parameter helps assign the switch IP as the source IP. The vlan <id> [secondary <ip>] parameter helps assign the IP address of the specified VLAN interface as the source IP and an optional secondary source IP in A.B.C.D format.		
`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).

Example

The following command configures and enables a TACACS+ server as well as helps enable session authorization:

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

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4.1	The **source-interface** parameter and its options are introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa authentication-server windows (deprecated)

```
aaa authentication-server windows <windows_server_name>
```

Description

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

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.2	Deprecated.

aaa auth-survivability

```
aaa auth-survivability
   cache-lifetime <1-72>
   disable
   enable
   server-cert <server-cert-name>
```

Description

This command helps enable authentication survivability (or auth survivability) in Mobility Access Switches.

Syntax

Parameter	Description	Range	Default
`cache-lifetime <1-72>`	Specifies lifetime of the cached credential for survival server.	1–72	—
`disable`	Disables authentication survivability feature.	—	—
`enable`	Enables Disables authentication survivability feature.	—	
`server-cert <server-cert-name>`	Specifies Server Certificate for Survival Server.	—	—

Usage Guidelines

Enable this feature to support a survivable authentication framework against the remote link failure when working with the CPPM authentication servers. When enabled, this feature allows the Mobility Access Switches to authenticate the previously connected clients against the cached credentials if the connection to the authentication server is temporarily lost.

For EAP-TLS authentication, ensure that CPPM 6.5.1 or later version is used for authentication.

The cached credentials of a client will be deleted, if it fails the authentication via CPPM server. The credentials will be cached again if the subsequent authentication is successful.

The AAA timer dead time, by default, is set at 10 minutes. You can change it to 0 to disable the dead time.

```
(host) (config) #aaa timers dead-time ?
<0-60>      Auth server dead time in Minutes (Default is 10 minutes).
```

Example

The following command enables the authentication survivability feature in the Mobility Access Switch:

```
(host) (config) #aaa auth-survivability enable
```

Execute the following command to set the duration after which the authenticated credentials in the cache must expire:

```
(host) (config) #aaa auth-survivability cache-lifetime <1-72>
```

Execute the following command to specify a server certificate which will be used by the survival server to terminate EAP-TLS for 802.1X authentication:

```
(host)(config) #aaa auth-survivability server-cert <server-cert-name>
```

Command History

Release	Modification
ArubaOS 7.4.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa derivation-rules

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

Description

This command configures rules which assigns a role or VLAN to a client.

Syntax

Parameter	Description
`<STRING>`	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
`<attribute> <value>`	Specify one of the following conditions: • **contains:** Check if attribute *contains* the string in the <value> parameter. • **ends-with:** Check if attribute *ends with* the string in the <value> parameter. • **equals:** Check if attribute *equals* the string in the <value> parameter. • **not-equals:** Check if attribute *is not equal* to the string in the <value> parameter. • **starts-with:** Check if attribute *starts with* the string in the <value> parameter.
`set-value <STRING>`	Specify the user role or VLAN ID to be assigned to the client if the 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

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.

Examples

The example rule shown below sets a user role for clients whose mac address starts with 0C.

```
aaa derivation-rules user MAC-rules
   set role condition mac-addr starts-with 0C set-value mac_role1
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa inservice

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

Description

Use this command to bring an authentication server into 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

Release	Modification
ArubaOS 7.0	This command was introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

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`	Command provides the ability to reduce the number of passwords that can be guessed in a short period of time. It automatically clears the lockout after the configured "lock-out" minutes. 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`	Command configures the number of minutes a user is locked out. The lockout is cleared without administrator intervention. Range: 1 min to 1440 min (24 hrs). Default: 3.
`password-max-character-repeat`	Configures 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.
`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.

Parameter	Description
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. SeeUsage Guidelines 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: |	

Allowed Characters	Disallowed Characters
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
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Management Password Policy

aaa profile

```
aaa profile <profile-name>
   authen-failure-blacklist-time <seconds>
   authentication-dot1x <profile-name>
   authentication-mac <profile-name>
   clone <profile>
   dot1x-default-role <role>
   dot1x-server-group <group>
   download-role
   enforce-dhcp
   initial-role <role>
   l2-auth-fail-through
   mac-default-role <role>
   mac-limit <mac_limit> action {log | drop | shutdown [auto-recovery-time <timeout>]}
   mac-server-group <group>
   no ...
   preauth
   radius-accounting <server-group-name>
   radius-interim-accounting
   rfc-3576-server
   sip-authentication-role
   unreachable-role
   user-derivation-rules <profile>
   xml-api-server
```

Description

This command configures the AAA profile.

Syntax

Parameter	Description	Default	Range
`<profile-name>`	Name that identifies this instance of the profile.	"default"	
`auth-failure-blacklist-time`	Use this command to set the amount of time, in seconds, to blacklist a STA if it fails repeated authentications. A value of 0 blocks indefinitely.	—	
`authentication-dot1x <profile-name>`	Name of the 802.1x authentication profile associated with the AAA profile.	—	
`authentication-mac <profile-name>`	Name of the MAC authentication profile associated with the AAA profile.	—	
`clone <profile>`	Name of an existing AAA profile configuration from which parameter values are copied.	—	

Parameter	Description	Default	Range
`dot1x-default-role <role>`	Use this command to assign a dot1x default role. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role.	guest	
`dot1x-server-group <group>`	Name of the server group used for 802.1x authentication.	—	
`download-role`	Use this command to download the role attribute details from ClearPass Policy Manager (CPPM) and assign the role to the client, iIf the user-role does not exist in Mobility Access Switch,	enabled	
`enforce-dhcp`	Use this command to obtain IP address using DHCP.		
`initial-role <role>`	Use this command to a assign role to a user before authentication takes place.	logon	
`l2-auth-fail-through`	Use this command to proceed with the next available authentication mechanism when one fails.		
`mac-default-role <role>`	Use this command to a assign a MAC authentication default role. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role.	guest	
`mac-limit <mac_limit>`	Use this command to enable the MAC limit option and configure the number of MAC addresses that can be allowed on an untrusted port.	`disabled`	`1-512`

Parameter	Description	Default	Range
`action {log | drop | shutdown}`	Specifies the action to take when the number of MAC addresses exceeds the configured limit. • **log**— a syslog is generated and the interface is marked as interface error **log**; any new MAC addresses beyond the configured MAC limit are dropped by the software. • **drop**— a syslog is generated and the interface is marked as interface error **drop**; any new MAC addresses beyond the configured MAC limit are dropped by the hardware. • **shutdown**—a syslog is generated and the interface is marked as interface error **shutdown**; the interface is brought down; recovery can be done either by clearing the interface error from CLI or configuring the auto-recovery-time option to bring the port UP on timer expiry.	—	—
`auto-recovery-time <timeout>`	The auto-recovery timer applies only when you have configured the **shutdown** action.	—	0–65535 s
`mac-server-group <group>`	Name of the server group used for MAC authentication. See.	—	
`no`	Negates any configured parameter.	—	
`preauth`	Enables the **preauth** role on the Mobility Access Switch. This role is assigned to a client until it derives the final role after passing through all the configured authentication methods. Hence, the policies defined on an intermediate role do not get applied on the client traffic. This avoids the clients from obtaining an IP address through DHCP in a subnet different from the final VLAN derived.	Disabled	

Parameter	Description	Default	Range
`radius-accounting <server-group-name>`	Use this command to assign a server group for RADIUS accounting.	—	
`radius-interim-accounting`	Use this command to send RADIUS interim accounting records.		
`rfc-3576-server`	Use this command to configure RFC server with AAA profile.		
`sip-authentication-role <role>`	Role applied to a user after a successful SIP authentication.		
`unreachable-role <role>`	Role applied to a user when AAA servers are unreachable.		
`user-derivation-rules <profile>`	User attribute profile from which the user role or VLAN is derived.	—	

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.

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 zachjennings
   authentication-dot1x dot1xprof
```

Enable the MAC Limit option on the untrusted ports of Mobility Access Switches using the following CLI command:

```
(host) (config) #aaa profile <profile-name>
(host) (AAA Profile "<profile-name>") #mac-limit <mac_limit> action {log | drop | shutdown
[auto-recovery-time <timeout>]}
```

This command enables the MAC limit option, includes the number of MAC addresses that can be allowed on an untrusted port, and the action to take when the number of MAC addresses exceeds the configured limit.

Related Command

Command	Description
show port-error-recovery	This command is used to verify that the configured action was enforced when the number of MAC addresses exceeded the configured MAC limit on untrusted port.
clear port-error-recovery	This command is used to manually recover the port errors on a specific interface or on all interfaces. In this case, you can clear the log/drop/shutdown errors on all untrusted ports or on a specific interface.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.2	The **download-role** parameter was introduced.
ArubaOS 7.2.3	The **unreachable-role** command was introduced.
ArubaOS 7.3.1	The **preauth** command was introduced.
ArubaOS 7.4.1.9	The **mac-limit** parameter and the **action** subparameter were introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa query-user

```
aaa query-user <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.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

aaa radius-attributes

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

Description

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

Syntax

Parameter	Description
`<STRING>`	Attribute name (alphanumeric string).
`<INT>`	Associated attribute ID (integer), and type (date, integer, IP address, or string).
`date`	Attribute type is Date.
`integer`	Attribute type is Integer.
`ipaddr`	Attribute type is IP address.
`string`	Attribute type is String.

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 "Aruba-User-Role":

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

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa rfc-3576-server

```
aaa rfc-3576-server <server-ip-addr>
   key <psk>
   no
```

Description

This command designates 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
`<server-ip-addr>`	IP address of the server.
`key <psk>`	Shared secret to authenticate communication between the RADIUS client and server.
`no`	Negates any configured parameter.

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>`	Variable name of the server group.	—
`allow-fail-through`	Command allows traffic that fails authentication to connect with the server.	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.	

Parameter	Description	Default
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.	—
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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa tacacs-accounting server-group

```
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`	Enable accounting of all commands of specified type.	—	—
`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 36 and aaa server-group on page 55).

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa test-server

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

Description

Use this command to test the MSCHAPV2 and PAP authentication servers..

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.
`<password>`	Password to use to test the authentication server.

Usage Guidelines

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

Example

The following commands verifies that the internal database is responding correctly:

```
aaa test-server pap internal kgreen lkjHGfds

Authentication successful
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

aaa timers

```
aaa timers
   dead-time <minutes>
   idle-timeout <number>
   logon-lifetime <0-255>
   stats-timeout <1-300>
```

Description

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

Syntax

Parameter	Description	Range	Default
`dead-time <minutes>`	Option to set the authentication server dead time in minutes.	0-50	10 minutes
`idle-timeout <1-15300>`	Option to set user logon lifetime in minutes or seconds.	1 to 255 minutes (30 to 15300 seconds)	5 minutes (300 seconds)
`logon-lifetime`	Option to set user logon lifetime in minutes.	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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

aaa user clear-sessions

```
aaa user clear-sessions <ip address>
```

Description

This command clears ongoing sessions for the specified client.

Syntax

Parameter	Description
`<ip-addr>`	IP address variable.

Example

The following command clears ongoing sessions for a client:

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

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

aaa user delete

```
aaa user delete <ip address> | all | ap-ip-addr | ap-name | mac | name | role
```

Description

This command deletes user sessions.

Syntax

Parameter	Description
`<ip address>`	IP address variable
`all`	Delete all users
`mac <mac address>`	Match MAC address
`name <STRING>`	Match user name
`role <STRING>`	Match role name

Example

The following command deletes a role:

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

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

aaa user logout

```
aaa user logout <ip address>
```

Description

Use this command to logout a user's IP address.

Syntax

Parameter	Description
`<ipaddr>`	IP address variable.

Usage Guidelines

This command logs out an authenticated user.

Example

The following command logs out a client:

```
aaa user logout 10.1.1.236
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

activate firmware

```
activate firmware check|upgrade
```

Description

Issue this command to trigger the Activate firmware upgrade services.

Syntax

Parameter	Description
`check`	The **activate firmware check** command enables the Mobility Access Switch to automatically check Activate to see if there is a new image version to which that switch can upgrade.
`upgrade`	If the **activate firmware check** command shows that a new version is available, the **activate firmware upgrade** command prompts the Mobility Access Switch to attempt to download and upgrade to the new image.

Usage Guidelines

If the **activate firmware check** command shows that a new version is available, you will be prompted to download and upgrade to the new image.

Example:

```
(host)(config)# activate firmware update
This might take several minutes and will result in reloading the device.
Do you want to proceed? [y/n]:
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable mode

activate-service-firmware

```
activate-service-firmware
```

Description

Issue this command to enable or disable the Activate firmware upgrade services. These features are enabled by default.

Syntax

Parameter	Description
`enable`	Issue the command **activate-service-firmware enable** to enable this feature.
`no`	Disable this feature using the command **activate-service-firmware no enable**.

Usage Guidelines

If the Activate firmware service is enabled, the **activate firmware check** command enables the Mobility Access Switch to automatically check Activate to see if there is a new image version to which that switch can upgrade. If a new version is available, the **activate firmware upgrade** command prompts the Mobility Access Switch to attempt to download and upgrade to the new image.

Example:

```
(host)(config)#  #activate-service-firmware enable
```

Related Commands

Parameter	Description
`show activate-service-firmware`	Issue this command to verify that the Activate firmware upgrade services are either enabled or disabled.

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration mode

add stacking

```
add stacking interface stack <module/port> [member <id> | all]
```

Description

Add a stacking interface to a specified member or to all ArubaStack members.

Syntax

Parameter	Description
`interface stack <module/port>`	Enter the keywords **interface stack** followed by the stacking interface in module/port format.
`[member <id> | all]`	Enter the keyword **member** followed by the member ID number or to add stacking interface to all members, enter the keyword **all**.

Usage Guidelines

Use this command to add a stacking interface; it also converts existing network interfaces to stacking ports.

Example

The following example adds an interface to all members of the ArubaStack.

```
(host)(config) #add stacking interface stack 1/2 member all
```

If an interface is already configured on the ArubaStack, a message is returned as follows:

```
(host)(config) #add stacking interface stack 1/2 member all

Member-id: 0
============
Interface already configured for stacking

Member-id: 1
============
Interface already configured for stacking

Member-id: 2
============
Interface already configured for stacking
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

arp

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

Description

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

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
```

Related Commands

Command	Description
show arp	Displays all the ARP entries.

Command History

Release	Modification
ArubaOS 7.4	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode.

aruba-central

```
aruba-central
   enable
   no
```

Description

This command enables Mobility Access Switch to connect to the Aruba Central portal through Activate.

Syntax

Parameter	Description
`enable`	Enables the Mobility Access Switch to poll Activate and connect to Aruba Central.
`no`	Disables the Mobility Access Switch from polling Activate for Aruba Central URL.

Usage Guidelines

This command is enabled by default. You can disable this if you do not wish to manage your switch through Aruba Central.

Example

The following command configures enables the Mobility Access Switch to poll Activate for Aruba Central portal URL:

```
(host) (config) #aruba-central
(host) (Aruba Central) #enable
```

Related Commands

Command	Description
show aruba-central	Displays the status of Aruba Central configuration on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.3.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode.

auto-config

```
auto-config disable
```

Description

Use this command to disable auto configuration.

Syntax

Parameter	Description	Default
`Disable`	Disables auto configuration.	Enabled

Example

```
(host)#auto-config disable
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable

backup

```
backup {flash}
```

Description

This command backs up compressed critical files in flash.

Syntax

Parameter	Description
`flash`	Backs up flash directories to flashbackup.tar.gz file.

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Config

backup interface

```
backup interface [gigabitethernet <slot/module/port> | port-channel <number>]
```

Description

Configure the backup interface.

Syntax

Parameter	Description	Range	Default
`gigabitethernet <slot/module/port>`	Enter the keyword **gigabitethernet** followed by the slot, module, port of the Gigabit Ethernet interface you want to add to HSL as a backup.	—	—
`port-channel <number>`	Enter the keyword **port-channel** followed by the port-channel number of the port channel interface you want to add to HSL as a backup.	0 to 7	—

Usage Guidelines

When a primary link goes down, the backup link becomes active. By default, when the link comes up it goes into the standby mode as the other interface is activated.

Example

In the following example, the primary interface is Gigabit Ethernet 0/0/10 and the backup interface is Gigabit Ethernet 0/0/11:

```
(host) (config) #interface gigabitethernet 0/0/10
(host) (gigabitethernet "0/0/10") #backup interface gigabitethernet 0/0/11
```

Related Command

Command	Description
show hot-standby-link	List the status of hot standby link interfaces.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Interface Config (gigabitethernet "*slot/module/port*") or (port-channel *number*)

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 Mobility Access Switch.

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 Mobility Access Switch. The banner is specific to the Mobility Access Switch 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 Mobility Access Switch 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 Mobility Access Switch. This Mobility Access
Switch 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 Mobility Access Switch. This Mobility Access Switch 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 Mobility Access Switch. This Mobility Access Switch 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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

boot

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

Description

This command reloads the switch.

Syntax

Parameter	Description
`cf-test`	Sets the type of compact flash test to run at boot time.
`fast`	Performs a fast test with no media tests.
`read-only`	Performs a read only media test.
`read-write`	Performs a read-write media test.
`config-file`	Configures the boot file the system uses to boot.
`<file-name>`	Name of boot file.
`oldpartition`	Repartition to old 50M image layout.
`system: 0|1`	Enter the keyword system followed by the partition number (0 or 1) that you want the switch to use during the next boot (login). NOTE: A reload is required before the new boot partition takes effect.
`verbose`	Prints extra information for debugging the system at boot time.

Usage Guidelines

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

- `cf-test`

  Test the flash during boot.
- `config-file`

  Sets the configuration file to use during boot.
- `system`

  Specifies the system partition on the switch to use during the next boot (login).
- `verbose`

  Print extra debugging information during boot. The information is sent to the screen at boottime. 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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Configuration Mode (config)

clear

```
clear
   aaa
   arp
   counters
   crash
   crypto
   datapath
   dhcp-snooping-database
   diagnostics
   dot1x
   igmp-snooping
   interface
   ip
   ipc
   lldp
   log
   loginsession
   mac-address-table
   mac-learning-log
   mld-snooping
   neighbor-devices
   port
   port-error-recovery interface
   rmon log-table
   snmp
   stacking
   vrrp
```

Description

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

Syntax

Parameter	Description
aaa	Clears 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—Clears all server statistics. • internal—Clears Internal server statistics. • ldap—Clears LDAP service statistics. • radius—Clears RADIUS server statistics. • tacacs—Clears TACACS server statistics.
state	Clears internal status of authentication modules. Parameters: • configuration—Clears all configured objects. • debug-statistics—Clears debug statistics. • messages—Clears authentication messages that were sent and received.
arp	Clears ARP entries. • arp ip—Clears the specified IP address ARP from the ARP Table • all—Clears the entire ARP Table
counters	Clears the counters in one of the following interfaces: • gigabitethernet—Clear counters for a gigabit ethernet interface port. • oam—Clear operation, administration, and management counters. • port-channel id or all—Clears port channel from all interfaces or a specified ID (range 0 to 7) • stacking interface stack—module/port to clear counters of a specific stacking interface or all to clear counters of all stacking interfaces. • tunnel—Clear counters for a particular tunnel or all tunnels.
crash	Clears crash files and directories.
crypto	Clears the following crypto state: • dp—Clears crypto latest DP packets. • ipsec sa peer <ip-address>—Delete active IPSec sessions or force IPSec to re-establish new Security Association (SA) for a peer IP. • isakmp sa peer <source-ip>—Clears active IKE connections for a peer IP.

Parameter	Description
`datapath`	Clears datapath statistics from policer management-counter statistic
`dhcp-snooping-database`	Clears DHCP snooping configuration. • all—Clears dynamic DHCP snooping entries on all the interfaces • vlan<id>—Clears DHCP snooping configuration on a specific VLAN ID. • vlan<id> mac—Clears dynamic dhcp snooping entries on a specific VLAN ID with the specific mac address.
`diagnostics interface gigabitethernet`	Clears the Time-Domain Reflectometer (TDR) on a specific interface or all interfaces: • <slot/module/port> cable • all cable
`dot1x`	Clears all 802.1x specific counters and supplicant statistics. Use the following parameters: • counters • supplicant-info
`igmp-snooping`	Clears IGMP Snooping statistics: • counters—Clears statistics • membership—Clears membership • mrouter—Clears dynamically learnt multicast router port
`interface local management ip-address member <member-id>`	Clears the local management interface IP address of the member ID
`ip dhcp binding`	Clears DHCP server binding
`ipc`	Clears all inter process communication statistics.
`lldp`	Clears LLDP statistics interface gigabitethernet in slot/module/port format.
`log`	Clears the following log information: • all—Clears all logging information from the Mobility Access Switch. • errorlog—Clears system error and critical error logs. • network—Clears network-specific logs. • security—Clears security-specific logs. • system—Clears system-specific logs. • user—Clears user-specific logs. • user-debug—Clears user-debug logs.
`loginsession`	Clears login session information for a specific login session, as identified by the session id.
`mac-address-table`	Clears the MAC forwarding table.
`mac-learning-log`	Clears the MAC learning logs

Parameter	Description
`mld-snooping`	Clears the following Multicast Listener Discovery (MLD) snooping statistic/configuration: • counters—Clear MLD snooping statistics. • membership vlan <id>—Clear MLD snooping membership on a VLAN. • mrouter vlan <id>—Clear dynamically learnt multicast router port on VLAN.
`neighbor-devices`	Clears the following neighbor device information: • cdp-statistics interface gigabitethernet <slot/module/port>— Clears CDP RX statistics for a gigabit ethernet port. • interface gigabitethernet <slot/module/port>—Clears neighbor device information for a gigabit ethernet interface port.
`port`	Clears all port statistics that includes link-event counters or all counters. Use the following parameters: • link-event • stats
`port-error-recovery interface`	Clears the following layer 2 interface port errors: • gigabitethernet <slot/module/port> • port-channel
`rmon log-table`	Clears RMON log table.
`snmp`	Clears the following SNMP parameters: • fault—Clears a specific or all faults. • trap-queue—Clears SNMP traps in queue.
`stacking member-id <id>`	Clears a stack member ID to free up a slot number from the active stack. This is applied to all stack members from the Primary. **NOTE:** You can not execute this command from a Line Card.
vrrp <id> statistics	Clears VRRP operational statistics.

Usage Guidelines

The command clears 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
```

The following example clears system and critical error logs from the Mobility Access Switch:

```
(host) #clear log errorlog
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1	Introduced **stacking** and **diagnostics** parameters (TDR statistics).
ArubaOS 7.3	Introduced the **dhcp-snooping-database, log**, and **vrrp <id> statistics** parameters.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

clear arp

```
clear arp {all|<ip-address>}
```

Description

This command clears the entries in the ARP table.

Syntax

Parameter	Description
`all`	Clears all the entries in the ARP table.
`<ip-address>`	Clears only the specified IP address in the ARP table.

Usage Guidelines

Use this command to clear the entries in the ARP table.

Example

```
(host)(config) #clear arp all
```

Related Command

Command	Description
show arp	Displays the list of ARP entries.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

clear ip ospf

```
clear ip ospf {process | statistics [interface vlan <id>]}
```

Description

Clears the dynamic OSPF related information.

Syntax

Parameter	Description
`process`	Restarts the OSPF process.
`statistics`	Clears the OSPF statistics.
`interface vlan <id>`	Specifies the VLAN interface.

Example

The example below restarts the OSPF process.

```
(host) #clear ip ospf process
```

The example below clears the dynamic OSPF related information.

```
(host) #clear ip ospf statistics interface vlan 1
```

Related Command

Command	Description
`router ospf`	Configures the global OSPF parameters.
`interface-profile ospf-profile`	Configures an OSPF interface profile.

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration

clear mac-address-table

```
clear mac-address-table [vlan <vlan-id>]|[interface {gigabitethernet <slot/module/port>}|
{port-channel <id>}]|[mac <mac address>]|sticky
```

Description

This command clears all learned MAC addresses stored in the MAC address table.

Syntax

Parameter	Description
`vlan <vlan-id>`	Clear MAC addresses learned on the specified VLAN.
`interface gigabitethernet <slot/module/port>`	Clear MAC addresses learned on the specified Gigabit Ethernet port.
`interface port-channel <id>`	Clear MAC addresses learned on the specified port-channel.
`sticky`	Clear all the sticky MAC address.

Example

The following example removes MAC addresses learned on VLAN 1 from the MAC address table.

```
(host)(config) #clear mac-address-table vlan 1
```

The following example removes a specific Sticky MAC address on an interface from the MAC address table:

```
(host)(config)# clear mac-address-table interface <interface-name> mac <mac address> sticky
```

Related Command

Command	Description
`show mac-address-table`	Displays the MAC address table

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4	The `sticky` parameter is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config mode (config)

clear mld-snooping counters vlan

```
clear mld-snooping counters vlan <id>
```

Description

This command clears MLD-Snooping counters on a VLAN.

Example

```
(host) #clear mld-snooping counters vlan 1
```

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

clear mld-snooping membership vlan

```
clear mld-snooping membership vlan <id>
```

Description

This commands clears MLD-Snooping membership on a VLAN.

Example

```
(host) #clear  mld-snooping membership vlan 1
```

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

clear mld-snooping mrouter vlan

```
clear mld-snooping mrouter vlan <id>
```

Description

This commands clears multicast router port a specific VLAN.

Example

```
(host) #clear  mld-snooping mrouter vlan 1
```

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

clear port-error-recovery

```
clear port-error-recovery [interface {gigabitethernet <slot/mod/port> | port-channel <id>} |
statistics | untrusted {interface gigabitethernet <slot/mod/port>}]
```

Description

This command is used to manually recover the port errors on a specific interface or on all interfaces.

Syntax

Parameter	Description
`interface {gigabitethernet <slot/mod/port> | port-channel <id>}`	Optional parameter to specify the trusted interface on which you want to clear the port errors.
`statistics`	Optional parameter to clear port errors and recovery statistics.
`untrusted interface {gigabitethernet <slot/mod/port>}`	Optional parameter to clear log/drop/shutdown errors in the following cases: • All untrusted ports. • A specific untrusted port by using the **interface** parameter.

Usage Guidelines

Use this command to manually recover the port errors on a specific interface or on all interfaces.

Example

The following command clears the errors on gigabitethernet 0/0/42:

```
(host) (config) #clear port-error-recovery interface gigabitethernet 0/0/42
```

The following command clears the errors on port channel 3:

```
(host) (config) #clear port-error-recovery interface port-channel 3
```

The following command clears the port errors on all the interfaces:

```
(host) (config) #clear port-error-recovery
```

Execute the following **clear** command to clear the log/drop/shutdown errors on a specific untrusted interface:

```
(host) #clear port-error-recovery untrusted interface gigabitethernet <slot>/<module>/<port>
```

Execute the following **clear** command to clear the log/drop/shutdown errors on all untrusted ports:

```
(host) #clear port-error-recovery untrusted
```

Command History

Release	Modification
ArubaOS 7.1.3.0	This command was introduced.
ArubaOS 7.4.1.9	The **untrusted** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

clear rmon log-table

```
clear rmon log-table
```

Description

This command clears all the entries from the rmon log-table.

Syntax

No parameters.

Usage Guidelines

Use this command to clear all the entries from the rmon log-table.

Example

```
(host) #show rmon log-table

RMON Log Table:
---------------
Log Id  Event Id  Creation Time       Description
------  --------  -------------       -----------
2       3         3-21-2012@20-08-18  Falling threshold log: ifHCInOctets.455
1       3         3-21-2012@20-07-22  Rising threshold log: ifHCInOctets.455


(host) #clear rmon log-table
(host) #show rmon log-table

RMON Log Table:
---------------
Log Id  Event Id  Creation Time  Description
------  --------  -------------  -----------
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

clock set

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

Description

This command sets the date and time.

Syntax

Parameter	Description	Range	Default
`year`	Sets the year. Requires all 4 digits.	—	Numeric
`month`	Sets the month. Requires the first three letters of the month.	—	Alphanumeric
`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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

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 time zone 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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration Mode

clock timezone

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

Description

This command sets the time zone on the controller.

Syntax

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

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 time zone is set to UTC.

Example

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

```
clock timezone PST -8
```

Command History

This command was introduced in ArubaOS 7.0

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

clone

```
clone <source>
```

Description

Copy (*clone*) data from another (source) PVST+ profile.

Syntax

Parameter	Description
`<source>`	Enter the name of the PVST profile that you want to clone (copy).

Example

In the example below, the data from profile *default* is copied to the profile *TechPubs*.

```
(host)(pvst-profile "TechPubs") #clone default
```

Related Command

Command	Description
`show vlan-profile pvst-profile`	Display the settings for the specified profile name.

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config Mode (`pvst-profile "<profile-name>"`) and (`interface-profile pvst-port-profile <profile-name>`)

copy flash:

```
copy flash: <srcfilename> <destination> <destfilename>
```

Description

Copy files from flash file system.

Syntax

Parameter	Description
`<srcfilename>`	Enter the name of the file you are copying from.
`<destination>`	Destination can be any one of the following: • flash: • ftp: • tftp: • scp: • member flash: • usb: <usbfilename> [usbpartition <number>] • member <id> usb: <usbfilename> [usbpartition <number>]
`<destfilename>`	Enter the name of the destination file.

Usage Guidelines

Use this command to copy a file from the flash file system.

Example

The following command copies the file techpubs to techpubs2 in the flash.

```
(host)#copy flash: techpubs flash: techpubs2
```

If your file names are invalid, the system will alert you as follows:

```
Invalid file name
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3	Following options were added for destination. • member flash: • usb: <usbfilename> [usbpartition <number>] • member <id> usb: <usbfilename> [usbpartition <number>]

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

copy ftp:

```
copy ftp: <ftphost> <user> <imagefilename> [member: <id>] system: <partition 0|1>]
```

Description

Copy from a ftp host to upgrade either the system or a specified member.

Syntax

Parameter	Description
`<ftphost>`	Enter the IP address of your FTP server in dotted decimal format.
`<user>`	Enter the user name.
`<imagefilename>`	Enter the image file name.
`member: <id>`	Optionally, enter the keyword **member:** followed by the member's ID to upgrade a particular member from the FTP server.
`system: <partition 0|1>`	Optionally, enter the keyword **system: partition** followed by the partition number (either **0** or **1**) to upgrade from the FTP server to the specified partition.

Usage Guidelines

Use this command to copy files or to copy an image for upgrade to a system partition or to a specified member. For more information about upgrading, see the Upgrade Chapter of the Release Notes.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

copy member:

```
copy member: <member id> {flash: <srcfilename> <destination> <destfilename>} | {usb:
<filename> [usbpartition <number>] <destination> <destfilename>}
```

Description

Copy a file from a member's flash to a <destination>.

Syntax

Parameter	Description
`member: <id>`	Enter the keyword **member:** followed by the member's ID.
`<srcfilename>`	Enter the name of the file you are copying from.
`<destination>`	Enter one of the following: • ftp: • scp: • tftp: • usb • member <id> flash • member usb
`<destfilename>`	Enter the name of the destination file.
`usb:`	External USB.
`<filename>`	Enter the complete path to the file on your USB device.
`usbpartition <number>`	Enter the USB partition number.
`<destination>`	Enter one of the following: • ftp: • scp: • tftp: • usb • member <id> flash • member usb
`<destfilename>`	Enter the name of the destination file.

Usage Guidelines

Copy from a designated stack member's flash.

Example

The following command copies the file on a member to a flash via

```
(host)#copy member: 2 flash: techpubs1 ftp: techpubs2
```

If your file names are invalid, the system will alert you as follows:

```
Invalid file name
```

Related Command

Command	Description
copy flash:	Copy from flash to a destination.
copy ftp:	Upgrade via FTP server.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4	The **usb** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

copy running-config

```
copy running-config <destination> <destfilename>
```

Description

Copy the running configuration to the USB or Flash.

Syntax

Parameter	Description
<destination>	Destination can be any one of the following: • flash: • ftp: • member: • scp: • startup-config • tftp: • usb:
<destfilename>	Enter the name of the destination file.

Usage Guidelines

Use this command to copy a running configuration file into the flash or USB:

Example

The following command copies the file techpubs to techpubs2 in the flash.

```
(host)#copy running-config flash: techpubs2
```

If your file names are invalid, the system will alert you as follows:

```
Invalid file name
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3	Following options were added for destination. • **member flash:** • **usb:** • **scp:**

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

copy scp:

```
copy scp: <scphost> <username> <filename> [flash: <destfilename> [member: <id>] system:
<partition 0|1>]
```

Description

Copy using secure file transfer (scp).

Syntax

Parameter	Description
`<scphost>`	Enter the SCP host address in dotted decimal format.
`<username>`	Enter the user name for the secure login.
`<filename>`	Enter the file name to copy.
`flash: <destfilename>`	Enter the keyword **flash:** followed by the destination file name.
`member: <id>`	Enter the keyword **member:** followed by the member's ID.
`system: <partition 0|1>`	Enter the keyword **system: partition** followed by the partition number (either **0** or **1**).

Usage Guidelines

Use this command to copy files or to copy an image for upgrade. For more information about upgrading, see the Upgrade Chapter of the Release Notes.

Example

Below is an upgrade example using the scp. The bold type is entered by the user, the remainder is generated by the system.

```
(host)#copy scp: 1.1.1.1 tftp ArubaOS_MAS_7.1.0.0_30627 system: partition 0
Password:****

The authenticity of host '1.1.1.1 (1.1.1.1)' can't be established.
RSA key fingerprint is 0d:c8:a2:74:ec:3f:16:5e:78:61:3e:33:3f:2f:4b:c4.

Are you sure you want to continue(y/n): y

Upgrading partition 0
Secure file copy:.............................
File copied successfully.
Saving file to flash:...
Member-2:The system will boot from partition 0 during the next reboot.
......
Member-0:The system will boot from partition 0 during the next reboot.
Member-1:The system will boot from partition 0 during the next reboot.
```

Related Commands

Command	Description
copy ftp:	Copy using a FTP server.
copy tftp:	Copy using a TFTP server

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

copy startup-config

```
copy startup-config <destination> <destfilename>
```

Description

Copy the startup configuration options to USB or flash.

Syntax

Parameter	Description
`<destination>`	Destination can be any one of the following: • flash: • ftp: • tftp: • scp: • member : • usb:
`<destfilename>`	Enter the name of the destination file.

Usage Guidelines

Use this command to copy the startup configuration options to USB or flash.

Example

The following command copies the startup configuration to techpubs in the USB.

```
(host)#copy startup-config usb: techpubs
```

If your file names are invalid, the system will alert you as follows:

```
Invalid file name
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3	Following options were added for destination. • scp: • member : • usb

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

copy tftp:

```
copy tftp: <ftphost> <user> <imagefilename> [member: <id>] system: <partition 0|1>]
```

Description

Copy from a tftp host to upgrade either the system or a specified member.

Syntax

Parameter	Description
`<ftphost>`	Enter the IP address of your FTP server in dotted decimal format.
`<user>`	Enter the user name.
`<imagefilename>`	Enter the image file name.
`member: <id>`	Optionally, enter the keyword **member:** followed by the member's ID to upgrade a particular member from the FTP server.
`system: <partition 0|1>`	Enter the keyword **system: partition** followed by the partition number (either **0** or **1**) to upgrade from the FTP server to the specified partition.

Usage Guidelines

Use this command to copy files or to copy an image for upgrade to a system partition or to a specified member. For more information about upgrading, see the Upgrade Chapter of the Release Notes.

Related Commands

Command	Description
copy ftp:	Copy using a FTP server.
copy usb:	Copy using USB storage.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

copy usb:

```
copy usb: {<filename> [usbpartition <number>] <destination> <destfilename>} | {snapshot
system: partition [0|1]}
```

Description

Copy from USB storage to a <destination>.

Syntax

Parameter	Description
<filename>	Enter the complete path to the file on your USB device.
usbpartition <number>	Enter the USB partition number.
<destination>	Enter one of the following: • ftp: • scp: • tftp: • member <id> flash • member usb • member <id> system: partition [0|1]
<destfilename>	Enter the name of the destination file.
snapshot system: partition 0 | 1	Enter the keywords **snapshot system: partition** followed by the either partition number (**0** or **1**).

Usage Guidelines

Use this command to copy files from USB storage.

Example

The following command copies the file to USB storage:

```
(host)#copy usb: techpubs1 usbpartition 1 flash: techpubs2
```

If your file names are invalid, the system will alert you as follows:

```
Invalid file name
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.3	The **usbpartition <number>** and **snapshot system: partition [0|1]** parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

crypto aruba-vpn

```
crypto aruba-vpn
   interface {loopback <aruba-vpn-interface-loopback-number> | vlan <aruba-vpn-vlan-id>}
   peer-ip <aruba-vpn-peer-ip>
```

Description

This command configures Aruba VPN Tunnel parameters.

Syntax

Parameter	Description
`interface {loopback <aruba-vpn-interface-loopback-number> | vlan <aruba-vpn-vlan-id>}`	Specify the Aruba VPN tunnel interface. You can configure the following options: • Loopback interface —allowed range is 0-63 • VLAN interface—allowed range is 1-4094
`peer-ip`	Specify the peer IP address to configure the Aruba VPN tunnel peer.

Usage Guidelines

Use this command to configure Aruba VPN tunnel with a controller at the datacenter which acts as the peer.

Example

The following command establishes Aruba VPN tunnel with the peer IP, 192.168.165.2 on the VLAN interface 1:

```
(host) (config) #crypto aruba-vpn
(host) (config-aruba-vpn) # peer-ip 192.168.165.2
(host) (config-aruba-vpn) # interface vlan 1
```

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	All parameters are available in the base OS.	Configuration mode

crypto ipsec

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

Description

This command configures IPsec parameters.

Syntax

Parameter	Description
`mtu <max-mtu>`	Configure the IPsec Maximum Transmission Unit (MTU) size. The supported range is 1024 to 1500 and the default is 1500.
`transform-set <transform-set-name>`	Create or modify a transform set.
`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-null-hmac`	Use ESP with no authentication. This option is not recommended.
`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 **set2**:

```
(host) (config)# crypto ipsec transform-set set2 esp-3des esp-md5-hmac
```

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	All parameters are available in the base OS.	Config mode on MAS

crypto isakmp policy

```
crypto isakmp policy
   authentication pre-share|rsa-sig
   encryption 3DES|AES128|AES192|AES256|DES
   group 1|2
   hash md5|sha|sha1-96
   prf PRF-HMAC-MD5|PRF-HMAC-SHA1
   lifetime <seconds>
   version v1|v2
```

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. This is the default group setting.
`2`	Use the 1024-bit Diffie Hellman prime modulus group.
`hash`	Configure the IKE hash algorithm
`md5`	Use MD5 as the hash algorithm.
`sha`	Use SHA-160 as the hash algorithm. This is the default policy algorithm.

Parameter	Description
SHA1-96	Use SHA1-96 as the hash algorithm.
prf	Set one of the following pseudo-random function (PRF) values for an IKEv2 policy: • PRF-HMAC-MD5 • PRF-HMAC-SHA1 (default)
lifetime <seconds>	Specify the lifetime of the IKE security association (SA), from 300 - 86400 seconds.
version	Specify the version of IKE protocol for the IKE policy • **v1**: IKEv1 • **v2**: IKEv2

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 values.

Example

The following command configures an ISAKMP peer IP address and subnet mask.

```
(host)(config) #crypto isakmp policy 1
(host)(config-isakmp) #auth rsa-sig
```

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	All other parameters are supported in the base OS.	Config mode on MAS

crypto-local ipsec-map

```
crypto-local ipsec-map <map> <priority>
   dst-net <ipaddr> <mask>
   force-natt {disable|enable}
   interface {loopback <ipsec-map-loopback-interface> | vlan <ipsec-map-vlan-id>}
   local-fqdn <local_id_fqdn>
   no ...
   peer-cert-dn <peer-dn>
   peer-fqdn any-fqdn|{peer-fqdn <peer-id-fqdn>}
   peer-ip <ipaddr>
   pre-connect {disable|enable}
   set ca-certificate <cacert-name>
   set ikev1-policy
   set ikev2-policy
   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>
   standby-interface vlan <id> preempt
   version v1|v2
```

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.	—	Disabled
`interface`	Allows you to set an interface for tunnel source	—	—
`loopback <ipsec-map-loopback-interface>`	Assigns a loopback interface number	—	—

Parameter	Description	Range	Default
`vlan <ipsec-map-vlan-id>`	Assigns a VLAN ID	—	—
`no`	Negates a configured parameter.	—	—
`local-fqdn <local_id_fqdn>`	If the MAS has a dynamic IP address, you must specify the fully qualified domain name (FQDN) of the MAS to configure it as a initiator of IKE aggressive-mode.		
`peer-cert-dn <peer-dn>`	If you are using IKEv2 to establish a site-to-site VPN to a remote peer, identify the peer device by entering its certificate subject name in the Peer Certificate Subject Name field		
`peer-ip <ipaddr>`	If you are using IKE to establish a site-to-site VPN to a statically addressed remote peer, identify the peer device by enteringIP address of the peer gateway. **NOTE:** If you are configuring an IPsec map for a static-ip MAS with a dynamically addressed remote peer, you must leave the peer gateway set to its default value of 0.0.0.0.	—	—

Parameter	Description	Range	Default
`peer-fqdn`	For site-to-site VPNs using PSK with dynamically addressed peers, specify a fully qualified domain name (FQDN) for the MAS.	any-fqdn fqdn-id	any-fqdn
`any-fqdn`	If the MAS is defined as a dynamically addressed responder, you can select **any-fqdn** to make the MAS a responder for all VPN peers,		
`fqdn-id <peer-id-fqdn>`	Specify the FQDN of a peer to make the MAS a responder for one specific initiator only.		
`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 MAS. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the MAS.	—	—
`set ikev1-policy`	Selects the IKEv1 policy for the ipsec-map	—	—
`set ikev2-policy`	Selects the IKEv2 policy for the ipsec-map	—	—

Parameter	Description	Range	Default
`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 MAS. Use the **show crypto-local pki ServerCert** command to display the server certificates that have been imported into the MAS.	—	—

Parameter	Description	Range	Default
`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.	—	—
`standby-interface vlan <id>`	A backup VPN interface in case the primary VPN goes down.	—	—
`preempt`	(Optional) Disables preemption on the standby interface which is enabled by default.	—	Enabled
`version v1|v2`	Select the IKE version for the IPsec map. • **v1**: IKEv1 • **v2**: IKEv2	—	v1

Usage Guidelines

You can use MAS 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. 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 MAS, or with one static and one dynamically addressed MAS. 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 MAS with a dynamic IP address must be configured to be the initiator of IKE Aggressive-mode for Site-Site VPN, while the MAS with a static IP address must be configured as the responder of IKE Aggressive-mode.

Examples

The following commands configure site-to-site VPN between two MAS:

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

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

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

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

For the Pre-shared-key:

```
(host) (config) #crypto-local isakmp key <key> address <ipaddr> netmask <mask>
```

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

```
(host) (config) #crypto-local ipsec-map <name2> <priority>
(host) (config-ipsec-map) #ssrc-net <ipaddr> <mask>
(host) (config-ipsec-map) #sdst-net <ipaddr> <mask>
(host) (config-ipsec-map) #speer-ip 0.0.0.0
(host) (config-ipsec-map) #speer-fqdn fqdn-id <peer_id_fqdn>
(host) (config-ipsec-map) #sinterface vlan <id>
```

For the Pre-shared-key:

```
(host) (config) #crypto-local isakmp key <key> fqdn <fqdn-id>
```

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

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

For the Pre-shared-key for All FQDNs:

```
(host) (config) #crypto-local isakmp key <key> fqdn-any
```

You can configure the standby VPN using the following CLI commands:

```
(host) (config) #crypto-local ipsec-map mapA 10
(host) (config-ipsec-map) # peer-ip 20.1.1.2
(host) (config-ipsec-map) # local-fqdn test.arubanetworks.com
(host) (config-ipsec-map) # interface vlan 2
(host) (config-ipsec-map) # src-net 4.1.1.0 255.255.255.255
(host) (config-ipsec-map) # dst-net 3.1.1.0 255.255.255.255
(host) (config-ipsec-map) # standby-interface vlan 4
```

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.
ArubaOS 7.4	The **standby-interface vlan** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	All parameters are available in the base operating system.	Config mode on MAS

crypto-local isakmp dpd

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

Description

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

Syntax

Parameter	Description	Range	Default
`idle-timeout`	Idle timeout, in seconds.	10–3600	22 seconds
`retry-timeout`	Configures IKE DPD retry timout	2–60	2 seconds
`retry-attempts`	Configures IKE DPD retry attempts	3–10	3 attempts

Usage Guidelines

DPD is enabled by default on the Mobility Access Switch 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

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

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

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 MAS 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

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Access Switch

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

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode

crypto-local pki

```
crypto-local pki
   CRL <name> <filename>
   IntermediateCA <name> <filename>
   OCSPResponderCert <certname> <filename>
   OCSPSignerCert <certname> <filename>
   PublicCert <name> <filename>
   ServerCert <name> <filename>
   TrustedCA <name> <filename>
   global-oscp-signer-cert
   rcp <name>
   service-ocsp-responder
```

Description

Issue this command to configure a local certificate, OCSP signer or responder certificate and Certificate Revocation List (CRL). You can also list revocation checkpoints and enable the responder service.

Syntax

Parameter	Description
`CRL`	Specifies a Certificate Revocation list. Validation of the CRL is done when it imported through the WebUI (requires the CA to have been already present). CRLs can only be imported through the WebUI.
`<name>`	Name of the CRL.
`<filename>`	Original imported filename of the CRL.
`IntermediateCA`	Configures an intermediate CA certificate
`<name>`	Name of the intermediate CA certificate.
`<filename>`	Original imported filename of the CRL.
`OCSPResponderCert`	Configures a OCSP responder certificate.
`<certname>`	Name of responder certificate.
`<filename>`	Original imported filename of the responder certificate.
`OCSPSignerCert`	Configures a OCSP signer certificate.
`<certname>`	Name of the signer certificate.
`<filename>`	Original imported filename of the signer certificate.
`PublicCert`	Public key of a certificate. This allows an application to identify an exact certificate.
`<certname>`	Name of the signer certificate.
`<filename>`	Original imported filename of the signer certificate.

Parameter	Description
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 MAS.
<certname>	Name of the signer certificate.
<filename>	Original imported filename of the signer certificate.
TrustedCA	Trusted CA certificate. This can be either a root CA or intermediate CA. Aruba encourages (but does not require) an intermediate CA's signing CA to be the MAS itself.
<certname>	Name of the signer certificate.
<filename>	Original imported filename of the signer certificate.
global-ocsp-signer-cert	Specifies the global OCSP signer certificate to use when signing OCSP responses if there is no check point specific OSCP signer certificate present. If the ocsp-signer-cert is not specified, OCSP responses are signed using the global OCSP signer certificate. If this is not present, than an error message is sent out to clients. **NOTE:** The OCSP signer certificate (if configured) takes precedence over the global OCSP signer certificate as this is check point specific.
rcp <name>	Specifies the revocation check point. A revocation checkpoint is automatically created when a TrustedCA or IntermediateCA certificate is imported on the MAS.
service-ocsp-responder	This is a global knob that turns the OCSP responder on or off. The default is off (disabled). To enable this option a CRL must be configured for this revocation checkpoint as this is the source of revocation information in the OCSP responses.

Usage Guidelines

This command lets you configure the MAS to perform real-time certificate revocation checks using the Online Certificate Status Protocol (OCSP) or traditional certificate validation using the Certificate Revocation List (CRL) client.

Example

This example configures the MAS as an OCSP responder.

The revocation check point is specified as CAroot. (The revocation check point CAroot was automatically created when the CAroot certificate was previously uploaded to this MAS.) The OCSP signer certificate is RootCA-Ocsp_signer. The CRL file is Security1-WIN-05PRGNGEKAO-CA-unrevoked.crl The OCSP responder is enabled.

```
crypto-local pki service-ocsp-responder
crypto-local pki rcp CARoot
   ocsp-signer-cert RootCA-Ocsp_signer
   crl-location file Security1-WIN-05PRGNGEKAO-CA-unrevoked.crl
  enable-ocsp-responder
```

Related Commands

Command	Description	Mode
show crypto-local pki	This command shows local certificate, OCSP signer or responder certificate and CRL data and statistics.	Config mode

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode

crypto pki

```
crypto pki csr
   {rsa key_len <key_val> |{ec curve-name <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
`rsa key_len <key_val>`	Generate a certificate signing request with a Rivest, Shamir and Adleman (RSA) key with one of the following supported RSA key lengths: • 1024 • 2048 • 4096
`ec curve-name <key_val>`	Generate a certificate signing request with an elliptic-curve (EC) key with one of the following EC types: • secp256r1 • secp384r1
`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 install a CSR for the Captive Portal feature.

Example

The following command installs a server certificate in DER forma

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

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

crypto pki-import

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

Description

Use this command to 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

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

database synchronize

```
database synchronize
```

Description

Synchronize the Primary and Secondary databases.

Usage Guidelines

Periodic database synchronization is enabled by default and runs every two minutes. Best practices recommends that you manually synchronize the database prior to changing your Primary and Secondary member's roles (see system switchover).

Related Commands

Command	Description
show database synchronize	Display the database synchronization details.
system switchover	Gracefully switches the Secondary member to become the Primary member.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

delete

```
delete usb: <usbpathname> [usbpartiton <number>]
member id usb: <usbpathname> [<usbpathname> usbpartiton <number>]
```

Description

This command deletes an existing USB directory.

Syntax

Parameter	Description	Range	Default
`member id`	Enter a stack member ID.	—	—
`<usbpathname>`	Deletes the content of member USB.	—	—
`usbpartition <number>`	Deletes the USB directory in multipartition member.	—	—
`usb:`	External USB.	—	—
`<usbpathname>`	Deletes the content of USB.	—	—
`usbpartition <number>`	Deletes the content of multipartitioned member of USB.	—	—

Usage Guidelines

Delete the content of a USB directory.

Example

```
(host) #delete usb: test1 usbpartition 1
Successfully deleted the path test1 at external USB drive
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

delete stacking

```
delete stacking interface stack <module/port> member <id>
```

Description

Delete a stacking port. This command can be executed locally or from the from the primary.

Syntax

Parameter	Description
`interface stack <module/port>`	Enter the keywords **interface stack** followed by the stacking interface in <module/port> format.
`member <id>`	Enter the keyword **member** followed by the member ID of the stack on which the interface is to be deleted. This can be executed only from the primary Mobility Access Switch.

Usage Guidelines

Delete a stacking port from the ArubaStack.

Related Command

Command	Description
clear	Clears stacking from your running configuration.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.3.0.1	The **member <id>** parameter is added to enable deleting a port from the primary Mobility Access Switch.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

device-group

```
device-group ap
   aaa-profile <profile_name>
   auto-lacp
   enable
   enet-link-profile <profile_name>
   gvrp-profile <profile_name>
   ip access-group {in <ACL_name>|out <ACL_name>|session <session>}
   lldp-profile <profile_name>
   mstp-profile <profile_name>
   mtu <mtu>
   no
   poe-profile <profile_name>
   policer-profile <profile_name>
   port-security-profile <profile_name>
   pvst-port-profile <profile_name>
   qos trust {aruba-device|auto|disable|dot1p|dscp|pass-through}
   qos-profile <profile_name>
   shutdown {<interface-list>|add <interface-list>|remove <interface-list>}
   switching-profile <profile_name>
   trusted port
```

Description

This command dynamically configures an interface based on the type of device connected to it. It uses LLDP to detect the type of device connected to an interface and applies a device-group configuration (a set of predefined configuration) on the interface based on the device-type.

Syntax

Parameter	Description
`aaa-profile`	Applies an existing AAA profile to this interface.
`auto-lacp`	Enables Auto-LACP. **NOTE:** Starting from ArubaOS 7.4.1.1, Auto-LACP is supported.
`enable`	Enables auto device configuration for AP device-type.
`enet-link-profile`	Applies an existing Ethernet link profile to this interface.
`gvrp-profile`	Applies an existing Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) profile to this interface.
`ip access-group`	Applies IP-based access control lists (ACL). This parameter has the following sub-parameters: • **in <ACL_name>**: Add or delete ingress ACLs. • **out <ACL_name>**: Add or delete egress ACLs. • **session <session>**: Add or delete session ACLs.
`lldp-profile`	Applies an existing LLDP profile to this interface. By default, the **device-group-default** profile is applied.
`mstp-profile`	Applies an existing Multiple Spanning Tree Protocol (MSTP) profile to this interface.

Parameter	Description
`mtu`	Sets the Maximum Transmission Unit (MTU) on the interface between 64 and 9216 (in bytes).
`no`	Disables any configured parameter.
`poe-profile`	Applies an existing Power over Ethernet profile to this interface. By default, the **device-group-default** profile is applied.
`policer-profile`	Applies an existing policer profile to this interface.
`port-security-profile`	Applies an existing port security profile to this interface.
`pvst-port-profile`	Applies an existing Per VLAN Spanning Tree (PVST) port profile to this interface.
`qos trust`	Apply QoS trust for the following trust mode: • **aruba-device**: Trust Differentiated Services Code Point (DSCP) or 802.1p for Aruba devices only. For rest, apply pass-through. • **auto**: Trust DSCP for IP packets; 802.1p for non-IP packets. • **disable**: Disable QoS trust and reset DSCP or 802.1p to 0 (lowest priority). • **dot1p**: Trust 802.1p. • **dscp**: Trust DSCP. • **pass-through**: Pass through DSCP or 802.1p. The default value is set to **auto**.
`qos-profile`	Apply an existing QoS profile to this interface.
`shutdown`	Enable or disable an interface. This parameter has the following sub-parameters: • **<interface-list>**: Replace the existing list with the new list. Enter valid interface(s) in ascending order. • **add <interface-list>**: Add interface(s) to the current list. Enter valid interface(s) in ascending order. • **remove <interface-list>**: Remove interface(s) from the current list, Enter valid interface(s) in ascending order.
`switching-profile`	Apply an existing switch port profile to this interface.
`trusted port`	Set this interface a trusted port.

Usage Guidelines

When device-group configuration is enabled for a device-type and if a device in the device-type is detected on an interface:

- Any previous configuration on the interface is overwritten by the device-group configuration.
- Any new configuration on the interface, including the administrative operation (interface shutdown) can be done only through device-group configuration and not using the interface commands.
- When the device is disconnected from the interface, the original configuration on the interface that existed before the device detection is restored after the LLDP entry of the device gets removed.

You can edit and customize any device-group configuration provided on the Mobility Access Switch but cannot create a new configuration for a device-type.

Example

The following commands enable auto device configuration for AP device-type:

```
(host) (config) #device-group ap
(host) (device-group access-point) #enable
```

The following commands enable Auto-LACP:

Before enabling auto-LACP, you must enable **device-group ap**.

```
(host) (config) #device-group ap
(host) (device-group access-point) #enable
(host) (device-group access-point) #auto-lacp
(host) (device-group access-point) #show interface port-channel auto-lacp
port-channel 2 is administratively Up, Link is Up, Line protocol is Up
Hardware is Port-Channel, LACP enabled, Address is 00:1a:1e:1b:01:00
Description: Link Aggregate
Created by Auto-LACP Link Aggregate
Member port(s):
GE0/0/18 is administratively Up, Link is Up, Line protocol is Up (LACP-I)
GE0/0/20 is administratively Up, Link is Up, Line protocol is Up
Speed: 1 Gbps
Interface index: 1443
MTU 1514 bytes
Flags: Access, Trusted
Link status last changed: 0d 00h:00m:28s ago
Last clearing of counters: 0d 00h:00m:28s ago
Statistics:
Received 130 frames, 64722 octets
1 pps, 1.862 Kbps
0 broadcasts, 0 runts, 1 giants, 0 throttles
1522 error octets, 0 CRC frames
30 multicast, 100 unicast
Transmitted 90 frames, 11844 octets
1 pps, 1.384 Kbps
3 broadcasts, 0 throttles
0 errors octets, 0 deferred
0 collisions, 0 late collisions
```

Related Commands

Command	Description
show device-group	This command displays the device-group attached interfaces.
show device-group-config	This command displays the device-group configuration.

Command History

Release	Modification
ArubaOS 7.4	This command was introduced.
ArubaOS 7.4.1.1	Support for Auto-LACP feature is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

dhcp-snooping-database

dhcp-snooping-database **<mac> gigabitethernet <slot/module/port> <ip_address>**

Description

This command adds a static binding on a VLAN.

Syntax

Parameter	Description	Range	Default
mac	MAC address of the interface.	—	—
gigabitethernet <slot/module/port>	Enter the Gigabit Ethernet interface.	—	—
ip_address	IP address of the interface.	—	—

Usage Guidelines

Use this command to add a static binding on a VLAN.

To delete a static binding on a VLAN, use the following command:

```
(host) ("vlan id") #no dhcp-snooping-database <mac> gigabitethernet <slot/module/port> <ip_
address>
```

Example

The following example adds a static binding on a VLAN:

```
(host) (config) #vlan 2
(host) (VLAN "2") #dhcp-snooping-database 00:00:00:00:00:01 gigabitethernet 1/0/20 1.1.1.1
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

dir

```
dir <member_id>
```

Description

This command displays a list of files stored in the flash file system.

Syntax

Parameter	Description
`<member_id>`	Enter the member ID.

Usage Guidelines

Use this command to view the system files associated with the Mobility Access Switch.

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

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

dir member

```
dir member <id>
   usb
   <usbpathname> [usbpartition <number>]
```

Description

This command displays the content of a USB directory.

Syntax

Parameter	Description
`<id>`	Member ID of the stack.
`usb`	External USB.
`<usbpathname>`	Directory content of member USB.
`usbpartition <number>`	Directory content of member of a multipartitioned USB.

Usage Guidelines

Use this command to view the content of a USB directory.

Example

The following command displays the files currently residing on the USB directory:

```
(host) #dir member 1 usb: aajtak
Member-id: 1
------------
drwxr-xr-x    2 root     root         4096 Sep 10 15:49 fr
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

dir usb

```
dir usb <usbpathname> [usbpartition <number>]
```

Description

This command displays the content of a USB directory.

Syntax

Parameter	Description
`<usbpathname>`	Directory content of the USB.
`usbpartition <number>`	Directory content of the multipartitioned USB.

Usage Guidelines

Use this command to view the content of a USB directory.

Example

The following command displays the files currently residing on the USB directory:

```
(host) #dir usb: aajtak
drwxr-xr-x    2 root     root         4096 Sep 10 15:49 fr
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

downloadable-role-delete

```
downloadable-role-delete <role>
```

Description

This command allows to delete the downloadable roles from the ClearPass Policy Manager (CPPM) under specific conditions.

Syntax

Parameter	Description
`<role>`	Specifies the downloadable role to delete.

Usage Guidelines

You can delete roles downloaded from the CPPM server if the following conditions are met:

- No user references it.
- It is in Complete or Incomplete state.

The following error message is displayed if you try to delete a role that is not downloaded from CPPM or a nonexisting role: **Invalid role <role-name>**

Example

The following sample CLI command deletes the abc_profile-3023-8 user role:

```
(host) #downloadable-role-delete abc_profile-3023-8
```

Command History

Release	Modification
ArubaOS 7.4.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

eject

```
eject
   usb
   member
```

Description

This command ejects an USB.

Syntax

Parameter	Description
`usb`	Eject the external USB.
`member`	Eject the member ID of the stack.

Usage Guidelines

Use this command to eject an USB.

Example

The following command ejects an USB:

```
(host) (config) #eject usb
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.3	The **usb** and **member** parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

encrypt

```
encrypt {disable|enable}
```

Description

This command allows passwords and keys to be displayed in plain text or encrypted.

Syntax

Parameter	Description	Default
`disable`	Disables encryption and passwords and keys are displayed in plain text.	—
`enable`	Enables encryption, so 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

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable

firewall

```
firewall
   {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|enforce-tcp-sequence|log-icmp-error|prohibit-arp-spoofing|prohibit-
   ip-spoofing |prohibit-rst-replay|session-idle-timeout <seconds>|session-mirror-destination
   [ip-address <A.B.C.D>|port <slot/module/port>]|session-mirror-ipsec peer
   <ipsecpeer>|session-voip-timeout <seconds>}
```

Description

This command configures firewall options on the Mobility Access Switch.

Syntax

Parameter	Description	Range	Default
`disable-stateful-sccp-processing`	Disables SCCP processing.	—	enabled
`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 there is no VoIP or VoWLAN traffic on the network.	—	enabled
`drop-ip-fragments`	When enabled, all IP fragments are dropped. You should not enable this option unless instructed to do so by an Aruba representative.	—	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 Aruba representative, as doing so may create unnecessary overhead on the Mobility Access Switch.	—	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
`enforce-tcp-sequence`	Enforces the TCP sequence numbers for all packets.	—	disabled
`log-icmp-error`	Logs received ICMP errors. You should not enable this option unless instructed to do so by an Aruba representative.	—	disabled

Parameter	Description	Range	Default
`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, source and destination IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.	—	enabled in IPv4 disabled in IPv6
`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 Aruba representative.	—	disabled
`session-idle-timeout <seconds>`	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 Aruba representative. **NOTE:** Configuring the value to 0 sets the session-idle-timeout to the factory defaults, i.e. the session will time out within 15 seconds.	0, 16-300	0
`session-mirror-destination[ip-address <A.B.C.D>|port <slot/-module/port>`	Configures either the IP address or the port as the mirror destination. **NOTE:** You can only configure one of the options (IP address or port) as the mirror destination.	–	–
`session-mirror-ipsec peer <ipsecpeer>`	Configures session mirror of all the frames that are processed by IPSec.	–	–
`session-voip-timeout <seconds>`	Time, in seconds, that a voice session can be idle before it is removed from the session table. **NOTE:** Configuring the value to 0 sets the session-voip-timeout to the factory defaults, i.e. the VoIP session will time out within 15 seconds.	0, 16-300	0

Usage Guidelines

This command configures global firewall options on the Mobility Access Switch.

Example

The following command disables the SIP ALG on the Mobility Access Switch:

```
(host)(config) #firewall disable-stateful-sip-processing
```

Related Command

Command	Description
show firewall	This command shows all firewall policies currently configured on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode

gvrp

```
gvrp
   enable
   join-time <milliseconds>
   leave-all-time <milliseconds>
   leave-time <milliseconds>
   no..
```

Description

These commands enable and configure the GVRP global profile settings.

Syntax

Parameter	Description	Range	Default
`enable`	Enables GVRP.	—	disable
`join-time <milliseconds>`	Join timer interval in milliseconds.	1–65535	200
`leave-all-time <milliseconds>`	Leave-all timer interval in milliseconds.	1–65535	10000
`leave-time <milliseconds>`	Leave timer interval in milliseconds.	1– 65535	600
`no`	Removes the specified configuration parameter.	—	—

Usage Guidelines

Use this command to enable and configure GVRP in global profile.

Example

The following command enables and configures GVRP profile:

```
(host)# gvrp
(host)(Global GVRP configuration)# enable
(host)(Global GVRP configuration)# join-time 200
(host)(Global GVRP configuration)# leave-time 600
(host)(Global GVRP configuration)# leave-all-time 10000
```

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

halt

```
halt [<member_id> | local]
```

Description

Halt the system or a specific member.

Syntax

Parameter	Description
`<member_id>`	Enter the member ID that you want to halt.
`local`	Enter the keyword local to halt the local switch.

Usage Guidelines

The halt command *halts* the stack without rebooting the stack. The **`halt`** command and the **`halt <member_id>`** command must be executed from the Primary. The **`halt local`** command can be execute from any member in the stack.

Example

The following command halts (without rebooting) member 2 of the stack.

```
(host)# halt 2
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1	Added **halt** local option.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

interface gigabitethernet

```
interface gigabitethernet <slot/module/port>
   aaa-profile <profile_name>
   backup interface {gigabitethernet <slot/module/port> | port-channel <0-7>}
   clone <source>
   description <name>
   enet-link-profile <profile_name>
   gvrp-profile <profile_name>
   igmp-snooping mrouter-vlan [add|delete] <vlan-list>
   ip access-group [in | out] <ACL_name>
   lacp-profile <profile_name>
   lldp-profile <profile_name>
   mirroring-in-profile <profile_name>
   mirroring-out-profile <profile_name>
   mstp-profile <profile_name>
   mtu <64-7168>
   no {...}
   oam-profile
   poe-profile <profile_name>
   policer-profile <profile_name>
   port-security-profile <profile_name>
   preemption delay <10-300>
   preemption mode {forced|off}
   qos trust
   qos-profile <profile_name>
   shutdown
   switching-profile <profile_name>
   trusted port
   tunneled-node-profile <profile_name>
   voip-profile <profile_name>
```

Description

This command configures a Gigabit Ethernet port individually on the switch with various profiles and parameters. You need to create the profile before assigning that profile to an interface. To create a profile, see the corresponding sections in this guide.

Syntax

Parameter	Description	Range	Default
`aaa-profile <profile_name>`	Applies the specified AAA profile to the interface.	—	—
`backup interface {gigabitethernet <slot/module/port>| port-channel <0-7>}`	Specifies the secondary interface in the HSL group.	—	—
`clone <source>`	Copies data from another Gigabit Ethernet interface.	—	—
`description <name>`	Specifies a name for the interface.	Upto 63 characters; can begin with a numeric character	GE-X/X/X
`gvrp-profile <profile_name>`	Applies the specified GVRP link profile to the interface.	—	—
`enet-link-profile <profile_name>`	Applies the specified ethernet link profile to the interface.	—	—
`igmp-snooping mrouter-vlan [add|delete] <vlan-list>`	Adds or deletes the specified VLAN IDs as the multicast router VLAN IDs for IGMP snooping.	—	—
`ip access-group [in | out] <ACL_name>`	Adds an ingress or egress access-control-list to the interface.	—	—

Parameter	Description	Range	Default
`lacp-profile <profile_name>`	Applies the specified LACP profile to the interface.	—	—
`lldp-profile <profile_name>`	Applies the specified LLDP profile to the interface.	—	—
`mirroring-in-profile <profile_name>`	Applies the specified ingress mirroring profile to the interface.	—	—
`mirroring-out-profile <profile_name>`	Applies the specified egress mirroring profile to the interface.	—	—
`mstp-profile <profile_name>`	Applies the specified MSTP profile to the interface.	—	—
`mtu <64-7168>`	Sets the number of MTUs in bytes.	64–7168	1514
`no {...}`	Removes the specified configuration parameter.	—	—
`oam-profile <profile_name>`	Applies the specified OAM profile to the interface.	—	—
`poe-profile <profile_name>`	Applies the specified PoE profile to the interface.	—	—
`policer-profile <profile_name>`	Applies the specified policer profile to the interface.	—	—

Parameter	Description	Range	Default
`port-security-profile <profile_name>`	Applies the specified port security profile to the interface.	—	—
`preemption delay <seconds>`	Specifies the preemption delay in seconds.	10–300	100
`preemption mode {forced | off}`	**forced**—Forces preemption of backup. **off**—Does not force preemption of backup.	—	Off
`qos trust`	Enables QoS trust mode.	—	Untrusted
`qos-profile <profile_name>`	Applies the specified QoS profile to the interface.	—	—
`shutdown`	Disables the interface.	—	Enabled
`switching-profile <profile_name>`	Applies the specified switching profile to the interface.	—	—
`trusted port`	Sets the port to trusted mode.	—	Untrusted
`tunneled-node-profile <profile_name>`	Applies the specified tunneled node profile to the interface.	—	—
`voip-profile <profile_name>`	Applies the specified VoIP profile to the interface.	—	—

Usage Guidelines

Use this command when you need to configure a Gigabitethernet interface with unique parameter values that makes the interface distinct from other interfaces. If you need to configure the same parameter values to multiple interfaces, then do not use this command. In such a scenario, use the `interface-group` command. If you do not apply any profile, then the default profile is applied.

Starting from ArubaOS 7.4.1, the following warning message is displayed on the Mobility Access Switch if you apply the GVRP profile on an interface without enabling global GVRP:

Warning: GVRP not enabled globally.

The sample command output with the warning message is as follows:

```
(host) (gigabitethernet "0/0/1") #switching-profile vlan10
(host) (gigabitethernet "0/0/1") #gvrp-profile vlan10
Warning: GVRP not enabled globally.
```

Example

The following example configures the various profiles and parameters for an interface:

```
interface gigabitethernet 0/0/1
   aaa-profile GENERAL
   backup interface gigabitethernet 0/0/2
   description GeneralInterface
   enet-link-profile ENET_LINK
   igmp-snooping mrouter-vlan add 100-200
   ip access-group in ACL_General
   lldp-profile default
   mirroring-in-profile MIRROR
   mirroring-out-profile MIRROR
   mstp-profile MSTP_GENERAL
   mtu 2054
   poe-profile PoE_General
   preemption delay 200
   preemption mode forced
   qos trust
   qos-profile QoS_General
   no shutdown
   switching-profile Switching_General
   trusted port
   voip-profile VOIP_General
```

Related Commands

Command	Description
show interface gigabitethernet	Issue this command to display information about a specified Gigabit Ethernet interface.
show interface-profile	Displays the specified profile configuration parameters and values.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4.1	A warning message is displayed when GVRP profile is applied on an interface without enabling global GVRP.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

interface-group gigabitethernet

```
interface-group gigabitethernet {default|<group-name>}
   aaa-profile <profile_name>
   apply-to <interface range>
   clone <source>
   enet-link-profile <profile_name>
   igmp-snooping mrouter-vlan [add|delete] <vlan-list>
   ip access-group in <in>
   lacp-profile <profile_name>
   lldp-profile <profile_name>
   mac-limit <limit> action {drop|log|shutdown}
   mirroring-in-profile <profile_name>
   mirroring-out-profile <profile_name>
   mstp-profile <profile_name>
   mtu <64-7168>
   tunneled-node-profile <profile-name>
   no {...}
   poe-profile <profile_name>
   policer-profile <profile_name>
   qos trust
   qos-profile <profile_name>
   shutdown
   switching-profile <profile_name>
   trusted port
   tunneled-node-profile <profile-name>
   voip-profile <profile_name>
```

Description

This command applies the same configuration parameters to a group of Gigabit Ethernet interfaces.

Syntax

Parameter	Description	Range	Default
`aaa-profile <profile_name>`	Applies the specified AAA profile to interface group.	—	—
`apply-to`	Specifies the interfaces that are part of this group. Example: 0/0/1-0/5,0/0/10,0/0/21-0/25	—	—
`clone <source>`	Copies data from another gigabitethernet interface.	—	—

Parameter	Description	Range	Default
`enet-link-profile <profile_name>`	Applies the specified ethernet link profile to the interface group.	—	—
`ip access-group in <in>`	Adds an ingress access-control-list to the interface group.	—	—
`lacp-profile <profile_name>`	Applies the specified LACP profile to the interface group.	—	—
`lldp-profile <profile_name>`	Applies the specified lldp profile to the interface group.	—	—
`mac-limit <limit> action {drop|log|shutdown}`	Configures the maximum number of MACs that can be learned on this interface. The drop action drops all further MAC learning requests and packets from unknown MACs. The log option just logs system message that the limit is reached.The shutdown option shuts the port down when the specified MAC limit is exceeded.	—	1
`mirroring-in-profile <profile_name>`	Applies the specified ingress mirroring profile to the interface group.	—	—
`mirroring-out-profile <profile_name>`	Applies the specified egress mirroring profile to the interface group.	—	—
`igmp-snooping mrouter-vlan [add|delete] <vlan-list>`	Configures the interfaces in this group as multicast router interfaces.	—	—

Parameter	Description	Range	Default
`mstp-profile <profile_name>`	Applies the specified MSTP profile to the interface group.	—	—
`mtu <64-7168>`	Sets the number of MTUs in bytes.	64-7168	1514
`tunneled-node-profile <profile_name>`	Applies the specified tunneled node profile to the interface group.	—	—
`no {...}`	Removes the specified configuration parameter.	—	—
`poe-profile <profile_name>`	Applies the specified PoE profile to the interface group.	—	—
`policer-profile <profile_name>`	Applies the specified policer profile to the interface group.	—	—
`qos trust`	Enables QoS trust mode on the interfaces that are part of this group.	—	Untrusted
`qos-profile <profile_name>`	Applies the specified QoS profile to the interface group.	—	—
`shutdown`	Disables the interfaces in this group.	—	Enabled
`switching-profile <profile_name>`	Applies the specified switching profile to the interface group.	—	—

Parameter	Description	Range	Default
`trusted port`	Sets the ports in this group to trusted mode.	—	Untrusted
`tunneled-node-profile <profile_name>`	Applies the specified tunneled node profile to the interface.	—	—
`voip-profile <profile_name>`	Applies the specified VOIP profile to the interface group.	—	—

Usage Guidelines

Use this command when you want to apply the same configuration to multiple interfaces. Note that the port-channels are different from interface groups. When you use the interface-group command, it applies the same configuration to all the interfaces included in that group. When you use the port-channel command, the interface members included in the port-channel join together and act as a single interface.

Example

The following example configures the various profiles and parameters for an interface group:

```
interface-group gigabitethernet GENERAL
   aaa-profile AAA_General
   apply-to 0/0/1-0/0/15,0/0/19
   enet-link-profile ENET_LINK_GENERAL
   igmp-snooping mrouter-vlan add 100-200
   ip access-group in ACL_General
   lldp-profile LLDP_General
   mac-limit 25 action drop
   mirroring-in-profile MIRRORING
   mirroring-out-profile MIRRORING
   mstp-profile MSTP_General
   mtu 2045
   poe-profile PoE_General
   qos trust
   qos-profile QoS_General
   no shutdown
   switching-profile Switching_General
   trusted port
   voip-profile VOIP_General
```

Related Commands

Command	Description
show interface-group-config gigabitethernet	Displays the interface configuration for the specified group.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

interface loopback

```
interface loopback <0-63>
   clone <source>
   description <description>
   ip address <address> [secondary]
   no {...}
   exit
```

Description

This command configures the loopback interfaces.

Syntax

Parameter	Description	Range	Default
`loopback <0-63>`	Specifies an identification number for the loopback interface.	0–63	—
`clone <source>`	Copies the configuration from another loopback interface.	—	—
`description <description>`	Specifies a name for the loopback interface.	—	—
`ip address <address>`	Assigns the specified IP address to the loopback interface.	—	—
`secondary`	Configures the entered IP address as a secondary IP address.	—	—
`no {...}`	Removes the specified configuration.	—	—

Usage Guidelines

Use this command to configure the loopback interfaces.

Example

The following example configures a loopback interface:

```
(host)(config)# interface loopback 1
   description loopback01
   ip address 1.1.1.1 netmask 255.255.255.0
   exit
```

Related Commands

Command	Description
show interface loopback	This command displays the loopback interface information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

interface mgmt

```
interface mgmt
   description <name>
   ip address <address> netmask <netmask>
   ipv6 address {[link-local <X:X:X:X::X>]|[<X:X:X:X::X> prefix_len <prefix_length>]}
   no {...}
   shutdown
   exit
```

Description

This command configures the management port on the switch. The management port is a dedicated interface for out-of-band management purposes. This interface is specifically available for the management of the system and cannot be used as a switching interface. You can configure only the IP address and description for this interface. The management port can be used to access the Mobility Access Switch from any location and configure the system.

Syntax

Parameter	Description	Range	Default
`description <description>`	Specifies an identification name for the management interface.	Upto 63 characters;can begin with a numeric character	—
`ip address <address> netmask <netmask>`	Assigns the specified IP address to the management interface.	—	—
ipv6 address	Assigns the specified IPv6 address to the management interface	—	—
`link-local <X:X:X:X::X>`	Configures the specified IPv6 address as the link local address for this interface.	—	—
`<X:X:X:X::X> prefix_len <prefix_length>`	Specify the IPv6 prefix/prefix-length to configure the global unicast address for this interface.	—	—
`no {...}`	Removes the specified configuration parameter for the management interface.	—	—
`shutdown`	Disables the management interface	—	Disabled

Usage Guidelines

Use this command to configure the management port. Use the **ipv6 address** option to modify the auto-configured link local address or configure the global unicast address of the management interface.

Example

The following example configures the management interface:

```
(host)(config) #interface mgmt
(host)(mgmt)#description MGMT
(host)(mgmt)#ip address 10.13.6.1
(host)(mgmt)#no shutdown
```

The following command modifies the auto-configured link local address of the management interface to fe80::20b:86ff:fe6a:2800.

```
(host)(config)#interface mgmt(host)(mgmt)#ipv6 address link-local fe80::20b:86ff:fe6a:2800
```

The following command configures the global unicast address of the management interface to 2cce:205:160:100::fe.

```
(host)(mgmt)#ipv6 address 2cce:205:160:100::fe prefix_len 64
```

Related Command

Command	Description
show interface mgmt	This command displays the management interface information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1	The **ipv6 address** option was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

interface port-channel

```
interface port-channel <0-63>
   backup interface {gigabitethernet <slot/module/port>|port-channel <0-63>}
   clone <source>
   description <name>
   enet-link-profile <profile_name>
   igmp-snooping mrouter-vlan [add|delete] <vlan-list>
   ip access-group {in <in> |out <out>}
   mac-limit <limit> action {drop|log|shutdown}
   mirroring-in-profile <profile_name>
   mirroring-out-profile <profile_name>
   mstp-profile <profile_name>
   mtu <64-9216>
   no {...}
   policer-profile <profile_name>
   port-channel-members {<interface-list> | {{add | delete} gigabitethernet
   <slot/module/port>}}
   port-security-profile <profile_name>
   preemption delay <10-300>
   preemption mode {forced | off}
   qos trust
   qos-profile <profile_name>
   shutdown
   switching-profile <profile_name>
```

Description

This command creates a port-channel.

Syntax

Parameter	Description	Range	Default
`port-channel <0-63>`	Specifies the port-channel ID.	0–63: For all Mobility Access Switches except S1500 Mobility Access Switch. 0–7: For the S1500 Mobility Access Switch.	—
`backup interface <stac/module/port>`	Specifies the secondary interface in the HSL group.	—	—
`clone <source>`	Copies data from another gigabitethernet interface.	—	—

Parameter	Description	Range	Default
`description <name>`	Specifies a name for the port-channel.	1–32 characters; cannot begin with a numeric character	—
`enet-link-profile <profile_name>`	Applies the specified ethernet link profile to the port-channel.	—	—
`igmp-snooping mrouter-vlan [add|delete] <vlan-list>`	Adds or deletes the specified VLAN IDs as the multicast router VLAN IDs for IGMP snooping.	—	—
`ip access-group {in <in> |out <out>}`	in <in> - Adds ingress access-control-list to the port-channel. out <out> - Adds egress access-control-list to the port-channel.	—	—
`mac-limit <limit> action {drop|log|shutdown}`	Configures the maximum number of MACs that can be learned on this interface. The drop action drops all further MAC learning requests and packets from unknown MACs. The log option just logs system message that the limit is reached. The shutdown option shuts down the interface when the specified MAC limit is reached.	—	1

Parameter	Description	Range	Default
`mirroring-in-profile <profile_name>`	Applies the specified ingress mirroring profile to the port-channel.	—	—
`mirroring-out-profile <profile_name>`	Applies the specified egress mirroring profile to the port-channel.	—	—
`mstp-profile <profile_name>`	Applies the specified MSTP profile to the port-channel.	—	—
`mtu <64-9216>`	Sets the number of MTUs in bytes.	64-9216	1514
`no {...}`	Delete command	—	—
`port-channel-members {interface-list | {{add | delete} gigabitethernet <slot/module/port>}}`	Adds or deletes the specified interfaces to/from the port-channel.	—	—
`port-security-profile <profile_name>`	Applies the specified port security profile to the interface.	—	—
`policer-profile <profile_name>`	Applies the specified policer profile to the port-channel.	—	—
`preemption delay <seconds>`	Specifies the preemption delay in seconds.	10-300	100
`preemption mode {forced | off}`	**forced**—Forces preemption of backup. **off**—Does not force preemption of backup.	—	Off.

Parameter	Description	Range	Default
qos trust	Enables QoS trust mode.	—	—
qos-profile <profile_name>	Applies the specified QoS profile to the port-channel.	—	—
shutdown	Disables the port-channel.	—	Enabled.
switching-profile <profile_name>	Applies the specified switching profile to the port-channel.	—	—

Usage Guidelines

Use this command to create a static port-channel.

Example

The following example configures a port-channel with profiles, parameters, and member interfaces:

```
host) (config) #show interface port-channel 1
port-channel 1 is administratively Up, Link is Up, Line protocol is Up
Hardware is Port-Channel, Address is 00:0b:86:6a:70:c0
Description: Link Aggregate
Member port(s):
   GE0/0/4 is administratively Up, Link is Up, Line protocol is Up
   GE0/0/5 is administratively Up, Link is Up, Line protocol is Up
Speed: 2 Gbps
Interface index: 1445
MTU 1514 bytes
Flags: Access, Trusted
Link status last changed: 0d 02h:25m:57s ago
Last clearing of counters: 0d 02h:25m:57s ago
Statistics:
   Received 4973595 frames, 1272848056 octets
   668 pps, 1.383 Mbps
   32 broadcasts, 0 runts, 0 giants, 0 throttles
   0 error octets, 0 CRC frames
   13602 multicast, 4959961 unicast
   Transmitted 23674 frames, 6226872 octets
   0 pps, 0 bps
   39 broadcasts, 0 throttles
```

Related Command

Command	Description
show interface port-channel	Displays the port-channel information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

interface-profile ddns-profile

```
interface-profile ddns-profile <profile-name>
   clone <profile>
   hostname
   interval
   no
   password
   service-url
   username
```

Description

Use the `ddns-profile <profile-name>` command to configure a Dynamic Domain Name Server (DDNS) profile.

Syntax

Parameter	Description	Range	Default
`clone`	Copy data from another ddns-profile	_	_
`hostname`	Host name of the client whose IP is to be updated using DDNS.	_	_
`interval`	The frequency (in minutes/days) at which the DDNS update happens.	15 minutes – 30 days	7 days
`no`	Delete command.	_	_
`password`	A valid password with a maximum of 16 characters. Allowed characters are letters, digits, hyphen (**-**), dot (**.**) and underscore (_).	_	_
`service-url`	Service URL is the update URL that is used to send the DDNS updates to the DDNS server. Every DDNS server site has its own service update URL. Example: myonlineportal.net/updateddns.	_	_
`username`	A valid username. Allowed characters are letters, digits, hyphen (**-**), dot (**.**), at (@), and underscore (_).	_	_

Example

A sample DDNS profile configuration is provided below:

```
(host)(config) #interface-profile ddns-profile ddns1
(host) (DDNS profile "ddns1") #username John
(host) (DDNS profile "ddns1") #password monika
(host) (DDNS profile "ddns1") #service-url dynupdate.no-ip.com/nic/update
(host) (DDNS profile "ddns1") #interval 0 7 0
(host) (DDNS profile "ddns1") #hostname arubamas.no-ip.info
```

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

interface-profile dhcp-relay-profile

```
interface-profile dhcp-relay-profile <profile-name>
   clone <profile>
   helper-address
   no
   option82
   source-ip
```

Description

Use the `ip dhcp relay-profile <profile-name>` command to configure a DHCP relay profile.

Syntax

Parameter	Description	Range	Default
clone	Copies data from another DHCP relay profile.	_	_
<profile>	Name of DHCP relay profile to be copied.	_	_
helper-address	DHCP helper address.	_	_
<address>	A.B.C.D format.	_	_
no	Delete command.	_	_
option82	Option 82	_	_
circuit-identifier	Circuit identifier.	_	Disabled
- interface-name	Use interface-name in circuit ID.	_	_
- vlan	Use VLAN in circuit ID.	_	_
remote-identifier	Remote identifier.	_	Disabled
- host-name	Use host name.	_	_
- mac	Use MAC address.	_	_
- <user-defined field>	Configure any string.	_	Disabled
source-ip	Set or change source IP of the relay packet.	_	Disabled
- giaddr	Set giaddr as source IP. By default, the source IP address in the relayed packet is set to the IP address of the outgoing RVI. The source IP address of the relay packet can be changed to take the incoming RVI.	_	_

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.1.1	Added host-name, mac, <user-defined field>, and giaddr.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

interface-profile enet-link-profile

```
interface-profile enet-link-profile {default|<profile-name>}
   autonegotiation
   duplex {auto|full|half}
   speed {10 | 100 | 1000 | 10000 | 10m_100m | auto}
   flowcontrol {auto|lossless|on|off}
   no {...}
   exit
```

Description

This command creates an Ethernet link profile that can be assigned to an interface, interface group, or port-channel.

Syntax

Parameter	Description	Range	Default
`default`	Modifies the default Ethernet link profile.	—	—
`<profile-name>`	Identification name for the non-default profile.	Upto 63 characters;can begin with a numeric character	—
`autonegotiation`	Enables auto-negotiation of port speed.	—	Enabled
`duplex {auto|full|half}`	Sets the duplex to one of the following parameters: • auto—Configures auto mode. • full—Configures full duplex mode. • half—Configures half duplex mode.	—	auto

Parameter	Description	Range	Default
`speed {10 | 100 | 1000 | 10000 | 10m_100m | auto}`	Sets the speed to one of the following parameters: • auto—Negotiates bandwidth dynamically between 10 and 1000/10000. • 10—10 Mbps. • 100—100 Mbps. • 1000—1 Gbps. • 10000—10 Gbps. • 10m_100m—10 to 100 Mbps. • auto—auto-negotiate	—	auto
`flowcontrol {auto|lossless|on|off}`	Sets the flowcontrol to one of the following parameters: • auto—Configures auto mode. • lossless—configures lossless mode. • on—configures on mode. • off—configures off mode.	—	off
`no {...}`	Removes the specified configuration.	—	—

Usage Guidelines

Use this profile to configure autonegotiation, duplex, speed, and flow control for the port. Creating an Ethernet Link profile does not apply the configuration to any interface or interface group. To apply the Ethernet Link profile, use the `interface gigabitethernet` and `interface-group` commands.

Example

The following example creates an Ethernet link profile:

```
interface-profile enet-link-profile ENET_LINK_General
   autonegotiation
```

```
duplex full
speed 1000
flowcontrol lossless
exit
```

Related Command

Command	Description
show interface-profile	Displays the specified Ethernet Link porfile information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

interface-profile gvrp-profile

```
interface-profile gvrp-profile <profile-name>
   clone <source>
   enable
   no..
   registrar-mode [forbidden|normal]
```

Description

These commands configure a GVRP profile.

Syntax

Parameter	Description	Default
`<profile-name>`	Enter a name for the GVRP profile.	—
`clone <source>`	Copies data from another GVRP profile.	—
`enable`	Enables or Disables GVRP profile.	Disabled
`registrar-mode`	Sets the registration mode as **normal** or **fobidden**.	normal
`normal`	In normal mode, Mobility Access Switchregisters and de-registers VLANs to or from its connected switches and IAPs.	—
`forbidden`	In forbidden mode, Mobility Access Switch cannot register nor de-register VLANs to or from its connected switches and IAPs.	—
`no {...}`	Removes the specified configuration parameter.	—

Usage Guidelines

Use these commands to configure a GVRP profile. The GVRP profile must then be applied to an interface for it to take effect. To apply the GVRP profile, use the **`interface gigabitethernet`** command.

Example

The following command configures GVRP profile on an interface:

```
(host)(config)# interface-profile gvrp-profile Enable-GVRP
(host)(Interface GVRP profile "gvrp")# enable
(host)(Interface GVRP profile "gvrp")# registrar-mode normal
(host)(config) # interface gigiabitethernet 0/0/10
(host)(gigabitethernet "0/0/10") # gvrp-profile gvrp
```

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

interface-profile igmp-profile

```
interface-profile igmp-profile <profile-name>
   clone <source>
   disable
   no
   query-interval <secs>
   version [v2|v3]
```

Description

Use this command to configure an IGMP profile on an interface.

Syntax

Parameter	Description	Range	Default
`clone`	Copies data from another interface IGMP profile.	_	_
`disable`	Disable IGMP.	_	Enabled
`no`	Delete command.	_	_
`query-interval <secs>`	Periodic interval in seconds at which IGMP queries are sent.	1–18000	125 secs
`version [v2|v3]`	Enables IGMP version 2 or version 3 based on the user input. By default, IGMP version 2 is enabled.	_	v2

Example

```
(host)(config) #interface-profile igmp-profile igmp-int-profile
(host)(Interface IGMP profile "igmp-int-profile") #query-interval 44
(host)(Interface IGMP profile "igmp-int-profile") #version v3
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.3.1	The **version** parameter was introduced to support IGMPv3.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

interface-profile lacp-profile

```
interface-profile lacp-profile <profile-name>
   group-id <0-63>
   independent-state
   mode {active|passive}
   no {...}
   port-priority <1-65535>
   timeout {long|short}
   exit
```

Description

This command creates a dynamic LACP port-channel profile that can be assigned to any interface or interface group.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Identification name for the LACP profile.	1–32 characters;can begin with a numeric character.	—
`group-id <0-63>`	Specifies the port-channel group ID.	• 0–63: For all Mobility Access Switches except the S1500 Mobility Access Switch. • 0–7: For S1500 Mobility Access Switch.	—
`independent-state`	Enables LACP Independent state. With this feature enabled, when ethernet ports in an LACP enabled device are connected to an LACP disabled device, the incompatible ports are put into Independent (I) state. When in Independent state, the ports continue to carry data traffic similar to any other single link without any change in the port configuration.	—	Enabled

Parameter	Description	Range	Default
`mode {active|passive}`	Sets the LACP port-channel to one of the following modes: • active—In active mode, a port-channel member can send participation requests to other ports in the port-channel. • passive—In passive, a port-channel member does not send participation requests to other ports. It can only receive and accept participation codes from other members.	—	passive
`port-priority <1-65535>`	Specifies the port priority for the port-channel interface.	1–65535	255
`timeout {long|short}`	Specifies the time timeout as long or short: • long—90 seconds. • short—3 seconds.	—	long
`no {...}`	Removes the specified LACP configuration parameter.	—	—

Usage Guidelines

Use this command to create an LACP profile. Creating an LACP profile does not apply the configuration to any interface or interface group. To apply the LACP profile, use the interface gigabitethernet and interface-group commands.

Example

The following example creates an LACP profile:

```
(host) (config)#interface-profile lacp-profile Port-Channel_01
group-id 1
mode active
port-priority 6553
timeout long
exit
```

Related Command

Command	Description
show interface-profile lacp-profile	Displays the LACP profile information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3.1	The **independent-state** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

interface-profile lldp-profile

```
interface-profile lldp-profile {lldp-factory-initial|default|<profile-name>}
   clone <source>
   lldp fast-transmit-counter <1-8>
   lldp fast-transmit-interval <1-3600>
   lldp med-tlv-select
   lldp receive
   lldp tlv-select
   lldp transmit
   lldp transmit-hold <1-100>
   lldp transmit-interval <1-3600>}
   med enable
   proprietary-neighbor-discovery
   no {...}
   exit
```

Description

This command creates an LLDP profile that can be assigned to any interface or interface group.

Syntax

Parameter	Description	Range	Default
`lldp-factory-initial |default`	Modifies the factory initial or the default LLDP profile.	—	—
`<profile-name>`	Identification name for the LLDP profile.	1–32 characters; can begin with a numeric character	—
`clone <source>`	Copies data from another LLDP profile.	—	—
`lldp fast-transmit-counter`	Set the number of the LLDP data units sent each time fast LLDP data unit transmission is triggered.	1–8	4
`lldp fast-transmit-interval`	Sets the LLDP fast transmission interval in seconds.	1-3600 seconds	1 second
`lldp med-tlv-select`	Allows you to enable or disable one of the following MED TLVs: • **network-policy** • **power-management**	—	Enabled
`lldp receive`	Enables processing of LLDP PDU received.	—	Disabled

Parameter	Description	Range	Default
`lldp tlv-select`	Allows you to enable or disable one of the following TLVs: • **aggregation-status** • **mac-phy-config** • **management-address** • **max-frame-size** • **port-description** • **port-vlan-id** • **power-management** • **system-capabilities** • **system-description** • **system-name** • **vlan-name**		Enabled
`lldp transmit`	Enables LLDP PDU transmit.	—	Disabled
`lldp transmit-hold <1-100>`	Sets the transmit hold multiplier.	1–100.	4
`lldp transmit-interval <1-3600>}`	Sets the transmit interval in seconds.	1–3600 seconds	30 seconds
`med enable`	Enables the LLDP MED protocol. **NOTE:** Depricated from ArubaOS 7.4.1.5.	—	Disabled
`proprietary-neighbor-discovery`	Enables proprietary neighbor discovery from protocols such as CDP.	—	Disabled
`no {...}`	Removes the specified LLDP configuration parameter. **NOTE:** The `no med enable` command is depricated from ArubaOS 7.4.1.5.	—	—

Usage Guidelines

Use this command to create an LLDP profile. Creating an LLDP profile does not apply the configuration to any interface or interface group. To apply the LLDP profile, use the `interface gigabitethernet` and `interface-group` commands.

Example

The following example creates an LLDP profile called LLDP_General:

```
interface-profile lldp-profile LLDP_General
   lldp fast-transmit-counter 2
   lldp fast-transmit-interval 50
   lldp receive
   lldp transmit
   lldp transmit-hold 60
   lldp transmit-interval 2500
   exit
```

Related Command

Command	Description
show interface-profile lldp-profile	Displays LLDP profile information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.2	**lldp fast-transmit-counter** and **lldp fast-transmit-interval** parameters were introduced.
ArubaOS 7.3	**lldp med-tlv-select** and **lldp tlv-select** parameters were introduced.
ArubaOS 7.4.1.5	The **med enable** and **med disable** commands are deprecated, as LLDP-MED option is set to Auto mode.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

interface-profile mirroring-profile

```
interface-profile mirroring-profile <profile-name>
   clone <source>
   destination gigabitethernet <slot/module/port>
   ratio <0-2047>
   no {...}
   exit
```

Description

This command creates a mirroring profile that can be assigned to any interface, or a interface group.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Identification name for the mirroring profile.	1–32 characters;can begin with a numeric character	
`clone <source>`	Copies data from another mirroring profile.		
`destination gigabitethernet <slot/module/port>`	Specifies the destination port to which the packets should be sent.		
`ratio <0-2047>`	Specifies the ratio of packets that should be mirrored. • 0—Does not mirror any packet to the destination. • 1—Mirrors all packets to the destination (1:1). This is the default. • 100—Mirrors 1 out of 100 packets to the destination. • 2047—Mirrors 1 out of 2,047 packets to the destination.	0–2047	1

Parameter	Description	Range	Default
`no {...}`	Removes the specified mirroring configuration parameter.	—	—

Usage Guidelines

Use this command to create a port mirroring profile. Creating a mirroring profile does not apply the configuration to any interface or interface group. To apply the mirroring profile, use the `interface gigabitethernet` and `interface-group` commands.

Example

The following example creates a port mirroring profile:

```
interface-profile mirroring-profile Mirroring
   destination gigabitethernet 0/0/19
   ratio 50
   exit
```

Related Command

Command	Description
`show interface-profile mirroring-profile`	Displays port mirroring profile information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

interface-profile mstp-profile

```
interface-profile mstp-profile <profile-name>
   bpdufilter [default | unconditional]
   bpduguard auto-recovery-time <recovery_timeout>
   clone
   instance {cost <port-cost> | priority <port-priority>}
   loopguard
   no
   point-to-point
   portfast trunk
   rootguard
```

Description

Creates a Multiple Spanning Tree Protocol (MSTP) profile on the Mobility Access Switch. Using this command, you can enable the loopguard, rootguard, BPDU guard, and Portfast features on the MSTP profile.

Syntax

Parameter	Description	Range	Default
`bpdufilter [default | unconditional]`	Configure BPDU filter in one of the following modes specified: • **Default**—If you enable the default BPDU filter on an interface, the Mobility Access Switch first verifies if it is a genuine edge-port by sending a few BPDUs (11 BPDUs). If no response is received, it enables BPDU filter (stops sending BPDUs) on this port.The BPDU filter gets disabled, if it receives any BPDUs from the remote-end port. • **Unconditional**—If you enable unconditional BPDU filter on an interface, the port disables BPDU processing irrespective of the portfast configuration. In this case, the port neither sends nor processes any BPDUs received on this interface.	—	Disabled
`bpduguard`	Enables BPDU guard functionality.	—	Disabled
`auto-recovery-timeout <auto-recovery-time>`	Enter the time in seconds to automatically activate the interface after it is shutdown. Specifying 0 disables the auto-recovery option.	0-65535	0
`instance`	Enter the MST instance number.	0 - 64	0

Parameter	Description	Range	Default
`cost <port-cost>`	Enter the keyword **cost** followed by the port cost value.	1 - 2000000000	—
`priority <port-priority>`	Enter the keyword **priority** followed by the priority value in increments of 16. For example, 16, 32, 48, 64, 80, 96, 112, etc. All other values are rejected.	0 - 240	128
`loopguard`	Enables loopguard on an interface MSTP profile.	—	—
`point-to-point`	Enables a broadcast interface as a point-to-point interface.	—	—
`portfast trunk`	Enables portfast on a trunk port.	—	—
`rootguard`	Enables rootguard on the MSTP interface profile.	—	—

Usage Guidelines

The BPDU guard functionality prevents malicious attacks on edge ports. When the malicious attacker sends a BPDU on the edge port, it triggers unnecessary STP calculation. To avoid this attack, use the BPDU guard on that edge port. The BPDU guard enabled port shuts down as soon as a BPDU is received.

Loopguard provides additional protection against Layer 2 forwarding loops (spanning tree loops). A spanning tree loop is created when a spanning tree blocking port, in a redundant topology, erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the spanning tree blocking port) is no longer receiving spanning tree BPDUs (Bridge Protocol Data Units).

If loopguard is enabled on a non-designated port receiving BPDUs, then that non-designated port is moved into the spanning tree loop-inconsistent blocking state.

The portfast and rootguard features cannot be enabled if loopguard is enabled.

When the link on a bridge port goes up, MSTP runs its algorithm on that port. If the port is connected to a host that does not support MSTP, it takes approximately 30 seconds for the port to transition to the forwarding state. During this time, no user data passes through this bridge port and some user applications may timeout. You can use the portfast functionality to avoid this.

Rootguard provides a way to enforce the root bridge placement in the network. The rootguard feature guarantees that a port will not be selected as Root Port for the CIST or any MSTI. If a bridge receives superior spanning tree BPDUs on a rootguard-enabled port, the port is selected as an Alternate Port instead of Root Port and no traffic is forwarded across this port.

By selecting the port as an alternate port, the rootguard configuration prevents bridges, external to the region, from becoming the root bridge and influencing the active spanning tree topology.

Best practices is that loopguard and rootguard are used on designated ports.

Example

```
(host) (config) #interface-profile mstp-profile mstp
(host) (Interface MSTP "mstp") #bpduguard auto-recovery-time 30
(host) (Interface MSTP "mstp") #instance 1 cost 200
(host) (Interface MSTP "mstp") #instance 1 priority 128
(host) (Interface MSTP "mstp") #portfast
(host) (Interface MSTP "mstp") #rootguard
```

Related Commands

Command	Description
show mstp-global-profile	View the global MSTP settings
show spanning-tree	View the spanning tree configuration
show spanning-tree mstp msti	View the details of a specific instance or a complete listing of all the MSTP instance settings.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.2	**bpduguard** command was introduced.
ArubaOS 7.3.2	**bpdufilter** command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

interface-profile oam-profile

```
interface-profile oam-profile <oam-profile-name>
   allow-loopback
   clone
   discovery-mode
   link-fault-action
   link-timeout
   no
   pdu-rate
   remote-loopback
```

Description

This command creates a OAM profile that can be applied to any interface.

Syntax

Parameter	Description	Range	Default
`allow-loopback`	Enables support for OAM local loopback.		Disabled
`clone <source>`	Clones configuration parameters from the specified OAM profile.		
`discovery-mode`	Enables OAM Discovery mode.	Active or Passive	Active
`link-fault-action`	Action taken on link-fault detection.	Syslog or Error-disable	Error-disable
`link-timeout`	Timeout out in seconds to declare a link fault.	2–10	5
`no`	Removes the command.		
`pdu-rate`	Maximum OAM PDUs sent per second.	1–10	5
`remote-loopback`	Puts remote device into loopback mode.		Disabled

Usage Guidelines

Use this command to create an OAM profile. Creating an OAM profile does not apply the configuration to any interface or interface group. To apply the OAM profile, use the **`interface gigabitethernet`** and **`interface-group`** commands.

```
(host) (OAM profile "oamtest") #allow-loopback
(host) (OAM profile "oamtest") #link-fault-action syslog
(host) (OAM profile "oamtest") #link-timeout 3
(host) (OAM profile "oamtest") #pdu-rate 8
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config mode (config)

interface-profile ospf-profile

```
interface-profile ospf-profile <profile-name>
   area <areaid>
   clone <source>
   cost <1-65535>
   dead-interval <1-65535>
   disable
   hello-interval <1-65535>
   message-digest-key [1-255] md5-passwd <md5-passwd>
   no {...}
   priority <0-255>
   retransmit-interval <1-3600>
   transmit-delay <1-65535>
```

Description

Configures an interface OSPF profile that can be applied to the Layer 3 routed VLAN interfaces and loopback interfaces.

There is a default profile named "default" that you can use or you can create your own profile name.

Syntax

Parameter	Description	Range	Default
`area <areaid>`	Enter the keyword **area** followed by the area identification, in A.B.C.D or decimal format, to configure an OSPF area.	0–4294967295	0.0.0.0
`clone <source>`	Enter the keyword **clone** followed by the name of the OSPF source profile that you want to copy (clone) data from.	—	—
`cost`	Enter the keyword **cost** followed by the cost value to set cost associated with the OSPF traffic on an interface.	1–65535	1
`dead-interval`	Enter the keywords **dead-interval** followed by the elapse interval, in seconds, since the last hello-packet is received from the router. After the interval elapses, the neighboring routers declare the router dead.	1–65535 seconds	40
`disable`	Enter the keyword **disable** to disable (or enable) an OSPF profile.	—	Enabled
`hello-interval`	Enter the keywords **hello-interval** followed by the elapse interval, in seconds, between hello packets sent on the interface.	1–65535 seconds	10
`message-digest-key <md5-key>`	Enter the keyword message-digest-key.	1–255	—

Parameter	Description	Range	Default
md5-passwd <md5-passwd>	The OSPF password in bytes.	1–16	—
priority	Enter the keyword **priority** followed by a value that sets the priority number of the interface to determine the designated router.	0–255	1
retransmit-interval	Enter the keywords **retransmit-interval** followed by the elapse time, in seconds, to set the retransmission time between link state advertisements for adjacencies belonging to the interface. Set the time interval so that unnecessary retransmissions do not occur.	1 to 3600 seconds	5
transmit-delay	Enter the keywords **transmit-delay** followed by the elapse time, in seconds, to set the delay time before re-transmitting link state update packets on the interface.	1 to 65535 seconds	1
no {...}	Removes the specified OSPF configuration.	—	—

Usage Guidelines

When configuring OSPF over multiple vendors, use this **cost** command to ensure that all routers use the same cost. Otherwise, OSPF may route improperly.

Example

The example below clones the OSPF profile named “techpubs” to the OSPF profile named “default”. The profile named “default”

```
(host) (Interface OSPF profile "techpubs") #clone default
(host) (Interface OSPF profile "techpubs") #
```

Related Command

Command	Description
router ospf	Configure the global OSPF parameters.

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.
ArubaOS 7.1.3	Message Digest Key introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

interface-profile pim-profile

```
interface-profile pim-profile <profile-name>
   clone <source>
   dr-priority <priority>
   hello-interval <secs>
   mode {sparse}
   no {...}
```

Description

Use this command to configure a PIM profile under an interface profile.

Syntax

Parameter	Description	Range	Default
`clone`	Copies data from another Interface PIM profile.	_	_
`disable`	Enable or disable PIM.	_	Enabled
`dr-priority`	Router priority that is advertised in the PIM “hello message.”	1–65535	1
`hello-interval`	Periodic interval at which PIM “hello messages” are sent.		30 sec
`mode`	Configures PIM mode.	_	sparse
`no`	Delete command.	_	_

Example

```
(host)(config) #interface-profile pim-profile aaa-pim-profile
(host)(Interface PIM profile "aaa-pim-profile") #mode sparse
```

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

interface-profile poe-profile

```
interface-profile poe-profile <profile-name>
   close <source>
   enable
   poe-maxpower <milliwatts>
   poe-priority {critical|high|low}
   time-range-profile <name>
```

Description

This command creates a PoE profile that can be assigned to any interface or interface group.

Syntax

Parameter	Description	Range	Default
`poe-factory-initial|default`	Modifies the factory initial or the default PoE profile.	—	—
`<profile-name>`	Identification name for the new PoE profile.	Upto 63 characters;can begin with a numeric character	—
`clone`	Copy data from another PoE profile	—	—
`enable`	Enables power over Ethernet.	—	Disabled
`poe-maxpower <milliwatts>`	Specifies the maximum power that can be supplied to the Ethernet interface in milliwatts.	—	30000
`poe-priority {critical|high|low}`	Specifies the PoE priority to one of the following: • critical • high • low When there is power shortage, the low priority ports are powered off before the high priority ports and then the critical priority ports. When ports have the same priority, the lowest port number is powered off before a higher port number.	—	low
`time-range-profile <name>`	Applies time range profile to the PoE interface.	—	—

Usage Guidelines

Use this command to create a PoE profile where the ethernet ports are supplied with Power over Ethernet. Creating a PoE profile does not apply the configuration to any interface or interface group. To apply the PoE profile, use the `interface gigabitethernet` and `interface-group` commands.

Example

The following example creates a power over Ethernet profile:

```
interface-profile poe-profile PoE_General
   enable
   poe-maxpower 10000
   poe-priority high
   time-range-profile sample
   mode periodic
   periodic start-day daily start-time 7:00 end-day daily end-time 18:00
   exit
```

Related Commands

Command	Description
show interface-profile	Displays the specified PoE profile information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

interface-profile port-security-profile

```
interface-profile port-security-profile <profile-name>
   clone
   dynamic-arp-inspection
   ip-src-guard
   ipv6-ra-guard action {drop|shutdown} auto-recovery-time <recovery-time>
   loop-protect [auto-recovery-time <recovery_timeout>]
   mac-limt <limit> action {drop|log|shutdown} auto-recovery-time <auto-recovery-time>
   no
   proxy-arp
   sticky-mac action {drop | shutdown} autorecovery-time <1-65535>]
   trust dhcp
```

Description

This command configures port security profile on an interface.

Syntax

Parameter	Description	Default
`<profile-name>`	Enter a name for the port security profile to be copied.	—
`dynamic-arp-inspection`	Enables Dynamic ARP Inspection.	—
`ip-src-guard`	Enables IP Source Guard functionality.	
`ipv6-ra-guard`	Configures RA guard action.	—
`action{drop|shutdown}`	When set to drop, the packet is dropped and a message is logged. When set to shutdown, the interface is shutdown.	—
`auto-recovery-time <recovery-time>`	Enter the recovery time in seconds to activate the interface after it is shutdown. Specifying 0 disables the auto-recovery option.	0
`loop-protect`	Enables Port Loop protect.	—
`auto-recovery-time <recovery_timeout>`	Enter the time in seconds to automatically activate the interface after it is shutdown. Specifying 0 disables the auto-recovery option.	0
`trust dhcp`	Enables DHCP trust mode.	—
`mac-limit`	Configures the maximum number of MACs that can be learned on this interface.	—
`<limit>`	Enter the MAC limit.	—

Parameter	Description	Default
action {drop|log|shutdown}	The drop action drops all further MAC learning requests and packets from unknown MACs. The log option just logs system message that the limit is reached. The shutdown option shuts the port down when the specified MAC limit is exceeded.	—
auto-recovery-timeout <auto-recovery-time>	Enter the recovery time in seconds to activate the interface after it is shutdown. Specifying 0 disables the auto-recovery option.	0
proxy-arp	Enables the proxy ARP functionality.	
sticky-mac	Enables Sticky MAC on the interface.	—
action {drop | shutdown}	Allows to configure a Sticky MAC action when Sticky MAC violation occurs.	Drop
autorecovery-time <0-65535>]	Allows to configure the autorecovery time for the mentioned action after Sticky MAC violation occurs	0
no {...}	Removes the specified configuration parameter.	—

Usage Guidelines

Use this command to create port security profile on an interface. Creating a port security profile does not apply the configuration to any interface or interface group. To apply the port-security profile, use the `interface gigabitethernet` and `interface port-channel` commands.

Examples

The following commands enable and configure RA guard profile on an interface:

```
(host)(config)# interface-profile port-security-profile RA-Guard1
  ipv6-ra-guard action drop auto-recovery-time 60
(host)(config)# interface gigabitethernet 0/0/6
  port-security-profile RA-Guard1
```

The following commands enable and configure DHCP trust on an interface:

```
(host)(config)# interface-profile port-security-profile ps1
  no trust dhcp
(host)(config)# interface gigabitethernet 0/0/6
  port-security-profile PS1
```

The following commands enable and configure Loop Protect on an interface:

```
(host) (config) #interface-profile port-security-profile Loop-Protect
  loop-protect auto-recovery-time 10
(host)(config)# interface gigabitethernet 0/0/6
  port-security-profile Loop-Protect
(host) (config) #interface port-channel 3
  port-security-profile Loop-Protect
```

The following commands configures MAC limit on an interface:

```
(host)(config)# interface-profile port-security-profile MAC_Limit
```

```
  mac-limit 30 action drop auto-recovery-time 50
(host)(config)# interface gigabitethernet 0/0/6
  port-security-profile MAC_Limit
```

The following commands enable and configure IPSG :

```
(host)(config)# interface-profile port-security-profile ipsg
  ip-src-guard
```

The following commands enable and configure DAI:

```
(host)(config)# interface-profile port-security-profile dai
  dynamic-arp-inspection
```

The following command enables Sticky-MAC:

```
(host)(config)# interface-profile port-security-profile <profile-name> sticky-mac
```

The following commands help configure a port security profile and enables proxy ARP:

```
(host) (config) #interface-profile port-security-profile "PARP"
(host) (Port security profile "PARP") #proxy-arp
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.
ArubaOS 7.4	The **sticky-mac**, **dynamic-arp-inspection**, and **ip-src-guard** parameters were introduced.
ArubaOS 7.4.0.2	The **action** and **auto-recovery-time** sub-parameters are introduced in the sticky-mac command.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

interface-profile pvst-port-profile

```
interface-profile pvst-port-profile <profile-name>
   bpdufilter [default | unconditional]
   bpduguard [auto-recovery-time <recovery_timeout>]
   clone
   loopguard
   no
   point-to-point
   portfast trunk
   rootguard
   vlan <vlan> [cost <cost> | priority <priority>]
```

Description-

Configure an interface PVST+ bridge.

Syntax

Parameter	Description	Range	Default
<profile-name>	Enter a PVST profile name.	—	—

Parameter	Description	Range	Default
`bpdufilter [default | unconditional]`	Configure BPDU filter in one of the following modes specified: • **Default**—If you enable the default BPDU filter on an interface, the Mobility Access Switch first verifies if it is a genuine edge-port by sending a few BPDUs (11 BPDUs). If no response is received, it enables BPDU filter (stops sending BPDUs) on this port.The BPDU filter gets disabled, if it receives any BPDUs from the remote-end port. • **Unconditional**—If you enable unconditional BPDU filter on an interface, the port disables BPDU processing irrespective of the portfast configuration. In this case, the port neither sends nor processes any BPDUs received on this interface.	—	Disabled
`bpduguard`	Enables BPDU guard functionality.	—	Disabled
`auto-recovery-timeout <auto-recovery-time>`	Enter the time in seconds to automatically activate the interface after it is shutdown. Specifying 0 disables the auto-recovery option.	0–65535	0
`loopguard`	Enables loopguard on an interface MSTP profile.	—	—
`point-to-point`	Enables a broadcast interface as a point-to-point interface.	—	—

Parameter	Description	Range	Default
`portfast trunk`	Enable portfast on a trunk.	—	—
`rootguard`	Enables rootguard on an interface MSTP profile.	—	—
`vlan <vlan>`	Enter the keyword **vlan** followed by the vlan spanning tree identifier.	1–4094	—
`cost <cost>`	Enter the keyword **cost** followed by the port-cost value.	1–2000000000	—
`priority <priority>`	Enter the keyword **priority** followed by the port priortity value (in increments of 16). Valid values are: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. All other values are rejected.	0 to 240	128

Usage Guidelines

Loopguard provides additional protection against Layer 2 forwarding loops (spanning tree loops). A spanning tree loop is created when a spanning tree blocking port, in a redundant topology, erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the spanning tree blocking port) is no longer receiving spanning tree BPDUs (Bridge Protocol Data Units).

If loopguard is enabled on a non-designated port receiving BPDUs, then that non-designated port is moved into the spanning tree loop-inconsistent blocking state

When the link on a bridge port goes up, PVST+ runs its algorithm on that port. If the port is connected to a host that does not “speak” PVST+, it takes approximately 30 seconds for the port to transition to the forwarding state. During this time, no user data passes through this bridge port and some user applications may time out.

Rootguard provides a way to enforce the root bridge placement in the network. The rootguard feature guarantees that a port will not be selected as Root Port. If a bridge receives superior spanning tree BPDUs on a rootguard-enabled port, the port is selected as an Alternate Port instead of Root Port and no traffic is forwarded across this port.

By selecting the port as an Alternate Port, the rootguard configuration prevents bridges, external to the region, from becoming the root bridge and influencing the active spanning tree topology.

Examples

The following example sets VLAN 2 port cost to 500.

```
(host)(Interface PVST bridge "techpubs") #vlan 2 cost 500
```

The following example enables and configures BPDU guard on an interface by using PVST profile:

```
(host) (config) #interface-profile pvst-port-profile BPDU_Guard
  bpduguard
  auto-recovery-time 30
```

Enable loopguard:

```
(host)(Interface PVST bridge "TechPubs") #loopguard
```

Associate to the interface:

```
(host)(config) #interface gigabitethernet 0/0/2
  (host)(gigabitethernet "0/0/2") #pvst-port-profile TechPubs
```

To immediately transition the bridge port into the forwarding state upon linkup, enable the PVST+ portfast feature.

```
(host)(config) #interface-profile pvst-port-profile TechPubs
```

The bridge port still participates in PVST+; if a BPDU is received, it becomes a normal port.

Portfast is operational only on access ports.

Enable rootguard:

```
(host)(Interface PVST bridge "TechPubs") #rootguard
```

Associate to the interface:

```
(host)(config) #interface gigabitethernet 0/0/2v
  (host)(gigabitethernet "0/0/2") #pvst-port-profile TechPubs
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.2	The **bpduguard** parameter was introduced.
ArubaOS 7.3.2	The **bpdufilter** command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

interface-profile switching-profile

```
interface-profile switching-profile {default|<profile-name>}
   access-vlan <vlan id>
   clone <source>
   native-vlan <vlan id>
   no
   storm-control-bandwidth <1-100>
   storm-control-broadcast
   storm-control-multicast
   storm-control-unknown
   switchport-mode {access|trunk}
   trunk allowed vlan [add|all|except|remove] <vlan list>
```

Description

This command creates a switching profile that can be applied to any interface, interface group, or a port-channel.

Syntax

Parameter	Description	Range	Default
`default`	Modifies the default switching profile.		
`<profile-name>`	Identification name for switching profile.	1-32 characters; can begin with a numeric character	
`access-vlan <VLAN-ID>`	Specifies the access VLAN ID.		1
`native-vlan <VLAN-ID>`	Specifies the native VLAN ID.		1
`storm-control-bandwidth <1-100>`	Specifies the storm control bandwidth.	1-100	50
`storm-control-broadcast`	Enables storm control for broadcast.		Enabled
`storm-control-multicast`	Enables storm control for multicast.		Disabled
`storm-control-unknown-unicast`	Enables storm control for unknown.		Enabled
`switchport-mode {access|trunk}`	Specifies the switch port mode as access or trunk: • **access**—Configures the port to be an access port. • **trunk**—Configures the port to be a trunk port.		access

Parameter	Description	Range	Default
`trunk allowed vlan [add|all|except|remove] <VLANs-List>`	Specifies the allowed VLANs on a trunk port.		1-4094
`no {...}`	Removes the specified configuration parameter.		

Usage Guidelines

Use this command to assign VLAN IDs to an interface. Creating a switching profile does not apply the configuration to any interface or interface group. To apply the switching profile, use the `interface gigabitethernet` and `interface-group` commands.

Example

```
interface-profile switching-profile Switching_General
   access-vlan 1
   switchport-mode access
   exit
```

Related Command

Command	Description
`show interface-profile switching-profile`	Displays the switching profile information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3.2	The allowed range for **storm-control-bandwidth** was changed from 50–100 to 1–100.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config mode (config)

interface-profile tunneled-node-profile

```
interface-profile tunneled-node-profile <profile-name>
   backup-controller-ip <IP-address>
   clone <source>
   controller-ip <IP-address>
   keepalive <1-40>
   mtu <1024-1500>
   no {...}
```

Description

This command creates a tunneled node profile that can be applied to any interface.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Identification name for the tunneled node profile.	1–32 characters; can begin with a numeric character	—
`backup-controller-ip <IP-address>`	Specifies the IP address of the back-up controller for establishing a tunneled node.	—	—
`clone <source>`	Copy configuration from another tunneled node server profile.	—	—
`controller-ip <IP-address>`	Specifies the IP address of the primary controller for establishing a tunneled node.	—	—
`keepalive <1-40>`	Specifies the keepalive time in seconds.	1–40 seconds	10
`mtu <1024-7168>`	Specifies the MTU on the path to the controller in bytes.	1024–1500	1400
`no {...}`	Removes the specifies configuration parameter.	—	—

Usage Guidelines

Use this command to create a tunneled node profile. Creating a Tunneled Nodes profile does not apply the configuration to any interface or interface group. To apply the Tunneled Nodes profile, use the `interface gigabitethernet` and `interface-group` commands.

Example

```
interface-profile tunneled-node-profile WLAN_Controller
   backup-controller-ip 10.5.18.2
   controller-ip 10.6.17.1
   keepalive 30
   mtu 1400
```

Related Command

Command	Description
show interface-profile tunneled-node-profile	Displays the tunneled node profile information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1.1	The **backup-controller-ip** parameter is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config mode (config)

interface-profile voip-profile

```
interface-profile voip-profile <profile-name>
   clone <source>
   no{...}
   voip-dot1p <priority>
   voip-dscp <value>
   voip-mode [auto-discover | static]
   voip-vlan <VLAN-ID>
```

Description

This command creates a VoIP profile that can be applied to any interface, interface group, or a port-channel.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of the VoIP profile.	1–32 characters; can begin with a numeric character	—
`voip-dot1p <priority>`	Specifies the dot1p priority.	—	—
`voip-dscp <value>`	Specifies the DSCP value for the voice VLAN.	—	—
`voip-mode [auto-discover | static]`	Specifies the mode of VoIP operation. • auto-discover - Operates VoIP on auto discovery mode. • static - Operates VoIP on static mode.	—	static
`voip-vlan <vlan id>`	Specifies the Voice VLAN ID.	—	—
`no {...}`	Removes the specifies configuration parameter.	—	—

Usage Guidelines

Use this command to create VoIP VLANs for VoIP phones. Creating a VoIP profile does not apply the configuration to any interface or interface group. To apply the VoIP profile, use the `interface gigabitethernet` and `interface-group` commands.

Example

```
interface-profile voip-profile VoIP_PHONES
   voip-dot1p 100
   voip-dscp 125
   voip-mode auto-discover
   voip-vlan 126
```

Related Command

Command	Description
show interface-profile voip-profile	Displays the VoIP profile information for VoIP phones.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1.3	The `voip-mode` parameter is added.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config mode (config)

interface range

```
interface range
   gigabitethernet <interface-list>
```

Description

This command configures a range of gigabit ethernet ports on the Mobility Access Switch.

Syntax

Parameter	Description
`gigabitethernet <interface-list>`	Specify a range of gigabit ethernet port on the Mobility Access Switch. **NOTE:** Enter valid interface member in ascending order.

Example

The following example configures gigabit ethernet ports from 0/0/1 to 0/0/5:

```
(host)(config) #interface range gigabitethernet 0/0/1-0/0/5
(host)(config-range)#
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

interface tunnel ethernet

```
interface tunnel ethernet <id>
   clone <source>
   description <LINE>
   destination-ip <address>
   inter-tunnel-flooding
   keepalive <interval> <retries>
   mtu <mtu>
   no {...}
   protocol <protocol>
   shutdown
   source-ip <address> {controller-ip | loopback <interface> | vlan <interface>}
   switching-profile <profile_name>
```

Descripton

This command configures an L2-GRE tunnel. By default, the tunnel is trusted.

Syntax

Parameter	Description	Range	Default
`<id>`	Identification number of the tunnel interface.	1–50	-
`clone <source>`	Name of the tunnel interface to copy. **NOTE:** Source IP and destination IP do not get copied. They need to be configured separately.	-	-
`description <LINE>`	Interface description upto 128 characters long.	1–128 characters	-
`destination ip <address>`	Set the destination IP address of the interface.	-	-
`inter-tunnel-flooding`	Enables inter-tunnel flooding.	-	enabled

Parameter	Description	Range	Default
`keepalive <interval> <retries>`	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.	**interval**: 1–86400 **retries**: 1–1024	disabled
`mtu <mtu>`	Maximum Transmission Unit (MTU) size for the interface.	1024–1500	1100
`no {...}`	Negates any configured parameter.	—	—
`protocol <protocol>`	Specifies 16-bit Generic Route Encapsulation (GRE) protocol number that uniquely identifies a Layer-2 tunnel. The Mobility Access Switch and the Mobility Controller at both endpoints of the tunnel must be configured with the same protocol number.	0– 65535	0
`shutdown`	Causes a hard shutdown of the interface.	—	—
`source-ip <address> {controller-ip | loopback <interface> | vlan <interface>}`	The local endpoint of the tunnel on the switch. This can be one of the following: • source IP address of the interface • controller IP address • the loopback interface configured on the switch • 802.1q VLAN interface number	**loopback**: 0– 63 **vlan**: 1–4094	—
`switching-profile <profile_name>`	Apply switch-port profile to the tunnel interface.	—	default

Usage Guidelines

Use this command to configure an L2-GRE tunnel and apply the switching profile.

Example

```
(host) (config) #interface tunnel ethernet 1
(host) (Tunnel "1") #description L2-GRE_Interface
(host) (tunnel "1") #source-ip 10.0.0.1
(host) (tunnel "1") #destination-ip 10.0.1.2
(host) (tunnel "1") #switching-profile mDNS_vlan_200
(host) (tunnel "1") #keepalive 30 5
```

The following sample command deletes the switching-profile from the interface tunnel 50:

```
(host) (config) #interface tunnel ethernet 50
(host) (Tunnel "50") #no switching-profile
```

Related Command

Command	Description
show interface tunnel	Displays L2 or L3 GRE tunnel interface information.

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.
ArubaOS 7.4.1	The **no switching-profile** command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

interface tunnel ip

```
interface tunnel ip <id>
   clone <source>
   description <LINE>
   destination-ip <address>
   ip <address>
   keepalive <interval> <retries>
   mtu <mtu>
   no {...}
   ospf-profile <interface name>
   protocol <protocol>
   shutdown
   source-ip <address> {controller-ip | loopback <interface> | vlan <interface>}
   switching-profile
```

Descripton

This command configures an L3-GRE tunnel. By default, the tunnel is trusted.

Syntax

Parameter	Description	Range	Default
`<id>`	Identification number of the tunnel interface.	1–50	—
`clone <source>`	Name of the tunnel interface to copy. **NOTE:** Source IP and destination IP do not get copied. They need to be configured separately.	—	—
`description <LINE>`	Interface description upto 128 characters long.	1–128 characters	—
`destination ip <address>`	Set the destination IP address of the interface.	—	—
`ip <address> <mask>`	Interface IP address and subnet mask	—	—
`keepalive <interval> <retries>`	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.	**interval**: 1–86400 **retries**: 1–1024	Disabled

Parameter	Description	Range	Default
`mtu <mtu>`	Maximum Transmission Unit (MTU) size for the interface.	1024– 1500	1100
`no {...}`	Negates any configured parameter.	–	–
`ospf-profile`	OSPF profile name to attach to L3 GRE tunnel.	–	–
`shutdown`	Causes a hard shutdown of the interface.	–	–
`source-ip <address> {controller-ip|loopback <interface>|vlan <interface>}`	The local endpoint of the tunnel on the switch. This can be one of the following: • source IP address of the interface • controller IP address • the loopback interface configured on the switch • 802.1q VLAN interface number	**loopback**: 0 - 63 **vlan**: 1–4094	–
`switching-profile`	Applies a switching profile to the interface		

Usage Guidelines

Use this command to configure an L3-GRE tunnel and attach the switching profile.

Example

The following sample commands help configure a tunnel:

```
(host) (config) #interface tunnel ip 1
(host) (Tunnel "1") #description L3-GRE_Interface
(host) (tunnel "1") #source-ip 192.0.2.1
(host) (tunnel "1") #destination-ip 192.0.2.98
(host) (tunnel "1") #keepalive 30 5
(host) (tunnel "1") #mtu 1100
(host) (Tunnel "1") #ip address 192.0.2.0 255.255.255.0
(host) (Tunnel "1") # ospf-profile TechPubs
```

Related Command

Command	Description
`show interface tunnel`	Displays L2 or L3 GRE tunnel interface information.

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

interface vlan

```
interface vlan <vlan-id>
   aruba-vpn-pool-profile
   clone <source>
   ddns-profile <profile_name>
   description <name>
   dhcp-relay-profile <profile-name>
   igmp-profile <profile_name>
   ip
           address {{<address> <netmask> [secondary]}| dhcp-client}
           directed-broadcast
           nat [inside | outside]
   ipv6 address {{<prefix> netmask <subnet-mask>}|{link-local <link-local>}}
   metric
   mtu <64-7168>
   no {...}
   ospf-profile <profile-name>
   pim-profile <profile-name>
   probe-profile <profile-name>
   session-processing
   shutdown
   vrrp-profile <id>
```

Description

This command creates routed VLAN interfaces.

Syntax

Parameter	Description	Range	Default
`aruba-vpn-pool-profile`	Applies the specified Aruba VPN pool profile to the interface.	—	—
`clone <source>`	Clones configuration parameters from the specified VLAN.	—	—
`ddns-profile <profile_name>`	Applies the specified dynamic Domain Name Server profile to the interface.	—	—
`description <name>`	Specifies a name for the VLAN interface.	1–32 characters; cannot begin with a numeric character	
`dhcp-relay-profile <profile-name>`	Assigns the specified DHCP Relay profile to the interface VLAN.	—	—

Parameter	Description	Range	Default
`igmp-profile <profile_name>`	Applies the specified IGMP profile to the interface.	—	—
`ip`	This command is used to assign an IPv4 address to the VLAN.	—	—
`access-group [in <acl> | out <acl> | session <acl>]`	Applies one of the following types of ACLs to the interface: • **in**—Applies the specified ingress ACL on the interface • **out**—Applies the specified egress ACL on the interface. • **session**—Applies the specified session ACL on the interface	—	—
`address {{<address> <netmask>}[secondary] | dhcp-client)`	Assigns the specified IP address to the VLAN interface. Additionally, by adding the secondary option, the IP address is assigned as the secondary IP for the VLAN interface. Alternatively, the VLAN interface can be configured to get the IP address from the DHCP client.	—	—
`directed-broadcast`	Enables IP directed broadcast. An IP directed broadcast enabled on VLAN interface allows a packet sent to the broadcast address of a subnet to which the originating device is not directly connected. For more information, refer ArubaOS 7.2 User Guide.	—	disabled

Parameter	Description	Range	Default
`nat [inside | outside]`	Enables Network Address Translation (NAT) on VLAN interfaces for inside or outside traffic. You can set	—	disabled
`ipv6 address {{<prefix> netmask <subnet-mask>}| link-local <link-local>}`	Assigns the specified IPv6 IP address to the VLAN interface. Alternatively, the VLAN interface can be configured to geet the IP address from the link local.	—	—
`metric`	Assigns a cost value for the VLAN interface.	—	—
`mtu <64-7168>`	Specifies the size of the jumbo frames in bytes	64–7168	1514
`no {...}`	Removes the specified configuration parameter.	—	—
`ospf-profile <profile-name>`	Assigns the specified OSPF interface profile to the interface VLAN.	—	—
`pim-profile <profile-name>`	Assigns the specified PIM interface profile to the interface VLAN.	—	—
`probe-profile`	Applies the specified probe-profile to the VLAN interface.	—	—
`session-processing`	Enables session processing on the interface for applying selective stateful firewall policy.	—	—
`shutdown`	Disables the VLAN interface.	—	—
`vrrp-profile <id>`	Apply VRRP profile to the VLAN inetrface.	—	—

Usage Guidelines

Use this command to create routed VLAN interfaces.

Example

```
(host)(config)# interface vlan 10
   ip address 10.10.10.10 netmask 255.255.255.0
   ip directed-broadcast
```

```
description Layer3
mtu 1500
no shutdown
exit
```

The following command modifies the auto-configured link local address of VLAN 1 to fe80::20b:86ff:fe6a:2800.

```
(host)(config)#interface vlan 1
(host)(vlan "1")#ipv6 address link-local fe80::20b:86ff:fe6a:2800
```

The following command configures the global unicast address of VLAN 1 to 2cce:205:160:100::fe.

```
(host)(config)#interface vlan 1
(host)(vlan "1")#ipv6 address 2cce:205:160:100::fe prefix_len 64
```

Related Command

Command	Description
`show interface vlan`	Displays the interface VLAN information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced for the VLAN interface 1.
ArubaOS 7.1	This command is supported for a total of 4094 VLAN interfaces.
ArubaOS 7.1.1	The **ipv6** parameter was introduced.
ArubaOS 7.2	A new parameter **directed-broadcast** is introduced to enable IP directed broadcast on a VLAN interface. A new parameter **secondary** is introduced to allow you to assign a secondary IP address to a VLAN interface. A new parameter **nat inside** is introduced to allow you to enable NAT on a VLAN interface.
ArubaOS 7.3	New parameters **vrrp-profile** and **sesssion-processing** were introduced.
ArubaOS 7.3.2	The **ip access-group out** parameter was introduced.
ArubaOS 7.4	The following new parameters are introduced: • **aruba-vpn-pool-profile** • **ddns-profile** • **ip nat outside** • **ip access-group session** • **metric** • **probe-profile**

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config mode (config)

ipv6-profile

```
ipv6-profile
   default-gateway <X:X:X:X::X>
```

Description

This command configures the IPv6 default gateway.

Syntax

Parameter	Description
`default-gateway <X:X:X:X::X>`	Specify the IPv6 address of the default gateway.

Usage Guidelines

Use this command to configure the IPv6 default gateway.

Example

The following command configures an IPv6 default gateway.

```
(host)(config)#ipv6-profile
(host)(ipv6-profile)#default-gateway 2cce:205:160:100::fe
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

ip access-list eth

```
ip access-list eth {<number>|<name>}
   deny {<ethtype> [<bits>]|any}
   no ...
   permit {<ethtype> [<bits>]|any}
```

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.	—
`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.	—

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.

Example

The following command configures an Ethertype ACL:

```
ip access-list eth 200
   deny 809b
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

ip access-list extended

```
ip access-list extended {<number>|<name>}
   deny <protocol> <source> <dest>
   no ...
   permit <protocol> <source> <dest>
```

Description

This command configures an extended access control list (ACL).

Syntax

Parameter	Description	Range
`extended`	Enter a name, or a number in the specified range.	100–199, 2000–2699
`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 and wildcard any: any source host: specify a single host IP address • eq: To match packets only on a given source port number • lt: To match packets with lower source port number • gt:To match packets with greater source port number • neq: To match packets not on a given source port number • range: To match packets in the range of source port numbers	—
`<dest>`	Destination, which can be one of the following: Destination address and wildcard any: any destination host: specify a single host IP address • eq: To match packets only on a given source port number • lt: To match packets with lower source port number • gt:To match packets with greater source port number • neq: To match packets not on a given source port number • range: To match packets in the range of source port numbers	—
`no`	Negates any configured parameter.	—
`permit`	Allow the specified packets.	

Parameter	Description	Range
<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 and wildcard any: any source host: specify a single host IP address • eq: To match packets only on a given source port number • lt: To match packets with lower source port number • gt:To match packets with greater source port number • neq: To match packets not on a given source port number • range: To match packets in the range of source port numbers	—
<dest>	Destination, which can be one of the following: Destination address and wildcard any: any destination host: specify a single host IP address • eq: To match packets only on a given destination port number • lt: To match packets with lower destination port number • gt:To match packets with greater destination port number • neq: To match packets not on a given source port number • range: To match packets in the range of source port numbers	—

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. You can also use the extended ACLs to match packets based on Layer 4 source ports and destination ports.

Example

The following command configures an extended ACL:

```
(host) (config) #ip access-list extended 100
  permit tcp host 1.1.1.1 eq 80 host 2.2.2.2 gt 440 established
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

ip access-list mac

```
ip access-list mac {<number>|<name>}
   deny {<macaddr>[<wildcard>]|any|host <macaddr>}
   no ...
   permit {<macaddr>[<wildcard>]|any|host <macaddr>}
```

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	—
`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	—

Usage Guidelines

MAC ACLs allow filtering of non-IP traffic. This ACL filters on a specific source MAC address or range of MAC addresses.

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 7.0	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

ip access-list session

```
ip access-list session <accname>
   <source> <dest> <service> <action> [<extended action>]
   no ...
```

Description

This command configures an access control list (ACL) session.

Syntax

Parameter	Description
`<accname>`	Name of an access control list session.
`<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 • **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 • **network**: specify the IP address and netmask • **user**: represents the IP address of the user
`<service>`	• **<0-255>**: Network service, which can be one of the following: • IP protocol number (0-255) • **STRING**: name of a network service (use the show netservice command to see configured services) • **any**: match any traffic • **tcp** **destination port number**: specify the TCP port number (0-65535) **source**: TCP/UDP source port number • **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**: Performs destination NAT on packets. Forward packets from source network to destination; re-mark them with destination IP of the target network. This action functions in tunnel/decrypt-tunnel forwarding mode. User should configure the NAT pool in the Mobility Access Switch. • **permit:** Forward packets. • **redirect tunnel <id>**: Specify the ID of the tunnel configured with the interface tunnel command. • **src-nat**: Performs source NAT on packets. Source IP changes to the outgoing interface IP address (implied NAT pool) or from the pool configured (manual NAT pool). This action functions in tunnel/decrypt-tunnel forwarding mode.

Parameter	Description
<extended action>	Optional action if rule is applied, which can be one of the following: • **blacklist**: blacklist user if ACL gets applied. • **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. • **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)
no	Negates any configured parameter.

Usage Guidelines

Session ACLs define traffic and firewall policies on the Mobility Access Switch. 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.

Examples

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 deny
```

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
```

The following example displays information for an ACL.

```
(host) (config-sess-common)#show ip access-list common
ip access-list session common

common
-------
Priority  Source          Destination  Service  Action  ...
--------  ------          -----------  -------  ------  ...
1         10.12.13.14     any          any      permit  ...
2         11:12:11:11::2  any          any      permit  ...


Queue  TOS  8021P  ...  ClassifyMedia  IPv4/6
-----  ---  -----  ...  -------------  ------
Low               ...                 4
Low               ...                 6
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Requires the PEFNG license	Config mode on master Mobility Access Switch

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
`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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

ip access-list stateless

```
ip access-list stateless <acc-name>
   <source>
   <destination>
   <service>
   <action>
   <extended-action>
   no
```

Description

This command configures a stateless access control list (ACL).

Syntax

Parameter	Description	Range
<acc-name>	Name of the stateless ACL.	—
<source>	Source of the traffic, which can be one of the following: • alias: This refers to using an alias for a host or network. • any: Acts as a wildcard and applies to any source address. • host: This refers to traffic from a specific host. When this option is chosen, you must enter the IP address of the host. • network: This refers to a traffic that has a source IP from a subnet of IP addresses. When this option is chosen, you must enter the IP address and network mask of the subnet.	—
<destination>	Destination of the traffic, which can be configured in the same manner as source.	—
<service>	Protocol, which can be one of the following: • <0-255>: Protocol number between 0–255 • STRING: Name of the network service • any: Any protocol • arp: Match ARP traffic • icmp: Internet Control Message Protocol • igmp: Internet Gateway Message Protocol • tcp <port>: Transmission Control Protocol • udp <port>: User Datagram Protocol	—
<action>	Action, which can be one of the following: • permit: Allow the specified packets. • deny: Reject the specified packets. • redirect tunnel <id> | ipsec <mapname>: Redirect packets to an L3-GRE tunnel.	—

Parameter	Description	Range
`<extended-action> (optional)`	This can be one of the following options: • blacklist: Automatically blacklists a client that is the source or destination of traffic matching this rule.This option is recommended for rules that indicate a security breach where the blacklisting option can be used to prevent access to clients that are attempting to breach the security. • log: Logs a match to this rule. This is recommended when a rule indicates a security breach, such as a data packet on a policy that is meant only to be used for voice calls. • policer-profile: Attaches the policer-profile to the ACL. • position: Configures the position of the ACE in the ACL. • qos-profile: QoS profile can be configured to assign specific TC/DP, DSCP, and 802.1p values. This option attaches the qos-profile to the ACL. • time-range: Time range for which this rule is applicable.	—

Usage Guidelines

A stateless ACL statically evaluates packet contents. The traffic in the reverse direction will be allowed unconditionally.

Examples

The following command configures a stateless ACL:

```
(host) (config) #ip access-list stateless STATELESS
   network 10.100.100.0 255.255.255.0 any tcp 8888 deny log
   any host 10.100.100.200 any deny log
   any any any permit
```

The following command configures and applies a Policy-Based Routing:

```
(host) (config) #ip access-list stateless st
   any any tcp 10 100 permit nexthop 200.0.0.5
   any any udp 10 100 redirect tunnel 10
   any any udp 10 100 redirect ipsec ipsec1
(host) (config) #interface vlan 100
   ip access-group in st
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.2	The **redirect tunnel** parameter was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

ip dhcp aruba-vpn-pool

```
ip dhcp aruba-vpn-pool <profile-name>
   client-count
   clone
   dns-server
   domain-name
   ip-range
   lease
   no
   option
   reserve
   server-type
```

Description

Use this command to configure Aruba VPN pool profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of the Aruba VPN pool profile.	_	_
`client-count`	Configure the number of DHCP clients per branch in Distributed DHCP scope.	_	_
`clone`	Copy data from another Aruba VPN pool.	_	_
`dns-server <address>`	(Optional) Create a DNS server in A.B.C.D format.	_	_
`domain-name`	(Optional) Specify a domain name.	_	_
`ip-range`	Range of IP addresses which can be divided in to multiple IP subnets for the specified client count in Distributed,L3 scope.	_	_
`<address1>`	Start address in A.B.C.D format.	_	_
`<address2>`	End address in A.B.C.D format.	_	_
`lease`	(Optional) Configure the client IP lease time.	_	_
`<days>`	Number of days.	0-4096	_
`<hours>`	Number of hours.	0–24	12
`<minutes>`	Number of minutes.	0–60	_
`<seconds>`	Number of seconds.	0–60	_
`no`	Delete Command.	_	_
`option`	(Optional) Configure DHCP server options.	_	_
`<code>`	Option code.	1–255	_

Parameter	Description	Range	Default
ip	IP address.	_	_
text	Text string.	_	_
<string>	IP address in A.B.C.D format, if 'ip' is chosen above text string, if 'text' is chosen above.	_	_
reserve	(Optional) Reserve the specified number of IP addresses in the beginning or end of the subnet.	_	_
server-type	Configure the server type for distributed DHCP scope. **NOTE:** Distributed, L3 mode is the only server-type supported.	_	Distributed, L3

Usage Guidelines

Ensure that you configure the following features on the Mobility Access Switch for Distributed, L3 DHCP scope to be functional.

- Enable **service dhcp**
- Establish Aruba VPN tunnel.

Apply the configured Aruba VPN pool profile to a VLAN interface.

You can configure up to six Aruba VPN pools and apply them to the required VLAN interfaces. You can apply only one profile per VLAN and cannot apply the same profile to another VLAN.

Example

Use the following commands to configure Distributed,L3 DHCP scope:

```
(host) (config)# service dhcp
(host) (config) #ip dhcp  aruba-vpn-pool Distributed,L3
(host) (Aruba VPN DHCP Pool "Distributed,L3") #ip-range 30.30.0.0 30.30.255.255
(host) (Aruba VPN DHCP Pool "Distributed,L3") #client-count 5
(host) (Aruba VPN DHCP Pool "Distributed,L3") # exit
(host) (config) #interface vlan 1
(host) (vlan "1") #dhcp-scope-profile Distributed,L3
```

Related Command

Command	Description
show ip dhcp aruba-vpn-pool	Displays the details of the configured Aruba VPN pool profiles on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.4	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

ip dhcp pool

```
ip dhcp pool <profile-name>
   clone
   default-router
   dns-server
   domain-name
   exclude-address
   hardware-address
   lease
   netbios-name-server
   network
   no
   option
   vendor-class-identifier
```

Description

Use the **`ip dhcp pool`** `<profile-name>` command to configure a DHCP server profile.

Syntax

Parameter	Description	Range	Default
`clone`	Copies data from another DHCP server profile.	_	_
`profile-name`	Name of DHCP server profile to be copied.	_	_
`default-router`	Creates a DHCP default router in A.B.C.D format.	_	_
`<address>`	Default router address.	_	_
`dns-server`	Creates a DNS server in A.B.C.D format.	_	_
`<address>`	DNS server address.	_	_
`domain-name`	Specifies a domain name.	_	_
`<name>`	Name of the domain.	_	_
`exclude-address`	Configures exclude addresses in A.B.C.D format.	_	_
`<address1>`	Start address in A.B.C.D format.	_	_
`<address2>`	End address in A.B.C.D format.	_	_

Parameter	Description	Range	Default
`hardware-address <mac> ip-address <address>`	Assigns a fixed IP address for a specific device using DHCP based on the MAC address of the device.	_	_
`lease`	Configures DHCP server pool lease times.	_	_
`<days>`	Number of days.	0-4096	_
`<hours>`	Number of hours.	0-24	_
`<minutes>`	Number of minutes.	0-60	_
`<seconds>`	Number of seconds.	0-60	_
`netbios-name-server`	Configures netbios name servers in A.B.C.D format.	_	_
`<address>`	Netbios name server address in A.B.C.D format.	_	_
`network`	DHCP server network pool.	_	_
`<address>`	Address in A.B.C.D format.	_	_
`<mask>`	Mask in A.B.C.D format.	_	_
`no`	Delete Command.	_	_
`option`	Configure DHCP server options.	_	_
`<code>`	Option code.	1-255	_
`ip`	IP address.	_	_
`text`	Text string.	_	_
`<string>`	IP address in A.B.C.D format, if 'ip' is chosen above text string, if 'text' is chosen above.	_	_
`vender-class-identifier`	Configures vendor-class-identifier.	_	_
`<string>`	Vendor-class-identifier string.	_	ArubaAP

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.3.2	The **hardware-address** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

ip nat pool

```
ip nat pool [<pool_name> <start_ip_src_nat_range> <end_ip_src_nat_range> <dest_ip> static]
```

Description

Use the ip nat pool command to create a Network Address Translation (NAT) pool on the Mobility Access Switch.

Syntax

Parameter	Description
`<pool_name>`	Name of the NAT pool.
`<start_ip_src_nat_range>`	The starting IP address of the source NAT range.
`<end_ip_src_nat_range>`	The ending IP address of the source NAT range.
`<dest_ip>`	The IP address of the destination NAT.
`static`	(Optional) Maps the NAT IP address on a one-to-one basis.

Example

The following sample configuration illustrates different NAT pool configuration:

NAT pool with source NAT option

```
(host) (config) #ip nat pool NAT_pool1 192.168.1.10 192.168.1.15
```

NAT Pool with dual NAT option

```
(host) (config) #ip nat pool dual_nat_pool1 192.168.1.10 192.168.1.15 172.16.10.1
```

Related Command

Command	Description
show ip nat pool	This command displays a list of IP NAT pools created in the network.

Command History

Release	Modification
ArubaOS 7.4	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

ip-profile

```
ip-profile
   controller-ip {ipsec <mapname> | loopback <interface> | vlan <interface>}
   default-gateway {<next-hop> | import dhcp}
   no
   prefix-list <prefix-list-name> seq <sequence-number> {[deny|permit] <network prefix
   A.B.C.D> <network mask A.B.C.D> [ge <bit-length> | le <bit-length>]}
   route <destip> <netmask> [<nexthop> | gre <tunnel-id> | ipsec <mapname>] | <metric>
```

Description

Configures the IP profile for the Mobility Access Switch.

Syntax

Parameter	Description	Range	Default
`controller-ip`	Configures the controller IP.	—	—
`ipsec <mapname>`	Use this command to configure the inner IP of the VPN tunnel as the controller IP.	—	—
`loopback <interface>`	Use this command to configure the loopback interface.	0–63	—
`vlan <interface>`	Use this command to specify the VLAN interface.	1–4094	—
`default-gateway`	Specifies the default gateway IP address or imports from DHCP server.	—	—
`<next-hop>`	Enter the IP address of the next-hop in dotted decimal format (A.B.C.D).	—	—
`import dhcp`	Use this command to import the default gateway from DHCP (when available) server.	—	—
`prefix-list <plist_name>`	Prefix list name.	—	—

Parameter	Description	Range	Default
`seq <sequence-number>`	Sequence number. Prefix lists are evaluated starting with the lowest sequence number and continue down the list until a match is made. Once a match is made, the permit or deny statement is applied to that network and the rest of the list is ignored. • **deny <network-prefix> <network mask>**— Specify IPv4 packets to reject. • **permit <network-prefix> <network mask>**— Specify IPv4 packets to forward. • **ge <bit-length>**— Minimum prefix length to be matched. • **le <bit-length>**— Maximum prefix length to be matched.	1 - 4294967287	—
`route <destip> <netmask>`	Specifies the static route for a destination IP.Enter the destination IP address in dotted decimal format (A.B.C.D).	—	—
`<nexthop>`	Use this command to configure the forwarding router's IP address.	—	—
`gre <tunnel-id>`	Use this command to configure the nexthop route using the GRE tunnel ID.	1 - 50	—
`ipsec <mapname>`	Use this command to configure the nexthop route using the IPSec map name	1 - 30	—
`<metric>`	Use this command to configure the cost to the specified destination prefix.	—	—

Usage Guidelines

Use this IP-profile to configure IPv4 default gateway, static routes, and prefix lists.

prefix-list option is used to configure IP prefix filtering. Prefix lists are used to either permit or deny the configured prefix based on the matching condition.

Any traffic that does not match any prefix-list entry is denied.

If only a ge value is entered, the range is the value entered for ge-length argument to a full 32-bit length. If only the le value is entered, the range is from the value entered for network-length argument to le-length argument. If a ge or le value is not used, the prefix list is processed using an exact match. If both ge and le values are

entered, the range falls between the values between the values used for the ge-length and le-length arguments. The behavior is described as follows:

network/length < ge-length <= le-length <= 32

The ge and le values are optional parameters.

Examples

The following example configures a default gateway in the IP profile:

```
(host)(config) #ip-profile
(host)(ip-profile) #default-gateway 2.2.2.2
```

The following examples configure static routes for the specified IP addresses:

```
(host)(ip-profile) #route 20.20.31.0 255.255.255.0 10.10.10.31
(host)(ip-profile) #route 20.20.32.0 255.255.255.0 10.10.10.32
(host)(ip-profile) #route 20.20.33.0 255.255.255.0 10.10.10.33
(host)(ip-profile) #no route 20.20.34.0 255.255.255.0 10.10.10.20
```

The following examples configure sequence numbers for the prefix-list test:

```
(host) (ip-profile) #prefix-list test seq 1 permit 5.5.5.0 255.255.255.0 ge 32
(host) (ip-profile) #prefix-list test seq 2 deny 6.6.6.0 255.255.255.0 ge 32
(host) (ip-profile) #prefix-list test seq 3 permit 10.10.0.0 255.255.255.0 ge 24 le 32
```

Related Command

Command	Description
show ip-profile	Displays the IP profile information which includes the default gateway IP address.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1	The **controller-ip** option was added.
ArubaOS 7.2	The **prefix-list** option was added.
ArubaOS 7.3	The **gre** parameter under the **route** command was added.
ArubaOS 7.4	The **ipsec** parameter under the **controller-ip** command is added.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

ip tacacs source-interface

```
ip tacacs source-interface {loopback | vlan <id> [secondary <ip>]}
```

Description

This command allows you to select a specific source-interface IP address for the outgoing TACACS packets.

Syntax

Parameter	Description
`loopback`	Assigns the switch IP as the source IP.
`vlan <id>`	Assigns the IP address of the specified VLAN interface as the source IP.
`secondary <ip>`	Assigns a secondary source IP address in A.B.C.D format. This parameter is optional.

Usage Guidelines

The global source-interface command is used to specify the source interface for all TACACS server request packets. If the source-interface IP address is configured at the profile level, it takes precedence over the global source interface IP address.

Examples

The following is a sample global source-interface command:

```
(host) (config) #ip tacacs source-interface vlan 55
```

Some sample profile-level source-interface commands are as follows:

```
(host) (config) #aaa authentication-server tacacs tac1
(host) (TACACS Server "tac1") #source-interface loopback
(host) (config) #aaa authentication-server tacacs tac2
(host) (TACACS Server "tac2") #source-interface vlan 55
```

Related Command

Command	Description
`show ip tacacs source-interface`	Displays the global source-interface configuration and the profile-level source-interface configuration.
`aaa authentication-server tacacs`	Specifies the source interface IP address at profile level for all TACACS server request packets.

Command History

Release	Modification
ArubaOS 7.4.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode.

lcd-menu

```
lcd-menu
   [no] disable [maintenance [factory-default| media-eject| qui-quick-setup |
   media-eject | system-halt | system-reboot | upgrade-image [parition0 | partition1]| upload-
   config]]
```

Description

This command disables the LCD menu either completely or only the specified operations.

Syntax

Parameter	Description	Default
`lcd-menu`	Enters the LCD menu configuration mode.	Enabled
`no`	Delete the specified LCD menu option.	
`disable`	Disables (or enables) the complete LCD menu.	Enabled
`maintenance`	Disables (or enables) the maintenance LCD menu.	Enabled
`factory-default`	Disables (or enables) the factory default LCD menu.	Enabled
`media-eject`	Disables (or enables) the media eject LCD menu.	Enabled
`qui-quick-setup`	Disables (or enables) the quick setup LCD menu.	Enabled
`system-halt`	Disables (or enables) the system halt LCD menu.	Enabled
`system-reboot`	Disables (or enables) the system reboot LCD menu.	Enabled
`upgrade-image`	Disables (or enables) the image upgrade LCD menu.	Enabled
`parition0` `partition1`	Disables (or enables) image upgrade on the specified partition (0 or 1).	Enabled
`upload-config`	Disables (or enables) the upload LCD menu.	Enabled

Usage Guidelines

You can use this command to disable executing the maintenance operations using the LCD menu. You can use the `no` form of these commands to enable the specific LCD menu. For example, the following commands enable `system halt` and `system reboot` options:

```
(host) (config) #lcd-menu
(host) (lcd-menu) #no disable menu maintenance system-halt
(host) (lcd-menu) #no disable menu maintenance system-reboot
```

You can use the following `show` command to display the current LCD settings:

```
(host)#show lcd-menu
lcd-menu
--------
Menu                                          Value
----                                          -----
menu maintenance upgrade-image partition0     enabled
menu maintenance upgrade-image partition1     enabled
```

```
menu maintenance system-reboot reboot-stack  enabled
menu maintenance system-reboot reboot-local  enabled
menu maintenance system-halt halt-stack      enabled
menu maintenance system-halt halt-local      enabled
menu maintenance upgrade-image               enabled
menu maintenance upload-config               enabled
menu maintenance factory-default             enabled
menu maintenance media-eject                 enabled
menu maintenance system-reboot               enabled
menu maintenance system-halt                 enabled
menu maintenance gui-quick-setup             enabled
menu maintenance                             enabled
menu                                         enabled
```

Examples

The following example disables the LCD menu completely:

```
(host) #configure terminal
(host) (config) #lcd-menu
(host) (lcd-menu) #disable menu
```

The following example disables executing the specified maintenance operation using the LCD menu:

```
(host) #configure terminal
(host) (config) #lcd-menu
(host) (lcd-menu) #disable menu maintenance ?
factory-default          Disable factory default menu
gui-quick-setup          Disable quick setup menu on LCD
media-eject              Disable media eject menu on LCD
system-halt              Disable system halt menu on LCD
system-reboot            Disable system reboot menu on LCD
upgrade-image            Disable image upgrade menu on LCD
upload-config            Disable config upload menu on LCD

(host) (lcd-menu) #disable menu maintenance upgrade-image ?
partition0               Disable image upgrade on partition 0
partition1               Disable image upgrade on partition 1
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

local-userdb add

```
local-userdb add {generate-username|username <name>} {generate-password|password <passwd>}
[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 creates a user account entry in the Mobility Access Switch'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 Aruba 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.	—	—

Parameter	Description	Range	Default
`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 Mobility Access Switch is used for authentication. Issue the **`aaa authentication-server internal use-local-switch`** command to use the internal database in a Mobility Access Switch; you then need to add user accounts to the internal database in the Mobility Access Switch.

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
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

local-userdb del

```
local-userdb {del username <name>|del-all}
```

Description

This command deletes entries in the Mobility Access Switch'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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

local-userdb export

```
local-userdb export <filename>
```

Description

This command exports the internal database to a file.

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

local-userdb-guest add

```
local-userdb-guest add {generate-username|username <name>} {generate-password|password
<passwd>} [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>]
[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.		
`guest-fullname`	The guest's full name.		
`guest-phone`	The guest's phone number.		
`mode`	Enables or disables the user account.	—	Disable

Parameter	Description	Range	Default
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 Mobility Access Switch is used for authentication. Issue the **aaa authentication-server internal use-local-switch** command to use the internal database in a Mobility Access Switch; you then need to add user accounts to the internal database in the Mobility Access Switch.

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
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

local-userdb-guest modify

```
local-userdb-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 Mobility Access Switch'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.		
`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	—

Parameter	Description	Range	Default
`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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

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 Mobility Access Switch'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 Aruba 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

Parameter	Description	Range	Default
`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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

local-userdb-guest del

```
local-userdb-guest del username <name>
```

Description

This command deletes entries in the Mobility Access Switch's internal database.

Syntax

Parameter	Description
`del username`	Deletes the user account for the specified username.

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

mgmt-server type amp

```
mgmt-server type amp
   config-server {host <ip-addr>|<host>} shared-secret <secret> group <group_name> folder
   <folder_name>
```

Description

Issue this command to associate the Mobility Access Switch with an AirWave configuration in a specified group and folder.

Syntax

Parameter	Description
`config-server {host <ip-addr>|<host>}`	IP address or host name of the AirWave server to be configured.
`shared-secret <secret>`	Shared secret for the AirWave server.
`group <group-name>`	Name of the AirWave group that contains the configuration for the Mobility Access Switch.
`folder <folder-name>`	Name of the AirWave folder that contains the configuration for the Mobility Access Switch.

Usage Guidelines

When the Mobility Access Switch connects to the AirWave server, it is assigned to the AirWave group and folder containing its group configuration. After the Mobility Access Switch appears as an associated device on the AirWave server,you must use AirWave to provision it with device-specific information (such as an IP address or port settings) before you allow the Mobility Access Switch to download its new configuration.

Example:

```
(host)(config)# mgmt-server type amp
(host)(mgmt-server-amp)# config-server host 192.0.2.0 shared-secret pwd123 group MAS folder
office4
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration mode

mkdir

```
mkdir
   member: <id> usb: <usbdirname> <usbpartition <number>>
   usb: <usbdirname> <usbpartition <number>>
```

Description

This command creates a new directory for USB .

Syntax

Parameter	Description	Range	Default
`member id`	Enter a stack member ID.	—	—
`<usbdirname>`	Creates the USB directory in a member of a stack.	—	—
`usbpartition <number>`	Creates the USB directory in multipartition member.	—	—
`usb:`	External USB.	—	—
`<usbdirname>`	Creates the USB directory.	—	—
`usbpartition <number>`	Creates the USB directory in multipartition.	—	—

Usage Guidelines

Use this command to create a new directory for USB.

Example

```
(host) #mkdir member: 1 usb: test2 usbpartition 1
Member-id: 1
------------
Successfully created the directory test2 at usb
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

mode-button

```
mode-button
   enable factory-default
```

Description

This command enables the **Mode** button and restores the S1500 Mobility Access Switches to factory default settings.

Syntax

Parameter	Description	Range	Default
`mode-button`	Enables the **Mode** button of the switch.	—	—
`enable factory-default`	Restores S1500Mobility Access Switches to factory default settings.	—	—

Usage Guidelines

Use this command to restore S1500 Mobility Access Switches to factory default settings.

After enabling the feature, push and hold the **Mode** button on the switch for about 15 seconds to reset it to the factory defaults. The Mobility Access Switch reboots after the reset.

Example

```
(host) (config) #mode-button
(host) (mode-button) #enable factory-default
```

Related Command

Command	Description
show mode-button	This command is used to verify the **Mode** button configuration of S1500 Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.4.0.2	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

mstp

```
mstp
   forward-delay
   hello-time
   instance
   max-age
   max-hops
   region-name
   revision
```

Description

Enters the Global MSTP mode and allows you to configure the forward delay time, refresh time, VLAN instance mapping, region name, maximum hops, and revision.

Syntax

Parameter	Description	Range	Default
`forward-delay`	Specifies the forward-delay time in seconds.	4– 30	15
`hello-time`	The time interval in seconds. at which the Bridge Protocol Data Units (BPDUs) are sent.	1–10	2
`instance <instance>`	An MSTP instance	0–64	0
`bridge priority <priority>`	Specify the bridge priority value in increments of 4096. **Valid values**: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.	0–61440	32768
`vlan <vlan-list>`	Specify the VLAN identifier value.	1–4094	—
`max-age`	Specify the time interval for the MSTP to maintain configuration information before refreshing that information	6–40	20
`max-hops`	Specify the maximum number of hops.	6–40	20
`region-name`	Specify the MSTP region names in bytes	1–32	—
`revision`	Specify the revision number.	0–65535	0

Usage Guidelines

MSTP allows users to map between a set of VLANs and to an MSTP instance (msti). By default, all VLANs are mapped to msti 0 unless you use the **vlan <vlan-list>** parameter to map it to a non-zero instance.

NOTE

For Mobility Access Switches to be in the same region, they must share the same name, the same version, and the same VLAN instance mapping. Any Mobility Access Switch that does not share these three characteristics with the remaining switches in the region will be seen as belonging to a different region.

Example

```
(host) (config) #mstp
(host) (Global MSTP) #forward-delay 10
(host) (Global MSTP) #hello-time 7
(host) (Global MSTP) #instance 44 bridge-priority 6144
(host) (Global MSTP) #max-age 22
(host) (Global MSTP) #max-hops 22
(host) (Global MSTP) #region-name my_region
(host) (Global MSTP) #revision 2
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

netdestination

```
netdestination <name>
   host <ipaddr> [position <number>]
   name <host_name>
   network <ipaddr> <netmask> [position <number>]
   no ...
```

Description

This command configures an alias for an IPv4 network host or subnet.

Syntax

Parameter	Description
`host`	Configures a single IPv4 host and its position in the list.
`name`	Name for this host or domain.
`network`	An IPv4 subnet consisting of an IP address and netmask.
`no`	Negates any configured parameter.

Usage Guidelines

Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the traffic source and/or destination IP in multiple session ACLs. Once you configure an alias, you can use it to manage network and host destinations from a central configuration point, because all policies that reference the alias will be updated automatically when you change the alias.

Example

The following command configures an alias for an internal network:

```
(host) (config) #netdestination Internal
   network 10.1.0.0 255.255.0.0
```

Related Command

Command	Description
show netdestination	This command displays a list of IPv4 network destinations.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3.2	Deprecated the **invert** and **range** parameters.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

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>`	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
```

Related Command

Command	Description
show netservice	This command displays a list of IPv4 network protocol services.

Command History

Version	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

ntp authenticate

```
ntp authenticate
```

Description

This command enables or disables NTP authentication.

Syntax

No parameters.

Usage Guidelines

Network Time Protocol (NTP) authentication enables the Mobility Access Switch to authenticate the NTP server before synchronizing local time with server. This helps identify secure servers from fradulent servers. This command has to be enabled for NTP authentication to work.

Example

The following command configures an NTP server:

```
(host) (config) #ntp authenticate
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

ntp authentication-key

```
ntp authentication-key <key-id> md5 <keyvalue>
```

Description

This command configures a key identifier and secret key and adds them into the database. NTP authentication works with a symmetric key configured by user. The key is shared by the client (Mobility Access Switch) and an external NTP server.

Syntax

Parameter	Description	Default
`<key-id>`	The key identifier is a string that is shared by the client (Mobility Access Switch) and an external NTP server. This value is added into the database.	—
`md5 <keyvalue>`	The key value is a secret string, which along with the key identifier, is used for authentication. This is added into the database.	—

Usage Guidelines

NTP authentication works with a symmetric key configured by user. The key is shared by the client (Mobility Access Switch) and an external NTP server. This command adds both the key identifier and secret string into the database.

Example

The following command configures the NTP authentication key. The key identifier is 12345 and the shared secret is 67890.

```
(host) (config) #ntp authentication-key 12345 md5 67890
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

ntp server

```
#ntp server <server-ip> [iburst] [key <key-id>]
```

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 Mobility Access Switch 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
`key <key-id>`	This is the key identifier used to authenticate the NTP server. This needs to match the key identifier configured in the **ntp authentication-key** command.	—

Usage Guidelines

You can configure the Mobility Access Switch to set its system clock using NTP by specifying one or more NTP servers.

Example

The following command configures an NTP server using the iburst optional parameter and using a key identifier “123456.”

```
(host) (config) #ntp server 10.1.1.245 iburst key 12345
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

ntp trusted-key

```
ntp trusted-key <keyid>
```

Description

This command configures an additional subset of trusted keys which can be used for NTP authentication.

Syntax

Parameter	Description	Default
`<keyid>`	An additional trusted string that can be used for authentication	—

Usage Guidelines

You can configure additional subset of keys which are trusted and can be used for NTP authentication.

Example

The following command configures an additional trusted key (84956) that can be used for NTP authentication.

```
(host) (config) #ntp trusted-key 84956
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

ospf-profile

```
ospf-profile <profile_name>
```

Description

Set an OSPF interface profile name.

Syntax

Parameter	Description
<profile_name>	Enter a profile name.

Usage Guidelines

Use this command to attach the OSPF profile name to the Routed VLAN Interface (RVI) or Loopback Interface.

Example

The following steps help assign an OSPF profile name to a Loopback Interface.

1. Create the loopback interface (3 in the example).

```
(host) (config) #interface loopback 3
(host) (loopback "3") #
```

2. Configure an IP address and Mask for the loopback.

```
(host) (loopback "3") #ip address 172.0.25.254 255.255.255.255
```

3. Attach the ospf-profile “techpubs” to the loopback interface.

```
(host) (loopback "3") #ospf-profile techpubs
```

4. Verify the loopback configuration:

```
(host) (loopback "3") #show interface loopback 3

loopback3 is administratively Up, Line protocol is Up
Hardware is Ethernet, Address is 00:0b:86:6a:f2:40
Description: Loopback
Internet address is 172.0.25.254, Netmask is 255.255.255.255
Interface index: 100663299
MTU 1514 bytes
```

Verify the interface configuration:

```
(host) (config) #show interface-config loopback 3

loopback "3"
------------
Parameter               Value
---------               -----
Interface OSPF profile  techpubs
IP Address              172.0.25.254/255.255.255.255
Interface description   N/A
```

Verify that the OSPF is enabled on a Loopback interface:

```
(host) #show ip ospf interface loopback 3

Interface is loopback3, line protocol is up
Internet Address 172.0.25.254, Mask 255.255.255.255, Area 0.0.2.0
```

```
Router ID 5.5.5.5, Network Type LOOPBACK, Cost: 10
Transmit Delay is 1 sec, State LOOP, Priority 1
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Neighbor Count is 0
Tx Stat: Hellos 0 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 0
Rx Stat: Hellos 0 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 0
         BadCksum 0 BadVer 0 BadNet 0 BadArea 0 BadDstAdr 0 BadAuType 0
         BadAuth 0 BadNeigh 0 BadMTU 0 BadVirtLink 0
```

Related Commands

Command	Description
interface loopback	Set the loopback interface
show interface loopback	View the interface loopback settings
show ip ospf	View the loopback interface

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

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 276.

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration and Enable modes

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 275.

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration and Enable modes

papi-security

```
papi-security {enhanced-security|key <key>}
no
```

Description

The papi-security command enforces advanced security options and provides an enhanced level of security. This command allows to enable or disable the PAPI Enhanced Security configuration and to configure a new security key if required.

Syntax

Parameter	Description	Range	Default
`enhanced-security`	Enables PAPI Enhanced Security		Disable
`key <key>`	Secret key that is used to authenticate messages between systems	10–64 characters	—
`no`	Disables the earlier configuration	—	—

Usage Guidelines

This command allows you to use advanced options that regulate PAPI communication between Mobility Access Switch and AirWave. When enhanced security is enabled, PAPI messages are authenticated at the receiving device and are denied if validation failed. If no key is configured, then Mobility Access Switch uses the default key.

All endpoint devices and AirWave must use the same key. Mismatch in secret key will result in error.

Examples

To enable the PAPI Enhanced Security mode, execute the following command:

```
(host) (config) #papi-security
(host) (PAPI Security Profile) #enhanced-security
```

To configure a new PAPI Enhanced Security key for Mobility Access Switch and AirWave, execute the following command:

```
(host) (PAPI Security Profile) #key 1234567890
```

Related Commands

Command	Description
show papi-security	Shows the status of the PAPI Enhanced Security configuration of the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.4.1.5	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration 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 Mobility Access Switch times out after two seconds.

Example

The following example pings 10.10.10.5.

```
(host) >ping 10.10.10.5
```

The sample Mobility Access Switch 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

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

ping ipv6

```
ping ipv6
   <X:X:X:X::X> | interface [mgmt <X:X:X:X::X> | vlan <vlan#> <X:X:X:X::X>]
```

Description

This command pings the specific IPv6 address.

Syntax

Parameter	Description
`<X:X:X:X::X>`	Specify the IPv6 global unicast address of the host to ping.
`interface mgmt <X:X:X:X::X>`	Specify the IPv6 link-local address of the host connected to the management interface.
`interface vlan <vlan#> <X:X:X:X::X>`	Specify the IPv6 link-local address of the host connected to the VLAN interface.

Usage Guidelines

Use this command to ping a specific IPv6 address.

Examples

The following command pings an IPv6 global unicast address:

```
(host) #ping ipv6 2cce:205:160:100::fe
```

The following command pings the IPv6 link-local address of the host connected to the management interface:

```
(host) #ping ipv6 interface mgmt fe80::20b:86ff:fe6a:2800
```

The following command pings the IPv6 link-local address of the host connected to VLAN 20:

```
(host) #ping ipv6 interface vlan 20 fe80::225:90ff:fe06:c84e
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.1.1	The parameter `interface vlan <vlan#> <X:X:X:X::X>` was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

ping <ip-address> mtu_discovery do

```
ping <ip-address> mtu_discovery {do|dont|want} size <value>
```

Description

This command helps you to find out the MTU path between the specified IP address and the Mobility Access Switch.

Syntax

Parameter	Description
`<ip-address>`	Specify the IP address of the controller.
`mtu_discovery {do|dont|want}`	Specify the MTU discovery requirement.
`size <value>`	Specify the value for size.

Usage Guidelines

Use this command to find out the MTU requirements for a tunneled node client.

Example

The following `ping` command helps find the MTU path between the IP address 10.16.7.1 of the controller and the Mobility Access Switch:

```
ping 10.16.7.1 mtu_discovery do size 1500
```

Related Command

Command	Description
show tunneled-node	Displays the tunneled node information

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

pkt-trace acl

```
pkt-trace acl <acl-name>
   disable
   enable
   log
   trace
   trace-hex-mask <tmask>
```

Description

This command helps to enable or disable packet tracing in the datapath.

Syntax

Parameter	Description
`disable`	Disables packet tracing in the datapath.
`enable`	Enables packet tracing in the datapath.
`log`	Enables writing packet trace data into log file.
`trace <name>`	Configures datapath trace options.
`trace-hex-mask <tmask>`	Configures datapath trace mask in Hex format.

Examples

The following command enables packet tracing for an ACL entry:

```
(host) # pkt-trace acl <ACL-name> enable
```

The following command disables packet tracing for an ACL entry:

```
(host) # pkt-trace acl <ACL-name> disable
```

The following sample pkt-trace acl command writes packet trace data into log file for the stated ACL bug:

```
(host) #pkt-trace acl acl-bug-58651 enable log trace acl-processing
```

Command History

Release	Modification
ArubaOS 7.4.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

pkt-trace-global

```
pkt-trace-global
   disable
   enable
   trace
   trace-hex-mask <tmask>
```

Description

This command helps to enable or disable the global packet tracing.

Syntax

Parameter	Description
`disable`	Disables global packet tracing in the datapath.
`enable`	Enables global packet tracing in the datapath.
`trace <name>`	Configures global datapath trace options.
`trace-hex-mask <tmask>`	Configure global datapath trace mask in Hex format. Use Hex value without 0x.

Examples

The following command enables global packet tracing:

```
(host) # pkt-trace-global enable
```

The following command disables global packet tracing:

```
(host) # pkt-trace-global disable
```

The following sample **pkt-trace global** command configures trace mask for ACL functionality:

```
(host) # pkt-trace-global enable trace-hex-mask 0 trace acl-processing
```

Command History

Release	Modification
ArubaOS 7.4.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

poe-management-profile

```
poe-management-profile slot <slot-number>
   cisco-compatibility
   clone <source>
   config-delay <config-delay>
   no {...}
   poe-guardband <1000-30000 milliwatts>
   poe-powermanagement {class | dynamic | static}
```

Description

Configures PoE global power management parameters on the Mobility Access Switch.

Syntax

Parameter	Description	Range	Default
`slot <slot-number>`	Specifies the stack member ID.	0–7	—
`cisco-compatibility`	Enable or disable Cisco® Pre-Standard compatibility. Cisco® legacy IP phone models such as 7940 and 7960 use a pre-standard Power Over Ethernet (PoE) detection mechanism and may not get powered up when connected to the Mobility Access Switch PoE models. ArubaOS for Mobility Access Switch introduces the functionality to provide PoE compatibility with Cisco® legacy IP phones. By default, this function is disabled. If you enable this function, the Mobility Access Switch changes the detection mechanism to give power to the Cisco® legacy IP phones.	—	Disabled
`clone <source>`	Copy data from another poe-management profile	–	–

Parameter	Description	Range	Default
`config-delay <config-delay>`	Introduces a time delay in milliseconds while applying the PoEconfiguration between each port. For example, if you configure a delay of 2 seconds and if the PoE configuration is applied on port 0 at t seconds, then the PoE configuration is applied on port 1 at t+2 seconds, port 2 at t+4 seconds and so on.	0–30000 in steps of 100.	2000
`no`	Delete a poe-management command	—	—
`poe-guardband <1000-30000 milliwats>`	Specifies the PoE guardband between 1000-30000 milliwatts in step of 1000.	1000–30000 milliwats in steps of 1000	11000
`poe-powermanagement {class|dynamic|static}`	The Mobility Access Switch supports three PoE power management modes: Static Mode—The power deducted from the total power pool is the maximum power for that interface. This mode ensures that the maximum power specified by you for the interface is always reserved and cannot be shared by other PDs. Dynamic Mode—The power allocated from the total power pool for each port is the actual power consumed at that port. You can allocate any unused portion of power to the other PDs. This is the default mode. Class-based Mode—The power allocated for each port from the total power pool is the maximum power available for the class of PD connected to that port.	—	class

Usage Guidelines

Use this command to set the global configuration for Power over Ethernet on the switch.

Example

The following example configure the power over Ethernet global parameters:

```
poe-management-profile slot 0
   cisco-compatibility
   poe-powermanagement dynamic
   poe-guardband 15000
```

Related Command

Command	Description
show poe-management-profile	This command displays total PoE pool information for the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.2.2	The **cisco-compatibility** parameter was introduced.
ArubaOS 7.3.2	The **config-delay** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

policer-profile

```
policer-profile <profile-name>
   cbs {k | m | g}
   cir <cir>
   clone <source>
   ebs [k | m | g]
   exceed-action drop | permit | remark
   exceed-profile <profile-name>
   no
   violate-action drop | permit
   violate-profile <profile-name>
```

Description

Use the policer-profile command in the configuration mode to create a Policer profile.

Syntax

Parameter	Description
`<profile-name>`	Name of the Policer profile.
`cbs`	Use this command to set the committed burst size. Range is 1 - 2147450880 bytes.
`k`	Option to set 1,000 byte burst size.
`m`	Option to set 1,000,000 byte burst size.
`g`	Option to set 1,000,000,000 byte burst size.
`cir`	Use this command to set the committed information rate.
`<cir>`	CIR value in Kbps. Range is 1-10230000.
`clone`	Use this command to copy an existing QoS profile.
`<source>`	Name of the QoS profile to be copied.
`ebs`	Use this command to set the committed burst size. Range is 1 - 2147450880 bytes.
`k`	Option to set 1,000 byte burst size.
`m`	Option to set 1,000,000 byte burst size.
`g`	Option to set 1,000,000,000 byte burst size.
`exceed-action`	Use this command to set the exceed action.
`drop`	Option to drop packet for exceed action.
`permit`	Option to do nothing for exceed action.
`remark`	Option to remark on packet in QoS profile for exceed action.

Parameter	Description
exceed-profile	QoS Profile for exceed action violations.
<profile-name>	Name of the profile.
no	Delete command.
violate-action	Use this command to set action for a QoS profile violation.
drop	Option to drop packet for violation.
permit	Option to do nothing for violation.
remark	Option to remark on packet in QoS profile.
violate-profile	Use this command to manage a QoS profile for violating packets.
<profile-name>	Name of the Profile.

Example

The following command helps create a Policer Profile from the Configuration mode:

```
(host) (config) #policer-profile policerProfile
(host) (Policer Profile "policerProfile") #
```

In the Policer Profile mode, the following commands are available:

- cbs
- cir
- clone
- ebs
- exceed-action
- exceed-profile
- no
- violate-action
- violate-profile

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration / Policer Profile subcommand mode

preemption

```
preemption [delay <seconds> | mode [off | forced]]
```

Description

Set the preemption mode to forced so you can configure the time delay (preemption) before the backup takes over from the primary. The preemption time (10 to 300 seconds) is recommended to avoid network flapping.

Syntax

Parameter	Description	Range	Default
`delay <seconds>`	Enter the keyword **delay** followed by the number of seconds you want to expire before the backup takes over from the primary interface. Range: Default:	10– 300 seconds (5 minutes)	100 seconds
`mode [off | forced]`	Enter the keyword **mode** followed by the keyword **forced** to enable preemption. To turn off preemption, enter the keywords **mode off**.		

Usage Guidelines

When a primary link goes down then comes back up, that link goes into standby mode by default, and the backup link remains active. You can force the primary interface to become active when it comes back up by configuring preemption in forced mode

Example

The following example enables preemption mode and sets the delay to 10 seconds.

```
(host) (gigabitethernet "0/0/10") #preemption mode forced
(host) (gigabitethernet "0/0/10") #preemption delay 10
```

Related Command

Command	Description
show hot-standby-link	List the status of hot standby link interfaces.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Interface Config

probe-profile

```
probe-profile <profile-name>
   clone <source>
   destination <destip>
   no
   pkt-found-cnt <pkt-found-cnt>
   pkt-lost-cnt  <pkt-lost-cnt>
   pkt-send-freq <pkt-send-freq>
   protocol
```

Description

Use the **probe-profile** command in the configuration mode to create a Probe profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of the Probe profile.	—	—
`clone <source>`	Copy data from another probe profile	—	—
`destination <destip>`	The IP address of the destination to be probed.	—	—
`pkt-found-cnt <pkt-found-cnt>`	The minimum successful response packet count required to keep the probe status as Up.	2–32	6
`pkt-lost-cnt  <pkt-lost-cnt>`	The minimum failed response packet count required to change the probe status to Down.	2–32	6
`pkt-send-freq <pkt-send-freq>`	The frequency (in seconds) at which the probe packets are sent to the destination IP.	1–32	5
`protocol`	The protocol to be used for sending the probe packets. **NOTE:** ICMP is the only protocol supported currently.	ICMP	ICMP

Usage Guidelines

This command can be used to monitor the L3 uplink status using ping probe.

Related Commands

Command	Description
show probe	View the probe status of the interfaces where the probe profile is attached.
show probe-profile	View the probe profile configuration.

Example

The following sample configures a probe-profile, **L3Monitoring** and applies it to the VLAN interface 1:

```
(host) (config) #probe-profile L3Monitoring
(host) (probe profile "L3Monitoring") #destination 10.1.10.1
(host) (probe profile "L3Monitoring") #pkt-found-cnt 16
(host) (probe profile "L3Monitoring") #pkt-lost-cnt 16
(host) (probe profile "L3Monitoring") #pkt-send-freq 11
(host) (probe profile "L3Monitoring") #protocol icmp
(host) (config) # interface vlan 1
(host) (vlan "1") # probe-profile L3Monitoring
```

Command History

Release	Modification
ArubaOS 7.4	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration / Probe Profile

qos-profile

```
qos-profile <profile-name>
   clone <source>
   dot1p <priority>
   drop-precedence {high | low}
   dscp <rewrite-value>
   no
   traffic-class <traffic-class-value>
```

Description

Use the qos-profile command in the configuration mode to create a QoS profile.

Syntax

Parameter	Description
`<profile-name>`	Name of the QoS profile.
`clone`	Use this command to copy an existing QoS profile.
`<source>`	Name of the QoS profile to be copied.
`dot1p`	Use this command to set the dot1p user priority.
`<priority>`	Value of the priority. Range is 0–7.
`drop-precedence`	Use this command to set the drop precedence to high or low.
`high`	Option to set the drop precedence to high.
`low`	Option to set the drop precedence to low.
`dscp`	Use this command to set the dscp rewrite value.
`<rewrite-value>`	Value of the rewrite. Default is disabled. Range is 0-63.
`no`	Delete command.
`traffic-class`	Use this command to set the traffic-class value.
`<traffic-class-value>`	Value of the traffic class. Default is disabled. Range is 0-63.

Example

Use the following command to create a QoS profile from the Configuration mode:

```
(Host) (config) #qos-profile qosProfile
(Host) (QoS Profile "qosProfile")#
```

In the QoS Profile mode, the following commands are available:

- clone
- dot1p
- drop-precedence
- dscp
- no

- traffic-class

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration, QoS Profile

qos trust

```
qos trust aruba-device | auto | disable | dot1p | dscp | pass-through
```

Description

Configures QoS trust mode.

Syntax

Parameter	Description
`aruba-device`	In this particular mode, when an Aruba device is connected directly through LLDP (Example: IAP), the operation state of `qos trust` on that interface is set to `auto`.If Aruba device is not detected, then fall back to **pass-through** and preserve DSCP/802.1p markings. Even in case of any connectivity loss or port going down you can change the operation mode to `none` and reset it back when a device is detected.
`auto`	Option for (L2+L3) trust mode prioritizes DSCP over 802.1P. If the received frame is IP, the DSCP value is used for indexing the QoS profile. If the received tagged frame is non-IP, then the 802.1P value is used for indexing the QoS profile.
`disable`	Option to disable QoS trust (reset DSCP/802.1p to 0).
`dot1p`	Option for Layer 2 QoS Trust Mode. Port is configured to trust the IEEE 802.1P user priority. This is relevant for 802.1Q packets. This option does not allow the attachment of a qos-profile while configured on an interface.
`dscp`	Preserves DSCP value and use **qos-profile trusted** queuing mapping. This option does not allow the attachment of a qos-profile that is configured on an interface.
`pass-through`	Option to preserve the incoming DSCP/802.1p values. A **qos-profie <name>** can be attached to the interface to override and remark/queue according to **qos-profile <name>**.
`no qos trust`	All markings will be reset to 0 and creates a QoS untrust. A **qos-profie <name>** can be attached to the interface to remark/queue according to **qos-profile <name>**.

Usage Guidelines

Use the `qos-trust` command in the configuration-interface mode to configure Layer 3 QoS Trust on an interface.

- qos-profile configured is mutually exclusive with dscp, dot1p and auto modes.
- qos-profile configured takes priority in Disable and Passthrough mode.
- qos-profile config is allowed even with aruba-device option. But will take effect only if no aruba-device is detected.

Example

The following example provides a list of QoS trust modes:

```
(host)(gigabitethernet "6/6/6") #
```

```
(svl_techpubs)(gigabitethernet "6/6/6") #qos ?
trust                    QoS trust mode

(Host)(gigabitethernet "6/6/6") #qos trust ?
auto                     Trust DSCP for IP packets; 802.1P for non-IP packets
disable                  Disable QoS trust (reset DSCP/802.1p to 0)
dot1p                    Trust 802.1p
dscp                     Trust DSCP
aruba-device             In this mode, the oper state will be Auto in case neighbor device is
                         Aruba (Eg; IAP) else it will be none
pass-through             Pass-through DSCP/802.1p
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

rcli

```
rcli member <member_id>
```

Description

Remote CLI on a specified member.

Syntax

Parameter	Description
`<member_id>`	Enter the member ID.

Usage Guidelines

This command is only supported on a serial connection.

Example

Execute the following command remotely on a specific member:

```
(host)#  rcli member 1
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

reload

```
reload
   at <hours, minutes, month, date>
   cancel
   in <minutes>
   local <member> [in <minutes>|at <hours, minutes, month, date>]
```

Description

This command performs a reboot or the cold-start of the Mobility Access Switch or a stack member in or at a specific time and/or date.

Syntax

Parameter	Description	Range
`at <hours, minutes, month, date>`	Reloads or cold-starts the switch or stack at a specific time and date that are in the format: <hours, minutes, month, date>.	0–23, 0–60, 1–12, 1–31
`cancel`	Cancels the scheduled reload from the switch.	
`in <minutes>`	Reloads or cold-starts the stack or switch after the specified time.	0–60
`local member in <minutes>`	Reloads or cold-starts a stack member after the specified time.	0–60
`local <member> at <hours, minutes, month, date>`	Reloads or cold-starts a stack member at a specific time and date.	0–23, 0–60, 1–12, 1–31

Usage Guidelines

Use this command to reboot the Mobility Access Switch if required after making configuration changes or under the guidance of Aruba Networks customer support. The **`reload`** command powers down the Mobility Access Switch, making it unavailable for configuration. After the Mobility Access Switch 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 Mobility Access Switch during a reboot, use a local console connection.

After you use the **`reload`** command, the Mobility Access Switch prompts you for confirmation of this action. If you have not saved your configuration, the Mobility Access Switch 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 Mobility Access Switch.

If your configuration has already been saved, the Mobility Access Switch returns the following message:

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

- Enter **y** to reboot the Mobility Access Switch.
- 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 Mobility Access Switch:

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

The Mobility Access Switch returns the following messages:

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

The following command reloads the switch after 60 minutes:

```
(host) #reload in 60
```

The following command reloads the switch at a specific time and date:

```
(host) #reload at 1 50 7 12
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4.1	New options, **reload in** and **reload at**, were introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

rename

```
rename
   usb <oldfilename> <newfilename> [usbpartition <number>]
   member <id> <oldfilename> <newfilename> [usbpartition <number>]
```

Description

This command renames an existing system file.

Syntax

Parameter	Description
`usb`	Enter the USB.
`[usbpartition <number>]`	Enter the usb partition number.
`<oldfilename>`	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.
`member <id>`	Enter the member ID of the stack.
`[usbpartition <number>]`	Enter the usb partition number.
`<oldfilename>`	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 Mobility Access Switch. 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 Mobility Access Switch. If you attempt to rename the active configuration file, the Mobility Access Switch 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 encrypt.

Example

The following command changes the file named **test_configuration** to **deployed_configuration**:

```
(host) (config) #rename usb test_configuration deployed_configuration
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.3	The **usb** and **member <id>** parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

restore

```
restore [factory_default {certificate | stacking}] | [flash]
```

Description

Restores configuration, database (which stores roles, slot numbers, any previous Primary information and/or backup information), and the flash to the factory default.

Syntax

Parameter	Description
`factory_default`	Reverts the database, configuration, or the current default certificate to the factory default configuration.
`certificate`	Reverts the current default certificate to the factory default certificate.
`stacking`	Reverts to the factory default database and configuration.
`flash`	Restores flash directories from the flashbackup.tar.gz file.

Usage Guidelines

This command is used to restore configuration, database (which stores roles, slot numbers, any previous Primary information and/or backup information), and the flash to the factory default. This command is applied locally only; you can not execute this remotely.

This command *clears* the current configuration and stacking interface configuration.

Example

The following example restores the factory default certificate:

```
(host)#restore factory_default certificate
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1	The **stacking** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

rmon alarm

```
rmon alarm <alarm-index>
   alarm-profile <alarm-profile-name>
```

Description

This command creates and associates an alarm profile with the alarm entry.

Syntax

Parameter	Description	Range	Default
`<alarm-index>`	Index of the alarm entry.	1–65535	–
`alarm-profile <alarm-profile-name>`	Applies RMON alarm profile to an alarm entry.	—	–
`clone`	Copy data from another alarm profile.	—	—
`monitor`	Configures an OID to monitor.	—	—
`no`	Delete command.	—	—
`owner`	Configures the owner of this alarm entry.	—	config

Usage Guidelines

Associate `alarm-profile` with the `alarm-entry`. Please note that the `monitor-entity` must be set to valid OID before applying the alarm-profile.

Example

The following example creates and associates an `alarm-profile` with the `alarm-entry`:

```
(host) (config) #rmon alarm 1
   (alarm "1") #alarm-profile my_profile
   (alarm "1") #monitor gigabitethernet 0/0/2 oid-type in-errors-pkts
   (alarm "1") #owner aruba_1

(host) (config) #rmon alarm 2
   (alarm "2") #alarm-profile my_profile
   (alarm "2") #monitor ifInErrors.3
   (alarm "2") #owner aruba_2

(host) (config) #rmon alarm 3
   (host) (alarm "3") #alarm-profile my_profile
   (host) (alarm "3") #monitor port-channel 0 oid-type out-bcast-pkts
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

rmon alarm-profile

```
rmon alarm-profile <profile-name>
   clone <source>
   falling-event <event-index>
   falling-threshold-value <value>
   interval<interval>
   no..
   rising-event <event-index>
   rising-threshold-value <value>
   sample-type <absolute|delta>
   startup-alarm {falling|rising|rising-or-falling}
```

Description

This command creates an alarm profile to apply to alarm entry.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Enter the name of the alarm profile.	—	—
`clone <source>`	Copy data from another alarm profile.	—	—
`falling-event <event-index>`	Associate an event index or profile to the falling event.	—	—
`falling-threshold-value <value>`	Specifies the value at which the event is generated.	—	0
`interval <interval>`	Configures sampling period (in seconds) of the monitored variable.	—	10
`no`	Removes the specified configuration parameter.	—	—
`rising-event <event-index>`	Associate an event profile or index to the rising event.	—	—

Parameter	Description	Range	Default
`rising-threshold-value <value>`	Specifies the value at which the event is generated.	—	0
`sample-type <absolute|delta>`	Specifies whether the sample type is either delta or absolute. • When the sample-type is delta, the value of the selected variable at the last sample will be subtracted from the current value, and the difference is compared with the thresholds. • When the sample-type is absolute, the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval.	—	delta
`Initial-alarm <falling| rising| rising-or-falling`	Configures initial alarm (rising, falling, or either).	—	rising-or-falling

Usage Guidelines

To configure the alarm variable, first you have to create an alarm profile.

Examples

The following example creates an alarm-profile:

```
(host) (config) #rmon alarm-profile my_profile
(alarm profile "my_profile") #rising-event 1
   falling-event 2
   rising-threshold-value 2000
   falling-threshold-value 100
   startup-alarm rising
   sample-type absolute
   interval 10
```

The following example displays the details on the alarm-profile created:

```
(host) #show rmon-config alarm-profile my_profile

alarm profile "my_profile"
--------------------------
Parameter                                              Value
---------                                              -----
Interval at which samples need to be taken             10
Alarm sample type                                      absolute
Rising threshold against which to compare the value    2000
Falling threshold against which to compare the value   100
Rising event index                                     1
Falling event index                                    2
Initial alarm (rising, falling, or either)             rising
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

rmon etherstat

```
rmon etherstat <etherstat-index>{clone|monitor|owner}
```

Description

This command configures ethernet statistics collection on an interface.

Syntax

Parameter	Description	Range	Default
`<etherstat-index>`	Enter the index of the etherstat entry.	1–65535	—
`clone`	Copy data from another Etherstat index.	—	—
`monitor`	Configures an OID to monitor.	—	—
`no`	Delete command.	—	—
`owner`	Configure owner of an etherstat entry	—	config

Usage Guidelines

You have to first create an `etherstat-profile` with `profile-name` as etherstat index. Then associate the SNMP OID to monitor.

Example

The following rmon etherstat entries monitor the same OID:

```
(host) (config) #rmon etherstat 1
(host) (Etherstat index "1") #monitor gigabitethernet 0/0/3
(host) (config) #rmon etherstat 2
(host) (Etherstat index "2") #monitor ifIndex.4

(host) (config) #rmon etherstat 3
(host) (Etherstat index "3") #monitor port-channel 0
(host) (config) #rmon etherstat 4
(host) (Etherstat index "4") #monitor ifIndex.1441
```

The following example shows the SNMP ifIndex of a particular interface:

```
(host) #show interface port-channel 0
port-channel 0 is administratively Up, Link is Up, Line protocol is Up
Hardware is Port-Channel, Address is 00:0b:86:6b:51:c0
Description: Link Aggregate
Member port(s):
    GE0/0/1 is administratively Up, Link is Up, Line protocol is Up
Speed: 1 Gbps
Interface index: 1441
MTU 1514 bytes
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

rmon event

```
rmon event <event-index>{type|description|owner}
```

Description

This command configures an event entry.

Syntax

Parameter	Description	Range	Default
`<event-index>`	Index of the event entry.	1–65535	—
`type`	Specifies whether to send SNMPtrap or create log entry when the event occurs. • When type is log or log-and-trap, an RMON log entry is created when the event is triggered and sets the eventType in the RMON MIB to log or log-and-trap. • When type is trap or log-and-trap, SNMP trap is generated. • When type is none, no action is taken for this event.	—	—
`description`	Configures description of the event.	—	—
`owner`	Configures owner of the event.	—	config

Usage Guideline

Event-profile is used to specify the action to take when an alarm triggers an event.

Example

The following example configures an event entry:

```
(host) (config) #rmon event  1
(Event index "1") #description low_mcast
    (Event index "1") #owner Administrator
    (Event index "1") #type trap
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

rmon history

```
rmon history <history-index>{monitor|samples|sampling-interval|owner}
   no..
```

Description

This command enables the RMON history group of statistics on an interface.

Syntax

Parameter	Description	Range	Default
`<history-index>`	Specifies the index of the history entry.	1–65535	—
`monitor`	Configures the OID to monitor.	—	—
`samples`	Specifies the number of samples to sample the data.	1–65535	50
`sampling-interval`	Specifies the interval of each sample.	1–3600	1800
`owner`	Configures owner of the history group.	—	config
`no`	Deletes the configuration.		

Usage Guidelines

First create `history-profile` with `profile-name` as history index which is equivalent to `historyControlIndex` in `history ControlTable` of RMON MIB. Then associate the SNMP OID to monitor. If the interval is changed later then the older history will be lost and a new history collection will be created with the same history index.

The memory usage on the Mobility Access Switch will increase with the increase in the number of history samples and/or etherstat entries. The network administrator has to make sure that the configured samples or entries do not end up consuming all the available free memory.

Example

The following example enables the RMON history group of statistics on an interface.

```
(host) (config) #rmon history 1
(host) (History index "1") #monitor gigabitethernet 0/0/3
   (History index "1") #samples 10
   (History index "1") #sampling-interval 8
   (History index "1") #owner Administrator

(host) (config) #rmon history 2
(host) (History index "2") #monitor ifIndex.4
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

rogue-ap-containment

```
rogue-ap-containment
   action {default [auto-recovery-time <recovery_timeout>] | log}
   enable
   no
```

Description

Configure the rogue AP containment actions.

Syntax

Parameter	Description
`action`	Set one of the following containment actions: • default • log
`default`	If the MAC address is detected on a trunk port or on an untrusted access port, it is blacklisted and a message is logged into the syslog. If detected on a trusted access port, the port and the PoE are shutdown.
`auto-recovery-time <recovery_timeout>`	You can optionally configure the auto recovery time for the port in seconds. Default value is 300 seconds and the allowed range is 0-65535 seconds.
`log`	Discards the MAC address and logs it as blacklisted address.
`enable`	Enables rogue AP containment. This is enabled by default.
`no`	Delete command.

Usage Guidelines

Use this command to enable or disable rogue AP containment and configure the action to be taken on the list of MAC addresses received from IAP.

Example

The following sample enables rogue AP containment and sets the default action with an auto recovery time of 50 seconds:

```
(host) (rogue-ap-containment) #enable
(host) (rogue-ap-containment) #action default auto-recovery-time 50
```

Related Command

Command	Description
show rogue-ap-containment	View the rogue AP containment configuration.

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

router ospf

```
router ospf
   area <areaid> [stub [no-summary]] | [nssa [default-info-originate metric <cost> metric-type
   <mtype> [translate-always]] | [no-summary] | [translate-always]]
   area-range
   default-info-originate [always [metric <cost> metric-type <mtype>]] | [metric <cost>
   metric-type <mtype> [always]]
   disable
   disable-compatible-rfc1583
   distribute-list <distribute-list>
   no {...}re
   redistribute vlan {<vlan-ids> | add <vlan-ids> | remove <vlan-ids>}
   router-id <A.B.C.D>
   summary-address
```

Description

Configure the OSPF global profile.

Syntax

Parameter	Description	Range	Default
`area <areaid>`	Configures the area.	0–4294967295	0.0.0.0
`[stub [no-summary]] | [nssa [default-info-originate metric <cost> metric-type <mtype> [translate-always]] | [no-summary] | [translate-always]]`	Optionally, enter the following parameters to define an area type: • **stub** — Set an area as a stubby area • **no-summary** — set an area as a Totally Stubby Area (TSA) • **nssa** — Set an area as a Not So Stubby Area (NSSA) • **default-info-originate** — Send default Link State Advertisement (LSA) in NSSA • **metric** — Metric cost for the default route • **metric-type** — Set the metric type (N1 or N2 for NSSA) for the destination routing protocol • **translate-always** — Configures an NSSA Area Border Router (ABR) as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs.	**<cost>** — 1–65535 **<mtype>** — 1–2	**<mtype>** — 2

Parameter	Description	Range	Default
`area-range <ip> <netmask> <area-id>`	Configures the inter-area route summarization to consolidate and summarize the routes at the boundary	—	—
`default-info-originate [always [metric <cost> metric-type <mtype>]] | [metric <cost> metric-type <mtype> [always]]`	• **default-info-originate** — Generate default LSA • **always** — Generate default LSA when there is no default route • **metric** — Metric cost of the default route • **metric-type** — Set the metric type (E1 or E2) for the destination routing protocol	**<cost>** — 1–65535 **<mtype>** — 1–2	**<mtype>** — 2
`disable`	Enter the keyword **disable** to disable (or **no disable** to enable) an OSPF instance.	—	Enabled
`disable-compatible-rfc1583`	Disable RFC 1583 compatibility. Use the no parameter to enable this command.	—	Enabled
`distribute-list <distribute-list>`	Use this command to filter networks received in updates. **NOTE:** Before configuring distribute-list, ip-profile must be configured on the switch.	—	—
`redistribute vlan <vlan-ids>`	Enter the keywords **redistribute vlan** followed by the VLAN identification to redistribute the VLAN subnet.	—	—
`add <vlan-ids>`	Enter the keyword **add** followed by the VLAN identification to add the specified VLANs to the current list.	—	—
`remove <vlan-ids>`	Enter the keyword **remove** followed by the VLAN identification to remove the specified VLANs from the current list.	—	—
`router-id <router-id>`	Enter the keyword **router-id** followed by the router identification number (in dotted decimal format A.B.C.D) to configure the specified router.	—	—
`summary-address <ip> <netmask>`	Configures external route summarization.	—	—

Usage Guidelines

Configure the OSPF global commands.

Examples

Executing this command changes the mode as shown below:

```
(host) (config) #router ospf
(host) (Global OSPF profile) #area 1
```

Following example adds VLAN 2 to the redistribute subnet's current list.

```
(host) (Global OSPF profile) #redistribute vlan add 2
```

Following example creates an NSSA area which adds a default route to the NSSA area and configures an NSSA Area Border Router (ABR) as a forced NSSA LSA translator. The NSSA ABR router unconditionally translates Type-7 LSAs to Type-5 LSAs.

```
(host) (Global OSPF profile) #area 0.0.0.1 nssa default-info-originate metric 1 metric-type 1
translate-always
```

Before configuring distribute-list, prefix-list must be configured on the switch. To configure prefix-list, see ip-profile. Following example configures distribute-list with aruba prefix-list name.

```
(host) (Global OSPF profile) #distribute-list aruba
```

Related Commands

Command	Description
interface-profile ospf-profile	Configures an OSPF interface profile.
ip-profile	This command is used to configure IP prefix filtering. Prefix lists are used to either permit or deny the configured prefix based on the matching condition.

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.
ArubaOS 7.2	The following new parameters were introduced: • **stub no-summary** • **nssa** • **default-info-originate** • **disable-compatible-rfc1583** • **distribute-list**
ArubaOS 7.3.1	The following parameters were introduced: • **area-range** • **summary-address**

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

router pim

```
router pim
<rp-address> <group-range> <grpmask>
ssm
```

Description

Use this command to configure global PIM profile.

Syntax

Parameter	Description
`rp-address <rp-address>`	Configures IP address of RP.
`group range <group-range>`	Configures group range serviced by this RP.
`grpmask <grpmask>`	Configures group address mask.
`ssm`	Enables PIM-SSM protocol.
`no`	Delete command.

Example

```
(host)(Global PIM profile) #rp-address 1.1.1.1 group-range 1.1.1.1 1.1.1.1
```

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.
ArubaOS 7.3.1	The **ssm** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

run diagnostic interface gigabitethernet

```
run diagnostics interface gigabitethernet
   <slot/module/port> cable
```

Description

Run a Time-Domain Reflectometer (TDR) diagnostic test on a specific gigabitethernet interface. TDR is a measurement technique used to characterize and locate faults in metallic cables such as twisted pair. TDR transmits a short rise electric pulse across the conducting cable and if the cable is properly terminated, the entire electric pulse is absorbed on the other end. If any faults exist in the cable, some of the incident signal is sent back towards the source. TDR also:

- Locates the position of faults within meters
- Detects and reports open circuits, short circuits, and impedance mismatches in a cable
- Detects pair swap (straight/crossover) on each pair of cable in twisted pair cable
- Detects pair polarity (positive/negative) on each channel pairs in a cable

TDR is not supported over management interfaces, Direct Attach Cables (DAC) or Fiber interfaces.

Syntax

Parameter	Description
`<slot/module/port> cable`	Specifies the cable on which the TDR diagnostic will be executed.

Usage Guidelines

Use this command to execute a TDR diagnostic test on a specific gigabitethernet interface.

Example

`run diagnostics interface gigabitethernet <slot/module/port> cable`

Related Command

Command	Description
show diagnostics interface gigabitethernet	Display the results of the TDR diagnostic test.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

service rmon

```
service rmon
```

Description

This command enables rmon service on the Mobility Access Switch.

Syntax

No parameters.

Usage Guidelines

By default, `service rmon` is disabled. When the `service rmon` command is disabled, the rmon data is not populated in the CLI display command but all the other configurations can be performed. When the `service rmon` command is enabled, all the configurations that are performed earlier would be applied.

Example

The following command enables rmon service on the Mobility Access Switch:

```
(host)(config)# service rmon
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

set interface local-mgmt

```
set interface local-mgmt [ip-address <address> netmask <mask> gateway <gw> member <id>] | [no-shut] | [shut]
```

Description

Set the local management interface or administratively bring an interface up or down.

Syntax

Parameter	Description
`ip-address <address>`	Enter the keyword **ip-address** followed by the IP address of the local management interface in A.B.C.D. format.
`netmask <mask>`	Enter the keyword **netmask** followed by the netmask address in A.B.C.D. format.
`gateway <gw>`	Enter the keyword **gateway** followed by the gateway address in A.B.C.D. format to set the gateway for the local management access.
`member <id>`	Enter the keyword **member** followed by a member's ID number.
`no shut`	Enter the keywords **no shut** to change the admin state of the management interface to UP.
`shut`	Enter the keyword **shut** to change the admin state of the management interface to DOWN.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

set stacking activate

```
set stacking activate
```

Description

Activate an ArubaStack.

Usage Guidelines

This command activates the ArubaStack and runs the distributed election algorithm on all local ArubaStack members. Only currently connected members are considered in the election algorithm. Any previous ArubaStack members, which are no longer connected, are “forgotten” by the current members of the ArubaStack.

This command can not be executed remotely.

Example

Activate the ArubaStack as follows:

```
(host)# set stacking activate
(host)#
```

If you execute this command on an ArubaStack that is already activated, a message notifying you of the ArubaStack’s status is returned as follows:

```
(host)# set stacking activate
Stack already active
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

set stacking interface stack

```
set stacking interface stack <module/port> [member <id> | all] | [shut | no-shut]
```

Description

Administratively bring an ArubaStack port up or down.

Syntax

Parameter	Description
`<module/port>`	Enter the stacking interface details in module/port format.
`member <id>`	Enter the keyword **member** followed by a member's ID number.
`all`	Enter the keyword **all** to set all member information in the ArubaStack.
`no-shut`	Enter the keywords **no-shut** to change the administrative state of the stacking interface to UP.
`shut`	Enter the keyword **shut** to change the administrative state of the stacking interface to DOWN. **NOTE:** The shut option is available on local members only.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

set stacking renumber

```
set stacking renumber <id> <new-id>
```

Description

Renumber a member's slot number to a new slot number. You cannot renumber a primary and a secondary stack member.

Syntax

Parameter	Description
`<id>`	Existing slot number.
`<new-id>`	New slot number.

Usage Guidelines

Starting from ArubaOS 7.4.1.1, the set stacking renumber command in the Mobility Access Switch is modified to allow a user renumber any stack member except the primary and secondary stack members. The Mobility Access Switch displays the following error message if a user tries to renumber the primary and secondary stack members:

```
ERROR: Renumber involving Primary or Backup member-id is not allowed
```

Example

Execute the following command to renumber a stack member from stack ID 1 to stack ID 4:

```
(host) #set stacking renumber 1 4
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.4.1.1	This command was modified to allow renumbering any stack member except the primary and the secondary stack members.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

set stacking swap

```
set stacking swap <id1> <id2>
```

Description

Swap two members existing slot numbers.

Syntax

Parameter	Description
`<id1>`	Member ID number.
`<id2>`	Second Member ID number.

Usage Guidelines

This command can only be used on linecard members; you can *not* swap Primary or Secondary member's slot numbers.

Example

The command below swaps slot numbers.

```
(host)#set stacking swap id2 id0
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

set traceflags

```
set traceflags
   dpa
   dpe
   dpa-sos
```

Description

Use this command for setting trace flags for various packet forwarding functions.

Syntax

Parameter	Description
`dpa`	Set logs for the following hardware packet forwarding functions: • ace—Set debug of ACE operations • acl—Set debug of ACL operations • all—Set debug of all supported operations • auth—Set debug of AUTH operations • bss—Set debug of BSS operations • crypto-key—Set debug of CRYPTO-KEY operations • fdb—Set debug of FDB operations • ipsecsa—Set debug of IPSECSA operations • l3mcrt— Set debug of L3 MULTICAST ROUTE operations • lif—Set debug of LIF operations • mc2rt—Set debug of MC2RT operations • mcrt—Set debug of MCRT operations • mcrt-sta—Set debug of MCRT-STA operations • msti-state—Set debug of MSTI-STATE indications • mstp-entry—Set debug of MSTP-ENTRY operations • nat—Set debug of NAT operations • nh— Set debug of Next Hop operations • pif—Set debug of PIF operations • qos—Set debug of QOS operations • role—Set debug of role operations • route—Set debug of ROUTE operations • sapm-ap-info—Set debug of SAPM-AP-INFO operations • ssm-ind—Set debug of SSM indications • station—Set debug of STATION operations • user—Set debug of USER operations • user-key—Set debug of USER-KEY operations • vassign—Set debug of VASSIGN operations • vlan—Set debug of VLAN operations

Parameter	Description
`dpe`	Set logs for the following packet forwarding functions in the hardware engine: • all— Set debug of all supported operations • devrt— Set debug of DEVRT operations • efltr— Set debug of EFLTR operations • fdb— Set debug of FDB operations • fdb-age— Set debug of FDB AGE operations • fdb-intr— Set debug of FDB DMA operations • l3mcrt— Set debug of L3 MULTICAST ROUTE operations • pcl—Set debug of PCL operations • policer—Set debug of POLICER operations • port—Set debug of PORT operations • qos—Set debug of QOS operations • route—Set debug of L3 ROUTE operations • sysinfo—Set debug of SYSINFO operations • user—Set debug of USER operations • vassign—Set debug of VASSIGN operations • vidx—Set debug of VIDX operations • vlan—Set debug of VLAN operations
`dpa-sos`	Set logs for the following software packet forwarding functions: • ace—Set debug of ACE operations • acl—Set debug of ACL operations • all—Set debug of all supported operations • auth—Set debug of AUTH operations • contract—Set debug of CONTRACT operations • fdb—Set debug of FDB operations • lif—Set debug of LIF operations • mcrt —Set debug of MCRT operations • mcrt-sta—Set debug of MCRT-STA operations • nat-pool—Set debug of NAT-POOL operations • nh—Set debug of Next Hop operations • nodeinfo—Set debug of NODEINFO operations • route —Set debug of ROUTE operations • service—Set debug of SERVICE operations • station —Set debug of STATION operations • user —Set debug of USER operations • user-key—Set debug of USER-KEY operations • vlan —Set debug of VLAN operations • vlif —Set debug of VLIF operations

Usage Guidelines

This command can be used for troubleshooting packet forwarding functions in the software and hardware using the log files.

Example

You can use the following commands for troubleshooting NAT operations using DPA logs:

```
(host) #set traceflags dpa nat
```

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show aaa authentication all

```
show aaa authentication all
```

Description

Show authentication statistics for your switch, 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 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 switch, 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 switch using TACACS+ and RADIUS authentication methods.

```
(host) #show aaa authentication all

Auth Method Statistics
----------------------
Method  Success  Failures
------  -------  --------

tacacs 12 2Radius 9 1
```

Related Commands

Command	Description
aaa authentication dot1x	Use this command to enter the aaa authentication dot1x profile mode.
aaa authentication mac	Use this command to enter the aaa authentication mac profile mode.
aaa authentication mgmt	Use this command to enter the aaa authentication mgmt profile mode.
aaa authentication wired	Use this command to enter the aaa authentication wired profile mode.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa authentication captive-portal

```
show aaa authentication captive-portal [<profile-name> | customization]
```

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.
`customization`	Displays captive portal customization information.

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.

The following example displays if a captive portal profile is customized:

```
(host) #show aaa authentication captive-portal

Captive Portal Authentication Profile List
------------------------------------------
Name            References  Profile Status
----            ----------  --------------
c-portal        2
remoteuser                                                    1
portal1                                                       1


Total: 4
(host) #show aaa authentication captive-portal customization

Captive-Portal Customization
----------------------------
Profile   Customized
-------   ----------
cp1       Yes
default No
```

The **Profile** column lists the number of captive portal profiles and the **Customized** column indicates whether a captive portal profile is customized or not.

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 *c-portal*.

```
(host) #show aaa authentication captive-portal c-portal

Captive Portal Authentication Profile "c-portal"
------------------------------------------------
Parameter                                       Value
---------                                       -----
Default Role                                    guest
Default Guest 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
Login page                                      /auth/index.html
Welcome page                                    /auth/welcome.html
Show Welcome Page                               Yes
Add switch IP address in the redirection URL    Disabled
Adding user vlan in redirection URL             Disabled
Add a controller interface in the redirection URL  N/A
Allow only one active user session              Disabled

White List
```

The output of this command includes the following parameters:

Parameter	Description
`Default Role`	Role assigned to the captive portal user upon login.
`Default Guest Role`	Guest 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.

Parameter	Description
`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.
`Logon wait minimum wait`	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 maximum wait`	Maximum 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.
`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.
`Add switch IP interface in the redirection URL`	Shows the IP address of a Mobility Access Switch's interface added to the redirection URL, if enabled.
`Adding user vlan in redirection URL`	VLAN ID of the user in the redirection URL when external captive portal servers are used.
`Allow only one active user session`	If enabled, only one active user session is allowed at any time. This feature is disabled by default.

Parameter	Description
`Add a controller interface in the redirection URL`	IP address of one of the interface in the redirection URL when external captive portal servers are used.
`White List`	Shows the configured white list on an IPv4 or IPv6 network destination. The white list contains authenticated websites that a guest can access.
`Show the acceptable use policy page`	If enabled, the captive portal page will show the acceptable use policy page before the user logon page. This feature is disabled by default.

Related Commands

Command	Description
`aaa authentication captive-portal`	Use aaa authentication captive-portal to configure the parameters displayed in the output of this show command.

Command History

Release	Modification
Aruba 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode (config)

show aaa authentication dot1x

```
show aaa authentication dot1x <profile-name>
```

Description

This command shows information for 802.1X authentication profiles.

Parameter	Description
<profile-name>	The name of an existing 802.1X authentication profile.

Usage Guidelines

Issue this command without the **<profile-name>** option 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.

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
dot1x         5
dot1xtest                       0

Total:3
```

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 default

802.1X Authentication Profile "default"
---------------------------------------
Parameter                                                  Value
---------                                                  -----
Max authentication failures                                0
Enforce Machine Authentication                             Disabled
Machine Authentication: Default Machine Role               guest
Machine Authentication Cache Timeout                       24 hr(s)
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
Authentication Server Retry Interval                       30 sec
Authentication Server Retry Count                          2
```

```
Framed MTU                                                          1100 bytes
Number of times ID-Requests are retried                             3
Maximum Number of Reauthentication Attempts                         3
Maximum number of times Held State can be bypassed                  0
Reauthentication                                                    Disabled
Termination                                                         Disabled
Termination EAP-Type                                                N/A
Termination Inner EAP-Type                                          N/A
Enforce Suite-B 128 bit or more security level Authentication       Disabled
Enforce Suite-B 192 bit security level Authentication               Disabled
Token Caching                                                       Disabled
Token Caching Period                                                24 hr(s)
CA-Certificate                                                      N/A
Server-Certificate                                                  N/A
TLS Guest Access                                                    Disabled
TLS Guest Role                                                      guest
Ignore EAPOL-START after authentication                             Disabled
Handle EAPOL-Logoff                                                 Disabled
Ignore EAP ID during negotiation.                                   Disabled
...
```

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

Parameter	Value
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.
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.
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 switch to not respond to authentication requests from a client while the switch is in a held state after the authentication failure.
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.)
Termination	Shows if 802.1X termination is enabled or disabled on the switch.
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.
Enforce Suite-B 128 bit or more security level Authentication	Shows if Suite-B 128 bit or more security level authentication enforcement is enabled or disabled.
Enforce Suite-B 192 bit security level Authentication	Shows if Suite-B 192 bit or more security level authentication enforcement is enabled or disabled.

Parameter	Value
Token Caching	If this feature enabled (and EAP-GTC is configured as the inner EAP method), token caching allows the switch 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 switch.
Server-Certificate	Name of the Server certificate used by the switch to authenticate itself to the client.
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 switch 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 switch will Ignore EAP IDs during negotiation.

Related Command

Command	Description
aaa authentication dot1x	Use this command to enter the aaa authentication dot1x profile mode.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa authentication mac

```
show aaa authentication mac [<profile-name>]
```

Description

This command shows information for MAC authentication profiles.

Syntax

Parameter	Description
<profile-name>	The name of an existing MAC authentication profile.

Usage Guidelines

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.

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 upperMax Authentication failures 3
```

Related Command

Command	Description
aaa authentication mac	Use this command to enter the aaa authentication mac profile mode.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

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 switch.

```
(host) #show aaa authentication mgmt
Management Authentication Profile
---------------------------------
Parameter     Value
---------     -----
Default Role  root
Server Group  Servgroup1
Enable        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 switch uses for authentication management. • **root**, the super user role (default). • **network-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.
`Enable`	The **Enable** parameter indicates whether or not management authentication is enabled or disabled.

Related Command

Command	Description
`aaa authentication mgmt`	Use this command to enter the aaa authentication mgmt profile mode.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa authentication-server all

```
show aaa authentication-server all
```

Description

View authentication server settings for both external authentication servers and the internal switch 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.

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.
`FQDN`	The Fully-Qualified Domain Name of the server, if configured.
`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 and clear 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.

Related Commands

Command	Description
`aaa authentication-server radius`	This command configures a RADIUS server.
`aaa authentication-server tacacs`	This command configures a TACACS server.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa authentication-server internal

```
show aaa authentication-server internal [statistics]
```

Description

View authentication server settings for the internal switch database.

Example

The output of the command below shows that the internal authentication server has been 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.
`Status`	Shows if the server is enabled of disabled

Include the **statistics** parameter to display additional details for the internal server.

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.
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 switch timed out an authentication request.

Parameter	Description
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 Command

Command	Description
aaa server-group	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.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

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.

Include the **<ldap_server_name>** parameter to display additional details for an individual server.

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.
`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: (objectclass=*).
`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

Related Command

Command	Description
aaa authentication-server ldap	This command configures an LDAP server.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

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.

Example

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.

Include the **<rad_server_name>** parameter to display additional details for an individual server.

The output of this command includes the following parameters:

Parameter	Description
`host`	IP address of the RADIUS server
`Key`	Shared secret between the switch and the authentication server.
`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 switch before the server is marked as down.
`Timeout`	Maximum time, in seconds, that the switch 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.
`Source Interface`	The source interface VLAN ID number.
`Use MD5`	If enabled, the RADIUS server will use a MD5 hash of the cleartext password.
`Mode`	Shows whether this server is **Enabled** or **Disabled**.

Related Command

Command	Description
aaa authentication-server radius	This command configures a RADIUS server.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

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.

Example

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.

Include the **<tacacs_server_name>** parameter to display additional details for an individual server.

The output of this command includes the following parameters:

Parameter	Description
`host`	IP address of the TACACS+ server
`Key`	Shared secret between the switch and the authentication server.
`TCP Port`	TCP port used by the server.
`Retransmits`	Maximum number of retries sent to the server by the switch before the server is marked as down.
`Timeout`	Maximum time, in seconds, that the switch waits before timing out the request and resending it.
`Mode`	Shows whether this server is **Enabled** or **Disabled**.

Related Command

Command	Description
`aaa authentication-server tacacs`	This command configures a TACACS server.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

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.

Include the **<windows_server_name>** parameter to display additional details for an individual server.

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa authentication wired

Description

View wired authentication settings for a client device that is directly connected to a port on the switch.

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 switch is a profile named “secure_profile_3.”

```
(host) #show aaa authentication wired
Wired Authentication Profile
----------------------------
Parameter    Value
---------    -----
AAA Profile  Secure_profile_3
```

Related Command

Command	Description
aaa authentication wired	Use this command to enter the aaa authentication wired profile mode.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa deny-inter-user-traffic roles

```
show aaa deny-inter-user-traffic roles
```

Description

View the list of user roles on which deny inter-user traffic is enabled:

Example

The following command displays the list of user roles on which deny inter-user traffic is enabled:

```
(host) #show aaa deny-inter-user-traffic roles
  Maximum number of user roles supported: 7
  Enabled on user roles:
  ----------------------
  Role3
  guest
```

Related Command

Command	Description
user-role	Using this command , you can create a user-role and enable deny-inter-user traffic for that role.

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa derivation-rules

```
show aaa derivation-rules [server-group <group-name>|user <name>]
```

Description

Show derivation rules based on user information or configured for server groups.

Syntax

Parameter	Description
`server-group <group-name>`	Name of a server group
`user <name>`	Name of a user rule group

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
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 switch 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) (config) #show aaa derivation-rules user user44

User Rule Table
---------------
Priority  Attribute Operation  Operand            Action    Value
--------  --------- ---------  -------            ------    -----
1         macaddr    equals     00:25:90:06:96:42 set role  authenticated

Total Hits  New Hits  Description
----------  --------  -----------
56           18
```

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.
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 switch 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 Command

Command	Description
aaa authentication-server windows (deprecated)	This command configures rules which assigns an AAA profile, role or VLAN to a client based upon the client's association with an AP.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

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).

Usage Guidelines

If you define a RADIUS server using the FQDN of the server rather than its IP address, the switch will periodically generate a DNS request and cache the IP address returned in the DNS response. Issue this command to view the IP addresses that currently correlate to each RADIUS server FQDN.

Example

The output of this command shows the IP addresses for two RADIUS servers.

Related Command

Command	Description
aaa authentication-server radius	This command configures a RADIUS server.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa password-policy mgmt

```
show aaa password-policy mgmt [statistics]
```

Description

Show the current password policy for management users.

Parameter	Description
`statistics`	Include this optional parameter to show the numbers of failed login attempts and any lockout periods for management user accounts.

Example

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.

Parameter	Description
`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.
`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 switch 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 switch 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 switch 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
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa profile

```
show aaa profile [<profile-name>]
```

Description

Show a list of all AAA profiles, or configuration details for a single AAA profile.

Syntax

Parameter	Description
<profile-name>	Name of an AAA profile.

Usage Guidelines

Issue this command without the <profile-name> option to display the entire AAA profile list, including profile status and the number of references to each profile. Include a profile name to display detailed AAA configuration information for that profile.

Example

Below is an output of the AAA profile named “default.”

```
(host) #show aaa profile default

AAA Profile "default"
---------------------
Parameter                              Value
---------                              -----
Initial role                           logon
MAC Authentication Profile             N/A
MAC Authentication Default Role        guest
MAC Authentication Server Group        default
802.1X Authentication Profile          N/A
802.1X Authentication Default Role     guest
802.1X Authentication Server Group     N/A
Download Role from ClearPass           Enabled
L2 Authentication Fail Through         Enabled
RADIUS Accounting Server Group         N/A
RADIUS Interim Accounting              Disabled
XML API server                         N/A
AAA unreachable role                   N/A
RFC 3576 server                        N/A
User derivation rules                  N/A
SIP authentication role                N/A
Enforce DHCP                           Disabled
Authentication Failure Blacklist Time  3600 sec
```

Related Command

Command	Description
aaa profile	Use this command to enter the AAA profile mode.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1.1	Output parameters were corrected.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa radius-attributes

```
show aaa radius-attributes
```

Description

Show RADIUS attributes recognized by the switch.

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
Revoke-Text                     316    String
WISPr-Session-Term-End-Of-Day   10     Integer  WISPr      14122
WISPr-Redirection-URL           4      String   WISPr      14122
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
WISPr-Bandwidth-Min-Down        6      Integer  WISPr      14122
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
DB-Entry-State                  318    String
Acct-Tunnel-Packets-Lost        86     Integer
Tunnel-Connection-Id            68     String
Session-Timeout                 27     Integer
...
MS-CHAP-LM-Enc-PW               5      String   Microsoft  311
   ...
```

Related Command

Command	Description
aaa authentication-server radius	This command configures a RADIUS server.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

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 switch with no current users.

```
(host) #show aaa state configuration

Authentication State
--------------------
Name                            Value
----                            -----
Switch IP                       10.6.2.253
Current/Max/Total IPv4 Users    0/6/14
Current/Max/Total User Entries  0/4/15
Current/Max/Total Stations      121/190/367550
Configured user roles            21
Configured destinations         32
Configured services              77
Configured Auth servers         9
Auth server in service          9

Successful authentications
--------------------------
Web  MAC  VPN RadAcct Management
---  ---  ---  ------ ----------
138  0    0    10117   0

Failed authentications
----------------------
Web  MAC  VPN RadAcct Management
---  ---  ---  ------ ----------
48   0    0    0      0    0

Idled users              = 3366
fast age                 = Disabled
```

The output of the `show aaa state configuration` command includes the following parameters:

Parameter	Description
`Switch IP`	IP address of the switch.
`Current/Max/Total IPv4 Users`	Current number of IPv4 users on the switch/Maximum number of IPv4 users that can be assigned to the switch at any time/Total number of IPv4 users that have been assigned to the switch since the last switch reboot.
`Current/Max/Total User Entries`	Current number of users on the switch/Maximum number of users that can be assigned to the switch at any time/Total number of users that have been assigned to the switch since the last switch reboot.
`Current/Max/Total Stations`	Current number of stations registered with the switch/Maximum number of stations that can be registered with the switch at any time/Total number of stations that have registered the switch since the last switch reboot.
`Configured user roles`	Number of configured user roles.
`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.
`Idled users`	Total number of users that are not broadcasting data to an AP.
`fast age`	When the **fast age** feature allows the switch 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.

Related Command

Command	Description
`show aaa authentication all`	Show authentication statistics for your switch, including authentication methods, successes and failures.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa state debug-statistics

```
show aaa state debug-statistics
```

Description

Show debug statistics for switch authentication, authorization and accounting.

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
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 control path.
8021q	Number of 802.1q (VLAN tag) packets sent between the datapath and the control path.
non-ip	Number of non-ip type packets sent between the datapath and the control path.
zero-ip	Number packets sent without an internet protocol (IP).
loopback	If **1**, the switch 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 control path, 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.

Parameter	Description
`idled users due to MAC mismatch`	For internal use only.
`Logon lifetime iteration`	Number of users deleted for lack of activity.
`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 control path and the datapath.

Related Command

Command	Description
`show aaa authentication all`	Show authentication statistics for your switch, including authentication methods, successes and failures.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa state messages

```
show aaa state messages
```

Description

Display numbers of authentication messages sent and received.

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
```

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 switch 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 switch 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 switch was last reset.

Related Command

Command	Description
`show aaa authentication all`	Show authentication statistics for your switch, including authentication methods, successes and failures.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa state station

```
show aaa state
how aaa state station <A:B:C:D:E:F>
```

Description

Display AAA statistics for a station.

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
```

Related Command

Command	Description
show aaa authentication all	Show authentication statistics for your switch, including authentication methods, successes and failures.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa state user

```
show aaa state user <ip-addr>
```

Description

Display statistics for an authenticated user.

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

Example

The following example 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 2011)
```

Related Command

Command	Description
show aaa authentication all	Show authentication methods, successes and failures.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa tacacs-accounting

```
show aaa tacacs-accounting
```

Description

Show TACACS accounting configuration.

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
Commands        all

Server-Group servgroup1
```

The output of this command includes the following parameters:

Parameter	Description
`Mode`	Shows if the TACACS accounting feature is enabled or disable
`Commands`	The server group that contains the active TACACS server. The output of this parameter can be any of the following: • **action** : Reports action commands only. • **all** : Reports all commands. • **configuration:** Reports configuration commands only • **show:** Reports show commands only
`Server-Group`	The server group that contains the active TACACS server.

Related Command

Command	Description
`aaa tacacs-accounting server-group`	This command configures reporting of commands issued on the switch to a TACACS+ server group.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa timers

```
show aaa timers
```

Description

Show AAA timer values.

Example

The example below shows that the switch has all default timer values:

```
(host) #show aaa timers
User idle timeout = 300 seconds
Auth Server dead time = 10 minutes
Logon user lifetime = 5 minutes
User Interim stats frequency = 300 seconds
```

Related Command

Command	Description
aaa timers	Use this command to set the dead time for an authentication server that is down.
aaa timers	Use this command to set the maximum lifetime of idle users before timeout.
aaa timers	Use this command to set the maximum lifetime of unauthenticated users before timeout.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show aaa web admin-port

```
show aaa web admin-port
```

Description

Show the port numbers of HTTP and HTTPS ports used for web administration.

Example

The example below shows that the switch 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
```

Related Command

Command	Description
aaa authentication wired	Use this command to enter the Management Authentication Profile mode

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

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.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

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 switch.

```
(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. • 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. • stateless: Stateless ACL statically evaluates packet contents. The traffic in the reverse direction will be allowed unconditionally. • extended: Extended ACL permits or denies traffic based on the source or destination IP address or IP protocol.
`ACE Index`	Starting index entry for the ACL's access control entries.

Parameter	Description
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.
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
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration mode

show activate-service-firmware

```
show activate-service-firmware
```

Description

Issue this command to verify that the Activate firmware upgrade services are either enabled or disabled.

Syntax

No parameters.

Usage Guidelines

If the Activate firmware service is enabled, the **activate firmware check** command enables the Mobility Access Switch to automatically check Activate to see if there is a new image version to which it can upgrade. If a new version is available, the **activate firmware upgrade** command prompts the Mobility Access Switch to attempt to download and upgrade to the new image.

Example:

```
(host)(config)#  #show activate-service-firmware
activate-service-firmware
-------------------------
Parameter                 Value
---------                 -----
Activate Firmware Service  Enabled
```

Related Commands

Parameter	Description
activate-service-firmware	Use this command to enable or disable the Activate firmware upgrade services. These features are enabled by default.

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration mode

show alarms

```
show alarms [critical | major | minor | summary]
```

Description

Display the alarm status.

Syntax

Parameter	Description
`critical`	Enter the keyword **critical** to display the critical alarms.
`major`	Enter the keyword **major** to display the major alarms.
`minor`	Enter the keyword **minor** to display the minor alarms.
`summary`	Enter the keyword **summary** to display a summary of all alarms.

Example

The following command displays the alarm class, time, and a description of the alarm. In the output below the command, an optional power supply is absent. This is, of course, a minor alarm.

```
(host)#show alarms

  3 Active Alarms in the System
  -----------------------------
  Class  Time                        Description
  -----  ----                        -----------
  Minor  2011-10-28 23:50:05 (PDT)   Slot 0 Power Supply 1 Absent
  Minor  2011-10-28 23:49:54 (PDT)   Slot 1 Power Supply 1 Absent
  Minor  2011-10-28 23:49:54 (PDT)   Slot 2 Power Supply 1 Absent
```

The following command displays the Critical, Major, and Minor alarms by slot.

```
  (host)(config) #show alarms summary

  Slot   Critical  Major  Minor
  ----   --------  -----  -----
  0      0         0      1
  1      0         0      1
  2      0         0      1
  Total  0         0      3
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show arp

```
show arp
```

Description

This command displays the ARP table.

Usage Guidelines

Use this command to display the ARP table.

Example

The following example shows details of routes1

```
(host) (config) #show arp
Codes: * - Local Addresses, S - Static, A - Auth
Total ARP entries: 6
IPV4 ARP Table
--------------
Protocol    IP Address       Hardware Address   Interface  Age (min)
----------  ----------       ----------------   ---------  ---------
* Internet  192.168.210.26   00:0b:86:99:13:f7   vlan1      NA
* Internet  10.73.7.209      00:0b:86:99:13:f7   vlan10     NA
S Internet  10.73.7.222      ac:7f:3e:e6:cc:05   vlan10     NA
  Internet  192.168.210.1    f8:e4:fb:9a:37:2f   vlan1      NA
  Internet  192.168.210.254  e0:cb:4e:55:3e:28   vlan1      NA
```

The output of this command includes the following parameters:

Parameter	Description
`Protocol`	Protocol using ARP. Although the Mobility Access Switch 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

Command	Description
arp	Use this command to create static ARP entries.
clear arp	Clears the ARP entries.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show aruba-central

```
show aruba-central
```

Description

This command displays if Mobility Access Switch is enabled for connecting to Aruba Central portal through Activate.

Syntax

No parameters.

Example

You can use the following CLI command to view the current status of Aruba Central on the Mobility Access Switch:

```
(host) #show aruba-central

Aruba Central
-------------
Parameter                Value
---------                -----
Aruba Central IP/URL     Unknown
Connection Status        DOWN
Mode                     Monitor
Time of last disconnect  Tue Aug 26 15:25:35 2014
```

Related Commands

Command	Description
aruba-central	Displays the status of Aruba Central configuration on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.3.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode.

show cpuload

```
show cpuload
   current
   member <0-7>
```

Description

View CPU load on the system.

Syntax

Parameter	Description
`current`	Displays the overall CPU load on the system.
`member <0-7>`	Displays the CPU load on the specified member.

Example

The example below displays the CPU load on a member:

```
(host) #show cpuload member 0
Member-id: 0
------------
user 0.8%, system 0.7%, idle 98.6%
```

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show crypto dp

```
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 MAS log files, or to clear a crypto ISAKMP state associated with a specific IP address.

Example

The command show crypto dp sends debug information to CRYTPO logs.

```
(host) # show crypto
Datapath debug output sent to CRYPTO logs.
```

Related Command

Command	Description	Mode
crypto isakmp policy	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

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on or MAS

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 MAS.

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.

Example

The command **`show crypto transform-set`** shows the settings for both preconfigured and manually configured transform sets.

```
(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 }
Transform set default-boc-bm-transform: { esp-3des esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-cluster-transform: { esp-aes256 esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-1st-ikev2-transform: { esp-aes256 esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-3rd-ikev2-transform: { esp-aes128 esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-rap-transform: { esp-aes256 esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-remote-node-bm-transform: { esp-3des esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-aes: { esp-aes256 esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set newset: { esp-3des esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set name: { esp-aes256-gcm esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
```

Related Command

Command	Description	Mode
crypto ipsec	Use this command to configure IPsec parameters.	Config mode

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on or MAS

show crypto isakmp

```
show crypto isakmp
   key
   policy
   sa
   stats
   transports
   udpencap-behind-natdevice
```

Descriptions

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

Syntax

Parameter	Description
`key`	Show the IKE pre-shared keys.
`policy`	Show the following information for predefined and manually configured IKE policies: • IKE version • encryption and hash algorithms • authentication method • PRF methods, • DH group • lifetime settings
`sa`	Show the security associations
`peer <peer-ip>`	Shows crypto isakmp security associations for this IP.
`stats`	Show detailed IKE statistics. This information can be very useful for troubleshooting problems with ISAKMP.
`transports`	Shows IKE Transports.
`udpencap-behind-natdevice`	Shows the configuration if NAT-T is enabled if the MAS is behind a NAT device.

Usage Guidelines

Use the `show crypto isakmp` command to ver ISAKMP settings, statistics and policies.

Example

The command **`show crypto isakmp stats`** shows the IKE statistics.

```
(host) #show crypto isakmp policy

Default protection suite 10001
         Version 1
         encryption algorithm: 3DES - Triple Data Encryption Standard (168 bit keys)
         hash algorithm: Secure Hash Algorithm 160
         authentication method: Pre-Shared Key
         Diffie-Hellman Group: #2 (1024 bit)
         lifetime: [300 - 86400] seconds, no volume limit
```

```
Default RAP Certificate protection suite 10002
         Version 1
         encryption algorithm: AES - Advanced Encryption Standard (256 bit keys)
         hash algorithm: Secure Hash Algorithm 160
         authentication method: Rivest-Shamir-Adelman Signature
         Diffie-Hellman Group: #2 (1024 bit)
         lifetime: [300 - 86400] seconds, no volume limit
Default RAP PSK protection suite 10003
         Version 1
         encryption algorithm: AES - Advanced Encryption Standard (256 bit keys)
         hash algorithm: Secure Hash Algorithm 160
         authentication method: Pre-Shared Key
         Diffie-Hellman Group: #2 (1024 bit)
         lifetime: [300 - 86400] seconds, no volume limit
```

Related Command

Command	Description	Mode
crypto isakmp policy	Use this command to configure Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).	Config mode

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on or MAS

show crypto-local ipsec-map

```
show crypto-local ipsec [tag <ipsec-map-name>]
```

Description

Displays the current IPsec map configuration on the MAS.

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 MAS.

Example

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 "mapA" 10
   IKE Version: 2
   IKEv2 Policy: 10
   Security association lifetime: 7200 seconds
   PFS (Y/N): N
   Transform sets={ default-transform }
   Peer gateway: 20.1.1.2
   Local FQDN: test.arubanetworks.com
   Interface:  vlan 4
   Source network: 4.1.1.1/255.255.255.255
   Destination network: 3.1.1.1/255.255.255.255
   Pre-Connect (Y/N): N
   Tunnel Trusted (Y/N): Y
   Forced NAT-T (Y/N): N
```

Related Command

Command	Description	Mode
crypto-local ipsec-map	Use this command to configure IPsec mapping for site-to-site VPN.	Config mode

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on or MAS

show crypto-local isakmp

```
show crypto isakmp {ca-certificates}|{dpd}|{key}|{server-certificate}
```

Descriptions

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

Syntax

Parameter	Description
`ca-certificate`	Shows all the Certificate Authority (CA) certificate associated with VPN clients.
`dpd`	Shows the IKE Dead Peer Detection (DPD) configuration on the MAS.
`key`	Shows the IKE preshared key on the MAS 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 MAS for VPN clients.

Usage Guidelines

Use this command to view IKE parameters.

Examples

This example shows sample output for the **show crypto-local dpd** and the **show crypto-local key** commands:

```
(host) #show crypto-local isakmp ca-certificate
ISAKMP CA Certificates
----------------------
CA certificate name  Client-VPN  # of Site-Site-Maps
-------------------  ----------  -------------------
Aruba-Factory-CA     Y           0

(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 for ANY FQDN
---------------------------------------------------
Key
---
ISAKMP Local Pre-Shared keys configured by FQDN
-----------------------------------------------
FQDN of the host    Key
----------------    ---
servers.mycorp.com  ********

ISAKMP Local Pre-Shared keys configured by Address
--------------------------------------------------
IP address of the host  Subnet Mask Length  Key
----------------------  ------------------  ---
```

```
10.4.62.10              32                  ********

ISAKMP Global Pre-Shared keys configured by Address
---------------------------------------------------
IP address of the host  Subnet Mask Length  Key
----------------------  ------------------  ---
0.0.0.0                 0                   ********
```

Related Commands

Command	Description	Mode
crypto-local isakmp dpd	Use this command to configure IKE Dead Peer Detection (DPD) on the MAS.	Config mode
crypto-local isakmp key	Use this command to configure the IKE preshared key on the MAS for site-to-site VPN.	Config mode

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on or MAS

show crypto-local pki

```
show crypto-local pki
   CRL [<name> ALL|crlnumber|fingerprint|hash|issuer|lastupdate|nextupdate]
   IntermediateCA
   [<name>ALL|alias|dates|fingerprint|hash|issuer|modulus|purpose|serial|subject]

   OCSPResponderCert
   [<name>ALL|alias|dates|fingerprint|hash|issuer|modulus|purpose|serial|subject]

   OCSPSignerCert
   [<name>ALL|alias|dates|fingerprint|hash|issuer|modulus|purpose|serial|subject]

   PublicCert
   [<name>ALL|alias|dates|fingerprint|hash|issuer|modulus|purpose|serial|subject]

   ServerCert
   [<name>ALL|alias|dates|fingerprint|hash|issuer|modulus|purpose|serial|subject]

   TrustedCA
   [<name>ALL|alias|dates|fingerprint|hash|issuer|modulus|purpose|serial|subject]

   crl-stats
   ocsp-client-stats
   rcp
   service-ocsp-responder [stats]
```

Description

Issue this command to show local certificate, OCSP signer or responder certificate and CRL data and statistics.

Syntax

Parameter	Description
`CRL`	Shows the name, original filename, reference count and expiration status of all CRLs on this MAS.
`<CRL name> ALL`	Shows the version, signature algorithm, issuer, last update, next update, and CRL extensions and all other attributes of this CRL.
`<CRL name> crlnumber`	Shows the number of this CRL.
`<CRL name> fingerprint`	Shows the fingerprint of this CRL.
`<CRL name> hash`	Shows the hash number of this CRL.
`<CRL name> issuer`	Shows the issuer of this CRL.
`<CRL name> lastupdate`	Shows the last update (date and time) at which the returned status is known to be correct.
`<CRL name> nextupdate`	Shows the next date and time (date and time) where the responder retrieves updated status information for this certificate. If this information is not present, then the responder always holds up to date status information.

Parameter	Description
IntermediateCA	Shows the name, original filename, reference count and expiration status of this certificate. **NOTE:** IntermediateCA has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
OSCPResponderCert	Shows the name, original filename, reference count and expiration status of all ocsprespondercert certificates on this MAS. **NOTE:** OCSPResponderCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
OCSPSignerCert	Shows the OCSP Signer certificate. **NOTE:** OCSPSignerCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
PublicCert	Shows Public key information of a certificate. This certificate allows an application to identify an exact certificate. **NOTE:** PublicCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
ServerCert	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 MAS. **NOTE:** ServerCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
TrustedCA	Shows trusted CA certificate information. This certificate can be either a root CA or intermediate CA. Aruba encourages (but does not require) an intermediate CA's signing CA to be the MAS itself.
<name> ALL	Shows the version, signature algorithm, issuer, last update, next update, and CRL extensions and all other attributes of this certificate.
<name> alias	Shows this certificate's alias, if it exists.
<name> dates	Shows the dates for which this certificate is valid.
<name> fingerprint	Shows the certificate's fingerprint.
<name> hash	Shows the hash number of this certificate.
<name> issuer	Shows the certificate issuer.
<name> modulus	Shows the modulus which is part of the public key of the certificate.
<name> purpose	Shows the certificate's purposes such as if this is an SSL server, SSL server CA and so on.
<name> serial	Shows the certificate's serial number.
<name> subject	Shows the certificate's subject identification number.
crl-stats	Shows the CRL request statistics.
ocsp-client-stats	Shows the OCSP client statistics.

Parameter	Description
`rcp`	Shows the revocation check point.
`service-ocsp-responder [stats]`	Shows if OCSP responder service is enabled and shows statistics.

Usage Guidelines

Use the **show crypto-local pki** command to view all CRL and certificate status, OCSP client and OCSP responder status and statistics.

Examples

This example displays a list of all OCSP responder certificates on this MAS.

```
(host) (config) #show crypto-local pki OCSPResponderCert

Certificates
------------
Name                        Original Filename          Reference Count  Expired
--------------              -----------------          ---------------  -------
ocspJan28                   ocspresp-jan28.cer         0                No
ocspresp-standalone-feb21   ocspresp-feb21.cer         0                No
ocspRespFeb02               ocspresp-feb2.cer          1                No
OCSPresponder1              ocspresponder-new1.cer     0                No
ocspresponder2              subsubCA-ocsp-res-2.cer    0                No
OCSPresponderlatest         ocspresponder-latest.cer   0                No
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the OCSP responder certificate.
`Original Filename`	Name of the original certificate when it was added to the MAS.
`Reference Count`	Number of RCPs that reference this OCSP responder certificate, signer certificate or CRL.
`Expired`	Shows whether the MAS has enabled or disabled client remediation with Sygate-on-demand-agent.

This example shows the dates for which this OCSP responder certificate is valid.

```
(host) (config) #show crypto-local pki OCSPResponderCert ocspJan28 dates

notBefore=Jan 21 02:37:47 2011 GMT
notAfter=Jan 20 02:37:47 2013 GMT
```

This example displays the certificate's hash number.

```
(host) (config) #show crypto-local pki OCSPResponderCert ocspJan28 hash

91dcb1b3
```

This example shows the purpose and information about this certificate.

```
(host) (config) #show crypto-local pki OCSPResponderCert ocspJan28 purpose

Certificate purposes:For validation
```

```
SSL client : No
SSL client CA : No
SSL server : No
SSL server CA : No
Netscape SSL server : No
Netscape SSL server CA : No
S/MIME signing : No
S/MIME signing CA : No
S/MIME encryption : No
S/MIME encryption CA : No
CRL signing : No
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
```

This example displays the certificate's subject.

```
(host) (config) #show crypto-local pki OCSPResponderCert ocspJan28 subject

subject= /CN=WIN-T1BQQFMVDED.security1.qa.mycorp.com
```

Related Command

Command	Description	Mode
crypto-local pki	This command is saved in the configuration file and verifies the presence of the certificate in the MAS's internal directory structure.	Config mode

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode

show crypto map

```
show crypto ipsec map
```

Description

This command displays the IPsec map configurations.

Syntax

Parameter	Description
`map`	Specifies the global, dynamic, and default map configurations.

Usage Guidelines

Use the show crypto map command to view configuration for global, dynamic and default map configurations.

Example

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
         IKE Version: 1
         lifetime: [300 - 86400] seconds, no volume limit
         PFS (Y/N): N
         Transform sets={ default-transform, default-aes }
Crypto Map "GLOBAL-IKEV2-MAP" 10000 ipsec-isakmp
Crypto Map "default-local-master-ipsecmap" 9999 ipsec-isakmp
Crypto Map Template"default-local-master-ipsecmap" 9999
         IKE Version: 1
         lifetime: [300 - 86400] seconds, no volume limit
         PFS (Y/N): N
         Transform sets={ default-ml-transform }
         Peer gateway: 10.4.62.9
         Interface: VLAN 0
         Source network: 172.16.0.254/255.255.255.255
         Destination network: 10.4.62.9/255.255.255.255
         Pre-Connect (Y/N): Y
         Tunnel Trusted (Y/N): Y
         Forced NAT-T (Y/N): N
```

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode

show crypto pki csr

```
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 (CSR) for the captive portal feature.

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

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on or MAS

show database synchronize

```
show database synchronize
```

Description

View database synchronization details.

Usage Guidelines

Verify database synchronization; manual or periodic.

Example

The example below displays the database sychronization details including file sizes, automatic synchronization attempts, and any failed synchronization.

```
(host)#show database synchronize

   Last synchronization time: Mon Oct 24 04:55:49 2011
   To Primary member at 128.0.193.0:  succeeded
   Local User Database backup file size: 9267 bytes
   Cert Database backup file size: 2491 bytes
   Synchronization took 1 second

   40 synchronization attempted
   2 synchronization have failed

   Periodic synchronization is enabled and runs every 2 minutes
```

Related Command

Command	Description
database synchronize	Synchronize database

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show datapath debug

```
show datapath debug
   dma [counters|slot <id>|{{| begin}|{| exclude}|{| include}}]
   eap [counters|slot <id>|{{| begin}|{| exclude}|{| include}}]
   pkttrace-buffer [log {<number>|all}|slot <id>|{{| begin}|{| exclude}|
   {| include}}]
   trace-buffer slot <id>|{{| begin }|{| exclude}|{| include}]
```

Description

Displays the datapath advanced debugging information on DMA, EAP, packet trace buffer, and trace buffer.

Syntax

Parameter	Description
`dma [counters|slot <id>| {{| begin}|{| exclude}|{| include}}]`	Specify this parameter to display the datapath DMA statistics based on counters, slot ID, or by one of the output modifiers.
`eap [counters|slot <id>| {{| begin}|{| exclude}|{| include}}]`	Specify this parameter to display the datapath EAP termination statistics based on counters, slot ID, or by one of the output modifiers.
`pkttrace-buffer [log {<number>|all}|slot <id>| {{| begin }|{| exclude}|{| include}]`	Specify this parameter to display the datapath packet trace buffer based on the log line number, slot ID, or by one of the output modifiers.
`trace-buffer [slot <id>| {{{| begin }|{| exclude}|{| include}}]`	Specify this parameter to display the datapath trace buffer based on the slot id or by one of the output modifiers.

Example

The following example displays the datapath debug information:

```
(host) #show datapath debug trace-buffer
Datapath Trace Buffer Entries:
CPDNSok(      4f)     0x0         0x1          0x7f000001 0x1f        0x7         0x0
CPDNSok(      4f)     0x0         0x1          0x0        0x1f        0x7         0x0
WiredDOT1X(     239) 0x0         0xff         0x1        0x1004      0x0         0x9
WiredDOT1X(     239) 0x0         0xff         0x2        0x1004      0x0         0x9
WiredDOT1X(     239) 0x0         0xff         0xa        0x1004      0x0         0x9
WiredDOT1X(     239) 0x0         0xff         0xc8       0x1004      0x0         0x9
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4.1	The **trace-buffer** parameter was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration mode

show datapath dpe acl hits

```
show datapath dpe acl hits <acl ID> slot <slot Id>
```

Description

Displays internal ACL hit counters.

ArubaOS Mobility Access Switch supports only up to 2000 counters for ACLs.

Syntax

Parameter	Description
`acl hits <acl ID>`	Enter the ACL number. **NOTE:** You can get the ACL number from the `show acl acl-table` command.
`slot <slot Id>`	Enter the slot id.

Example

The following example displays the ACL hits:

```
(host) #show datapath dpe acl hits 33 slot 0

Datapath Element ACL Hits
-------------------------
Index   Source                       Destination                  Proto
-----   ------------------           -------------------          ------------------
127:    129.64.5.0 255.255.255.0     10.129.63.1 255.255.255.255  6 0-65535 22-22
128:    10.63.127.1 255.255.255.255  10.129.63.1 255.255.255.255  6 0-65535 22-22
129:    10.63.127.1 255.255.255.255  129.64.129.1 255.255.255.255 6 0-65535 22-22
130:    0.0.0.0 0.0.0.0              10.129.63.1 255.255.255.255  6 0-65535 22-22
131:    0.0.0.0 0.0.0.0              129.64.129.1 255.255.255.255 6 0-65535 22-22
132:    ::/0                         ::/0                         any

Pkts      Bytes
--------  --------
0         0
0         0
0         0
0         0
0         0
0         0
```

Command History

Release	Modification
ArubaOS 7.0	Command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration mode

show datapath session

```
show datapath session
```

Description

Displays the session table entries.

Example

The following example displays the session table entries:

```
(host) #show datapath session
Datapath Session Table Entries
------------------------------
Flags: F - fast age, S - src NAT, N - dest NAT
Source IP/     Destination IP  Prot SPort DPort  Cntr Prio ToS Age Destination TAge UsrIdx
Destination MAC
-------------  --------------  ---- ----- -----  ---- ---- --- --- ----------- ---- ------
192.168.5.10    192.168.1.20    17   8211  8218   0/0  0    0   0   1/0/0       5    0
192.168.1.20    192.168.1.10    17   8218  8211   0/0  0    0   0   1/0/0       5    0

UsrVer Flags
------ -----
0      FSI
0      FNCI
```

The output of this command includes the following parameters:

Parameter	Description
`Source IP`	Source IP address of the session entry.
`Destination IP`	Destination IP address of the session entry.
`Prot`	Indicates the protocol number.
`SPort`	Source port of the protocol.
`Dport`	Destination port of the protocol.
`Cntr`	Bandwidth contract. **NOTE:** This is not supported on Mobility Access Switch.
`Prio`	dot1p priority assigned to the user.
`ToS`	ToS value assigned to the user through the session ACL.
`Age`	Time elapsed in seconds since the session was last refreshed.
`Destination`	The interface on the Mobility Access Switch where the session or user exists.
`TAge`	Time elapsed in seconds since the session was created.
`UsrIdx`	User index entry.
`UsrVer`	Version of the user.
`Flags`	Flags if any, raised on the session.

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.
ArubaOS 7.4	The **S** and **N** flags are introduced in the output to indicate if source NAT and destination NAT operations are performed on the sessions.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration mode

show ddns-client

```
show ddns-client
```

Description

This command displays the updates that are sent to the server.

Example

```
(host) # show ddns-client
Dynamic DNS Client Information
------------------------------
Interface      Hostname            Service URL                     IP Address    Update Status
---------      --------            -----------                     ----------    -------------
vlan4          arubamas.no-ip.info dynupdate.no-ip.com/nic/update   4.4.4.10       Success
```

The output of this command includes the following information:

Command	Description
`Interface`	Displays the interface on which the DDNS profile is applied.
`Hostname`	Displays the host name of the DDNS.
`Service URL`	Displays the the update URL that is used to send the DDNS updates to the DDNS server.
`IP Address`	Displays the updated IP address of the client.
`Update Status`	Displays if the update was successfully sent or not.

Command History

Release	Modification
ArubaOS 7.4	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show device-group

```
show device-group
   interfaces [ap]
```

Description

This command displays the device-group attached interfaces.

Syntax

Parameter	Description
`interfaces`	Displays device-group attached interfaces.
`ap`	Option to display the device-group attached interfaces for the device type AP.

Example

The following command displays AP device-group attached interfaces:

```
(host) #show device-group interfaces ap

Device-Group Config Attached Interfaces
---------------------------------------
Device Type    Interface List
-----------    --------------
access-point   1/0/2,1/0/15-1/0/16,1/0/21-1/0/22,1/0/27-
1/0/28,1/0/32,1/0/40,1/0/42,1/0/46,2/0/16,
               2/0/28,2/0/42,2/0/46,3/0/2,3/0/15,3/0/18,3/0/29,3/0/40
```

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show device-group-config

```
show device-group-config
   ap
```

Description

This command displays the device-group configuration parameters.

Syntax

Parameter	Description
ap	Displays the device group configuration parameters for device-type AP.

Example

The following command displays the device group configuration parameters for device-type AP:

```
(host) #show device-group-config ap

device-group access-point (N/A)
-------------------------------
Parameter                       Value
---------                       -----
Enable Device Config            true
Interface MSTP Profile          default
Interface GVRP Profile          N/A
Interface PVST Profile          default
Interface LLDP Profile          device-group-default
Interface PoE Profile           device-group-default
Interface Ethernet Link Profile default
Interface QoS Profile           N/A
Interface Policer Profile       N/A
Interface AAA Profile           default
Interfaces To Shutdown          N/A
Interface MTU                   1514
Interface Ingress ACL           N/A
Interface Egress ACL            N/A
Interface Session ACL           N/A
Interface QoS Trust Mode        auto
Interface Switching Profile     default
Interface Security Profile      N/A
Interface Trusted Mode          Trusted
```

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show dhcp-snooping-database

```
show dhcp-snooping-database [gigabitethernet|port-channel|summary|vlan <vlan_id>]
```

Description

This command displays the DHCP snooping configuration information.

Syntax

Parameter	Description
`gigabitethernet`	Displays dhcp snooping configuration information on a Gigabit Ethernet interface.
`port-channel`	Displays dhcp snooping configuration information on a port channel.
`summary`	Displays the summary of the DHCP Snooping database.
`vlan <vlan_id>`	Displays the DHCP snooping learnt on the VLAN interface.

Usage Guidelines

Use this command to view the DHCP snooping configuration information.

Example

```
(host) #show  dhcp-snooping-database  vlan 6
Total DHCP Snoop Entries : 3
Learnt Entries : 1, Static Entries : 2

DHCP Snoop Table
----------------
MAC                IP         BINDING-STATE  LEASE-TIME                 VLAN-ID  INTERFACE
---                --         -------------  ----------                -------  ---------
00:00:00:60:4a:69  6.6.6.10   Dynamic entry  2013-09-06 10:50:05 (PST)  6
gigabitethernet1/0/2
00:00:11:22:44:55  4.4.4.4    Static entry   No lease time              6
gigabitethernet1/0/2
00:00:11:33:66:77  7.7.7.7    Static entry   No lease time              6
gigabitethernet1/0/11
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show diagnostics interface gigabitethernet

```
show diagnostics interface gigabitethernet
   <slot/module/port> cable
   all cable
```

Description

Displays the test results for the Time-Domain Reflectometer (TDR) cable diagnostics. The information returned by the test can be used to characterize and locate faults in metallic cables such as twisted pair.

Syntax

Parameter	Description
`<slot/module/port> cable`	Displays the TDR test results for a specific interface.
`all cable`	Displays the TDR test results for all gigabitethernet interfaces.

Usage Guidelines

This command returns the results from a TDR cable diagnostic for a specific gigabitethernet interface or all gigabitethernet interfaces upon which a TDR diagnostic was executed.

Example

If you execute this command before the test is complete, you will see the following:

```
#show diagnostics interface gigabitethernet 1/0/23 cable
   Interface name          : gigabitethernet1/0/23
   Test status             : Running
   Once the test has finished, you will see the following:
#show diagnostics interface gigabitethernet 1/0/23 cable

   Interface name          : gigabitethernet1/0/23
   Test status             : Completed
   Normal cable length     : 3 metres

   Pair 1-2
   --------
   Pair status             : Normal
   Polarity swap           : Positive
   Pair skew               : 0

   Pair 3-6
   --------
   Pair status             : Normal
   Polarity swap           : Positive
   Pair skew               : 8

   Pair 4-5
   --------
   Pair status             : Normal
   Polarity swap           : Positive
   Pair skew               : 0

   Pair 7-8
   --------
```

```
Pair status             : Normal
Polarity swap           : Positive
Pair skew               : 0

Channel 0:
Pair swap               : Straight

Channel 1:
Pair swap               : Straight
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show firewall

```
show firewall
```

Description

Display a list of global firewall policies.

Syntax

No parameters

Example

The following example shows all firewall policies currently configured on the Mobility Access Switch.

```
(host) (config) #show firewall
Global firewall policies
------------------------
Policy                                      Action    Rate      Port
------                                      ------    ----      ----
Enforce TCP handshake before allowing data  Disabled
Prohibit RST replay attack                  Disabled
Deny all IP fragments                       Disabled
Prohibit IP Spoofing                        Enabled
Log all received ICMP errors                Disabled
Per-packet logging                          Disabled
Session mirror destination                  Disabled
Stateful SIP Processing                     Disabled
Session Idle Timeout                        Disabled
Session VOIP Timeout                        Disabled
Stateful H.323 Processing                   Disabled
Stateful SCCP Processing                    Disabled
Monitor/police CP attacks                   Disabled
Rate limit CP untrusted ucast traffic       Enabled   1000 pps
Rate limit CP untrusted mcast traffic       Enabled   1000 pps
Rate limit CP trusted ucast traffic         Enabled   8000 pps
Rate limit CP trusted mcast traffic         Enabled   1000 pps
Rate limit CP route traffic                 Enabled   200 pps
Rate limit CP session mirror traffic        Enabled   200 pps
Rate limit CP auth process traffic          Enabled   500 pps
Prohibit ARP Spoofing                       Disabled
Stateful VOCERA Processing                  Disabled
Stateful UA Processing                      Disabled
Enforce TCP Sequence numbers                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.

Parameter	Description
Prohibit RST replay attack	If enabled, this setting closes a TCP connection in both directions if a TCP RST is received from either direction.
Deny all IP Fragments	If enabled, all IP fragments are dropped.
Prohibit IP Spoofing	When this option is enabled, source and destination IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.
Log all received ICMP errors	Shows if the Mobility Access Switch will log received ICMP errors.
Per-packet logging	If active, and logging is enabled for the corresponding session rule, this feature logs every packet.
Stateful SIP Processing	Shows if the Mobility Access Switch 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 WLAN traffic on the network
Session Idle Timeout	Shows if a session idle timeout interval has been defined.
Session VOIP Timeout	If enabled, an idle session timeout is defined for voice sessions.
Stateful H.323 Processing	Shows if the Mobility Access Switch has enabled or disabled stateful H.323 processing. This option is disabled and cannot be enabled in ArubaOS 7.3.
Stateful SCCP Processing	Shows if the Mobility Access Switch has enabled or disabled stateful SCCP processing.
Monitor/police CP attacks	If enabled, the Mobility Access Switch monitors a misbehaving user's inbound traffic rate. If this rate is exceeded, the Mobility Access Switch 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.
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 Mobility Access Switch.
Rate limit CP auth process traffic	Displays the traffic rate limit for traffic forwarded to the authentication process.

Parameter	Description
`Prohibit ARP Spoofing`	When this option is enabled, possible ARP spoofing attacks are logged and an SNMP trap is sent.
`Stateful VOCERA Processing`	VOCERA processing is disabled by default. **NOTE:** MadCap:autonum="NOTE: ">You cannot enable this option in this release.
`Stateful UA Processing`	UA processing is disabled by default. **NOTE:** You cannot enable this option in this release.
`Enforce TCP Sequence numbers`	If enabled, prevents data from passing between two clients until the three-way TCP handshake has been performed.
`Session mirror IPSEC`	Shows if the session mirror is configured for all the frames processed by IPSec.

Related Command

Command	Description	Mode
`firewall`	This command configures firewall options on the Mobility Access Switch.	Config mode

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Configuration Mode (config)

show gvrp-global-profile

```
show gvrp-global-profile
```

Description

Displays GVRP global profile settings.

Syntax

No parameters.

Example

The following example displays global GVRP status and current timer values:

```
(host) (config) #show gvrp-global-profile

Global GVRP configuration
-------------------------
Parameter       Value
---------       -----
GVRP status     Enabled
Join Time       200
Leave Time      600
Leave-all Time  10000
```

The output of this command displays the following parameters:

Parameter	Description	Range	Default
`GVRP status`	Displays status of the GVRP profile.	—	disable
`Join Time`	Join timer interval in milliseconds.	1–65535	200
`Leave Time`		1–65535	600
`Leave-all time`	Leave timer interval in milliseconds.	1–65535	10000

Command History

Release	Modification
ArubaOS 7.2	This command was introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show gvrp interfaces

```
show gvrp interfaces
```

Description

Displays the list of interfaces on which GVRP is enabled, GVRP state of that interface, and the registrar mode.

Syntax

No parameters.

Example

The following example displays the interfaces on which GVRP is enabled, GVRP state of that interface, and the registrar mode:

```
(host) (config) #show gvrp interfaces

Interface GVRP info
-------------------
Interface               State     Registrar Mode
---------               -----     --------------
gigabitethernet0/0/10   Enabled   Normal
gigabitethernet0/0/20   Disabled  N/A
port-channel1           Disabled  N/A
```

The output of this command displays the following parameters

Parameter	Description
`Interface`	Name of the interface.
`State`	State of GVRP profile.
`Registrar Mode`	Displays registrar mode (normal, forbidden, or N/A)

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show hot-standby-link

```
show hot-standby-link [gigabitethernet <slot/module/port> | port-channel <number>]
```

Description

Display details for a primary and backup link configured to use the hot standby link feature.

Syntax

Parameter	Description
`gigabitethernet <slot/module/port>`	Gigbit Ethernet interface, in the format slot/module/port.
`port-channel <number>`	Port channel ID (0-7).

Usage Guidelines

The hot standby link feature enables a Layer-2 interface (or port-channel) to back-up another Layer 2-interface (or port-channel) so that these interfaces become mutual backups.

Examples

To view details of HSL on an interface, use the following command.

```
(host) #show hot-standby-link gigabitethnernet 0/0/10

  HSL Interface Info
  ------------------
  Primary Interface: GE-0/0/10 (Active)  Backup Interface:  GE-0/0/11 (Standby)
  Preemption Mode: forced                Preemption Delay:  200
  Last Switchover Time: NEVER            Flap Count: 0
```

To view details of all HSL links, use the following command.

```
(host) #show hot-standby-link

  HSL Interfaces Info
  -------------------
  Primary     State   Backup      State      Last Switchover Time
  --------    ------  -------     ------     --------------------
  GE-0/0/10   Active  GE-0/0/11   Standby    Never
  GE-0/0/3    Down    PC-4        Down       Never
  PC-1        Down    GE-0/0/0    Active     Never
  PC-2        Down    PC-3        Down       Never
```

The output of these command includes the following information:

Parameter	Description
`Primary`	The Primary interface or a list of the primary interfaces for the HSL pair.
`State`	The state of the primary interface—Active, Down or Standby.
`Backup`	The backup interface or a list of the backup interfaces for the HSL pair.
`Preemption Mode`	This parameter shows if the current preemption mode is **forced** or **off**.

Parameter	Description
`Preemption Delay`	If preemption is in forced mode, the preemption delay defines the time before the primary link becomes active again.
`Last Switchover Time`	Amount of time, if any, that has elapsed since the last link switchover happened.
`Flap Count`	Number of times the active link switchover has happen.

Related Commands

Command	Description
`backup interface`	Configure a backup interface (Gigabit Ethernet or Port Channel).
`preemption`	Sets preemption mode and delay times for the hot standby link feature.
`show interface-config gigabitethernet`	This command displays the interface configuration information.
`show interface-config port-channel`	This command displays the port-channel configuration information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show igmp-snooping

```
show igmp-snooping counters|groups|membership|mrouter [vlan <vlan-id>]
```

Description

This command lists IGMP snooping counters, groups, membership, and multicast router information.

Syntax

Parameter	Description
`counters`	Displays the IGMP snooping counters.
`groups`	Displays the IGMP snooping groups.
`membership`	Displays the IGMP snooping membership information.
`mrouter`	Displays the IGMP snooping multicast router ports information.
`[vlan <vlan-id>]`	Displays the details only for the specified VLAN.
`[detail]`	Displays the details only for the specified VLAN in detail.

Usage Guidelines

By default, this command shows general information for all VLANs. Include the optional `vlan <vlan-id>` parameters to display detailed output for a single VLAN.

Examples

The following examples show the output from the show igmp-snooping groups, show igmp-snooping membership, show igmp-snooping mrouter commands.

```
(host) # show igmp-snooping groups
IGMP Snooping Multicast Route Table
-----------------------------------
VLAN  Group            Port List
----  -----            ---------
0100  224.0.1.40       GE 0/0/11
0100  239.255.255.250  GE 0/0/11

(host) # show igmp-snooping membership
IGMP Snooping Multicast Membership
----------------------------------
VLAN  Group       Port      Expiry    UpTime
----  -----       ----      ------    ------
0001  224.0.1.40  GE0/0/9   00:03:36  04:47:27
0001  225.0.1.1   GE0/0/9   00:00:00  00:01:25
1900  225.0.1.1   GE0/0/3   00:03:49  04:47:32
0003  225.0.1.1   GE0/0/9   00:00:00  04:46:30
0003  239.0.0.1   GE0/0/9   00:00:00  04:44:42
(host) # show igmp-snooping mrouter
Flags: D - Dynamic, S - Static, P - PIM, M - IGMP/MLD query
IGMP Snooping Multicast Router Ports
------------------------------------
VLAN  Elected-Querier  Ports (Flags)  Expiry    UpTime    Src-Ip
----  ---------------  -------------  ------    ------    ------
```

```
0001  10.10.10.6        GE0/0/9 (DM)    00:04:07  04:45:55  10.10.10.6
                        GE0/0/9 (DP)    00:04:09  04:45:34  10.10.10.6
0003  3.3.3.10          GE0/0/9 (DM)    00:04:15  04:45:25  3.3.3.10
                        GE0/0/9 (DP)    00:04:06  04:44:56  3.3.3.10
0300  20.20.20.1        GE0/0/9 (DM)    00:04:15  04:45:25  20.20.20.1
                        GE0/0/9 (DP)    00:04:05  04:45:13  20.20.20.1
(host) # show igmp-snooping mrouter vlan 1
Flags: D - Dynamic, S - Static, P - PIM, M - IGMP/MLD query
IGMP Snooping Multicast Router Ports
-------------------------------------
VLAN  Elected-Querier  Ports (Flags)  Expiry    UpTime    Src-Ip
----  ---------------  -------------  ------    ------    ------
0001  10.10.10.6       GE0/0/9 (DM)   00:03:25  04:35:30  10.10.10.6
                       GE0/0/9 (DP)   00:04:14  04:35:09  10.10.10.6

(host)# show igmp-snooping mrouter vlan 1 detail
Flags: D - Dynamic, S - Static, P - PIM, M - IGMP/MLD query
Vlan:0001 Elected-Querier:10.10.10.6
  GE0/0/9     (DM)  Expiry Time: 00:03:45  Uptime: 04:36:10
                Router IP: 10.10.10.6
                Router MAC: 00:19:06:55:15:40
  GE0/0/9     (DP)  Expiry Time: 00:04:04  Uptime: 04:35:49
                Router IP: 10.10.10.6
                Router MAC: 00:19:06:55:15:40
```

The output of this command incudes the following information:

Parameter	Description
VLAN	Name of the VLAN on which IGMP snooping has been configured.
Group	Group.
Port	Gigabit Ethernet port on the switch.
Expiry	Amount of time before the querier timeout interval expires.
Uptime	Amount of time the router ports have been active, in the format *hours:minutes:seconds.*
Elected-Querier	IP address of the IGMP querier configured on a switch.
Src-IP	Source IP.

Related Commands

Command	Description
vlan-profile igmp-snooping-profile	This command creates an IGMP snooping profile that can be applied to a VLAN.
show vlan-profile igmp-snooping-profile	This command displays a IGMP snooping profile and the associated parameters.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

show interface all

```
show interface all switchport <brief|detail|extensive>
```

Description

This command displays all the interface information in brief or detail..

Syntax

Parameter	Description
`switchport <brief|detail|extensive>`	Displays the interface information. • brief: provides a brief information on the interface. • detail: provides a more detailed information on the interface. • extensive: provides an extensive information on the interface.

Examples

The following examples display the information on all the interfaces:

```
(host) #show interface all switchport brief
GE0/0/0
Link is Down
Flags: Access, Untrusted
VLAN membership: 12
GE0/0/1
Link is Down
Flags: Access, Trusted
VLAN membership: 1
GE0/0/10
Link is Down
Flags: Access, Trusted
VLAN membership: 1
<output truncated>
(host) #show interface all switchport extensive
GE0/0/0
Link is Down
Flags: Access, Untrusted
VLAN membership:
VLAN tag  Tagness   STP-State
--------  --------  ---------
12        Untagged  DIS
GE0/0/1
Link is Down
Flags: Access, Trusted
VLAN membership:
VLAN tag  Tagness   STP-State
--------  --------  ---------
1         Untagged  DIS
<output truncated>
.
.
.
(host) #show interface all switchport detail
GE0/0/0
```

```
Link is Down
Flags: Access, Untrusted
VLAN membership:
VLAN tag  Tagness   STP-State
--------  --------  ---------
12        Untagged  DIS
GE0/0/1
Link is Down
Flags: Access, Trusted
VLAN membership:
VLAN tag  Tagness   STP-State
--------  --------  ---------
1         Untagged  DIS
GE0/0/10
Link is Down
Flags: Access, Trusted
VLAN membership:
VLAN tag  Tagness   STP-State
--------  --------  ---------
1         Untagged  DIS
.
.
.
(host) #show interface all switchport detail
GE0/0/0
Link is Down
Flags: Access, Untrusted
VLAN membership:
VLAN tag  Tagness   STP-State
--------  --------  ---------
12        Untagged  DIS
GE0/0/1
Link is Down
Flags: Access, Trusted
VLAN membership:
VLAN tag  Tagness   STP-State
--------  --------  ---------
1         Untagged  DIS
GE0/0/10
Link is Down
Flags: Access, Trusted
VLAN membership:
VLAN tag  Tagness   STP-State
--------  --------  ---------
1         Untagged  DIS
<output truncated>
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

show interface brief

```
show interface brief
   gigabitethernet <slot/module/port>
   port-channel {id <id> | all}
```

Description

This command displays all the interface information in brief.

Syntax

Parameter	Description
`gigabitethernet`	Displays the gigabit Ethernet interface information in brief.
`port-channel`	Displays the port-channel interface information in brief. This parameter has the following sub-parameters: • **id <id>** to display the Port-channel interface information for a specific port-channel interface ID. • **all**: to display all configured port-channel interface information in brief.

Example

The following example displays the interface details of Port channel 1

```
(host) #show interface brief port-channel 1
Interface       Admin   Link  Line Protocol  Speed/Duplex
---------       -----   ----  -------------  ------------
port-channel1   Enable  Down  Down           N/A
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.
ArubaOS 7.4.1.8	The **all** subparameter was introduced in the port-channel parameter.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable mode

show interface-config gigabitethernet

```
show interface-config gigabitethernet <slot/module/port>
```

Description

This command displays the interface configuration information.

Syntax

Parameter	Description
`<slot/module/port>`	The slot, module and port numbers of the interface, separated by slashes (/).

Example

The output of this command displays the following information:

```
(host) #show interface-config gigabitethernet 0/0/0

  gigabitethernet "0/0/0"
  -----------------------
  Parameter                                  Value
  ---------                                  -----
  Interface MSTP Profile                     default
  Interface Rapid PVST Profile               default
  Interface Tunneled Node Profile            N/A
  Interface VOIP Profile                     N/A
  Interface LLDP Profile                     lldp-factory-initial
  Interface PoE Profile                      poe-factory-initial
  Interface Ethernet Link Profile            default
  Interface LACP Profile                     N/A
  Interface QoS Profile                      N/A
  Interface Policer Profile                  N/A
  Interface AAA Profile                      N/A
  Interface Shutdown                         Disabled
  Interface MTU                              1514
  Interface Ingress ACL                      N/A
  Interface Egress ACL                       N/A
  Interface Session ACL                      N/A
  Interface QoS Trust Mode                   Disabled
  Interface Description                      N/A
  Interface Switching Profile                default
  Ingress Port Mirroring Profile             N/A
  Egress Port Mirroring Profile              N/A
  Static IGMP Multicast Router port for VLANs 0
  Static MLD Multicast Router port for VLANs  0
  Interface Trusted Mode                     Enabled
  HSL backup interface                       N/A
  HSL preemption mode                        Off
  HSL preemption delay                       100
  MAC-Limit (Action)                         N/A
  Configuration Derivation                   gigabitethernet0/0/0 default
```

The output of this command includes the following information:

Parameter	Description
Interface MSTP Profile	The MSTP profile applied to the interface.
Interface Tunneled Node Profile	The Tunneled Node profile applied to the interface.
Interface VOIP Profile	The VoIP profile applied to the interface.
Interface LLDP Profile	The LLDP profile applied to the interface.
Interface PoE Profile	The PoE profile applied to the interface.
Interface Ethernet Link Profile	The Ethernet Link profile applied to the interface.
Interface LACP Profile	The LACP profile applied to the interface.
Interface QoS Profile	The QoS profile applied to the interface.
Interface Policer Profile	The Policer profile applied to the interface.
Interface AAA Profile	The AAA profile applied to the interface.
Interface Shutdown	Shows if the interface has been disabled.
Interface MTU	Maximum Transmission Unit (MTU) value configured in bytes.
Interface Ingress ACL	Ingress Access Control List (ACL) configured for the interface.
Interface Egress ACL	Egress Access Control List (ACL) configured for the interface.
Interface Session ACL	Session Access Control List (ACL) configured for the interface.
Interface QoS Trust Mode	Shows if the QoS Trust Mode is enabled on this interface.
Interface Description	Description of the interface, if configured.
Interface Switching Profile	The Switching profile applied to the interface.
Ingress Port Mirroring Profile	If port mirroring is enabled, this feature can send copies of all or sampled packets seen on specific port (s) or port-channel to a destination. This parameter displays the ingress mirroring profile for the interface.
Egress Port Mirroring Profile	If port mirroring is enabled, this feature can send copies of all or sampled packets seen on specific port (s) or port-channel to a destination. This parameter displays the egress mirroring profile for the interface.
Static Multicast Router port for the VLAN	In IGMP snooping proxy mode, you can enable suppressing reports to multicast router ports. This parameter shows the VLAN ID configured as the multicast router VLAN IDs for IGMP snooping.
Interface Trusted Mode	Shows if trusted mode is enabled for the interface.

Parameter	Description
HSL backup interface	Hot Standby-Link (HSL) backup interface.
HSL preemption mode	When a primary link goes down, the backup link becomes active. By default, when this link comes back up, it goes into standby mode as the other backup interface is already activated. If preemption mode is enabled for the primary link, the primary interface to become active again once it comes back up. This parameter is disabled by default.
HSL preemption delay	If preemption mode is enabled, this parameter shows the configured preemption delay.
MAC-Limit (Action)	The maximum number of MACs that can be learned on this interface.
Configuration Derivation	The active configuration from interface and interface groups.

Related Commands

Command	Description
interface gigabitethernet	This command configures a Gigabit Ethernet port on the switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-config mgmt

```
show interface-config mgmt
```

Description

This command displays the management interface configuration information.

Syntax

No parameters.

Example

The output of this command displays the following information:

```
(host) #show interface-config mgmt

mgmt
----
Parameter                Value
---------                -----
Interface shutdown       Disabled
IP Address               10.16.48.28/255.255.255.0
IPv6 Address             N/A
IPv6 link local Address  N/A
Interface description    N/A
```

The output includes the following parameters:

Parameter	Description
`Interface Shutdown`	Shows if the interface shutdown feature is enabled or disabled for the management interface. By default this feature is disabled, (the interface is active).
`IP address`	IP address and netmask of the management interface.
`Interface Description`	Description of the management interface, if configured.

Related Commands

Command	Description
`interface mgmt`	This command configures the management port on the switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-config port-channel

```
show interface-config port-channel [<0-63>]
```

Description

This command displays the port-channel configuration information.

Syntax

Parameter	Description
<0-63>	Port-channel ID.

Usage Guidelines

By default, this command displays the entire list of defined port-channels, including their status and the number of references to each port-channel. Include a port-channel ID to display detailed configuration information for that port-channel.

Examples

The first example shows that the switch has one defined port-channel configuration. The References column shows that there are two other profiles with references to that port-channel configuration, and the Profile Status column indicates whether the settings are predefined. User-defined port-channels will not have an entry in the Profile Status column.

The second example displays the current settings of the **0** port-channel configuration.

```
(host) #show interface-config port-channel
port-channel List
-----------------
Name  References  Profile Status
----  ----------  --------------
0     2
Total:1

(host) #show interface-config port-channel 0
port-channel "0"
----------------
Parameter                                 Value
---------                                 -----
Interface MSTP profile                    default
Interface Ethernet link profile           pc_default
QoS Profile                               N/A
Policer Profile                           N/A
Interface Ingress Mirroring profile       N/A
Interface Egress Mirroring profile        N/A
Interface shutdown                        Disabled
mtu                                       1514
Ingress ACL                               N/A
QoS Trust                                 Disabled
Interface description                     N/A
Interface switching profile               default
Static Multicast Router port for the VLANs N/A
HSL backup interface                      N/A
HSL preemption mode                       off
HSL preemption delay                      100
```

```
MAC-Limit (Action)                          N/A
Port channel member list                    N/A
```

The output of this command includes the following information:

Parameter	Description
Interface MSTP profile	MSTP profile assigned to the port-channel interface.
Interface Ethernet link profile	Ethernet link profile assigned to the port-channel interface.
QoS Profile	QoS profile assigned to the port-channel interface.
Policer Profile	Policer profile assigned to the port-channel interface.
Interface Ingress Mirroring profile	Interface Ingress Mirroring profile assigned to the port-channel interface.
Interface Egress Mirroring profile	Interface Egress Mirroring profile assigned to the port-channel interface.
Interface shutdown	Shows if the port-channel interface has been administratively enabled or disabled
mtu	Maximum Transmission Units in bytes.
Ingress ACL	Access Control List assigned to the port-channel interface.
QoS Trust	Shows if QoS trust mode is enabled or disabled.
Interface description	Description of the interface, if configured.
Interface switching profile	Switching profile assigned to the port-channel interface.
Static Multicast Router port for the VLANs	Lists the VLAN IDs to be used as the multicast router VLAN IDs for IGMP snooping.
HSL backup interface	Hot Standby-Link (HSL) backup interface.
HSL preemption mode	When a primary link goes down, the backup link becomes active. By default, when this link comes back up, it goes into standby mode as the other backup interface is already activated. If preemption mode is enabled for the primary link, the primary interface to become active again once it comes back up. This parameter is disabled by default.
HSL preemption delay	If preemption mode is enabled, this parameter shows the configured preemption delay.
MAC-Limit (Action)	The maximum number of MACs that can be learned on this interface.
Port channel member list	List of port channels members.

Related Command

Command	Description
interface port-channel	This command creates a static port-channel.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-config tunnel

```
show  interface-config tunnel [ethernet <tunnel-id> | ip <tunnel-id>]
```

Description

This command displays the GRE tunnel configuration information.

Syntax

Parameter	Description
`ethernet <tunnel-id>`	Displays the L2 GRE tunnel configuration information for the specified tunnel ID.
`ip <tunnel-id>`	Displays the L3 GRE tunnel configuration information for the specified tunnel ID.

Usage Guidelines

By default, this command shows general information for all the L2 or L3 tunnels based on the parameter specified. Include the **<tunnel-id>** parameter to show detailed information for the specified tunnel.

Examples

The output of the first command in this example shows a list of tunnels. The **References** column lists the number of other profiles with references to the tunnel, and the **Profile Status** column indicates whether the profile is predefined.

The following examples show the detailed configuration settings for the IP tunnel 1.

```
(host) #show interface-config tunnel ip
Tunnel List
-----------
Name  References  Profile Status
----  ----------  --------------
1     0
3     0
7     0
Total:3

(host) #show interface-config tunnel ip 1
Tunnel "1"
----------
Parameter              Value
---------              -----
Tunnel Description     L3 Tunnel
Tunnel Source IP       10.1.30.4
Tunnel Destination IP  10.1.30.100
Ospf-profile           N/A
Tunnel Keepalive       30/6
Tunnel MTU             1100
Tunnel Shutdown        Disabled
```

The output of the command includes the following information:

Parameter	Description
Tunnel Description	Description of the tunnel that was specified while configuring the tunnel.
Tunnel Source IP	Source IP address of the tunnel.
Tunnel Destination IP	Destination IP address of the tunnel.
Ospf-profile	Name of the OSPF profile attached to the tunnel.
Tunnel Keepalive	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.
Tunnel MTU	Maximum Transmission Unit (MTU) size for the interface.
Tunnel Shutdown	Indicates if the hard shutdown of the interface is enabled or disabled.

The following examples show the detailed configuration settings for the ethernet tunnel 2:

```
(host) #show interface-config tunnel ethernet
Tunnel List
-----------
Name  References  Profile Status
----  ----------  --------------
2     0
23    0
Total:2

#show interface-config tunnel ethernet 2
Tunnel "2"
-----------
Parameter                 Value
---------                 -----
Tunnel Description        L2 Tunnel
Tunnel Source IP          10.1.30.4
Tunnel Protocol           0
Inter-Tunnel-Flooding     Enabled
Tunnel Keepalive          N/A
Tunnel Switching Profile  accessvlan100
Tunnel Trusted            Enabled
Tunnel MTU                1100
Tunnel Shutdown           Disabled
```

The output of the command includes the following information:

Parameter	Description
Tunnel Description	Description of the tunnel that was specified while configuring the tunnel.
Tunnel Source IP	Source IP address of the tunnel.
Tunnel Protocol	16-bit Generic Route Encapsulation (GRE) protocol number that uniquely identifies a Layer-2 tunnel.
Inter-Tunnel-Flooding	Indicates if inter-tunnel flooding is enabled or disabled.

Parameter	Description
`Tunnel Keepalive`	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.
`Tunnel Switching Profile`	Name of the Switching profile associated to the tunnel.
`Tunnel Trusted`	Indicates if trusted tunnel is enabled or disabled.
`Tunnel MTU`	Maximum Transmission Unit (MTU) size for the interface.
`Tunnel Shutdown`	Indicates if the hard shutdown of the interface is enabled or disabled.

Related Commands

Command	Description
`interface tunnel ethernet`	This command creates an L2 GRE tunnel.
`interface tunnel ip`	This command creates an L3 GRE tunnel.

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.
ArubaOS 7.3	The **ip** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-config vlan

```
show  interface-config vlan [<vlan-id>]
```

Description

This command displays the interface VLAN configuration information.

Syntax

Parameter	Description
<vlan-id>	VLAN ID

Usage Guidelines

By default, this command shows general information for all ports. Include the **<vlan-id>** parameter to show detailed information for the specified VLAN.

Examples

The output of the first command in this example shows a list of VLANs. The **References** column lists the number of other profiles with references to the VLAN, and the **Profile Status** column indicates whether the profile is predefined. User-defined VLANs will not have an entry in the **Profile Status** column

The second command in this example shows detailed configuration settings for VLAN 1.

```
(host) #show interface-config vlan
vlan List
---------
Name  References  Profile Status
----  ----------  --------------
1     0
Total:1
(host) #show interface-config vlan 100
   vlan "100"
   ----------
   Parameter                   Value
   ---------                   -----
   Interface description       N/A
   Interface OSPF profile      N/A
   Interface PIM profile       N/A
   I+A15nterface IGMP profile      N/A
   Interface DDNS profile      N/A
   Interface VRRP profile      N/A
   Probe Profile               N/A
   Directed Broadcast Enabled  Disabled
   Interface shutdown          Disabled
   Session-processing          Disabled
   metric                      0
   mtu                         1500
   IP Address                  N/A
   IP NAT Inside               Disabled
   IP NAT Outside              Disabled
   IPv6 Address                N/A
   IPv6 link local Address     N/A
   DHCP client                 Disabled
   DHCP relay profile          N/A
```

```
Aruba VPN Pool profile      N/A
Ingress ACL                 N/A
Egress ACL                  N/A
Session ACL                 N/A
```

The output of this command includes the following information:

Parameter	Description
`Interface OSPF profile`	Shows if the OSPF profile has been configured on the Routing Virtual Interface (RVI).
`Interface PIM profile`	Shows if the PIM profile has been configured on the RVI.
`Interface IGMP profile`	Shows if the IGMP profile has been configured on the RVI.
`Interface VRRP profile`	Shows if the VRRP profile is applied on this RVI.
`Directed Broadcast Enabled`	Shows if IP directed broadcast is enabled or not.
`Interface shutdown`	Shows if the VLAN interface has been disabled
`Session-processing`	Shows if session-processing is enabled on the VLAN interface. This is enabled by default.
`mtu`	Maximum transmission units allowed on the VLAN in bytes.
`IP Address`	The IP address of the VLAN interface. This IP address can be manually configured, or the VLAN interface can be configured to automatically get an IP address from the DHCP client.
`IP NAT Inside`	Shows if the IP NAT is enabled on the inside traffic.
`IPv6 Address`	Set Global IPv6 prefix of the interface.
`IPv6 link local Address`	Sets link local IPv6 prefix of interface.
`DHCP client`	Shows if the VLAN has been configured to get its IP address from a DHCP client. If this feature is disabled, the IP address must be manually configured.
DHCP relay profile	Shows if the dhcp relay profile is configured on ther RVI interface.
Ingress ACL	Shows the name of the ACL when an ingress ACL is applied on the VLAN.
Interface description	Description given to the VLAN, if configured.

Related Command

Command	Description
`interface vlan`	This command creates the VLAN interface for the switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3	The following new parameters as part of this show command were introduced: • **Interface VRRP profile** • **Ingress ACL**
ArubaOS 7.4	The following new parameters as part of this show command are introduced: • **Interface description** • **Interface DDNS profile** • **Probe Profile** • **metric** • **IP NAT Outside** • **Aruba VPN Pool profile** • **Egress ACL** • **Session ACL**

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface counters

```
show interface counters
```

Description

Displays a table of L2 interfaces counters.

Syntax

No parameters.

Example

The output of this command displays the following information:

```
(host) #show interface counters
Port                InOctets      InUcastPkts      InMcastPkts      InBcastPkts

GE0/0/0                  123                0                1                0
GE0/0/1               195787                0             1592                0
GE0/0/2               224690              741             1854                4
GE0/0/7               450256              308             3154                0
GE0/0/8               421784               86             3154               61
GE0/0/9               409952                0             3154               26
GE0/0/23                   0                0                0                0


Port               OutOctets     OutUcastPkts     OutMcastPkts     OutBcastPkts

GE0/0/0               195787                0             1592                0
GE0/0/1                  123                0                1                0
GE0/0/2               102037              389              118              131
GE0/0/7               674639              396             5044               31
GE0/0/8               459150              349             3169               12
GE0/0/9               405730                0             3170                0
GE0/0/23              196800                0             1600                0
```

The output of this command includes the following parameters:

Parameter	Description
`Port`	Port number.
`InOctets`	Number of octets received through the port.
`InUcast`	Pkts Number of unicast packets received through the port.
`InMcast`	Pkts Number of multicast packets received through the port.
`InBcast`	Pkts 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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface gigabitethernet

```
show interface gigabitethernet <slot/module/port> [counters|statistics|switchport
[brief|detail|extensive]|transceiver [detail]]
```

Description

Issue this command to display information about a specified Gigabit Ethernet port.

Syntax

Parameter	Description
`<slot/module/port>`	The slot, module and port numbers of the interface.
`counters`	Displays the counters for the specified interface.
`statistics`	Displays the statistics for the specified interface.
`switchport <brief|detail|extensive>`	Displays the interface information. • **brief**: Provides a brief information on the specified Gigabit ethernet interface. • **detail**: Provides a more detailed information on the specified Gigabit ethernet interface. • **extensive**: Provides an extensive information on the specified Gigabit ethernet interface.
`transceiver [detail]`	Displays the interface transceiver information. • **detail**: Displays L2 fiber transceiver diagnostic information.

Usage Guidelines

By default, this command displays detailed interface information. Include the optional counters or statistics parameters to display only counters and statistics data.

Examples

The output of this command displays the following information:

```
(host) (config) #show interface gigabitethernet 1/0/24

GE1/0/24 is administratively Up, Link is Down, Line protocol is Down
Hardware is Gigabit Ethernet, Interface is GE1/0/24, Address is 00:0b:86:6a:2f:da
Encapsulation ARPA, Loopback not set
Configured: duplex (Auto), Speed (Auto), FC (Off), Autoneg (On)
Auto negotiation in progress
Interface index: 169
MTU 1514 bytes
Link flaps: 1
Flags: Trunk, Trusted
Port shutdown reason : BPDU received
Link status last changed:       0d 00:00:00 ago
Last update of counters:        0d 00:00:00 ago
Last clearing of counters:      0d 00:00:00 ago
Statistics:
       Received 240 frames, 31806 octets
       0 pps, 0 bps
       0 unicast, 240 multicast, 0 broadcast
```

```
        0 runts, 0 giants, 0 throttles
        0 error octets, 0 CRC frames
        Transmitted 307 frames, 29461 octets
        0 pps, 0 bps
```

The following command displays the tranceiver details for the specified interface:

```
(host) #show interface gigabitethernet 0/1/0 transceiver detail
Vendor Name                                 : OPNEXT INC
Vendor Serial Number                        : L12J55161
Vendor Part Number                          : TRF2716AALB465
Aruba Supported                             : YES
Cable Type                                  : 1000BASE-SX
Connector Type                              : LC
Wave Length                                 : 850 nm
Last update of transceiver information      : 4 hours 41 min 50 sec
Module          Low Warning     Low Alarm       High Warning    High Alarm
Temperature     Threshold       Threshold       Threshold       Threshold
------------    ------------    ------------    ------------    ------------
37 C /          -10 C /         -15 C /         80 C /          85 C /
98.60 F         14.00 F         5.00 F          176.00 F        185.00 F
Low             Low             High            High
Warning         Alarm           Warning         Alarm
------------    ------------    ------------    ------------
Inactive        Inactive        Inactive        Inactive
Module          Low Warning     Low Alarm       High Warning    High Alarm
Voltage         Threshold       Threshold       Threshold       Threshold
------------    ------------    ------------    ------------    ------------
3404 mV         3100 mV         3000 mV         3500 mV         3600 mV
Low             Low             High            High
Warning         Alarm           Warning         Alarm
------------    ------------    ------------    ------------
Inactive        Inactive        Inactive        Inactive
Laser Bias      Low Warning     Low Alarm       High Warning    High Alarm
Current         Threshold       Threshold       Threshold       Threshold
------------    ------------    ------------    ------------    ------------
4 mA            1 mA            1 mA            14 mA           15 mA
Low             Low             High            High
Warning         Alarm           Warning         Alarm
------------    ------------    ------------    ------------
Inactive        Inactive        Inactive        Inactive
Laser TX        Low Warning     Low Alarm       High Warning    High Alarm
Power           Threshold       Threshold       Threshold       Threshold
------------    ------------    ------------    ------------    ------------
0.279 mW /      0.089 mW /      0.070 mW /      0.631 mW /      0.794 mW /
-5.54 dBM       -10.51 dBM      -11.55 dBM      -2.00 dBM       -1.00 dBM
Low             Low             High            High
Warning         Alarm           Warning         Alarm
------------    ------------    ------------    ------------
Inactive        Inactive        Inactive        Inactive
Laser RX        Low Warning     Low Alarm       High Warning    High Alarm
Power           Threshold       Threshold       Threshold       Threshold
------------    ------------    ------------    ------------    ------------
0.000 mW/       0.015 mW/       0.012 mW/       1.258 mW/       1.584 mW/
-40.00 dBM      -18.24 dBM      -19.21 dBM      1.00 dBM        2.00 dBM
Low             Low             High            High
Warning         Alarm           Warning         Alarm
------------    ------------    ------------    ------------
Active          Active          Inactive        Inactive
```

Parameter	Description
`GE <port> is...`	Shows if the port has been administratively enabled or disabled.
`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.
`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.
`Interface index`	Unique identifier for the interface useful in debugging.
`MTU bytes`	MTU size of the specified port in bytes.
`Port shutdown...`	Displays the reason for the port shutdown.
`link status last changed...`	Time since the link status changed.
`Last update of counters`	Time since the counters were updated. All current counters related to the specified port are listed in the output of this command.

Parameter	Description
`Last clearing of counters`	Time since the counters were cleared.
`Statistics`	Counters and statistics for received and transmitted data: Received statistics: • frames: Number of data frames received. • octets: Bytes of data received. • broadcasts: Number of broadcast frames received. • runts: Number of packets discarded because they were smaller than the minimum required packet size. • giants: Number of packets discarded because they were larger than the maximum required packet size. • throttles: Number of times the neighbouring interface has sent 802.3 flow control frames. • error octets: Bytes of data that had errors. • CRC frames: Number of frames with Cyclic redundancy check errors. • multicast: Number of multicast frames. • unicast: Number of unicast frames. Transmitted statistics: • frames: Number of data frames sent. • octets: Bytes of data sent. • broadcasts: Number of broadcast frames sent. • throttles: Number of times the interface's input buffers were exceeded. • errors octets: Bytes of data that had errors. • deferred: Number of deferred packets. • collisions: Number of collisions on this Ethernet segment. • late collisions: Number of collision errors that occurred after the first 512 bit times of data were transmitted.
`POE Information`	The Power-Over-Ethernet (POE) status of the specified port. For additional information on these output parameters, see show poe interface.

Related Commands

Command	Description
`interface gigabitethernet`	This command configures a Gigabit Ethernet port on the switch.
`show poe` `show poe interface`	These commands display PoE information for the switch or the switch interfaces.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3	Introduced **detail** sub-parameter under **transceiver** parameter.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-group-config gigabitethernet

```
show interface-group-config gigabitethernet [<group-name>]
```

Description

This command displays the interface group configuration information.

Syntax

Parameter	Description
<group-name>	Name of the interface group.

Usage Guidelines

By **default**, this command displays the entire list of Ethernet interface group configurations, including the configuration status and the number of references to each configuration. Include a configuration name to display detailed information for that interface group configuration.

Examples

The first example below shows that the switch has three Gigabit Ethernet interface group configurations. The **References** column lists the number of other profiles with references to the interface group, and the **Profile Status** column indicates whether the group is predefined. User-defined groups will not have an entry in the **Profile Status** column.

The second example shows current configuration settings for the **default** Gigabit Ethernet interface group.

```
(host) #show interface-group-config gigabitethernet
gigabitethernet List
--------------------
Name      References  Profile Status
----      ----------  --------------
default   2
Mgt       1
TechPubs  1
Total:3

(host) #show interface-group-config gigabitethernet default
gigabitethernet "default"
-------------------------
Parameter                                 Value
---------                                 -----
Interface group members                   ALL
Interface MSTP profile                    default
Interface Tunneled Node profile           N/A
Interface VOIP profile                    N/A
Interface LLDP profile                    lldp-factory-initial
Interface PoE profile                     poe-factory-initial
Interface Ethernet link profile           default
Interface LACP profile                    N/A
QoS Profile                               N/A
Policer Profile                           N/A
Interface AAA profile                     N/A
Interface Ingress Mirroring profile       N/A
Interface Egress Mirroring profile        N/A
Interface shutdown                        Disabled
```

```
mtu                                             1514
Ingress ACL                                     N/A
QoS Trust                                       Disabled
Interface switching profile                     default
Static Multicast Router port for the VLANs      N/A
Interface Trusted/Untrusted                     Trusted
MAC-Limit (Action)                              N/A
```

The output of this command includes the following information:

Parameter	Description
Interface group members	The memeber interfaces of the group.
Interface MSTP Profile	The MSTP profile applied to the interface group configuration.
Interface Tunneled Node Profile	The Tunneled Node profile applied to the interface group configuration.
Interface VOIP Profile	The VoIP profile applied to the interface group configuration.
Interface LLDP Profile	The LLDP profile applied to the interface group configuration.
Interface PoE Profile	The PoE profile applied to the interface group configuration.
Interface Ethernet Link Profile	The Ethernet Link profile applied to the interface group configuration.
Interface LACP Profile	The LACP profile applied to the interface group configuration.
QoS Profile	The QoS profile applied to the interface group configuration.
Policer Profile	The Policer profile applied to the interface group configuration.
Interface AAA Profile	The AAA profile applied to the interface group configuration.
Interface Ingress Mirroring Profile	If port mirroring is enabled, this feature can send copies of all or sampled packets seen on specific port (s) or port-channel to a destination. This parameter displays the ingress mirroring profile for the interface group configuration.
Interface Egress Mirroring Profile	If port mirroring is enabled, this feature can send copies of all or sampled packets seen on specific port (s) or port-channel to a destination. This output parameter displays the egress mirroring profile for the interface group configuration.
Interface Shutdown	Shows if the interface has been disabled in the group configuration.
MTU	Maximum Transmission Unit (MTU) value configured in bytes.

Parameter	Description
Ingress ACL	Ingress Access Control List (ACL) configured for the interface group configuration.
QoS Trust	Shows if the QoS Trust Mode is enabled on this interface group configuration.
Interface Switching Profile	The Switching profile applied to the interface group configuration.
Static Multicast Router port for the VLAN	In IGMP snooping proxy mode, you can enable suppressing reports to multicast router ports. This parameter shows the VLAN ID configured as the multicast router VLAN IDs for IGMP snooping.
Interface Trusted/Untrusted	Shows if trusted mode is enabled for the interface.
MAC-Limit (Action)	The maximum number of MACs that can be learned on this interface.

Related Command

Command	Description
interface-group gigabitethernet	This command applies the same configuration parameters to a group of Gigabit Ethernet interfaces.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface local-mgmt

```
show interface local-mgmt member <member-id>
```

Description

This command displays the local management interface information.

Syntax

Parameter	Description
`member <member-id>`	Specifies the member id (0–7).

Example

The output of this command displays the following information:

```
(host)# show interface local-mgmt member-id 3

Member-id: 3
------------
Ip/Mask          Gateway       Admin   Operational  Link
-------          -------       -----   -----------  ----
10.16.56.144/24  10.16.56.254  Enable  Up           Up
```

The output of this command includes the following parameters:

Parameter	Description
`Ip/Mask`	Interface IP address or the Interface netmask.
`Gateway`	Displays the gateway IP address of the interface.
`Admin`	Dispalys the admin status.
`Operational`	Displays the operational status.
`Link`	Displays the status of the interface link.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface loopback

```
show interface loopback <0-63>
```

Description

This command displays the loopback interface information.

Syntax

Parameter	Description
<0-63>	Specifies the loopback interface identification number.

Example

The output of this command displays the following information:

```
(host)# show interface loopback 1
loopback1 is administratively Up, Line protocol is Up
Hardware is Ethernet, Address is 00:0b:86:6b:57:80
Description: Loopback
Internet address is unassigned
Interface index: 100663297
MTU 1514 bytes
```

Related Command

Command	Description
interface loopback	This command configures a loopback interface.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface mgmt

```
show interface mgmt
```

Description

This command displays the management interface information.

Syntax

No parameters.

Example

The output of this command displays the following information:

```
(host) #show interface mgmt
mgmt is administratively Up, Link is Up
Hardware is Ethernet, Address is 00:0b:86:6a:42:01
Internet address is 10.16.48.28, Netmask is 255.255.255.0
Global Unicast address(es) :
IPV6 link-local address is fe80::20b:86ff:fe6a:4e00
Negotiated: duplex (Full), Speed (100 Mbps)
Interface index: 83886080
```

The output of this command includes the following parameters:

Parameter	Description
`mgmt`	Status of the management port
`Link`	Shows if the link is currently up or down
`Hardware`	Status of the interface hardware
`Address`	MAC address of the interface
`Internet Address`	Interface IP address
`Netmask`	Interface netmask
`Negotiated`	Negotiated transfer operation and speed
`Interface index`	Index number of the interface

Related Command

Command	Description
`interface mgmt`	This command configures the management port on the switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface port-channel

```
show interface port-channel
<id> {counters|statistics|switchport [brief|detail|extensive]}
all
auto-lacp
```

Description

This command displays the configuration, current status, and statistics for the specified port channel.

Syntax

Parameter	Description
`<id>`	Displays port-channel for a particular ID. This parameter has the following sub-parameters: • **counters**: Displays the layer 2 interface counters information. • **statistics**: Displays the layer 2 interface statistics information. • **switchport**: Displays the layer 2 information of the port channel in brief, detail, or extensive. Range: 0-63.
`all`	Displays all port-channels on the Mobility Access Switch.
`auto-lacp`	Displays auto LACP port-channel interfaces.

Example

The following command displays the details of port-channel 1:

```
(host) #show interface port-channel 1
  port-channel 1 is administratively Up, Link is Down, Line protocol is Down
  Hardware is Port-Channel, Address is 00:0b:86:6a:f2:40
  Description: Link Aggregate
  Member port(s):
  Speed: 0 Mbps
  Interface index: 1442
  MTU 1514 bytes
  Flags: Access, Trusted
  Link status last changed: 0d 00h:00m:00s ago
  Last clearing of counters: 0d 00h:00m:00s ago
  Statistics:
  Received 0 frames, 0 octets
  0 pps, 0 bps
  0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 error octets, 0 CRC frames
  0 multicast, 0 unicast
  Transmitted 0 frames, 0 octets
  0 pps, 0 bps
  0 broadcasts, 0 throttles
  0 errors octets, 0 deferred
  0 collisions, 0 late collisions
```

The following command shows auto-LACP port channel interfaces:

```
(host) #show interface port-channel auto-lacp

port-channel 1 is administratively Up, Link is Up, Line protocol is Down
Hardware is Port-Channel, LACP enabled, Address is 00:1a:1e:0d:c2:40
```

```
Description: Link Aggregate
Created by Auto-LACP Link Aggregate
Member port(s):
   GE1/0/15 is administratively Up, Link is Up, Line protocol is Up (LACP-I)
   GE3/0/15 is administratively Up, Link is Up, Line protocol is Up (LACP-I)
Speed: 0 Mbps
Interface index: 1442
MTU 1514 bytes
Flags: Access, Trusted
Link status last changed: 0d 02h:27m:43s ago
Last clearing of counters: 0d 02h:27m:43s ago
Statistics:
   Received 0 frames, 0 octets
   9 pps, 5.099 Kbps
   0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 error octets, 0 CRC frames
   0 multicast, 0 unicast
   Transmitted 0 frames, 0 octets
   33 pps, 17.848 Kbps
   0 broadcasts, 0 throttles
   0 errors octets, 0 deferred
   0 collisions, 0 late collisions

GE1/0/15:
Statistics:
   Received 59296 frames, 4004034 octets
   7 pps, 3.743 Kbps
   57754 broadcasts, 0 runts, 0 giants, 0 throttles
   0 error octets, 0 CRC frames
   296 multicast, 1246 unicast
   Transmitted 192317 frames, 13107032 octets
   24 pps, 12.761 Kbps
   180045 broadcasts, 0 throttles
   0 errors octets, 0 deferred
   0 collisions, 0 late collisions

GE3/0/15:
Statistics:
   Received 60620 frames, 4196064 octets
   2 pps, 1.356 Kbps
   58004 broadcasts, 0 runts, 0 giants, 0 throttles
   0 error octets, 0 CRC frames
   434 multicast, 2182 unicast
   Transmitted 197228 frames, 13639397 octets
   9 pps, 5.087 Kbps
   182523 broadcasts, 0 throttles
   0 errors octets, 0 deferred
   0 collisions, 0 late collisions
```

Related Command

Command	Description
interface port-channel	This command creates a static port-channel.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1	The **switchport** parameter was introduced.
ArubaOS 7.4.1.1	The **auto-lacp** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-profile

```
show interface-profile {dhcp-relay-profile|enet-link-profile|igmp-profile|lacp-profile|lldp-profile|mirroring-profile|mstp-profile|poe-profile|pvst-port-profile|switching-profile|tunneled-node-profile|voip-profile}
```

Description

This command displays a list of of interface profiles for the specified profile type.

Syntax

Parameter	Description
`dhcp-relay-profile`	Displays all the dhcp relay profiles
`enet-link-profile`	Displays all the Ethernet Link profiles.
`gvrp-profile`	Displays all the GVRP profiles.
`igmp-profile`	Displays an interface IGMP profile.
`lacp-profile`	Displays an LACP profile.
`lldp-profile`	Displays an LLDP profile.
`mirroring-profile`	Displays all the mirroring profile.
`mstp-profile`	Displays the interface of the MSTP.
`oam-profile`	Displays all the OAM profiles.
`ospf-profile`	Displays all the OSPF profiles.
`pim-profile`	Displays all thePIM profiles.
`poe-profile`	Displays all the Power over Ethernet profiles.
`port-security-profile`	Displays all the port security profiles.
`pvst-port-profile`	Displays an interface PVST bridge.
`switching-profile`	Displays a switching profile.
`tunneled-node-profile`	Displays a tunneled node server profile.
`voip-profile`	Displays a VOIP profile

Example

The output of the command in this example shows a list of parameters for MSTP profiles and their values.

```
(host) (config) #show interface-profile mstp-profile bpdu-guard

Interface MSTP "bpdu-guard"
---------------------------
Parameter                          Value
---------                          -----
Instance port cost                 N/A
```

```
Instance port priority                N/A
Enable point-to-point                 Disabled
Enable portfast                       Disabled
Enable rootguard                      Enabled
Enable loopguard                      Disabled
Enable bpduguard                      Enabled
Enable bpduguard auto recovery time   N/A
```

Related Commands

Command	Description
show profile-list interface-profile	This command displays a list of of interface profiles for the specified profile type.
show interface-profile switching-profile	This command displays the specified switching profile configuration information.
show interface-profile voip-profile	This command displays the specified VOIP profile configuration information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-profile ddns-profile

```
show interface-profile ddns-profile <profile-name>
```

Description

This command displays the DDNS profile configuration information.

Syntax

Parameter	Description
<profile-name>	Name of the profile.

Usage Guidelines

By default, this command displays the entire list of DDNS profiles, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Example

The following example displays the configuration details of the ddns-profile ddns1

```
(host) # show interface-profile ddns-profile ddns1
DDNS profile "ddns1"
--------------------
Parameter                                   Value
---------                                   -----
configured username                         John
configured password                         ******
Configured update interval [D:H:M]          0:7:0
configured service-url                      dynupdate.no-ip.com/nic/update
configured hostname                         arubamas.no-ip.info
```

Related Command

Command	Description
interface-profile ddns-profile	This command creates a dynamic DNS profile that can be assigned to any interface or interface group.

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-profile lacp-profile

```
show interface-profile lacp-profile <profile-name>
```

Description

This command displays the specified LACP profile configuration information.

Syntax

Parameter	Description
<profile-name>	Name of the profile.

Usage Guidelines

By default, this command displays the entire list of LACP profiles, 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 first example below shows that the switch has two LACP profiles. The References column lists the number of other profiles with references to the interface group, and the Profile Status column indicates whether the profile is predefined. User-defined groups will not have an entry in the Profile Status column.

The second example below shows the current settings for the LACP profile **profile2**.

```
(host) #show interface-profile lacp-profile
LACP List
---------
Name      References  Profile Status
----      ----------  --------------
profile1  2
profile2  0
Total:1

(host) #show interface-profile lacp-profile profile2
LACP "profile2"
---------------
Parameter         Value
---------         -----
Group identifier  65535
Priority          255
Mode              passive
Timeout           long
```

The output of this command includes the following information:

Parameter	Description
`Group identifier`	Identifies the port-channel group ID.
`Priority`	Specifies the port priority for the port-channel interface.
`mode`	Sets the LACP port-channel to one of the following modes: • **active**—In active mode, a port-channel member can send participation requests to other ports in the port-channel. • **passive**—In passive, a port-channel member does not send participation requests to other ports. It can only receive and accept participation codes from other members.
`timeout`	Specifies the time timeout as long or short: • **long**—90 seconds. • **short**—3 seconds.

Related Command

Command	Description
`interface-profile lacp-profile`	This command creates a dynamic LACP port-channel profile that can be assigned to any interface or interface group.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-profile lldp-profile

```
show interface-profile lldp-profile [<profile-name>]
```

Description

This command displays the specified Link Layer Discovery Protocol (LLDP) profile configuration information.

Syntax

Parameter	Description
<profile-name>	Name of the LLDP profile.

Usage Guidelines

Link Layer Discovery Protocol (LLDP), defined in the IEEE 802.1AB standard, is a Layer 2 protocol that allows network devices to advertise their identity and capabilities on the LAN. The switch supports simple one-way neighbor discovery protocol with periodic transmissions of LLDP PDUs.

By default this command displays the entire list of LLDP profiles, 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 first example below shows that the switch has three LLDP profiles. The **References** column lists the number of other profiles with references to the LLDP 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.

The second example shows current configuration settings for the LLDP profile **profile3**.

```
(host) #show interface-profile lldp-profile profile
LLDP Profile List
-----------------
Name                  References  Profile Status
----                  ----------  --------------
default               3
lldp-factory-initial  1
profile3              0
Total:3

(host) #show interface-profile lldp-profile profile3
LLDP Profile "profile3"
-------------------
Parameter                              Value
---------                              -----
LLDP pdu transmit                      Disabled
LLDP protocol receive processing       Disabled
Port Description TLV                   Enabled
System Name TLV                        Enabled
System Description TLV                 Enabled
System Capabilities TLV                Enabled
Management Address TLV                 Enabled
Port VlanID TLV                        Enabled
Vlan Name TLV                          Enabled
Aggregation Status TLV                 Enabled
MAC/PHY configuration TLV              Enabled
Maximum Frame Size TLV                 Enabled
```

```
Power Via MDI TLV                         Enabled
Network Policy TLV                        Enabled
Extended Power Via MDI TLV                Enabled
LLDP transmit interval (Secs)             30
LLDP transmit hold multiplier             4
LLDP fast transmit interval (Secs)        1
LLDP fast transmit counter                4
LLDP-MED protocol                         Disabled
Control proprietary neighbor discovery    Disabled
```

The output of this command includes the following information:

Parameter	Description
`LLDP pdu transmit`	Shows if LLDP Protocol Data Unit (PDU) transmission is enabled or disabled.
`LLDP protocol receive processing`	Shows if LLDP Protocol Data Unit (PDU) receive is enabled or disabled.
`LLDP transmit interval (Secs)`	The LLDP transmit interval, in seconds.
`LLDP transmit hold multiplier`	The LLDP transmit hold multiplier.
`LLDP fast transmit interval (Secs)`	The LLDP fast transmission interval, in seconds.
`LLDP fast transmit counter`	Number of the LLDP data units sent each time fast LLDP data unit transmission is triggered.
`LLDP-MED protocol`	Enables the LLDP MED protocol.
`Control proprietary neighbor discovery`	Shows if receiving of proprietary neighbor protocol packets is enabled. **NOTE:** This release of Mobility Access Switch supports Cisco Discovery Protocol (CDP).

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-profile mirroring-profile

```
show interface-profile mirroring-profile <profile-name>
```

Description

This command displays information about the port mirroring profile and its configuration.

Syntax

Parameter	Description
`<profile-name>`	Name of the profile.

Usage Guidelines

By default, this command displays the name of the current mirroring-profile. The **References** column lists the number of other profiles with references to the mirroring 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.

Include the optional **`<profile-name>`** parameter to view configuration details for the mirroring profile.

Examples

The output of the command in the first example below shows that the current mirroring-profile is named profile1. The output of the second command shows that the mirroring profile has defined port **0/0/3** as the destination port to which the packets should be sent.

```
(host) #show interface-profile mirroring-profile
Mirroring profile List
----------------------
Name      References  Profile Status
----      ----------  --------------
profile1  2
Total:1


(host) #show interface-profile mirroring-profile profile1
Mirroring profile "profile1"
---------------------------
Parameter             Value
---------             -----
gigabitethernet       0/0/3

Port mirroring ratio 1
```

The output of this command includes the following information:

Parameter	Description
`gigabitethernet`	Destination port to which the packets should be sent.
`Port mirroring ratio`	Ratio of packets that should be mirrored. • 0—Does not mirror any packet to the destination. • 1—Mirrors all packets to the destination (1:1). This is the default. • 100—Mirrors 1 out of 100 packets to the destination. • 2047—Mirrors 1 out of 2,047 packets to the destination.

Related Command

Command	Description
interface-profile mirroring-profile	This command creates a mirroring profile that can be assigned to any interface or interface group.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-profile mstp-profile

```
show interface-profile mstp-profile <profile-name>
```

Description

View the interface MSTP configuration.

Syntax

Parameter	Description
<profile-name>	Enter the name of the profile.

Example

The following example displays the listing of the interface MSTP profile names.

```
(host) #show interface-profile mstp-profile bpdu-guard
  Interface MSTP "bpdu-guard"
  ---------------------------
  Parameter                     Value
  ---------                     -----
  Instance port cost            N/A
  Instance port priority        N/A
  point-to-point                Disabled
  portfast                      Disabled
  portfast on trunk             Disabled
  rootguard                     Disabled
  loopguard                     Disabled
  bpduguard                     Enabled
  bpduguard auto recovery time  N/A
  bpdufilter unconditional      Disabled
  bpdufilter default            Disabled
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

show interface-profile oam-profile

```
show interface-profile oam-profile <profile-name>
```

Description

This command displays the name and configuration setting of the specified oam-profile.

Syntax

Parameter	Description
<profile-name>	Name of the profile.

Usage Guidelines

By default, this command lists the configured OAM profiles, including the status and the number of references for each. Include the profile name to display detailed information of a specific OAM profile.

Examples

The first example below shows that the OAM profile is named **oamtest**, and that there are three other profiles with references to the OAM profile. The Profile Status column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
OAM profile List
----------------
Name     References  Profile Status
----     ----------  --------------
oamtest  3
Total:1
```

The second example shows configuration details for **oamtest**.

```
(host) (config) #show interface-profile oam-profile oamtest

OAM profile "oamtest"
------------------
Parameter                        Value
---------                        -----
OAM discovery mode               active
OAM remote-loopback              Disabled
OAM local-loopback               Enabled
OAM PDU rate (PDU per second)    8
OAM link-fault timeout (seconds) 3
OAM link-fault action            syslog
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config mode (config)

show interface-profile ospf-profile

```
show interface-profile ospf-profile [default | <profile-name>]
```

Description

View the specified OSPF interface profile.

Syntax

Parameter	Description
`default`	Display the default OSPF profile configuration.
`<profile-name>`	Display the specified OSPF profile configuration.

Usage Guidelines

Use this command to view the specified OSPF profile configuration parameters.

Examples

The following show command displays the name of the configured OSPF interface profiles.

```
(host) (config) #show interface-profile ospf-profile

Interface OSPF profile List
---------------------------
Name       References  Profile Status
----       ----------  --------------
default    0
techpubs   0
Total:2
```

The following show command displays the details of the OSPF profile named “default.”

```
(host) (config) #show interface-profile ospf-profile default

Interface OSPF profile "default"
--------------------------------
Parameter             Value
---------             -----
Area                  0.0.0.0
Cost                  1
Dead-interval         40
Hello-interval        10
Retransmit-interval   5
Transmit-delay        1
Priority              1
State                 Enabled
```

Related Command

Command	Description
show router ospf	View the global OSPF profile configuration.

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode.

show interface-profile port-security-profile

```
show interface-profile port-security-profile <profile name>
```

Description

This command displays the details of the port security profile on an interface.

Syntax

Parameter	Description
`<profile name>`	Enter the name of the profile that you want to view.

Example

From ArubaOS 7.4.0.2, the output of this show command includes details about the **Sticky MAC Action** and the **Sticky MAC Auto Recovery Time** parameters as well.

```
(host) #show interface-profile port-security-profile profile1stky
Port security profile "profile1stky"
-----------------------------------
Parameter                              Value
---------                              -----
IPV6 RA Guard Action                   N/A
IPV6 RA Guard Auto Recovery Time       N/A
MAC Limit                              N/A
MAC Limit Action                       N/A
MAC Limit Auto Recovery Time           N/A
Sticky MAC                             Enabled
Sticky MAC Action                      Shutdown

Sticky MAC Auto Recovery Time          10 Seconds

Trust DHCP                             No
Port Loop Protect                      N/A
Port Loop Protect Auto Recovery Time   N/A
IP Source Guard                        N/A
Dynamic Arp Inspection                 N/A
```

Also, starting fromArubaOS 7.4.1.1, the **show interface-profile port-security-profile** command displays the status of the proxy ARP.

```
(host) #show interface-profile port-security-profile PARP
Port security profile "PARP"
----------------------------
Parameter                             Value
---------                             -----
IPV6 RA Guard Action                  N/A
IPV6 RA Guard Auto Recovery Time      N/A
MAC Limit                             N/A
MAC Limit Action                      N/A
MAC Limit Auto Recovery Time          N/A
Sticky MAC                            Disabled
Sticky MAC Action                     N/A
Sticky MAC Auto Recovery Time         N/A
Trust DHCP                            No
Port Loop Protect                     N/A
Port Loop Protect Auto Recovery Time  N/A
```

```
IP Source Guard                 N/A
Dynamic Arp Inspection          N/A
Proxy Arp                       Enabled
```

Related Command

Command	Description
interface-profile port-security-profile	Specify a name for your port security profile.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.4	The **Dynamic Arp Inspectio**n, **IP Source Guard**, and **Sticky MAC** parameters were introduced.
ArubaOS 7.4.0.2	The **Sticky MAC Action** and **Sticky MAC Auto Recovery Time** parameters in the output were introduced.
ArubaOS 7.4.1.1	The status of **Proxy ARP** was introduced in the command output .

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode (config)

show interface-profile pvst-port-profile

```
show interface-profile pvst-port-profile <profile name>
```

Description

Display the details of the interface PVST+ port profile.

Syntax

Parameter	Description
`<profile name>`	Enter the name of the profile that you want to view.

Example

```
(host) #show interface-profile pvst-port-profile TechPubs
Interface PVST bridge "TechPubs"
--------------------------------
Parameter                      Value
---------                      -----
Instance port cost             N/A
Instance port priority         N/A
point-to-point                 Enabled
portfast                       Disabled
portfast on trunk              Disabled
rootguard                      Disabled
loopguard                      Disabled
bpduguard                      Disabled
bpduguard auto recovery time   N/A
bpdufilter unconditional       Disabled
bpdufilter default             Disabled
```

Related Command

Command	Description
vlan-profile pvst-profile	Specify a name for your PVST+ profile.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode (config)

show interface-profile switching-profile

```
show interface-profile switching-profile [<profile-name>]
```

Description

This command displays the specified switching profile configuration.

Syntax

Parameter	Description
`<profile-name>`	Name of the switching profile.

Usage Guidelines

By default, this command displays the entire list of switching profiles, including the profile status and the number of references to each profile. Include a switching profile name to display detailed information for that profile's configuration.

Examples

The first example below shows that the switch has three switching profiles. The **References** column lists the number of other profiles with references to the switching profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined groups will not have an entry in the **Profile Status** column.

The second example shows configuration details for the switching profile **upstream-profile**.

```
(host) #show interface-profile switching-profile
switching profile List
----------------------
Name              References  Profile Status
----              ----------  --------------
default           4
profile5          0
Upstream-profile  1
Total:3

(host) #show interface-profile switching-profile Upstream-profile
switching profile "Upstream-profile"
-----------------------------------
Parameter                                          Value
---------                                          -----
Switchport mode                                    trunk
Access mode VLAN                                   1
Trunk mode native VLAN                             1
Enable broadcast traffic rate limiting             Enabled
Enable multicast traffic rate limiting             Disabled
Enable unknown unicast traffic rate limiting       Enabled
Max allowed rate limit traffic on port in percentage  50
Trunk mode allowed VLANs                           1-4094
```

The output of this command includes the following information:

Parameter	Description
`Switchport mode`	Shows whether the switch port is configured to be an access or trunk port • **access** mode—Configures the port to be an access port. • **trunk** mode—Configures the port to be a trunk port.
`Access mode VLAN`	The access VLAN ID.
`Enable broadcast traffic rate limiting`	Shows if the storm control feature has been enabled for broadcast traffic.
`Enable multicast traffic rate limiting`	Shows if the storm control feature has been enabled for multicast traffic.
`Enable unknown unicast traffic rate limiting`	Shows if the storm control feature has been enabled for unknown unicast traffic.
`Max allowed rate limit traffic on port in percentage`	The level of storm control, shown as a percentage of total interface speed. Range is 50 to100%.
`Trunk mode allowed VLANs`	Range of allowed VLANs on the trunk port.

Related Command

Command	Description
`interface-profile switching-profile`	This command is used to create a switching profile.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-profile tunneled-node-profile

```
show interface-profile tunneled-node-profile <profile-name>
```

Description

This command displays the name and configuration settings of the current tunneled node profile.

Syntax

Parameter	Description
`<profile-name>`	Name of the profile.

Usage Guidelines

By default, this command displays the name of the current tunneled node profile, including the status and the number of references to the tunneled node profile. Include the profile name to display detailed information for that tunneled node profile.

Example

The first example below shows that the tunneled node profile is named **tunnel1**, and that there are three other profiles with references to the tunneled node profile. The **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the **Profile Status** column.)

The second example shows configuration details for the current tunneled node profile.

```
(host) #show interface-profile tunneled-node-profile
Tunneled Node Server profile List
---------------------------------
Name    References  Profile Status
----    ----------  --------------
tunnel1 3
Total:1

(host)# show interface-profile tunneled-node-profile tunnel1
Tunneled Node Server profile "tunnel1"
Parameter                    Value
---------                    -----
Controller IP Address        1.1.1.1
Backup Controller IP Address 2.2.2.1
Keepalive timeout in seconds 10

MTU on path to controller 1400
```

The output of this command includes the following information:

Command	Description
`Controller IP Address`	Specifies the IP address of the controller.
`Keepalive timeout in seconds`	Specifies the keepalive time in seconds.
`MTU on path to controller`	Specifies the MTU on the path to the controller.

Related Command

Command	Description
interface-profile tunneled-node-profile	This command creates a tunneled node profile that can be applied to any interface.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface-profile voip-profile

```
show interface-profile voip-profile [<profile-name>]
```

Description

This command displays the specified VoIP profile configuration information.

Syntax

Parameter	Description
`<profile-name>`	Name of the profile.

Usage Guidelines

By default, this command displays the entire list of VoIP profiles, including the profile status and the number of references to each VoIP profile. Include a VoIP profile name to display detailed information for that profile's configuration.

Examples

The first example below shows that the switch has one VoIP profile. The **References** column lists the number of other profiles with references to the VoIP profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined groups will not have an entry in the **Profile Status** column.

The second example shows configuration details for the VoIP profile.

```
(host) #show interface-profile voip-profile
VOIP profile List
-----------------
Name      References  Profile Status
----      ----------  --------------
profile7  0
Total:1

(host) #show interface-profile voip-profile profile7
VOIP profile "profile7"
-----------------------
Parameter  Value
---------  -----
VOIP VLAN  1
DSCP       0
802.1 UP   0
VOIP Mode  auto-discover
```

The output of this command includes the following information:

Parameter	Description
`VOIP VLAN`	The Voice VLAN ID.
`DSCP`	The DSCP value for the voice VLAN.
`802.1 UP`	The 802.11p priority level.
`VOIP Mode`	The mode of VoIP operation. It can be auto-discover or static.

Related Command

Command	Description
interface-profile voip-profile	This command creates a VoIP profile that can be applied to any interface, interface group, or a port-channel.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1.3	`VOIP Mode` parameter is added.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface status

```
show interface status
```

Description

This command displays the status of the interface.

Syntax

No parameters.

Example

The output of this command displays the following information:

```
(host) #show interface status

Port      Name   Status       Vlan   Duplex   Speed     Type
----      ----   ------       ----   ------   -----     ----
GE0/0/0          connected    1      a-full   a-1 Gbps  10/100/1000Base-T
GE0/0/1          connected    1      a-full   a-1 Gbps  10/100/1000Base-T
GE0/0/2          connected    13     a-full   a-1 Gbps  10/100/1000Base-T
GE0/0/3          notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/4          disabled     1      auto     auto      10/100/1000Base-T
GE0/0/5          notconnect   -      auto     auto      10/100/1000Base-T
GE0/0/6          notconnect   -      auto     auto      10/100/1000Base-T
GE0/0/7          connected    13     full     1 Gbps    10/100/1000Base-T
GE0/0/8          connected    13     full     1 Gbps    10/100/1000Base-T
GE0/0/9          connected    13     full     1 Gbps    10/100/1000Base-T
GE0/0/10         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/11         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/12         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/13         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/14         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/15         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/16         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/17         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/18         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/19         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/20         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/21         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/22         notconnect   1      auto     auto      10/100/1000Base-T
GE0/0/23         connected    100    a-full   a-1 Gbps  10/100/1000Base-T
GE0/1/0          notconnect   1      n/a      n/a       1000/10000Invalid
GE0/1/1          notconnect   1      n/a      n/a       1000/10000Invalid
Pc0              connected    13     full     3 Gbps    10/100/1000Base-T
MGMT             connected    -      full     100 Mbps  10/100Base-T
```

The output of this command includes the following parameters:

Parameter	Description
`Port`	Port number.
`Name`	Name of the interface.
`Status`	Status of the interface.

Parameter	Description
`Vlan`	Displays the access or native vlan.
`Duplex`	Displays the current or configured transfer operation.
`Speed`	Displays the current or configured speed.
`Type`	Displays the media type.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface transceivers

```
show interface transceivers [brief]
```

Description

Issue this command to display transceiver diagnostic information in a tabular format.

Syntax

Parameter	Description
`brief`	Displays the transceiver diagnostic information in a tabular format.

Example

The output of this command displays the following information:

```
(host) (config) #show interface transceiver brief

Port      VendorName        VendorSN          ArubaSupported  CableType
----      ----------        --------          --------------  ---------
GE0/1/0   OPNEXT INC        L12J55161         YES             1000BASE-SX
```

Parameter	Description
`Port`	Displays the port number.
`VendorName`	Displays the name of the SFP vendor.
`VendorSN`	Displays the vendor serial number of the SFP transceiver.
`ArubaSupported`	Displays if the vendor SFP transceiver is supported by Aruba.
`CableType`	Displays the type of cable used.

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface tunnel

```
show interface tunnel [<id>] | brief | {{| begin}|{| exclude}|{| include}}
```

Description

This command displays all the tunnel interfaces configured in the switch.

Syntax

Parameter	Description	Range	Default
`<id>`	Shows tunnel interface information for a specific tunnel ID.	1–50	–
`brief`	Shows tunnel interface brief information	–	–
`{| begin}|{| exclude}|{| include}`	Options to show the output that begins with the line number, excludes, or includes the line that matches the specified number.	–	–

Example

Execute this command to display all the tunnel interfaces configured in the Mobility Access Switch:

```
(host) (Tunnel "50") #show interface tunnel 50
tunnel 50 is administratively Up, Line protocol is Down
Description: GRE Interface
Source unconfigured
Destination unconfigured
Tunnel mtu is set to 1100
Tunnel keepalive is disabled
Tunnel is an L2 GRE Tunnel
Protocol number 0
Tunnel is Trusted
Inter Tunnel Flooding is enabled
Switching-profile "default"
GRE Tunnel is up and running since: 00 00:00:00
```

The command output displays the switching-profile as **default** when no switching profile is applied to the interface tunnel.

The following show command provides the tunnel interface information in brief:

```
(host) (config) #show interface tunnel brief
TUNNEL CONFIGURATION
----------------------
Interface       Admin    Protocol   GRE Mode
---------       -----    --------   ---------
gre-tunnel10    Up       Down       L2 GRE
```

Related Commands

Command	Description
interface tunnel ethernet	This command configures an L2 GRE tunnel.
interface tunnel ip	This command configures an L3 GRE tunnel.

Command History

Release	Modification
ArubaOS 7.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show interface vlan

```
show interface vlan <vlan-id>
```

Description

This command displays the interface VLAN information.

Syntax

Parameter	Description
`<vlan-id>`	VLAN ID

Example

The following sample output displays the details of metric and probe configuration on VLAN 26:

```
(host) #show interface vlan 26
VLAN26 is administratively Up, Line protocol is Up
Hardware is CPU Interface, Address is 00:1a:1e:17:31:00
Description: 802.1Q VLAN
Internet address is 26.0.0.2, Netmask is 255.255.255.0
IPV6 link-local address is fe80::1a:1e00:1a17:3100
Global Unicast address(es):
Routing interface is enabled, Forwarding mode is enabled
Directed broadcast is disabled, BCMC Optimization disabled
Encapsulation 802, Loopback not set
Interface index: 50331674
MTU 1500 bytes
Metric 5
Probe Name: default, Probe Status: Up
Ospf-profile "default"
```

The output of this command includes the following parameters:

Parameter	Description
`VLAN26 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
`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 if directed broadcast and BCMC optimization is enabled

Parameter	Description
`Encapsulation`	Encapsulation type
`loopback...`	Loopback status
`MTU`	Maximum Transmission Units in bytes.
`Metric`	The metric value configured on the interface VLAN.
`Probe Name`	Name of the Probe profile applied on the interface.
`Ospf-profile`	Name of the OSPF profile applied on the interface.

Related Command

Command	Description
`interface vlan`	This command creates the VLAN interface for the switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1.1	IPv6 details were added to the output.
ArubaOS 7.4	Metric and Probe profile details are added to the output.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show inventory

```
show inventory
```

Description

Displays the hardware inventory of the Mobility Access Switch.

Syntax

No parameters.

Example

Issue this command to display the hardware component inventory of the Mobility Access Switch. The output of this command varies depending on the Mobility Access Switch model. The following is a sample output:

```
(host) #show inventory
Show Inventory
--------------
System Card Slot                : 0
SC Serial #                     : AW0000428 (Date: 06/19/11)
SC Model Name                   : ArubaS3500-48P
Mgmt Port HW MAC Addr           : 00:0b:86:6b:82:81
HW MAC Addr                     : 00:0b:86:6b:82:80 to 00:0b:86:6b:82:bf
CPLD Version                    : (Rev: 11)
PoE Firmware Version            : 4.1.5 (Build: 1)
CPU Assembly #                  : 2010095E (Rev: 02.B0)
CPU Serial #                    : AB24019190 (Date: 06/15/11)
Fantray                         : Present (Version: 1)
Module 1                        : Online
Module 1 Assembly #             : 2010140B (Rev: 01.00)
Module 1 Serial #               : UB33000099 (Date: 08/17/11)
Power Supply 0                  : Present (600W)
                                : 12V System Voltage Ok
                                : 56V PoE Voltage Ok
Power Supply 0 Serial #         : QCS111900Y0 (Date: 05/13/11)
Power Supply 0 Model No         : 2510056
Power Supply 0 Vendor Model No  : DCJ6002-02P (Rev: 66.0)
Power Supply 1                  : Present (600W)
                                : 12V System Voltage Ok
                                : 56V PoE Voltage Ok
Power Supply 1 Serial #         : QCS112900JH (Date: 07/20/11)
Power Supply 1 Model No         : 2510056
Power Supply 1 Vendor Model No  : DCJ6002-02P (Rev: 66.0)
<Intentionally Truncated>
```

The output includes the following parameters:

Parameter	Description
System Card Slot	System card slot number
SC Serial#	Serial number of the system card
SC Model#	Model number of the system card

Parameter	Description
Mgmt Port HW MAC Addr	MAC address of the mgmt port. This parameter is not valid for the Aruba S1500 Mobility Access Switch
HW MAC Addr	MAC address
CPLD Version	Revision of programmable logic device on system card.
PoE Firmware Version	Revision of the PoE Firmware version.
CPU Assembly #	Assembly number of the CPU
CPU Serial #	Serial number of the CPU
Fantray	Fantray status (present or absent)
Module 1	Status of module 1
Module 1 Assembly #	Assembly number of module 1
Module 1 Serial #	Serial number of module 1
Power Supply <power supply number>	Power supply <power supply number> status (present or absent)
Power Supply <power supply number> Serial #	Serial number of power supply <power supply number>
Power Supply <power supply number> Model No	Model number of power supply <power supply number>
Power Supply <power supply number> Vendor Model No	Vendor model number of power supply <power supply number>
System Temperature	Temperature of the system
System Voltages	Voltages of the system
Fantray Fan Tachometers	Fantray fan speed

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3	The **PoE Firmware Version, Power Supply <power supply number>, Power Supply <power supply number> Serial #, Power Supply <power supply number> Model No**, and **Power Supply <power supply number> Vendor Model No** parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

show ip access-list

```
show ip access-list
   STRING
   brief [ipv4]
```

Description

Display a table of all configured access control lists (ACLs), or show details for a specific ACL.

Syntax

Parameter	Description
`STRING`	Specify the name of a single ACL to display detailed information on that ACL.
`brief [ipv4]`	Display a table of information for all ACLs or IPv4 ACLs.

Example

```
(host) # show ip access-list brief

Access list table
-----------------
Name                    Type                    Use Count  Roles
----                    ----                    ---------  -----
allowall-stateless      stateless               1          authenticated
defualt                 stateless
denyall                 session                 1          denyall
denyall-stateless       stateless               1          denyall
dhcp-acl-stateless      stateless               1          guest
dns-acl-stateless       stateless               1          guest
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip dhcp aruba-vpn-pool

```
show ip dhcp aruba-vpn-pool <profile-name>
   extensive
```

Description

Displays a table of all configured Aruba VPN pool profiles.

Syntax

Parameter	Description
`<profile-name>`	Displays the configuration information of the specified Aruba VPN pool profile.
`extensive`	Displays the detailed information of all the Aruba VPN pool profiles configured on the Mobility Access Switch.

Examples

You can use the following CLI commands to verify the Aruba VPN Pool configuration:

```
(host) #show ip dhcp aruba-vpn-pool extensive
Aruba VPN DHCP Pool Table
-------------------------
Name         Vlan  DNS Server  Domain name  Lease time  IP Range
----         ----  ----------  -----------  ----------  --------
Distributed  1                              0:12:0:0    30.30.0.0-
,L3                                                     30.30.255.255
Client count  Reserve First  Reserve Last  Branch ID  Branch Netmask  Branch Router
------------  -------------  ------------  ---------  --------------  -------------
5             0              0             0.0.0.0    0.0.0.0         0.0.0.0

(host) #show ip dhcp aruba-vpn-pool
Aruba VPN DHCP Pool List
------------------------
Name            References  Profile Status
----            ----------  --------------
Distributed,L3  1           N/A
Total:1

(host) #show ip dhcp aruba-vpn-pool Distributed,L3
Aruba VPN DHCP Pool "Distributed,L3"
-----------------------------------
Parameter                        Value
---------                        -----
Domain name for the branch scope  N/A
DHCP pool lease time              0 days 12 hr 0 min 0 sec
Configure DNS servers             N/A
DHCP Option                       N/A
IP-Range                          30.30.0.0 30.30.255.255
DHCP Client Count                 5
DHCP Static First IP Count        0
DHCP Static Last IP Count         0
```

Related Command

Command	Description
ip dhcp aruba-vpn-pool	Use this command to create an Aruba VPN pool profile for Distributed DHCP scope.

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip dhcp binding

```
show ip dhcp binding <ip-address>
```

Description

Displays the DHCP Server binding table and binding information of a specific IP address.

Syntax

Parameter	Description
<ip-address>	Specify the IP address for which the binding information is to be viewed.

Examples

The following command displays the DHCP binding table:

```
(host) #show ip dhcp binding

lease 172.16.1.251 {
  starts Fri Oct 21 08:10:29 2011
  ends Fri Oct 21 20:10:29 2011
  binding state active;
  next binding state free;
  hardware ethernet 00:25:90:0a:95:e1;
  uid "\001\000%\220\012\225\341";
}
lease 172.16.1.254 {
  starts Fri Oct 21 09:21:30 2011
  ends Fri Oct 21 21:21:30 2011
  binding state active;
  next binding state free;
  hardware ethernet 00:25:90:0a:95:d2;
  uid "\001\000%\220\012\225\322";
}
lease 172.16.1.253 {
  starts Fri Oct 21 13:09:32 2011
  ends Sat Oct 22 01:09:32 2011
  binding state active;
  next binding state free;
  hardware ethernet 00:25:90:0a:96:42;
  uid "\001\000%\220\012\226B";
}
```

Related Command

Command	Description
ip dhcp pool	Use this command to configure a IP DHCP pool profile.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip dhcp database

```
show ip dhcp database
```

Description

Displays the complete IP DHCP database table.

Example

The following example shows the DHCP IP database table:

```
(host)#show ip dhcp database
DHCP enabled
# pool-1
subnet 172.16.1.0 netmask 255.255.255.0 {
default-lease-time 43200;
max-lease-time 43200;
option domain-name "www.test.com";
option vendor-class-identifier "testStr";
option vendor-encapsulated-options "172.16.0.254";
option routers 172.16.1.254;
option user-option-43 code 43 = ip-address;
option user-option-43 172.16.1.254;
range 172.16.1.1 172.16.1.254;
authoritative;
```

Related Command

Command	Description
ip dhcp pool	Use this command to configure a IP DHCP pool profile.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip dhcp pool

```
show ip dhcp pool <profile-name>
```

Description

Displays the list of the dhcp pools configured and information about their references.

Syntax

Parameter	Description
`<profile-name>`	Specify the name of the DHCP pool.

Example

The following command displays the DHCP pools configured on the Mobility Access Switch:

```
(host)#show ip dhcp pool

dhcp server profile List
------------------------
Name        References  Profile Status
----        ----------  --------------
pool-1      0
pool-2      0
pool-3      0
pool-4      0
Total:4
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the pool.
`References`	Number of references to the pool.
`Profile Status`	Status of the pool profile.

Related Command

Command	Description
ip dhcp pool	Use this command to configure a IP DHCP pool profile.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip dhcp reserved

```
show ip dhcp reserved
```

Description

Displays the DHCP reserved IP addresses assigned to the devices.

Syntax

Parameter	Description
<ipaddr>	Specify the IP address to view the DHCP reservation information.

Example

Use the following command to view the DHCP reserved IP assigned to the device:

```
(host) #show ip dhcp reserved
DHCP Server Device Reservation Information
-----------------------------------------
Vlan  Hardware Address   Reserved IP Address
----  ---------------    -------------------
4     00:00:ac:07:01:14  4.4.4.3
4     00:00:ac:07:01:13  4.4.4.2
```

The output of this command includes the following parameters:

Parameter	Description
Vlan	The VLAN interface of the DHCP reserved IP.
Hardware Address	The hardware address of the device for which DHCP IP is reserved.
Reserved IP Address	The IP address reserved for the device.

Related Command

Command	Description
ip dhcp pool	Use this command to configure an IP DHCP pool profile.

Command History

Release	Modification
ArubaOS 7.3.2	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip dhcp statistics

```
show ip dhcp statistics
```

Description

Show DHCP Server Settings and statistics.

Examples

The example below shows DHCP statistics for two configured networks.

```
(host) # show ip dhcp statistics

DHCPv4 enabled; DHCPv6 enabled
DHCP Pools
----------
Network Name  Type  Active  Configured leases  Active leases  Free leases  Expired leases
Abandoned leases
------------  ----  ------  -----------------  -------------  -----------  --------------  ---
-------------
2-2-2-nw      v4    Yes     242                0              242          0               0
3-2-2-nw      v4    Yes     254                0              254          0               0
test          v4    Yes     254                0              254          0               0
2011          v6    No      5                  -              -            -               -
2012          v6    No      5                  -              -            -               -
Current leases          750
Total leases            512
```

The output of this command includes the following parameters:

Parameter	Description
`Network Name`	Range of addresses that the DHCP server may assign to clients.
`Type`	Indicates the IP version of the DHCP server. It can be v4 or v6.
`Active`	Indicates if the DHCP server is active or not.
`Configured leases`	Number of leases configured on the DHCP server.
`Active leases`	Number of active DHCP leases.
`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`	Use this command to configure an IP DHCP pool profile.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip igmp groups

```
show ip igmp groups
```

Description

Use this command to display IP IGMP group information.

Example

The example below shows the IP IGMP group information.

```
(host)show ip igmp groups

IGMP Group Information
----------------------
Interface  Group       UpTime       Expiry       Last Reporter
---------  -----       ------       ------       -------------
vlan2      230.0.0.1   00h:00m:05s  00h:04m:15s  20.1.1.102
vlan2      230.0.0.2   00h:00m:05s  00h:04m:15s  20.1.1.102
vlan2      230.0.0.3   00h:00m:05s  00h:04m:15s  20.1.1.102
vlan2      230.0.0.4   00h:00m:05s  00h:04m:15s  20.1.1.102
vlan2      230.0.0.5   00h:00m:05s  00h:04m:15s  20.1.1.102
vlan2      230.0.0.6   00h:00m:05s  00h:04m:15s  20.1.1.102
vlan2      230.0.0.7   00h:00m:05s  00h:04m:15s  20.1.1.102
vlan2      230.0.0.8   00h:00m:05s  00h:04m:15s  20.1.1.102
vlan2      230.0.0.9   00h:00m:05s  00h:04m:15s  20.1.1.102
vlan2      230.0.0.10  00h:00m:05s  00h:04m:15s  20.1.1.102
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip igmp interfaces

```
show ip igmp interfaces
```

Description

Use this command to display IP IGMP interface information.

Example

```
(host) #show ip igmp interfaces vlan 2

vlan2 is up, line protocol is up
    Internet address is 20.1.1.4
    IGMP is enabled on the interface
    IGMP router version 2
    IGMP query interval is 125 seconds
    IGMP querier timeout is 255 seconds
    IGMP max query response time 10 seconds
    Last member query count 0
    Last member query response interval 10 ms
    IGMP activity: 10 joins, 0 leaves
    IGMP querying routers 20.1.1.1
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip igmp stats interface

```
show ip igmp stats interface
```

Description

Use this command to display IP IGMP interface information.

Example

```
(host) #show ip igmp stats interface vlan 2

IGMP Statistics
---------------
Interface  Counter     Value
---------  -------     -----
vlan2      Rx Queries  0704
           Rx Reports  2122
           Rx Leaves   0000
           Tx Queries  0002Command History
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip interface brief

```
show ip interface brief
```

Description

This command displays the interfaces with an IP address.

Syntax

No parameters.

Example

In this example, the **`show ip interface brief`** command shows details for the **VLAN 1**, **VLAN 400**, and **mgmt** interfaces.

```
Flags: S - Secondary IP address
Probe: U - Up, D - Down, U/O - Up & Own IP, N/A - Not Applicable
Interface                   IP Address / IP Netmask        Admin  Protocol   Probe Flags
vlan 1                      10.16.4.1 /255.255.255.0       Up     Up         U
vlan 400                    18.18.8.9 /255.255.255.0       Up     Down       N/A
loopback 0                  unassigned /unassigned         Up     Up         N/A
mgmt                        10.16.48.28 /255.255.255.0     Up     Up         N/A
```

The output of this command includes the following information:

Parameter	Description
`Interface`	Name of the switch interface.
`IP Address / IP Netmask`	IP address and IP netmask of the interface.
`Admin`	Shows if the port has been administratively enabled or disabled.
`Protocol`	Displays the status of the line protocol on the interface.
`Probe`	Displays the probe status of the interface. It can be one of the following: • U—The probe status of the interface is up. • D—The probe status of the interface is up • U/O—The probe status of the interface is up and the destination IP is the IP of the same Mobility Access Switch. • N/A—The probe status is not applicable for the interface.
`Flag`	Displays S if the interface has a secondary IP address.

Related Command

Command	Description
ip-profile	Configures the IP profile for the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4	The **Probe** column is added to the output.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip interface loopback

```
show ip interface loopback <loopback-id>
```

Description

This command displays the loopback information of an interface.

Syntax

Parameter	Description	Range
`<loopback-id>`	Loopback interface ID	0–63

Example

The **`show ip interface loopback`** command for the loopback interface ID 22 is as follows:

```
(host) (config) #show ip interface loopback 22
```

Related Command

Command	Description
ip-profile	Configures the IP profile for the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip interface vlan

```
show ip interface vlan <vlan-id>
```

Description

This command displays the VLAN information of an interface.

Syntax

Parameter	Description	Range
`<vlan-id>`	VLAN interface number	1–4094

Example

In this example, the **`show ip interface vlan`** command shows details for vlan 61.

```
(host) (config) #show ip interface vlan 61
vlan 61 is Up, protocol is Up
Internet address is 10.16.61.82/255.255.255.192
Address is statically configured
MTU is 1500
Metric 0
```

Related Command

Command	Description
ip-profile	Configures the IP profile for the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip nat pool

```
show ip nat pool
```

Description

Displays the Network Address Translation (NAT) pools configured in the network.

Example

The following show command displays OSPF information.

```
(host) #show ip nat pool
  NAT Pools
  ---------
  Name            Start IP      End IP        DNAT IP      Flags
  ----            --------      ------        -------      -----
  dual_nat_pool1  192.168.1.10  192.168.1.15  172.16.10.1  Static
  NAT_pool1       192.168.1.10  192.168.1.15  0.0.0.0
```

The table below describes the output of the command.

Column Name	Description
Name	Name of the NAT pool.
Start IP	The starting IP of the source NAT range.
End IP	The ending IP of the source NAT range.
DNAT IP	The IP address of the destination NAT.
Flags	Indicates if one-to-one mapping is configured for the NAT IP address.

Related Commands

Command	Description
ip nat pool	Use this command to create a NAT pool in the network.

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode.

show ip ospf

```
show ip ospf [border-routers] | [database area {<area-id> | detail} | debug route | interface
{brief | loopback <id> | vlan <id>}| neighbor | redistribute]
```

Description

View the OSPF IP runtime information.

Syntax

Parameter	Description
`border-routers`	View the border and boundary router details.
`database area <area-id>`	View the database information for the specified area identification.
`detail`	View the database detail.
`debug route`	View the debug route information.
`interface {brief | loopback <id> | vlan <id>}`	Enter the keyword **interface** followed by either keyword **loopback** or **vlan** and their identification information number to view interface loopback or VLAN information. Use the keyword **brief** to view the OSPF details in a brief tabular format.
`neighbor`	View the status of OSPF neighboring routers.
`redistribute`	View the OSPF route distribution information.

Example

The following show command displays the OSPF information.

```
(host) (config) #show ip ospf

  OSPF is currently running with Router ID 5.5.5.5
  Number of areas in this router is 2
  Area 0.0.0.0
          Number of interfaces in this area is 0
          Area is normal area
          SPF algorithm executed 1 times
  Area 0.0.0.1
          Number of interfaces in this area is 1
          Area is stub area
          Default route cost is 16
          SPF algorithm executed 1 times
  Tx --->: Hellos 0 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0
  Rx <---: Hellos 0 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0
  Errors : BadPkt 0 BadHdr 0 BadVer 0 BadCks 0 BadAuth 0
           NoMIf 0 NoIf 0 InvIf 0 InvMsk 0
           InvHInt 0 InvDInt 0 InvNbr 0 InvOpt 0
           MFmm 0 IFmm 0 SEQmm 0 InvLs 0
           BadLSR 0 BadVif 0 BadArea 0 BadMIF 0
           InvMD5 0 OwnPkt 0 InvAky 0 InvDDO 0
           PasvIf 0 DwnVif0 SameRtId 0 BadMTU 0
```

The table below describes the output in the preceding command.

Line Beginning with...	Description
`OSPF is currently ...`	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 stub area • number of times the SPF algorithm has been executed
`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.
`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.

From ArubaOS 7.4.1.8, the output of the **show ip ospf border-routers** command includes boundary router details in addition to the border router details. With this enhancement, the intra area and inter area routes are displayed correctly.

```
(host) #show ip ospf border-routers
OSPF Border Routers
---- ------ -------
Codes : i - Intra Area Route, I - Inter Area Route
i 2.2.2.2 [1] via 200.200.200.200, vlan200, ABR, Area 0.0.2.0, SPF 16
```

```
I 1.1.1.1 [2] via 200.200.200.200, vlan200, ASBR, Area 0.0.2.0, SPF 16
```

Related Commands

Command	Description
router ospf	Configure OSPF on the interface

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.
ArubaOS 7.4.1	The interface option **brief** was introduced.
ArubaOS 7.4.1.8	Information about autonomous system boundary router was added in the output of the **show ip ospf border-routers** command.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode.

show ip pim interface

```
show ip pim interface vlan <4094>
```

Description

Use this command to display IP PIM interface information.

Example

The example below shows the IP PIM interface information.

```
(host)#show ip pim interface

PIM Interface Information
-------------------------
Address    Interface  Ver/Mode  Nbr Cnt  Hello Intvl  DR prio  DR State  DR address
-------    ---------  --------  -------  -----------  -------  --------  -----------
20.1.1.1   vlan2      v2/S      3        30           1        NotDR     20.1.1.11
20.2.1.1   vlan3      v2/S      1        30           1        NotDR     20.2.1.4
20.3.1.1   vlan4      v2/S      1        30           1        NotDR     20.3.1.6
60.1.1.5   vlan6      v2/S      0        30           1        DR        60.1.1.5
```

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show ip pim mcache

```
show ip pim mcache
```

Description

Use this command to display IP multicast cache information.

Example

The following example shows the IP multicast mcache information.

```
(host)#show ip pim mcache

IP Multicast Cache
Flags: T - Bridge/Trapped, D - Discard, R - Route

(60.1.1.140/32,225.0.0.100/32), flags:R, IIF:vlan6
        vlan3
        vlan4
```

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show ip pim mroute

```
show ip pim mroute detail | group
```

Description

Use this command to display the IP PIM mroute information.

Example

The following example shows the IP PIM mroute information.

```
(host)#show ip pim mroute

IP Multicast Route Table
Flags:  D - Dense, S - Sparse, C - Connected, L - Local,
        J - Join SPT, P - Pruned, R - RP-bit set, T - SPT bit set
        F - Register Flag, N - Null Register, A - Assert Winner


(*,225.0.0.1), 03h:13m:27s, RP 10.10.10.10, flags: S
        Incoming Interface: vlan4, RPF nbr: 20.3.1.6
        Outgoing Interface List:

(60.1.1.140,225.0.0.100), 01h:43m:16s, RP 10.10.10.10, flags: STCF
        Incoming Interface: vlan6, RPF nbr: 0.0.0.0
        Outgoing Interface List:
                vlan3, 01h:43m:16s
                vlan4, 01h:43m:16s
```

Starting from ArubaOS 7.4.0.2, the counters for multicast route entries are included in the output of this command. For example:

```
(host)# show ip pim mroute
IP Multicast Route Table
Flags:  D - Dense, S - Sparse, s - SSM, C - Connected Receiver,
J - Join SPT, R - RP-bit set, T - SPT bit set
F - Register Flag, N - Null Register, A - Assert Winner
Total (*,G) Entries : 0
Total (S,G) Entries : 0
```

Total (*,G) Entries is the number of multicast routes to a specific group from any source.

Total (S,G) Entries is the number of multicast routes from a specific source to a specific group.

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.
ArubaOS 7.4.0.2	The counters for multicast route entries were included in the output.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show ip pim neighbor

```
show ip pim neighbor interface vlan 4
```

Description

Use this command to display IP PIM neighbor information.

Example

The example below shows the IP PIM neighbor information.

```
(host)#show ip pim neighbor

PIM Neighbor Information
------------------------
Interface  Neighbor IP  UpTime       Expiry
---------  -----------  ------       ------
vlan2      20.1.1.11    03h:13m:23s  00h:01m:19s
vlan2      20.1.1.5     03h:13m:23s  00h:01m:36s
vlan2      20.1.1.4     03h:13m:23s  00h:01m:43s
vlan3      20.2.1.4     03h:13m:19s  00h:01m:43s
vlan4      20.3.1.6     03h:13m:21s  00h:01m:25s
```

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show ip pim rp

```
show ip pim rp group <grp ip>
```

Description

Use this command to display IP PIM mroute information.

Example

The example below shows the IP PIM mroute information.

```
(host)#show ip pim mroute

IP Multicast Route Table
Flags:  D - Dense, S - Sparse, C - Connected, L - Local,
        J - Join SPT, P - Pruned, R - RP-bit set, T - SPT bit set
        F - Register Flag, N - Null Register, A - Assert Winner

(*,225.0.0.1), 03h:13m:27s, RP 10.10.10.10, flags: S
        Incoming Interface: vlan4, RPF nbr: 20.3.1.6
        Outgoing Interface List:

(60.1.1.140,225.0.0.100), 01h:43m:16s, RP 10.10.10.10, flags: STCF
        Incoming Interface: vlan6, RPF nbr: 0.0.0.0
        Outgoing Interface List:
                vlan3, 01h:43m:16s
                vlan4, 01h:43m:16s
```

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show ip pim rpf

```
show ip pim rpf
```

Description

Use this command to display IP PIM mroute information. TBD

Example

The example below shows the IP PIM mroute information.

```
(host)#show ip pim mroute

IP Multicast Route Table
Flags:  D - Dense, S - Sparse, C - Connected, L - Local,
        J - Join SPT, P - Pruned, R - RP-bit set, T - SPT bit set
        F - Register Flag, N - Null Register, A - Assert Winner

(*,225.0.0.1), 03h:13m:27s, RP 10.10.10.10, flags: S
        Incoming Interface: vlan4, RPF nbr: 20.3.1.6
        Outgoing Interface List:

(60.1.1.140,225.0.0.100), 01h:43m:16s, RP 10.10.10.10, flags: STCF
        Incoming Interface: vlan6, RPF nbr: 0.0.0.0
        Outgoing Interface List:
                vlan3, 01h:43m:16s
                vlan4, 01h:43m:16s
```

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show ip pim-ssm mcache

```
show ip pim-ssm mcache
```

Description

Use this command to display IP Source Specific Multicast cache information.

Example

Use the following command to view the SSM Range of Mroutes installed in the hardware:

```
(host) # show ip pim-ssm mcache
   IP Multicast Cache
   Flags: T - Bridge/Trapped, D - Discard, R - Route
   (99.99.99.100/32,232.1.2.3/32), flags:R, IIF:vlan356
   OIF:
   vlan4001
   (99.99.99.100/32,232.1.2.4/32), flags:R, IIF:vlan356
   OIF:
   vlan4001
   (99.99.99.100/32,232.1.2.5/32), flags:R, IIF:vlan356
   OIF:
   vlan4001
   (99.99.99.100/32,232.1.2.6/32), flags:R, IIF:vlan356
   OIF:
   vlan4001
   (99.99.99.100/32,232.1.2.7/32), flags:R, IIF:vlan356
   OIF:
   vlan4001
   (99.99.99.100/32,232.1.2.8/32), flags:R, IIF:vlan356
   OIF:
   vlan4001
```

Command History

Release	Modification
ArubaOS 7.3.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show ip pim-ssm mroute

```
show ip pim-ssm mroute
```

Description

Use this command to display IP PIM-SSM Mroute information.

Example

The following example shows the SSM range of Mroutes:

```
(host) #show ip pim-ssm mroute
   IP Multicast Route Table
   Flags:  D - Dense, S - Sparse, s - SSM, C - Connected Receiver,
   J - Join SPT, R - RP-bit set, T - SPT bit set
   F - Register Flag, N - Null Register, A - Assert Winner
   (99.99.99.100,232.1.2.3), 04h:30m:18s/00h:00m:00s, flags: sSJ
   Incoming Interface: vlan356, RPF nbr: 3.5.5.6
   Outgoing Interface List:
   vlan4001, 04h:30m:18s
   (99.99.99.100,232.1.2.4), 04h:30m:18s/00h:00m:00s, flags: sSJ
   Incoming Interface: vlan356, RPF nbr: 3.5.5.6
   Outgoing Interface List:
   vlan4001, 04h:30m:18s
   (99.99.99.100,232.1.2.5), 04h:30m:18s/00h:00m:00s, flags: sSJ
   Incoming Interface: vlan356, RPF nbr: 3.5.5.6
   Outgoing Interface List:
   vlan4001, 04h:30m:18s
   (99.99.99.100,232.1.2.6), 04h:30m:18s/00h:00m:00s, flags: sSJ
   Incoming Interface: vlan356, RPF nbr: 3.5.5.6
   Outgoing Interface List:
   vlan4001, 04h:30m:18s
   (99.99.99.100,232.1.2.7), 04h:30m:18s/00h:00m:00s, flags: sSJ
   Incoming Interface: vlan356, RPF nbr: 3.5.5.6
```

Starting from ArubaOS 7.4.0.2, the counters for multicast route entries are included in the output of this command. For example:

```
(host) #show ip pim-ssm mroute
IP Multicast Route Table
Flags:  D - Dense, S - Sparse, s - SSM, C - Connected Receiver,
J - Join SPT, R - RP-bit set, T - SPT bit set
F - Register Flag, N - Null Register, A - Assert Winner
Total (S,G) Entries : 0
```

Total (S,G) Entries is the number of multicast routes from a specific source to a specific group.

Command History

Release	Modification
ArubaOS 7.3.1	This command was introduced.
ArubaOS 7.4.0.2	The counters for multicast route entries were included in the output.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show ip pim stats interface vlan

```
show ip pim stats interface vlan <1-4094>
```

Description

Use this command to display IP PIM statistics.

Example

The example below shows IP PIM statistical information.

```
PIM Statistics
--------------
Interface  Counter                Value
---------  -------                -----
vlan4      Rx Hellos              0394
           Rx Join/Prune          70927
           Rx Join                0000
           Rx Prune               0000
           Rx Register-Stop       0000
           Rx Asserts             0000
           Tx Hellos              0389
           Tx Join/Prune          0000
           Tx Join                0000
           Tx Prunes              0000
           Tx Register            698391
           Tx Asserts             0000
           Invalid Hellos         0000
           Invalid Join/Prune     0000
           Invalid Join           0000
           Invalid Prune          0000
           Invalid Register       0000
           Invalid Register-Stop  0000
           Invalid Asserts        0000
```

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show ip-profile

```
show ip-profile
```

Description

This command displays the default gateway information.

Syntax

No parameters.

Example

The output of this command displays the following information:

```
(config) #show ip-profile
ip-profile "default"
--------------------
Parameter             Value
---------             -----
Default Gateway       10.18.7.254
Import DHCP Gateway   Disabled
controller-ip         N/A
prefix-list list1    seq 1 permit 5.5.5.0 255.255.255.0 ge 32
prefix-list list2    seq 2 deny 6.6.6.0 255.255.255.0 ge 32
prefix-list list3    seq 3 permit 10.10.0.0 ge 24 le 32
```

The output parameters of the preceding command are explained in the following table:

Parameter	Description
`Default gateway`	IP address of the default gateway.
`Import DHCP gateway`	Indicates if the default gateway was configured using DHCP.
`prefix-list <list-name>`	Displays prefix list(s) configured on the IP profile.
`route`	Displays the routes configured on the IP profile.

Related Command

Command	Description
ip-profile	Configures the IP profile for the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.2	Prefix list information was added.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip route

```
show ip route
   <route_ip>
   ospf
   static
   summary
```

Description

This command displays the various types of IP routes in the routing table.

Syntax

Parameter	Description
`<route_ip>`	Displays the specified IP route.
`ospf`	Displays the OSPF routes only.
`static`	Displays the static routes only.
`summary`	Displays the summary of all the routes.

Usage Guidelines

Use this command to view the existing IP routes.

Examples

The examples below show the details of routes1

```
(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 10.18.7.254 to network 0.0.0.0 at cost 39
S     0.0.0.0/0 [39/0] via 10.18.7.254
C     10.10.10.0 is directly connected: vlan1
C     10.10.10.1 is directly connected: vlan1
C     10.10.10.20 is directly connected: vlan1
C     10.10.10.31 is directly connected: vlan1
C     10.10.10.32 is directly connected: vlan1
C     10.10.10.33 is directly connected: vlan1
M     10.18.7.0 is connected mgmt-intf: 10.18.7.125
M     10.18.7.125 is connected mgmt-intf: 10.18.7.125
M     10.18.7.254 is connected mgmt-intf: 10.18.7.125
S     20.20.31.0 [0] via 10.10.10.31
S     20.20.32.0 [0] via 10.10.10.32
S     20.20.33.0 [0] via 10.10.10.33
S     20.20.34.0 [0] via 10.10.10.20
(host) #show ip route 50.50.50.0 netmask 255.255.255.0
Codes: C - connected, R - RIP
          O - OSPF, O(IA) - Ospf inter Area
          O(E1) - OSPF Ext  Type 1, O(E2) - Ospf Ext  Type 2
          M - mgmt, S - static, * - candidate default
          D - DHCP
S        50.50.50.0/24 [0] via 12.1.1.252
(host) #show ip route ospf
```

```
Codes: C - connected, R - RIP
          O - OSPF, O(IA) - Ospf inter Area
          O(E1) - OSPF Ext Type 1, O(E2) - Ospf Ext Type 2
          M - mgmt, S - static, * - candidate default
O         100.1.0.0/24 [2] via 100.2.0.103
O(E2)     100.5.0.0/24 [11] via 100.2.0.120
O         192.3.2.0/24 [2] via 100.2.0.103
O(E1)     192.12.1.0/24 [11] via 100.2.0.120
(host) #show ip route static
Codes: C - connected, R - RIP
          O - OSPF, O(IA) - Ospf inter Area
          O(E1) - OSPF Ext  Type 1, O(E2) - Ospf Ext  Type 2
          M - mgmt, S - static, * - candidate default
          D - DHCP
Gateway of last resort is 10.16.56.254 to network 0.0.0.0 at cost 39
S       * 0.0.0.0  /0 [39] via 10.16.56.254
S         50.50.50.0/24 [0] via 12.1.1.252
S         60.60.60.0/24 [0] via 12.1.1.252
S         60.60.60.1/32 [0] via 12.1.1.252
S         60.60.60.2/32 [0] via 12.1.1.252
S         60.60.60.3/32 [0] via 12.1.1.252
S         60.60.60.4/32 [0] via 12.1.1.252
```

Related Commands

Command	Description
show arp	Displays the list of ARP entries.
clear arp	Clears the ARP entries.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.1.1	**ospf**, a new parameter, was introduced.
ArubaOS 7.1.3	**summary**, a new parameter, was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip source-guard

```
show ip source-guard
```

Description

Displays all the interfaces on which IPSG is enabled, and the type of IPSG filter.

Syntax

No parameters.

Example

```
(host) #show ip source-guard
IPSG interface Info
-------------------
Interface   IPSG
----------  ----
GE0/0/12    Enabled
GE0/0/20    Enabled
GE1/0/20    Enabled
GE1/0/24    Enabled
GE2/0/16    Enabled
GE2/0/20    Enabled
GE3/0/8     Enabled
GE3/0/20    Enabled
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show ip tacacs source-interface

```
show ip tacacs source-interface
```

Description

This command helps display the global and profile-level source-interface configurations for all TACACS server request packets.

Syntax

Not applicable.

Examples

The following sample displays the output of the show ip tacacs source-interface command for the global and profile-level configurations mentioned here:

- The global source-interface is configured as vlan 55.
- The profile-level source-interfaces are configured as loopback and vlan 55 for two server profiles.

```
(host) (config) #show ip tacacs source-interface
Global TACACS source interface:
vlan: 55
ip: 55.0.0.2
loopback: disabled
Per-server client source IP addresses:
Server "tac1": loopback enabled
Server "tac2": vlan 55, IP 55.0.0.2
```

Related Command

Command	Description
ip tacacs source-interface	Allows global source-interface configuration and the profile-level source-interface configuration.

Command History

Release	Modification
ArubaOS 7.4.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration and Enable modes.

show ipv6 interface

```
show ipv6 interface
```

Description

Displays all the ipv6 interface details.

Syntax

No parameters.

Example

The output of this command shows the details of all the IPv6 interfaces on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode

show ipv6 interface brief

```
show ipv6 interface brief
```

Description

Displays the ipv6 interfaces.

Syntax

No parameters.

Example

The output of this command shows the IPv6 interfaces on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode

show ipv6 neighbors

```
show ipv6 neighbors
```

Description

Displays the neighboring ipv6 devices in the network.

Syntax

No parameters.

Example

The output of this command shows the neighboring IPv6 devices in the network.

Command History

Release	Modification
ArubaOS 7.1	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode

show ipv6 route

```
show ipv6 route
```

Description

Displays the IPv6 routing table.

Usage Guidelines

Use this command to view the IPv6 routing table on the Mobility Access Switch.

Examples

The example below shows the ipv6 routing table on the Mobility Access Switch:

Command History

Release	Modification
ArubaOS 7.1	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode

show lacp

```
show lacp {<0-63> counters|internal|neighbor}|sys-id
```

Description

This command displays LACP port-channel and LACP neighbor information.

Syntax

Parameter	Description
`<0-63>`	Port-channel ID.
`counters`	Displays the port-channel counters information.
`internal`	Displays the port-channel internal information.
`neighbor`	Displays the port-channel neighbor information.
`sys-id`	Displays the system ID used by LACP.

Example

The following four commands display detailed LACP information for the switch. The output of these commands is described in the table below.

```
(host) #show lacp 2 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
LACP Neighbor Table
-------------------
Port    Flags  Pri    OperKey  State  Num   Dev Id
----    -----  ---    -------  -----  ---   ------
GE 1/2  SA     32768  0x2      0x3d   0xc0  00:13:19:6A:4D:80
GE 1/3  SA     32768  0x2      0x3d   0xc2  00:13:19:6A:4D:80
GE 1/1  SA     32768  0x2      0x3d   0xc1  00:13:19:6A:4D:80


(host) #show lacp 2 counters

LACP Counter Table
------------------
Port    LACPDUTx  LACPDURx  MrkrTx  MrkrRx  MrkrRspTx  MrkrRspRx  ErrPktRx
----    --------  --------  ------  ------  ---------  ---------  --------
GE 1/2  95        92        0       0       0          0          0
GE 1/3  96        90        0       0       0          0          0
GE 1/1  92        88        0       0       0          0          0


(host) #show lacp 2 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
LACP Internal Table
-------------------
```

```
Port     Flags  Pri  AdminKey  OperKey  State  Num  Status
----     -----  ---  --------  -------  -----  ---  ------
GE 1/2   SA     255  0x3       0x3      0x3d   0x3  up
GE 1/3   SA     255  0x3       0x3      0x3d   0x4  up
GE 1/1   SA     255  0x3       0x3      0x3d   0x2  up

(host) #show lacp sys-id
32768,00:0B:86:61:66:14
```

The output of the show lacp commands includes the following information:

Parameter	Description
Port	Interface slot/port number.
Flags	This column lists the following flags for the LACP port, when applicable: • S - Device is requesting slow LACPDUs • F - Device is requesting fast LACPDUs • A - Device is in Active mode • P - Device is in Passive mode
Pri	Port priority for the port-channel interface.
OperKey	Operational key assigned to this port by LACP, in hexadecimal format.
State	The state options.
Num	The hex options.
Dev Id	Device ID of the neighbor port.
LACPDUTx	Number of LACP packets sent front the port.
LACPDURx	Number of LACP received by the port.
MrkrTx	Number of LACP marker packets sent from the port.
MrkrRx	Number of LACP marker packets received by the port.
MrkrRspTx	Number of LACP marker response packets sent from the port.
MrkrRspRx	Number of LACP marker response packets received by the port.
ErrPktRx	Number of error or unknown packets received by LACP for the port.
AdminKey	Administrative key assigned to this port by LACP, in hexadecimal format.
Status	Shows if port is enabled or disabled.
sys-id	The system ID is comprised of the LACP system priority and the switch's MAC address.

Related Command

Command	Description
interface-profile lacp-profile	This command creates a dynamic LACP port-channel profile that can be assigned to any interface or interface group.

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show lacp-system-profile

```
show lacp-system-profile
```

Description

This command displays the priority value for the LACP system profile.

Syntax

No parameters.

Example

The output of the example below shows that the current LACP system profile has a priority of **37000**.

```
(host) #show lacp-system-profile
lacp-system-profile
-------------------
Parameter                     Value
---------                     -----
LACP priority for the system  37000
```

Related Command

Command	Description
interface-profile lacp-profile <profile-name> port-priority <1-65535>	This command creates a dynamic LACP port-channel profile and specifies the port priority for the port-channel interface.

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show layer2 interface-errors

```
show layer2 interface-errors
```

Description

This command displays the Layer 2 interface errors.

Syntax

No parameters.

Example

The output of this command in the example below shows there are currently no layer-2 errors on the switch. If there were any errors, this output would display the name of the interface that triggered the error in the **Interface** column, and give a description of the error in the **Error** column.

```
(host) #show layer2 interface-errors
Layer-2 Interface Error Information
-----------------------------------
Interface  Error
---------  -----
```

Related Commands

Command	Description
show interface all	This command displays the interfaces information either in detail or in brief.

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show lcd

```
show lcd [slot <number>]
```

Description

View the LCD status.

Syntax

Parameter	Description
`slot <number>`	Enter the keyword **slot** followed by the slot number to view (0 to 7)

Example

The command below displays the LCD status for each slot.

```
(host)#show lcd

Slot 0:
--------
LCD:
    0 : Primary
    svl_techpubs 00

LED status:
    Power  LED:   Green
    Status LED:   Green
    Stack  LED:   Green

Port LED mode: Speed

Slot 1:
--------
LCD:
    1 : Secondary
    svl_techpubs 00

LED status:
    Power  LED:   Green
    Status LED:   Green
    Stack  LED:   Green Blinking

Port LED mode: Speed

Slot 2:
--------
LCD:
    2 : Linecard
    svl_techpubs 00

LED status:
    Power  LED:   Green
    Status LED:   Green
    Stack  LED:   OFF

Port LED mode: Speed
```

Command History

Release	Modification
ArubaOS 7.1	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

show lldp interface

```
show lldp interface [gigabitethernet <slot/module/port>]
```

Description

This command displays the LLDP interfaces information.

Syntax

Parameter	Description
`<slot/module/port>]`	Displays the LLDP interface information for the specified port number.

Usage Guidelines

By default, this command displays details for the entire list of LLDP interfaces. Include a slot/module/port number to display information only for that one interface.

Example

The example shows two commands. The output of **show lldp interface** command displays information for all LLDP interfaces.

The second example only shows information for the GE0/0/1 interface.

```
(host) #show lldp interface
LLDP Interfaces Information
---------------------------
Interface  LLDP TX  LLDP RX  LLDP-MED  TX interval  Hold Timer
---------  -------  -------  --------  -----------  ----------
GE0/0/0    Enabled  Enabled  Enabled   30           120
GE0/0/1    Enabled  Enabled  Enabled   30           120
GE0/0/2    Enabled  Enabled  Enabled   30           120
GE0/0/3    Enabled  Enabled  Enabled   30           120
GE0/0/4    Enabled  Enabled  Enabled   30           120
GE0/0/5    Enabled  Enabled  Enabled   30           120
<output truncated>

(host) #show lldp interface gigabitethernet 0/0/0

Interface: gigabitethernet0/0/0
LLDP Tx: Enabled, LLDP Rx: Enabled
LLDP-MED: Enabled
Transmit interval: 30, Hold timer: 120
```

The output of these commands includes the following information:

Parameter	Description
Interface	Name of an LLDP interface.
`LLDP TX`	Shows if LLDP Protocol Data Unit (PDU) transmission is enabled or disabled.
`LLDP RX`	Shows if the switch has enabled or disabled processing of received LLDP PDUs.

Parameter	Description
`LLDP-MED`	Shows if LLDP MED protocol is enabled or disabled.
`TX interval`	The LLDP transmit interval, in seconds.
`Hold Timer`	The LLDP transmit hold multiplier.

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show lldp neighbor

```
show lldp neighbor [interface gigabitethernet <slot/module/port> [detail]]
```

Description

This command displays information about LLDP peers.

Syntax

Parameter	Description
`<slot/module/port>]`	Displays the LLDP interface information for the specified port number.
`detail`	Includes details.

Usage Guidelines

The LLDP protocol allows switches, routers, and wireless LAN access points to advertise information about themselves such as identity, capabilities, and neighbors to other nodes on the network. Use this command to display information about with switch's LLDP peers.

By default, this command displays LLDP neighbors for the entire list of LLDP interfaces. Include a slot/module/port number to display neighbor information only for that one interface.

Example

The command in the first example below shows that the ports **GE4/0/1** and **GE4/0/2** recognize each other as an LLDP peers.

```
(host)#show lldp neighbor
Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone, (O)Other
LLDP Neighbor Information
-------------------------
Local Intf  Chassis ID        Capability  Remote Intf  Expiry-Time (Secs)
---------  -----------        ----------- -----------  ------------------
GE4/0/1    00:0b:86:6a:25:40  B:R         GE0/0/17     105
GE4/0/2    00:0b:86:6a:25:40  B:R         GE0/0/18     105

System name
-----------
ArubaS3500
ArubaS3500
Number of neighbors: 2

(host) #show lldp neighbor interface  gigabitethernet 1/0/40 detail

Interface: gigabitethernet1/0/40, Number of neighbors: 1
------------------------------------------------------------
Chassis id: d8:c7:c8:ce:0d:63, Management address: 192.168.0.252
Interface description: bond0, ID: d8:c7:c8:ce:0d:63, MTU: 1522
Device MAC: d8:c7:c8:ce:0d:63
Last Update: Thu Sep 27 10:59:37 2012
Time to live: 120, Expires in: 103 Secs
System capabilities : Bridge,Access point
Enabled capabilities: Access point
System name: IAP-105
```

```
System description:
  ArubaOS (MODEL: 105), Version 6.1.3.4-3.1.0.0 (35380)
Auto negotiation: Supported, Enabled
Autoneg capability:
  10Base-T, HD: yes, FD: yes
  100Base-T, HD: yes, FD: yes
  1000Base-T, HD: no, FD: yes
Media attached unit type: 1000BaseTFD - Four-pair Category 5 UTP, full duplex mode (30)
MAC:          7c:d1:c3:c7:e9:72: Blacklist
MAC:          9c:b7:0d:7d:0b:72: Blacklist
MAC:         7c:d1:c3:d1:02:c8: Blacklist
```

The second example shows details for the neighbor port.

The output of the **`show lldp neighbor`** command includes the following information:

Parameter	Description
`Local Intf`	Slot, module and port number of a switch port.
`Chassis ID`	MAC address of the LLDP Peer.
`Capability`	This column shows the capabilities of the peer to operate as a router, bridge, access point, phone or other network device.
`Remote Intf`	Remote interface.
`Expiry-time`	Expiry time.
`System Name`	Name of the peer system, as supplied by the peer.

The output of the **`show lldp neighbor interface gigabitethernet <slot/module/port> detail`** command varies, depending upon the type of LLDP peer detected. The output in the example above contains the following information:

Parameter	Description
`Interface`	Name of the switch port for which you are viewing LLDP neighbor information.
`Number of Neighbors`	Number of LLDP neighbors seen by the switch port.
`Chassis id`	MAC address of the neighbor device.
`Management address`	MAC address of the neighbor's management port.
`Interface description`	Description of the LLDP neighbor interface.
`ID`	Interface ID of the LLDP neighbor interface.
`MTU`	Maximum Transmission Unit size allowed by the neighbor device in bytes.
`Device MAC`	Shows the MAC address of the IAP connected to the MAS port.
`Last Update`	Date and time the neighbor device's status changed.
`Time to live`	Time, in seconds, for which this information is valid.
`Expires in`	Time, in seconds, before this information is considered invalid.

Parameter	Description
System capabilities	This column shows the capabilities of the peer to operate as a router, bridge, access point, phone or other network device.
Enabled capabilities	This column if the peer has been actively configured to operate as a router, bridge, access point, phone or other network device.
System name	Name of the peer system, as supplied by the peer.
System description	Description of the peer system, as supplied by the peer.
Auto negotiation	Shows if link auto-negotiation is enabled for the peer interface.
Media attached unit type	This parameter displays additional details about an LLDP-MED device attached to the interface. The specific details depend upon the capabilities of the device.
VLAN	VLAN ID assigned to the peer interface.
pvid	Indicates if the VLAN ID is assigned to the peer access port.
MAC	Shows the MAC address of the rogue AP detected by the Instant AP(IAP), which is blacklisted by the MAS.
LLDP-MED	Shows details for LLDP-MED (Media Endpoint Discovery), if applicable.
Device Type	Type of LLDP-MED device connected to the peer interface.
Capability	Capabilities of the LLDP-MED device connected to the peer interface.

Command History

Release	Modification
ArubaOS 7.0	Command introduced
ArubaOS 7.2	The MAC and Device MAC parameters were introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show lldp statistics

```
show lldp statistics [interface gigabitethernet <slot/module/port>]
```

Description

This command displays LLDP statistics information.

Syntax

Parameter	Description
`<slot/module/port>`	Displays the LLDP statistics information for the specified port number.

Usage Guidelines

By default, this command displays LLDP statistics for the entire list of LLDP interfaces. Include a slot/module/port number to display statistics only for that one interface.

Example

The example command below shows LLDP statistics for the Gigabit Ethernet interface **0/0/0**.

```
(host) #show lldp statistics interface gigabitethernet 0/0/0

LLDP Statistics
---------------
Interface             Received  Unknow TLVs  Malformed  Transmitted
---------             --------  -----------  ---------  -----------
gigabitethernet0/0/0  1249      0            0          1249
```

The output of this command includes the following information:

Parameter	Description
`Interface`	Name of an LLDP interface
`Received`	Number of packets received on that interface
`Unknown TLVs`	Number of LLDP Protocol Data Units (PDUs) with an unknown type-length-value (TLV).
`Number of Malformed packets`	Number of malformed packets received on that interface
`Transmitted`	Number of packets transmitted from that interface

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show log security

```
show log security{[<lines>][all][member]}
```

Description

Shows the Mobility Access Switch's security logs.

Syntax

Parameter	Description
`member`	Stack member.
`<id>`	Enter the member id of the stack.
`all-members`	Displays the log output for all the members of a stack.
`all`	Shows all the security logs for the Mobility Access Switch.
`Lines`	Start displaying the log output from the specified number of lines from the end of the log.

Example

This example shows the Mobility Access Switch's security logs.

```
(host) (config) # show  log security 10

Oct 18 11:25:17 :124004:  <DBUG> |authmgr|  group "gig_prof" instance "1/0/24" changed
0.............................
Oct 18 11:25:17 :128008:  <ERRS> |l2m|  BPDU received on gigabitethernet1/0/24, shutting down
the interface state :3
```

Command History

Release	Modification
ArubaOS 7.2	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show mac-address-table

```
show mac-address-table [{interface gigabitethernet <slot/module/port>}|summary|{vlan<vlan-id>}]|sticky
```

Syntax

Parameter	Description
`interface gigabitethernet <slot/module/port>`	Displays the MAC addresses associated with the specified port.
`summary`	Displays the summary of the MAC addresses learnt.
`vlan<vlan-id>`	Displays the MAC addresses associated with the specified VLAN.
sticky	Displays the sticky MAC address stored.

Description

This command displays the MAC addresses stored in the MAC address table.

Usage Guidelines

The MAC address table is used to forward traffic between ports on the Mobility Access Switch. The table includes addresses learned by the Mobility Access Switch. This command displays the manually entered, dynamically learnt, and those learnt by authentication associated with specific ports and VLANs.

Example

For example, the following output is displayed:

```
(host) #show mac-address-table

Total MAC address: 0
Learnt: 5, Static: 6, Auth: 0

MAC Address Table
-----------------
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  ----------------
00:0b:86:00:00:00    Mgmt          1     vlan 1
00:0b:86:f0:05:60    Mgmt          1     vlan 1
00:0b:86:00:00:00    Mgmt          62    vlan 62
00:0b:86:f0:05:60    Mgmt          62    vlan 62
00:0b:86:00:00:00    Mgmt          4095  vlan 4095
00:0b:86:f0:05:60    Mgmt          4095  vlan 4095
00:00:cc:aa:1c:00    Sticky        1     GE0/0/12
00:00:cc:aa:1c:01    Sticky        1     GE0/0/12
00:00:cc:aa:1c:02    Sticky        1     GE0/0/12
00:00:cc:aa:1c:03    Sticky        1     GE0/0/12
00:00:cc:aa:1c:04    Sticky        1     GE0/0/12
```

The output of this command includes the following information:

Command	Description
`Total MAC address`	Total number of MAC addresses in the MAC address table.
`Learnt`	Number of learned MAC addresses.
`Static`	Number of static (User-defined) MAC addresses.
`Auth`	Number of MAC addresses added as a result of authentication.
`Destination Address`	Destination MAC address
`Address Type`	Destination address type
`VLAN`	Associated VLAN
`Destination Port`	Destination port

Related Command

Command	Description
`clear mac-address-table`	Clears the MAC address table.

Command History

Release	Modification
ArubaOS 7.0	Command introduced
ArubaOS 7.3	The **sticky** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show member

```
<id> usb
```

Descriptions

This command displays the USB device information.

Syntax

Parameter	Description
<id>	Enter the member ID of the stack.
usb	Enter the USB.

Examples

The following example displays the USB device information.

```
(host) #show  member 1 usb
Member-id: 1
------------
USB Device Table
----------------
Address  Product      Vendor  ProdID  Serial                Type
-------  -------      ------  ------  ------                ----
2        USB DISK     058f    6387    AA04012700011854      Storage
2        Cruzer Edge  0781    556b    200542553313D9F2EC20  Storage
(ArubaS1500-24P) #show  member all usb
Member-id: 0
------------
USB Device Table
----------------
Address  Product   Vendor  ProdID  Serial            Type
-------  -------   ------  ------  ------            ----
2        USB DISK  058f    6387    AA04012700011875  Storage
2        v125w     03f0    3307    AA16194200000000  Storage
Member-id: 1
------------
USB Device Table
----------------
Address  Product      Vendor  ProdID  Serial                Type
-------  -------      ------  ------  ------                ----
2        USB DISK     058f    6387    AA04012700011854      Storage
2        Cruzer Edge  0781    556b    200542553313D9F2EC20  Storage
Member-id: 2
------------
USB Device Table
----------------
Address  Product   Vendor  ProdID  Serial            Type
-------  -------   ------  ------  ------            ----
2        USB DISK  090c    1000    AA04012700008216  Storage
```

Command History

Release	Modification
ArubaOS 7.3	This command was sintroduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode

show memory

```
show memory
   all
   auth
   cfgm
   cmica
   cmicm
   debug
   dpa
   fpcli
   im
   l2m
   l3m
   member <id>
   profmgr
   rmon
   sm
   snmpd
   survival
   syslogdwrap
   trapd
   {|begin <line>}|{|exclude <line>}|{|include <line>}
```

Descriptions

This command displays the memory information.

Syntax

Parameter	Description
`all`	Displays the memory information for all processes for either a specific member or for all members.
`auth`	Displays the memory information for auth process.
`cfgm`	Displays the memory information for cfgm process.
`cmica`	Displays the memory information for cmica process.
`cmicm`	Displays the memory information for cmicm process.
`debug`	Displays the memory debug information.
`dpa`	Displays the memory information for dpa process.
`fpcli`	Displays the memory information for fpcli process.
`im`	Displays the memory information for im process.
`l2m`	Displays the memory information for l2m process.
`l3m`	Displays the memory information for l3m process.
`{member <id>|all}`	Displays the memory information for a specific process for either a specific remote stacking member or for all members.

Parameter	Description
profmgr	Displays the memory information for profmgr process
rmon	Displays the memory information for rmon process
sm	Displays the memory information for stackmgr process
snmpd	Displays the memory information for snmpd process.
survival	Displays the memory information for survival process.
syslogdwrap	Displays the memory information for syslogdwrap process.
trapd	Displays the memory information for trapd process.
{|begin <line>}| {|exclude <line>}| {|include <line>}	Displays the memory information based on the output modifiers.

Examples

The following example displays the memory information.

```
(host) #show memory
Memory (Kb): total: 760784, used: 417040, free: 343744
```

The output of the **show memory** command for the dpa process is provided in the following sample:

```
(host) #show memory dpa
Memory page usage for dpa
Task Block Usage Summary:
Min/Max Used Block Sizes 4 1024
Allocated blocks/bytes 671 52388
Free blocks/bytes 3169 78652
Total bytes 131040
Total Block Alloc Calls 5316
Allocated Page Usage:
Page Size: 4096
Total pages allocated 254
Total bytes allocated 1040384
task_block_malloc pages 222
task_block_alloc pages 32
task_page_alloc() page Q 0
pool_alloc_page() pages 3
Allocated MultiPage Usage:
multipage blks/pages in use 11 219
multipage allocations/frees 11 0
multipage max page request 145
multipage max reused 0
multipage Q pages/blocks 0 0
multipages broken down 0
multipages returned to OS 0
Growable arrays (GDAs, GCAs * 2, BVs)
Current growable arrays 0
Number of growths 0
Max allocation in bytes 0
Task Memory (malloc, calloc, realloc, free)
Mallocs: 1157
Callocs: 0
Reallocs: 0
Reallocs for more: 0
```

```
Reallocs for less: 0
Reallocs for initial: 0
Frees: 1019
Bytes requested: 720403
Bytes allocated: 744720
Bytes wasted: 24160
Most outstanding allocs: 192
Largest request: 589856
Currently outstanding allocs: 138
RUSAGE Stats:
rusage: ru_maxrss 0: ix 0 id 0 is 0: times 1 0
paging: rec 2997 faults 0 nswap 0: in/out 0 0
sigs: 0 cw: 3577
```

The output of the **show memory** command for the dpa process for member id 3 is provided in the following sample:

```
(host) #show memory dpa member 3
Member-id: 3
------------
Memory page usage for dpa
Task Block Usage Summary:
Min/Max Used Block Sizes    4     1024
Allocated blocks/bytes      886   60208
Free blocks/bytes           3277  79024
Total bytes                       139232
Total Block Alloc Calls     23513686
Allocated Page Usage:
Page Size:                  4096
Total pages allocated       268
Total bytes allocated       1097728
task_block_malloc pages     234
task_block_alloc pages      34
task_page_alloc() page Q    0
pool_alloc_page() pages     3
Allocated MultiPage Usage:
multipage blks/pages in use 11    231
multipage allocations/frees 11    0
multipage max page request  145
multipage max reused        0
multipage Q pages/blocks    0     0
multipages broken down      0
multipages returned to OS   0
Growable arrays (GDAs, GCAs * 2, BVs)
Current growable arrays     0
Number of growths           0
Max allocation in bytes     0
Task Memory (malloc, calloc, realloc, free)
Mallocs:                      936
Callocs:                      0
Reallocs:                     0
Reallocs for more:            0
Reallocs for less:            0
Reallocs for initial:         0
Frees:                        803
Bytes requested:              744667
Bytes allocated:              769424
Bytes wasted:                 24600
Most outstanding allocs:      234
Largest request:              589856
Currently outstanding allocs: 133
RUSAGE Stats:
rusage: ru_maxrss 0: ix 0 id 0 is 0: times 846 866
```

```
paging: rec 3079 faults 0 nswap 0: in/out 0 0
sigs: 0 cw: 31572547 33
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4.1.1	• The **dpa** parameter was introduced. • The output of the show memory debug command is enhanced to include debug information for l3m, l2m, dpa, stackmgr, cmicm, and cmica processes.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode and Enable mode.

show mgmt-server type amp

```
show mgmt-server type amp
```

Description

Issue this command to show information about an AirWave server associated with the Mobility Access Switch.

Syntax

No Parameters

Usage Guidelines

When the Mobility Access Switch connects to the AirWave server, it is assigned to the AirWave group and folder specified by the output of this command. After the Mobility Access Switch appears as an associated device on the AirWave server,you must use AirWave to provision the Mobility Access Switch with device-specific information (such as an IP address or port settings) before you allow it to download its new configuration.

Example:

```
(host)(config)#show mgmt-server type amp
amp-server
----------
Parameter          Value
---------          -----
Host IP            109.0.2.0
Host Name          N/A
AMP Shared Secret  ********
AMP Device Group   MAS_Group_1
AMP Device Folder  Branch
```

The output of this command includes the following information:

Parameter	Description
`Host IP`	IP address of the AirWave server.
`Host Name`	Name of the AirWave server.
`AMP Shared Secret`	Shared secret for the AirWave server.
`AMP Device Group`	Name of the AirWave group that contains the configuration for the Mobility Access Switch.
`AMP Device Folder`	Name of the AirWave folder that contains the configuration for the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration mode

show mirroring

```
show mirroring
```

Description

This command displays the mirroring information.

Syntax

Parameter	Description
`Mirroring Profile Name`	Displays the list of mirroring profiles.
`Mirroring Ratio`	Ratio of packets that are mirrored. 0—Does not mirror any packet to the destination. 1—Mirrors all packets to the destination (1:1). This is the default. 100—Mirrors 1 out of 100 packets to the destination. 2047—Mirrors 1 out of 2,047 packets to the destination.
`Mirroring Destination`	The port on which all the monitored traffic is sent out.
`Ingress mirrored ports`	Displays the list of ports whose ingress traffic will be mirrored.
`Egress mirrored ports`	Displays the list of ports whose egress traffic will be mirrored.

Example

This command displays the mirroring information:

```
(host) (config) #show mirroring

Mirroring Profile Name : ana1
Mirroring Ratio        : 1
Mirroring Destination  : GE0/0/4
Ingress mirrored ports : GE0/0/2, GE0/0/23, Pc0 Egress mirrored ports : GE0/0/2
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show mld-snooping counters

```
show mld-snooping counters vlan <id>
```

Description

This command displays counters for all VLANs or for the specified VLAN interface.

Syntax

Parameter	Description
`vlan <id>`	(Optional) Specify the VLAN interface.

Example

```
(host) #show mld-snooping counters

  MLD Snooping Counters
  ---------------------
  Name                    Value
  ----                    -----
  received-total          0005
  received-queries        0001
  received-v1-reports     0004
  received-leaves         0000
  received-pim-v6         0000
  received-unknown-types  0000
  len-errors              0000
  checksum-errors         0000
  forwarded               0000
```

Command History

Release	Modification
ArubaOS 7.2	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show mld-snooping groups

```
show mld-snooping groups vlan <vlan id>
```

Description

This command displays the MLD multicast addresses detected on the Mobility Access Switch. You can also view the MLD multicast addresses detected on a VLAN.

Syntax

Parameter	Description
`vlan <id>`	(Optional) Specify the VLAN interface.

Example

```
(host) #show mld-snooping groups

  MLD Snooping Multicast Route Table
  ----------------------------------
  VLAN  Group     Port List
  ----  -----     ---------
  0001  ff03::1   GE0/0/0 GE0/0/4
  0001  ff03::2   GE0/0/0 GE0/0/4
  0001  ff03::3   GE0/0/0 GE0/0/4
  0001  ff03::4   GE0/0/0 GE0/0/4

(host) #show mld-snooping groups vlan 1

  MLD Snooping Multicast Route Table
  ----------------------------------
  VLAN  Group     Port List
  ----  -----     ---------
  0001  ff03::1   GE0/0/0 GE0/0/4
  0001  ff03::2   GE0/0/0 GE0/0/4
  0001  ff03::3   GE0/0/0 GE0/0/4
  0001  ff03::4   GE0/0/0 GE0/0/4
  0001  ff03::5   GE0/0/0 GE0/0/4
```

Command History

Release	Modification
ArubaOS 7.2	Command introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show mld-snooping membership

```
show mld-snooping membership
```

Description

This command displays the detected MLD multicast membership information.

Example

```
(host) #show mld-snooping membership

   MLD Snooping Multicast Membership
   ---------------------------------
   VLAN  Group     Port       Expiry    UpTime
   ----  -----     ----       ------    ------
   0001  ff03::1   GE0/0/0    00:02:12  00:02:08
   0001  ff03::2   GE0/0/0    00:02:13  00:02:07
   0001  ff03::3   GE0/0/0    00:02:14  00:02:06
   0001  ff03::4   GE0/0/0    00:02:15  00:02:05
   0001  ff03::5   GE0/0/0    00:02:16  00:02:04

(host) #show mld-snooping membership detail

Flags: H - IGMP/MLD listener, M - Multicast Router

Group:ff03::1 Vlan:0001
  Port: GE0/0/0    Expiry: 00:00:30 Uptime: 00:03:50
        (H)  IP: fe80::200:24ff:fef9:7ccf MAC: 00:00:24:f9:7c:cf
Group:ff03::2 Vlan:0001
  Port: GE0/0/0    Expiry: 00:00:31 Uptime: 00:03:49
        (H)  IP: fe80::200:24ff:fef9:7ccf MAC: 00:00:24:f9:7c:cf
Group:ff03::3 Vlan:0001
  Port: GE0/0/0    Expiry: 00:00:32 Uptime: 00:03:48
        (H)  IP: fe80::200:24ff:fef9:7ccf MAC: 00:00:24:f9:7c:cf
Group:ff03::4 Vlan:0001
  Port: GE0/0/0    Expiry: 00:00:33 Uptime: 00:03:47
        (H)  IP: fe80::200:24ff:fef9:7ccf MAC: 00:00:24:f9:7c:cf
Group:ff03::5 Vlan:0001
  Port: GE0/0/0    Expiry: 00:00:34 Uptime: 00:03:46
        (H)  IP: fe80::200:24ff:fef9:7ccf MAC: 00:00:24:f9:7c:cf

(host) #show mld-snooping membership vlan 1

   MLD Snooping Multicast Membership
   ---------------------------------
   VLAN  Group     Port       Expiry    UpTime
   ----  -----     ----       ------    ------
   0001  ff03::1   GE0/0/0    00:02:12  00:02:08
   0001  ff03::2   GE0/0/0    00:02:13  00:02:07
   0001  ff03::3   GE0/0/0    00:02:14  00:02:06
   0001  ff03::4   GE0/0/0    00:02:15  00:02:05
   0001  ff03::5   GE0/0/0    00:02:16  00:02:04
```

Command History

Release	Modification
ArubaOS 7.2	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show mld-snooping mrouter

```
show mld-snooping mrouter [detail | vlan <id>]
```

Description

This command displays the MLD-snooping mrouter port information. You can also view the MLD snooping mrouter port information in detail or on a per VLAN basis.

Syntax

Parameter	Description
`detail`	Displays the mrouter information in detail.
`vlan <id>`	Specify the VLAN interface.

Example

```
(host)show mld-snooping mrouter

   Flags: D - Dynamic, S - Static, P - PIM, M - IGMP/MLD query

   MLD Snooping Multicast Router Ports
   -----------------------------------
   VLAN  Elected-Querier  Ports (Flags)  Expiry    UpTime
   ----  ---------------  -------------  ------    ------
   0001  fef1::d0d0       GE0/0/4 (DM)   00:04:12  00:00:08

(host)show mld-snooping mrouter detail

   Flags: D - Dynamic, S - Static, P - PIM, M - IGMP/MLD query

   Vlan:0001 Elected-Querier:fef1::d0d0
     GE0/0/4     (DM)  Expiry Time: 00:04:06  Uptime: 00:00:14
                    Router IP: fef1::d0d0
                    Router MAC: 00:00:00:00:03:00
host)show mld-snooping mrouter vlan 1

   Flags: D - Dynamic, S - Static, P - PIM, M - IGMP/MLD query

   MLD Snooping Multicast Router Ports
   -----------------------------------
   VLAN  Elected-Querier  Ports (Flags)  Expiry    UpTime
   ----  ---------------  -------------  ------    ------
   0001  fef1::d0d0       GE0/0/4 (DM)   00:04:11  00:00:09
```

Command History

Release	Modification
ArubaOS 7.2	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show mode-button

```
show mode-button
```

Description

This command displays the Mode button configuration for the S1500 Mobility Access Switch.

Syntax

Parameter	Description
`mode-button`	Displays the **Mode** button configuration for S1500 Mobility Access Switch.

Example

The example for the output of the show command is as follows:

```
(host) #show mode-button
mode-button (N/A)
-----------------
Parameter       Value
---------       -----
factory-default enabled
```

Related Command

Command	Description
mode-button	This command enables the **Mode** button and restores the S1500 Mobility Access Switches to factory default settings.

Command History

Release	Modification
ArubaOS 7.4.0.2	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show mstp-global-profile

Description

View the MSTP global profile information.

Example

```
(host)(config) #show mstp-global-profile

Global MSTP
-----------
Parameter                 Value
---------                 -----
MSTP region name          25
MSTP revision             0
Instance bridge priority  28 36864
Instance vlan mapping     4 1
MSTP hello time           2
MSTP forward delay        15
MSTP maximum age          20
MSTP max hops             20
```

The values in the output are detailed in the table below.

Parameter	Value
`MSTP region name`	The name of the region.
`MSTP revision`	The revision number.
`Instance bridge priority`	The instance number followed by its bridge priority value.
`Instance vlan mapping`	The instance number followed by the VLAN identifiers mapped to that instance.
`MSTP hello time`	The number of seconds configured for the MSTP Hello Time.
`MSTP forward delay`	The number of seconds configured for the MSTP Forward Delay.
`MSTP maximum age`	The time, in second, that the system waits before a refresh.
`MSTP max hops`	The time, in seconds, for the maximum hops.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show neighbor-devices phones

```
show neighbor-devices phones
```

Description

This command displays the neighboring phones in the network and the Voice VLAN associated with the phones.

Syntax

No parameters.

Usage Guidelines

Use this command to view the neighboring phones in the network and the Voice VLAN associated with the phones.

Examples

```
host) #show neighbor-devices phones
Neighbor Phones
---------------
Interface   Protocol   Phone MAC          Voice VLAN
---------   --------   ---------          ----------
GE0/0/6     CDPv2      00:1b:54:c9:e9:fd  -
GE0/0/47    CDPv2      00:1b:54:c9:e9:fd  5
```

The output of this command includes the following information:

Parameter	Description
`Interface`	The interface in which the phone is discovered.
`Protocol`	The protocol used to discover the phone.
`Phone MAC`	MAC address of the discovered phone.
`Voice VLAN`	The Voice VLAN associated to the discovered phone. In the above output, "-" under the Voice VLAN column denotes that either Voice VLAN is not available or VoIP is not configured to run in auto-discover mode.

Command History

Release	Modification
ArubaOS 7.1.3	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show netdestination

```
show netdestination [STRING | ipv4 <STRING>]
```

Description

This command displays a list of IPv4 network destinations.

Syntax

Parameter	Description
`STRING`	Name of destination.
`ipv4`	Show IPv4 network destinations.

Example

```
(host) #show netdestination Mywhite-list

Mywhite-list
------------
Position  Type    IP addr       Mask-Len/Range
--------  ----    -------       --------------
1         host    10.16.22.18   32
2         range   10.16.22.19   10.16.22.30
```

Related Commands

Command	Description
netdestination	This command configures an alias for an IPv4 network host, subnetwork, or range of addresses.

Command History

Release	Modification
ArubaOS 7.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show netservice

```
show netservice [STRING]
```

Description

This command displays a list of IPv4 network protocol services.

Syntax

Parameter	Description
STRING	Name of protocol service.

Example

```
(host) #show netservice

Services
--------
Name                    Protocol   Ports       ALG   Type
----                    --------   -----       ---   ----
any                     0          0
arp                     udp        0           sip
svc-dhcp                udp        67-68
svc-dns                 udp        53
```

Related Commands

Command	Description
netservice	This command configures an alias for network protocols.

Command History

Release	Modification
ArubaOS 7.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show oam brief

```
show oam brief
```

Description

This command displays the status of OAM on your Mobility Access Switches.

Syntax

No parameters.

Example

The **`show oam brief`** command displays a quick overview of the ports on which OAM is enabled.

```
OAM      Link-fault     Loopback     Link  Oper
Interface Mode    Action      Local   Remote  State State Remote MAC
--------- ------- ----------- ------- ------- ----- ----- -----------------
GE0/0/1   Active  Syslog      Enable  Disable Up    Up    00:0b:86:6a:4f:04
GE0/0/2   Active  Syslog      Enable  Disable Up    Up    00:0b:86:6a:4f:03
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config mode (config)

show oam counters

```
show oam counters
```

Description

This command displays a table of OAM counters on your Mobility Access Switches.

Syntax

No parameters.

Example

The show oam counters command displays the total PDUs received and transmitted, as well as the number of errors, on OAM-enabled ports.

```
Total PDU   Error PDU   Unknown PDU Total PDU   Transmit
Interface Received    Received    Received    Transmitted Discarded
--------- ----------- ----------- ----------- ----------- -----------
GE0/0/1           295           0           0         295           0
GE0/0/2           295           0           0         295           0
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config mode (config)

show papi-security

```
show papi-security
```

Description

The show papi-security command displays the status of PAPI security configuration on the Mobility Access Switch.

Usage Guidelines

Use this show command to verify the status of PAPI enhanced security configuration on the Mobility Access Switch. The PAPI key value is shown in encrypted format.

Examples

To verify the status of the PAPI Enhanced Security configuration, execute the following command:

```
(host) (config) #show papi-security
PAPI Security Profile
---------------------
Parameter               Value
---------               -----
PAPI Key                ********
Enhanced security mode Disabled
```

Related Commands

Command	Description
netservice	Enables or disables the PAPI Enhanced Security configuration on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.4.1.5	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration and Enable modes

show poe

```
show poe [controller]
```

Description

This command displays PoE information for the switch or the switch interfaces.

Syntax

Parameter	Description
`controller`	Displays PoE pool information for the switch.

Usage Guidelines

By default, the **`show poe`** command displays brief PoE information for all interfaces. Include the **controller** parameter to display PoE information for the switch.

Example

The examples below show some of the information displayed by the **`show poe`** commands.

```
(host) # show poe
Port      Status  Voltage(mV)  Current(mA)  Power (mW)
----      ------  -----------  -----------  ----------
GE0/0/0   On      55500        74           4100
GE0/0/1   Off     N/A          N/A          N/A
GE0/0/2   On      55800        50           2700
GE0/0/3   Off     N/A          N/A          N/A
GE0/0/4   Off     N/A          N/A          N/A
GE0/0/5   On      55900        80           4400
<Intentionally Truncated>

(host) # show poe controller
Linecard  PowerBudget(W)  Power Consumption(W)  GuardBand(mW)  PoE Management
--------  --------------  --------------------  -------------  --------------
0         689             7                     11000          Dynamic
```

The output of these commands include the following information:

Parameter	Description
`Port`	Name of the switch port.
`Status`	Indicates if PoE is enabled for the port.
`Voltage (mV)`	Port voltage, in millivolts.
`Current(mA)`	Port current, in milliamperes.
`Power (mW)`	Port power, in milliwatts.
`Linecard`	Specifies the module number.

Parameter	Description
PowerBudget	The switch allocates power to the PoE ports from a set PoE power budget. This parameter shows the cumulative power budget of all ports, in watts. The PowerBudget output for the different Mobility Access Switches are as follows: • S1500-12P: 100 • S1500-24P/48P: 400 • S2500-24P/48P : 400 • S3500-24P/48P: 400 with single PSU or 689 with dual PSU • S3500-48PF: 850 with single PSU or 1465 with dual PSU
Power Consumption	Current switch PoE power consumption, in watts.
GuardBand	The PoE guard band feature provides protection when there is a sudden spike in the power consumed by endpoint devices that could potentially impact other PoE-enabled ports. This parameter shows the amount of power reserved by the switch to prevent other PoE enabled ports from powering off and then on again.
PoE Management	This parameter shows the PoE management mode used by the switch. • Static Mode—The power deducted from the total power pool is the maximum power for that interface. This mode ensures that the maximum power specified by you for the interface is always reserved and cannot be shared by other endpoint devices. • Dynamic Mode—The power allocated from the total power pool for each port is the actual power consumed at that port. You can allocate any unused portion of power to the other PDs. This is the default mode. • Class-based Mode—The power allocated for each port from the total power pool is the maximum power available for the class of PD connected to that port.

Related Commands

Command	Description
interface-profile poe-profile	This command creates a PoE profile that can be assigned to any interface or interface group.
poe-management-profile	Configures PoE global power management parameters on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

show poe interface

```
show poe interface [brief]|[gigabitethernet <slot/module/port>]
```

Description

This command displays detailed PoE information for one or all port interfaces.

Syntax

Parameter	Description
`interface`	Displays PoE pool information for switch interfaces.
`brief`	Show general PoE status information for all interfaces
`gigabitethernet <slot/module/port>`	Show detailed PoE status for the specified Gigabit Ethernet slot/module/port.

Usage Guidelines

By default, this command shows detailed PoE information for all ports. Include the **`brief`** parameter to show general information for each interface, or include the **`interface gigabit <slot/module/port>`** parameter to show detailed PoE information for the specified interface only

Example

The output of the first command in this example shows detailed PoE information for the specified port interface. The second example shows general information for all ports:

```
(host) #show poe interface gigabitethernet 0/0/5

GE0/0/5: Administratively Enable, Port status: On
Maximum power: 30000 mW, Power consumption: 4400 mW
Port voltage: 56000 mV, Port current: 80 mA
PD class: Class-0, Priority: Low, PSE port status: On
Time-range: Periodic
   Start: daily, 18:00:00 PST
   End: daily, 09:00:00 PST

(host) #show poe interface
GE0/0/0
-------
GE0/0/0: Administratively Enable, Port status: On
Maximum power: 30000 mW, Power consumption: 4100 mW
Port voltage: 55500 mV, Port current: 74 mA
PD class: Class-3, Priority: High, PSE port status: On
GE0/0/1
-------
GE0/0/1: Administratively Enable, Port status: Off
Maximum power: 30000 mW, Power consumption: 0 mW
Port voltage: 0 mV, Port current: 0 mA
PD class: Class-0, Priority: Low, PSE port status: Off, PD detection in progress
GE0/0/2
-------
GE0/0/2: Administratively Enable, Port status: On
Maximum power: 30000 mW, Power consumption: 2700 mW
Port voltage: 55800 mV, Port current: 48 mA
```

```
PD class: Class-0, Priority: Low, PSE port status: On
<Intentionally Truncated>

(host) #show poe interface brief
PoE Interface Brief
-------------------
Interface  Admin    Consumption(mW)  Port Priority  Port Status
---------  -----    ---------------  -------------  -----------
GE0/0/0    Enable   4100             High           On
GE0/0/1    Enable   0                Low            Off
GE0/0/2    Enable   2700             Low            On
GE0/0/3    Enable   0                Low            Off
GE0/0/4    Enable   0                Low            Off
GE0/0/5    Enable   4400             Low            On
<Intentionally Truncated>
```

This command includes the following information:

Parameter	Description
`Interface`	The name and enable/disable status of a port.
`Port Status`	Shows if PoE has been enabled for the port.
`Maximum Power`	Shows the maximum power that can be supplied to the ethernet interface in milliwatts. The default value is 30000 mW.
`Power consumption`	Power consumed by the port, in milliwatts.
`Port Voltage (mV)`	Port voltage, in millivolts.
`Port Current(mA)`	Port current, in milliamperes.
`Power (mW)`	Port power, in milliwatts.
`PD Class`	Class of powered devices used by the port.
`Port Priority`	When you have a power shortage in the PoE pool, you can configure PoE port priority to define which PoE ports should be provided with power while disabling power on other ports until enough power is available for all the PoE ports. This parameter shows the current port setting.
`PSE Port Status`	Shows if the port is currently acting as a a PSE (Power sourcing equipment) for a powered device.

Related Commands

Command	Description
`interface-profile poe-profile`	This command creates a PoE profile that can be assigned to any interface or interface group.
`show poe`	This command displays PoE information for the switch or the switch interfaces.

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show poe-management-profile

```
show poe-management-profile slot [<slot-number>]
```

Description

This command displays total PoE pool information for the Mobility Access Switch.

Syntax

Parameter	Description	Range
`slot [<slot-number>]`	Stack member ID.	0–7

Example

This example shows that the device currently uses a dynamic PoE power management.

```
(host) #show poe-management-profile slot 2

poe-management profile "2"
------------------
Parameter                          Value
---------                          -----
Power Management Algorithm         dynamic
Guard band for PoE controller      11000
Cisco Pre-Standard compatibility   Enabled
```

The output of this command includes the following information:

Parameter	Description
Power Management Algorithm	This parameter shows the PoE management mode used by the switch. **`Static`**—The power deducted from the total power pool is the maximum power for that interface. This mode ensures that the maximum power specified by you for the interface is always reserved and cannot be shared by other endpoint devices. **`Dynamic`**—The power allocated from the total power pool for each port is the actual power consumed at that port. You can allocate any unused portion of power to the other PDs. This is the default mode. **`Class`**—The power allocated for each port from the total power pool is the maximum power available for the class of PD connected to that port.
Guard band for PoE controller	The PoE guard band feature provides protection when there is a sudden spike in the power consumed by endpoint devices that could potentially impact other PoE-enabled ports. This parameter shows the amount of power reserved by the switch to prevent other PoE enabled ports from powering off and then on again.
Cisco Pre-Standard compatibility	ArubaOS for Mobility Access Switch introduced the functionality to provide PoE compatibility with Cisco® legacy IP phones. By default, this function is disabled.

Related Commands

Command	Description
poe-management-profile	Configures PoE global power management parameters on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.0	Command introduced
ArubaOS 7.2.1	The **Cisco Pre-Standard compatibility** parameter was introduced in the output of this command.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show port-error-recovery

```
show port-error-recovery
```

Description

Displays the list of ports that are detected with port errors and the time at which they will be recovered automatically, if auto-recovery is enabled.

Syntax

Parameter	Description
`untrusted`	Displays the log/drop/shutdown errors on all untrusted ports.

Example

The following example shows the list of ports that are detected with port errors:

```
(host) #show port-error-recovery

Layer-2 Interface Error Information
-----------------------------------
Interface      Error                              Recovery Time
---------      -----                              -------------
Pc5            Shutdown (Loop Detected)           2012-02-08 16:42:45 (PST)
GE0/0/42       Shutdown (Loop Detected)           No Auto recovery
Pc1            Shutdown (Loop Detected)           2012-02-07 16:45:40 (PST)
Pc2            Shutdown (RA Guard)                2012-02-08 16:42:45 (PST)
GE0/0/14       Log      (Mac Limit Exceeded)      No Auto recovery
GE0/0/2        Drop     (DHCP Trust Error)        2012-02-07 16:45:40 (PST)
```

The output of this command displays the following parameters:

Parameter	Description
`Interface`	Name of the interface.
`Error`	The error detected on the interface.
`Recovery Time`	The time at which the interface will be automatically activated, if `auto-recovery` option is enabled.

You can verify that the configured action in the untrusted port is enforced when the number of MAC addresses exceeds the configured MAC limit. To verify it, execute the following **show** command:

```
(host) #show port-error-recovery untrusted
```

Command History

Release	Modification
ArubaOS 7.1.3	Command introduced.
ArubaOS 7.4.1.9	The **untrusted** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show port-security

```
show port-security <interface-name>
```

Description

Displays if the port security features are enabled or disabled on the interface.

Syntax

Parameter	Description
`<interface-name>`	Specify the interface for which you need to check the port-security operational state.

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show port stats

```
show port stats
```

Description

This command displays statistics for packets and bytes sent and received on all switch ports.

Syntax

No parameters.

Usage Guidelines

This **`show port stats`** command displays information about packets and bytes sent and received by the port. The **`show port status`** command display information about the configuration of each port.

Example

The command below shows a count of packets, bytes, error bytes and CRC errors for all switch ports. The output in the example below has been split into two separate tables to better fit in this document. In the switch command-line interface, this output appears in a single, wide table.

```
(host) #show port stats
Port                    PacketsIn       PacketsOut      BytesIn         BytesOut
gigabitethernet0/0/0    100259          1604100         19550289        204522732
gigabitethernet0/0/1    1604100         100259          204522732       19550289
gigabitethernet0/0/2    0               0               0               0
gigabitethernet0/0/3    0               0               0               0
gigabitethernet0/0/4    0               0               0               0
gigabitethernet0/0/5    0               0               0               0
   ...

InputErrorBytes    OutputErrorBytes    CRCError

0                  0                   0
0                  0                   0
0                  0                   0
0                  0                   0
0                  0                   0
0                  0                   0
   ...
```

The output of this command includes the following information:

Parameter	Description
`Port`	Name of the switch port.
`PacketsIn`	Number of packets received by the port.
`PacketsOut`	Number of packets sent by the port.
`BytesIn`	Number of bytes received by the port.
`BytesOut`	Number of bytes sent by the port.

Parameter	Description
`InputErrorBytes`	Number of bytes with errors received by the port.
`OutputErrorBytes`	Number of bytes with errors sent by the port.
`CRCError`	Number of frames with Cyclic Redundancy Check (CRC) errors.

Related Commands

Command	Description
`show port status`	This command displays status information for all the interfaces.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show port status

```
show port status
```

Description

This command displays link status information for all the interfaces.

Syntax

No parameters.

Usage Guidelines

Use the **show port status** command to display information about the port configuration. The **show port status** command displays information about packets and bytes sent and received by the port.

Example

The following command shows the current status of each port on the switch.

```
(host) #show port status
Interface   Admin    Line Protocol   Link   PoE       Trusted   Mode
---------   -----    -------------   ----   ---       -------   ----
GE0/0/0     Enable   Up              Up     Enable    No        Access
GE0/0/1     Enable   Down            Down   Enable    No        Access
GE0/0/2     Enable   Up              Up     Enable    No        Access
GE0/0/3     Enable   Down            Down   Enable    No        Access
GE0/0/4     Enable   Down            Down   Enable    No        Access
GE0/0/5     Enable   Up              Up     Enable    No        Access
<Intentionally Truncated>
```

The output of this command includes the following information:

Parameter	Description
Interface	Name of the port interface.
Admin	Shows if the port has been administratively enabled or disabled.
Line Protocol	Status of the line protocol on the port.
Link	Status of the link.
PoE	Shows if the port is PoE capable or not.
Trusted	Shows if the port has been configured as a trusted port.
Mode	Shows if the port's switching profile has the port configured in access or tunnel mode.

Related Commands

Command	Description
show port stats	This command displays statistics for packets and bytes sent and received on all switch ports.

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show port trusted

```
show port trusted
```

Description

This command displays the trusted ports.

Syntax

No Parameters

Example

The output of this command lists the switch ports that have been configured as a trusted port.

```
(host) #show port trusted
port-channel1
gigabitethernet0/0/19
gigabitethernet0/0/20
gigabitethernet0/0/21
gigabitethernet0/0/22
gigabitethernet0/0/23
gigabitethernet0/0/0
gigabitethernet0/0/1
gigabitethernet0/0/2
gigabitethernet0/0/3
gigabitethernet0/0/4
gigabitethernet0/0/5
gigabitethernet0/0/6
<output truncated>
```

Related Commands

Command	Description
interface gigabitethernettrusted port	Sets the port to trusted mode.

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show probe

```
show probe
```

Description

This command displays the probe status of the interfaces where the probe profile is attached.

Syntax

No parameters.

Example

The output of the following command displays the probe status of the interfaces where the probe profile is attached.

From ArubaOS 7.4.0.3, the output of the show probe command displays a new **Flags** column that indicates the cause due to which the probe status of the interface is down.

The cause can be one of the following:

- IP is your own-ip
- Protocol is down for the interface
- IP not assigned for the interface
- MAC is not resolved for the route next-hop
- Route is not present for the probe destination
- URL is not resolved

```
(host) #show probe
IPV4 PROBE Table
----------------
Vlan   Server          Protocol Port Probe-State Sent Received Flags
-----  ------          -------- ---- ----------- ---- -------- -----
vlan1  10.16.44.110    ICMP     N/A  Own-IP       N/A  N/A     IP is your own-ip
vlan1  10.16.52.8      ICMP     N/A  Up           2    1       N/A
vlan1  www.google.com  ICMP     N/A  Up           1    0       N/A
vlan50 10.16.52.8      ICMP     N/A Down          N/A  N/A     Protocol is down for the
interface
Total Probe host entries: 4
```

Related Command

Command	Description
probe-profile	Create and configure a probe-profile

Command History

Release	Modification
ArubaOS 7.4	Command was introduced
ArubaOS 7.4.0.3	**Flags**, a new column, is introduced in the output of the show probe command.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show probe-profile

```
show probe-profile
```

Description

This command displays the details of the probe profiles configured on the system.

Syntax

Parameter	Description
<probe-profile>	Name of the probe-profile for which you want to view the details.

Example

The following command displays the configuration on a probe-profile named **L3Monitoring**:

```
(host)  #show probe-profile L3Monitoring
probe profile "L3Monitoring"
---------------------------------
Parameter                     Value
---------                     -----
Destination IP                10.1.10.1
Packet Lost Count             16
Packet Found Count            16
Packet Send Frequency (Secs)  11
Protocol                      icmp
```

The following command displays the list of probe-profiles configured and their references:

```
(host) #show probe-profile
probe profile List
------------------
Name          References  Profile Status
----          ----------  --------------
default       0           N/A
L3Monitoring  1           N/A
test          0           N/A
Total:3
```

Related Command

Command	Description
probe-profile	Use this command to configure a probe-profile.

Command History

Release	Modification
ArubaOS 7.4	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show profile-errors

```
show profile-errors
```

Description

This command displays the errors in the profiles.

Syntax

No parameters.

Example

The output of this command lists any profiles with configuration errors, and gives a brief description of the error.

```
(host) #Invalid Profiles
----------------
Profile                          Error
-------                          -----
time-range-profile "absolute"    End time must be later then current time
time-range-profile "gst"         End time must be later then current time
```

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show profile-hierarchy

```
show profile-hierarchy
```

Description

This command is reserved for future use.

show profile-list

```
show profile-list
   aaa
   interface
   interface-group
   interface-profile
   ip
   poe-management-profile
   policer-profile
   qos-profile
   rmon
   time-range-profile
   vlan
   vlan-profile
```

Description

Use this command to display a list of profiles in the specified category.

Syntax

Parameter	Description
`aaa`	Displays AAA configuration.
`interface`	Select an interface for configuration.
`interface-group`	Select an interface group to configure.
`interface-profile`	Displays the list of interface profiles.
`ip`	Displays the IP address of the interface.
`poemanagement member-id 0`	Displays the list of PoE (Power over Ethernet) management profiles.
`policer-profile`	Displays the list of policer profiles.
`qos-profile`	Displays the list of QoS profiles.
`rmon {alarm | alarm-profile | etherstat | event | history }`	Displays the remote monitoring parameters.
`time-range-profile`	Configures a time range profile.
`vlan`	Displays all the VLANs.
`vlan-profile`	Displays the details of one of the following VLAN profiles: • igmp-snooping-profile • mld-snooping-profile • pvst-profile • dhcp-snooping-profile

Example

The output of the command in this example shows a list of policer profiles. The **References** column lists the number of other profiles with references to the policer 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 profile-list policer-profile

Policer Profile List
--------------------
Name      References  Profile Status
----      ----------  --------------
default   0
Policer1  2
Total:2
```

Related Commands

Command	Description
interface-group gigabitethernet	This command applies the same configuration parameters to a group of Gigabit Ethernet interfaces.

Command History

Release	Modification
ArubaOS 7.0	Command introduced.
ArubaOS 7.1.3	The **rmon** parameter was introduced.
ArubaOS 7.3	The **dhcp-snooping-profile** was introduced under **vlan-profile**.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show profile-list interface

```
show profile-list interface
   gigabitethernet [page] [start]
   loopback [page] [start]
   port-channel [page] [start]
   tunnel ethernet [page] [start]
   vlan [page] [start]
```

Description

This command displays the list of profiles in the specified category.

Syntax

Parameter	Description
`gigabitethernet`	Displays the list of Gigabit Ethernet interfaces.
`page`	Number of items to display.
`start`	Index of first item to display.
`loopback`	Displays the list of Loopback interfaces.
`page`	Number of items to display.
`start`	Index of first item to display.
`port-channel`	Displays the list of port channels.
`page`	Number of items to display.
`start`	Index of first item to display.
`tunnel ethernet`	Displays the list of tiunnel ethernet interfaces.
`page`	Number of items to display.
`start`	Index of first item to display.
`vlan`	Displays the list of VLAN interfaces.
`page`	Number of items to display.
`start`	Index of first item to display.

Example

The output of this command shows a list of Gigabit Ethernet interface profiles. The **References** column lists the number of other profiles with references to the gigabitethernet 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 profile-list interface gigabitethernet
gigabitethernet List
--------------------
Name    References  Profile Status
```

```
----   ----------  --------------
0/0/0  0
Total:1
```

The following command shows the list of port-channel interfaces, and lists the other profiles with references to that port channel. This example shows that there are two other profiles that reference port-channel

```
(host) #show profile-list interface port-channel

port-channel List
-----------------
Name  References  Profile Status
----  ----------  --------------
1     2
Total:1
```

Related Commands

Command	Description
interface gigabitethernet	This command configures a Gigabit Ethernet port on theMobility Access Switch.
interface loopback	This command configures a loopback interface on the Mobility Access Switch.
interface port-channel	This command configures a port channel on the Mobility Access Switch.
interface tunnel ethernet	This command configures a tunnel ethernet port on the Mobility Access Switch.
interface vlan	This command configures a VLAN interface on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show profile-list interface-group

```
show profile-list interface-group gigabitethernet [page][start]
```

Description

This command displays the list of gGigabit Ethernet interface group profiles.

Syntax

Parameter	Description
`page`	Number of items to display.
`start`	Index of first item to display.

Example

The output of this command shows a list of Gigabit Ethernet interface-group profiles. The **References** column lists the number of other profiles with references to the gigabitethernet interface-group profile, and the **Profile Status** column indicates whether the interface-group profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show profile-list interface-group gigabitethernet

gigabitethernet List
--------------------
Name       References  Profile Status
----       ----------  --------------
default    0
corporate  0
Total:2
```

Related Commands

Command	Description
`interface gigabitethernet`	This command configures a Gigabit Ethernet port on the switch.

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show profile-list interface-profile

```
show profile-list interface-profile
   dhcp-relay-profile
   enet-link-profile
   gvrp-profile
   igmp-profile
   lacp-profile
   lldp-profile
   mirroring-profile
   mstp-profile
   oam-profile
   ospf-profile
   pim-profile
   poe-profile
   port-security-profile
   pvst-port-profile
   switching-profile
   tunneled-node-profile
   voip-profile
```

Description

This command displays a list of of interface profiles for the specified profile type.

Syntax

Parameter	Description
dhcp-relay-profile	Shows all the dhcp relay profiles.
enet-link-profile	Show all Ethernet Link profiles.
gvrp-profile	Shows all the GVRP profiles.
igmp-profile	Shows all the interface IGMP profiles.
lacp-profile	Shows all the LACP profiles.
lldp-profile	Shows all the LLDP Profiles.
mirroring-profile	Shows all the Mirroring profiles.
mstp-profile	Shows all the Interface MSTPs.
oam-profile	Shows all the OAM profiles.
ospf-profile	Shows all the OS{PF profiles.
pim-profile	Shows all the PIM profiles.
poe-profile	Shows all the Power over Ethernet profiles.
port-security-profile	Shows all the Port Security profiles.
pvst-port-profile	Shows all the Interface PVST bridges.

Parameter	Description
`switching profile`	Shows all the switching profiles.
`tunneled-node-profile`	Shows all the tunneled node server profiles.
`voip-profile`	Shows all the VOIP profiles.

Examples

The output of the command in this example shows a list of Power over Ethernet profiles. The **References** column lists the number of other profiles with references to the PoE 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 profile-list interface-profile  poe-profile

Power over Ethernet profile List
--------------------------------
Name                 References  Profile Status
----                 ----------  --------------
default              14
poe-factory-initial  1
Total:2
```

The example below shows that the Mobility Access Switch has two LACP profiles. The **References** column lists the number of other profiles with references to the LACP 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 profile-list interface-profile lacp-profile

LACP List
---------
Name  References  Profile Status
----  ----------  --------------
profile1   8
Profile2   8
Total:2
```

The example below shows that the tunneled node profile is named **tunnel1**, and that there are three other profiles with references to the tunneled node profile. 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 profile-list interface-profile tunneled-node-profile

Tunneled Node Server profile List
---------------------------------
Name     References  Profile Status
----     ----------  --------------
tunnel1  3
```

The output of the following command in this example shows a list of LLDP profiles. The **References** column lists the number of other profiles with references to the LLDP 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 profile-list interface-profile lldp-profile

LLDP Profile List
-----------------
Name                  References  Profile Status
----                  ----------  --------------
```

```
default                0
lldp-factory-initial   1
Total:2
```

The following command displays the name of the current mirroring-profile. The **References** column lists the number of other profiles with references to the mirroring 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 profile-list interface-profile mirroring-profile

Mirroring profile List
----------------------
Name      References  Profile Status
----      ----------  --------------
profile2  0
Total:1
```

Related Commands

Command	Description
show interface-profile	This command displays a list of of interface profiles for the specified profile type.

Command History

Release	Modification
ArubaOS 7.0	Command introduced

show profile-list vlan

```
show profile-list vlan [page] [start]
```

Description

Use this command to display a list of VLAN profiles.

Syntax

Parameter	Description
`page`	Number of items to display.
`start`	Index number of first item to display.

Example

The output of the command in this example shows a list of VLAN profiles. The **References** column lists the number of other profiles with references to the VLAN 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 profile-list vlan
VLAN List
---------
Name  References  Profile Status
----  ----------  --------------
1     0
10    0
Total:2
```

Related Commands

Command	Description
`interface vlan`	This command creates the VLAN interface for the switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show profile-list vlan-profile

```
show profile-list vlan-profile
   igmp-snooping-profile
   mld-snooping-profile
   pvst-profile
   dhcp-snooping-profile
```

Description

This command displays the list of profiles in the specified category.

Syntax

Parameter	Description
`igmp-snooping-profile`	Displays the list of IGMP snooping profiles.
`mld-snooping-profile`	Displays the list of MLD snooping profiles.
`pvst-profile`	Displays the list of PVST profiles.
`dhcp-snooping-profile`	Displays the DHCP snooping information.

Example

The output of the command in this example shows a list of IGMP snooping profiles. The **References** column lists the number of other profiles with references to the IGMP snooping 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 profile-list vlan-profile igmp-snooping-profile
igmp-snooping-profile List
--------------------------
Name                          References  Profile Status
----                          ----------  --------------
default                       2
igmp-snooping-factory-initial  1
profile123                    0
Total:3
```

Related Command

Command	Description
vlan-profile igmp-snooping-profile	This command creates an IGMP snooping profile that can be applied to a VLAN.
vlan-profile mld-snooping-profile	This command creates an MLD snooping profile that can be applied to a VLAN.
vlan-profile pvst-profile	This command creates a PVST profile that can be applied to a VLAN.

Command History

Release	Modification
ArubaOS 7.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

show qos-profile trusted

```
show qos-profile trusted [<profile-name> | output modifiers]
```

Description

Use the show qos-profile trusted command in enable mode to display QoS profile information.

Example

The example below shows the QoS profile information.

```
(svl_techpubs)(config) #show  qos-profile trusted

Default Trusted QoS Profiles
----------------------------
Name          TC   DP   DSCP(Upd)   Dot1p(Upd)   Token
----          --   --   ---------   ----------   -----
def-dscp-0    0    0    0(n)        0(n)         0t5r
def-dscp-1    0    0    0(n)        0(n)         1
def-dscp-2    0    0    0(n)        0(n)         2
def-dscp-3    0    0    0(n)        0(n)         3
def-dscp-4    0    2    0(n)        0(n)         4
def-dscp-5    0    2    0(n)        0(n)         5
def-dscp-6    0    2    0(n)        0(n)         6
def-dscp-7    0    2    0(n)        0(n)         7
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of QoS profile.
TC	Traffic Classification (0-7)
DP	Drop Precedence (0-2)
DSCP (Upd)	DSCP Rewrite Value (Flag to indicate DSCP value should be rewritten.)
Dot1p (Upd)	Dot1P Rewrite Value (Flag to indicate DSCP value should be rewritten.)
Token	Internal use only.

Command History

Release	Modification
ArubaOS 7.1	Command introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show references

```
show references
   aaa
   gvrp
   interface {gigabitethernet|mgmt|port-channel|vlan} [<profile-name>]
   interface-group gigabitethernet <group-name>
   interface-profile {enet-link-profile|lacp-profile|lldp-profile|mstp-profile|poe-
   profile|tunneled-node-profile} <profile-name>
   ip dhcp pool <profile-name> [page] [start]
   ip-profile <profile-name>
   ipv6-profile [page] [start]
   lacp <profile-name>
   lcd-menu [page] [start]
   mstp <profile-name>
   poe-management-profile slot <slot>
   policer-profile <profile-name>
   qos-profile <profile-name>
   rmon
   router
   service
   spanning-tree
   stack-profile
   time-range-profile
   traceoptions <profile-name>
   user-role <role_name>
   vlan <vlan>
   vlan-profile {igmp-snooping-profile|pvst-profile} [<profile-name>]
   web-server [page][start]
```

Description

This command displays the list of references to the specified interface or profile.

Syntax

Parameter	Description
`interface`	Display the list of references to an individual interface.
`gigabitethernet <profile-name>`	Display references to the specified Gigabit Ethernet interface.
`mgmt <profile-name>`	Display references to the specified management interface.
`port-channel <profile-name>`	Display references to the specified port-channel interface.
`vlan <profile-name>`	Display references to the specified VLAN.
`interface-group gigabitethernet <group-name>`	Displays the list of references to a Gigabit Ethernet group profile.
`interface-profile`	Display the list of references to an interface profile.

Parameter	Description
enet-link-profile <profile-name>	Display references to the specified Ethernet link profile.
lacp-profile <profile-name>	Display references to the specified LACP profile.
lldp-profile <profile-name>	Display references to the specified LLDP profile.
mstp-profile <profile-name>	Display references to the specified MSTP profile.
poe-profile <profile-name>	Display references to the specified PoE profile.
tunneled-node-profile <profile-name>	Display references to the specified tunneled node profile.
ip dhcp <pool>	Display references to a dhcp server profile.
ip-profile <profile-name>	Display references to the specified.
ipv6-profile	Display references to the ipv6-profile.
page	Number of items to display.
start	Index of first item to display.
lacp <profile-name>	Display references to the specified.
lcd-menu	Enable or disable LCD menus.
page	Number of items to display.
start	Index of first item to display.
mstp <profile-name>	Display references to the specified MSTP profile.
poemanagement member-id <member-id>	Displays the list of references to the PoE management profile. **NOTE:** The stack member-ID is always 0, as stacking support is not available in this release.
policer-profile <profile-name>	Display references to the specified policer profile.
qos-profile <profile-name>	Display references to the specified QoS profile.
rmon	Display the references to the specified remote monitoring parameters.
alarm	Display the references to the parameters of alarm entry.
alarm-profile	Display the references to the alarm profile.
etherstat	Display the references to the parameters of etherstat entry.
event	Display the references to the parameters of event entry.

Parameter	Description
history	Display the references to the parameters of history entry.
router	Display the references to the following profiles: • Global OSPF profile • Global PIM profile
service	Display references to one of the following services: • DHCP • RMON
spanning-tree	Display references to Spanning Tree.
stack-profile	Display references to stack-profile.
time-range-profile	Displays a time-range-profile.
traceoptions <profile-name>	Display references to the specified trace options profile.
user-role <role_name>	Displays the access rights for a particular user role.
vlan <vlan>	Displays references to a vlan.
vlan-profile	Displays vlan profile references.
igmp-snooping profile	Show references to an igmp-snooping-profile.
mld-snooping-profile	Show references to an mld-snooping-profile.
pvst-profile	Show references to a pvst-profile.
web-server	Displays web server configuration.
page	Number of items to display.
start	Index of first item to display.

Example

The example below shows that the interface port-channel 1 and the Gigabit Ethernet interface group **default** reference the **default** MSTP profile.

```
(host) #show references interface-profile mstp-profile default

References to Interface MSTP "default"
--------------------------------------
Referrer                                                Count
--------                                                -----
interface port-channel "1" mstp-profile                 1
interface-group gigabitethernet "default" mstp-profile  1
Total References:2
```

The output of the command in the example below shows that VLAN 1 and VLAN 7 both reference the IGMP snooping profile **default.**

```
(host) #show references vlan-profile igmp-snooping-profile igmp-snooping-factory-initial
```

```
References to igmp-snooping-profile "default"
---------------------------------------------
Referrer                        Count
--------                        -----
vlan "7" igmp-snooping-profile  1
vlan "1" igmp-snooping-profile  1
Total References:2
```

The command below is an example for viewing references

```
(host) show references vlan-profile mld-snooping-profile default

References to mld-snooping-profile "default"
--------------------------------------------
Referrer                          Count
--------                          -----
vlan "1" mld-snooping-profile     1
vlan "1111" mld-snooping-profile  1
Total References:2
```

The example below shows that the interface-group **default** makes a single reference to the LLDP profile **lldp-factory-initial**.

```
(host) #show references interface-profile lldp-profile lldp-factory-initial

References to LLDP Profile "lldp-factory-initial"
-------------------------------------------------
Referrer                                                Count
--------                                                -----
interface-group gigabitethernet "default" lldp-profile  1
Total References:1
```

The example below shows that the interface port-channel **1** and the Gigabit Ethernet interface group **default** reference the mirroring profile **profile2**:

```
(host) #show references interface-profile mirroring-profile profile2

References to Mirroring profile "profile2"
------------------------------------------
Referrer                                                    Count
--------                                                    -----
interface port-channel "1" mirroring-in-profile             1
interface-group gigabitethernet "default" mirroring-in-profile  1
Total References:2
```

The example below shows that the interface port-channel 1 and the Gigabit Ethernet interface groups **corpadm**, **backup** and **branch_2** all reference the **lacp1** LACP profile.

```
(host) #show references interface-profile lacp-profile lacp1
References to LACP profile "lacp1"
----------------------------------------
Referrer                                              Count
--------                                              -----
interface port-channel "1" lacp-profile                       1
interface-group gigabitethernet "corpadm" lacp-profile    1
interface-group gigabitethernet "backup" lacp-profile     1
interface-group gigabitethernet "branch_2" lacp-profile   1
Total References:4
```

The output of the command in the example below shows that three interfaces reference the tunneled node profile **tunnel1**.

```
(host)#show references interface-profile tunneled-node-profile tunnel1

References to Tunneled Node Server profile "tunnel1"
```

```
-------------------------------------------------
Referrer                                                Count
--------                                                -----
interface gigabitethernet "0/0/6" tunneled-node-profile  1
interface gigabitethernet "0/0/7" tunneled-node-profile  1
interface gigabitethernet "0/0/8" tunneled-node-profile  1
Total References:3
```

The first example below shows that the port-channel interface 1 and the Gigabit Ethernet interface groups **default**, **mgt** and **corporate** all reference the default switching profile. The second example shows that no interfaces or interface groups reference vlan 16.

```
(host) #show references interface-profile switching-profile default
References to switching profile "default"
-----------------------------------------
Referrer                                                    Count
--------                                                    -----
interface port-channel "0" switching-profile                1
interface-group gigabitethernet "default" switching-profile   1
interface-group gigabitethernet "Mgt" switching-profile       1
interface-group gigabitethernet "corporate" switching-profile 1
Total References:4

(host) #show references vlan 16
References to VLAN "16"
-----------------------
Referrer  Count
--------  -----
Total References:0
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

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 the **show rights** command shows the list of roles in the roles table.

```
(host) #show rights
RoleTable
---------
Name             ACL  ACL List                                  Type
----             ---  --------                                  ----
Employee_1       61                                              User
Role1            45                                              User
Role3            47                                              User
ap-role          49                                              User
authenticated    6    allowall-stateless/                        User
default          51                                              User
denyall          17   denyall-stateless/                         User
denydhcp         22   denydhcp/                                  User
employee         53   mDNS_redirect/                             User
guest            4    http-acl-stateless/,                       User
                      https-acl-stateless/,
                      dhcp-acl-stateless/,
                      icmp-acl-stateless/,
                      dns-acl-stateless/
guest-logon      55                                              User
logon            1    logon-control-stateless/                   User
preauth          15                                              User
stateful-dot1x   57                                              User
test             59                                              User
```

The following command shows the policy details for the role 'logon'.

```
(host) # show rights logon
Derived Role = 'logon'
 Periodic reauthentication: Disabled
 Deny inter-user traffic: Enabled
 ACL Number = 2/0/3
access-list List
----------------
Position  Name                      Type       Location
--------  ----                      ----       --------
1         logon-control-stateless   stateless
logon-control-stateless
-----------------------
```

```
Priority Source Destination Service Action TimeRange Log Expired QoS
-------- ------ ----------- ------- ------ --------- --- ------- ---
1         user   any         udp 68   deny
2         any    any         svc-icmp permit
3         any    any         svc-dns  permit
4         any    any         svc-dhcp permit
5         any    any         svc-natt permit

Policer  Blacklist Mirror IPv4
-------  --------- ------ ----
                          4
                          4
                          4
                          4
                          4
Expired Policies (due to time constraints) = 0
```

Command History

Release	Modification
ArubaOS 7.0	Command introduced.
ArubaOS 7.4	The **Deny inter-user traffic** status information was added to the output.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration mode

show rmon alarms

```
show rmon alarms {brief | entry <index>}
```

Description

This command is used to display the alarms on the device either briefly or detailed on alarm entry index basis.

Example

```
(host)# show rmon alarms brief

Total: 1 entry

RMON Alarm Table:
-----------------
RMON Alarm Table
----------------
Alarm Index  Variable      Rising Threshold Value  Falling Threshold Value  Owner
-----------  --------      ----------------------  -----------------------  -----
1            ifInErrors.8  10                      0                        config

(host) #show rmon alarms entry 1

Alarm 1 is active, owned by config
    Monitors ifHCInMulticastPkts.1 every 10 seconds
    Taking delta sample, last value was 0
    Rising threshold value is 300, assigned to event 1
    Falling threshold value is 100, assigned to event 1
```

Command History

Release	Modification
ArubaOS 7.1.3	Command introduced

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

show rmon alarm-oid

```
show rmon alarm-oid
```

Description

This command is used to list the alarm-oids supported on a device to use as an alarm variable.

Example

The following example displays the alarm-oids supported on a device to use as an alarm variable:

```
(host)#show rmon alarm-oid

Supported OID List
------------------
Object Name                    Object Identifier
-----------                    -----------------
ifOutOctets                    1.3.6.1.2.1.2.2.1.16
ifInUcastPkts                  1.3.6.1.2.1.2.2.1.11
ifOutUcastPkts                 1.3.6.1.2.1.2.2.1.17
ifOutBroadcastPkts             1.3.6.1.2.1.31.1.1.1.5
ifInErrors                     1.3.6.1.2.1.2.2.1.14
ifHCInOctets                   1.3.6.1.2.1.31.1.1.1.6
ifHCInUcastPkts                1.3.6.1.2.1.31.1.1.1.7
ifHCInMulticastPkts            1.3.6.1.2.1.31.1.1.1.8
ifHCOutMulticastPkts           1.3.6.1.2.1.31.1.1.1.12
ifHCOutBroadcastPkts           1.3.6.1.2.1.31.1.1.1.13
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show rmon-config alarm

```
show rmon-config alarm [index]
```

Description

This command displays all the alarms in the system.

Example

The following example displays all the alarms in the system:

```
(host) #show rmon-config alarm

alarm List
----------
Name  References  Profile Status
----  ----------  --------------
1     0
3     0
Total:2

(host) #show rmon-config alarm 1

alarm "1"
---------
Parameter                 Value
---------                 -----
RMON Alarm Profile        al1
OID to monitor            ifHCOutBroadcastPkts.8
Owner of this alarm entry config
```

Command History

Release	Modification
ArubaOS 7.1.3	Command introduced

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

show rmon-config alarm-profile

```
show rmon-config alarm-profile [profile-name]
```

Description

This command displays all the alarm-profiles existing in the system.

Example

The following example displays all the alarm-profiles existing in the system:

```
(host) #show rmon-config alarm-profile

alarm profile List
------------------
Name  References  Profile Status
----  ----------  --------------
al1   1
Total:1

(host) #show rmon-config alarm-profile al1

alarm profile "al1"
-------------------
Parameter                                              Value
---------                                              -----
Interval at which samples need to be taken             10
Alarm sample type                                      delta
Rising threshold against which to compare the value    10
Falling threshold against which to compare the value   0
Rising event index                                     1
Falling event index                                    1
Initial alarm (rising, falling, or either)             rising-or-falling
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

show rmon-config etherstat

```
show rmon-config etherstat [index]
```

Description

This command displays all the etherstat entries that exist in the system.

Example

The following command displays all the etherstat entries that exist in the system.:

```
(host) #show rmon-config etherstat

Etherstat index List
--------------------
Name  References  Profile Status
----  ----------  --------------
1     0
2     0
3     0
Total:3


(host) #show rmon-config etherstat  1

Etherstat index "1"
-------------------
Parameter                     Value
---------                     -----
OID to monitor                ifIndex.19
Owner of this etherstat entry  config
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

show rmon-config event

```
show rmon-config event [index]
```

Description

This command is used to display the configuration done for a specific event index.

Example

The following example displays the configuration done for an event:

```
(host) #show rmon-config event

Event index List
----------------
Name  References  Profile Status
----  ----------  --------------
1     2
Total:1

The following example displays the configuration done for a specific event index:

(host) #show rmon-config event 1

Event index "1"
---------------
Parameter                      Value
---------                      -----
Description of the event       rmon_event
Owner of the event             config
Type of the event              log-and-trap
```

Command History

Release	Modification
ArubaOS 7.1.3	Command introduced

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

show rmon-config history

```
show rmon-config history [index]
```

Description

This command is used to display all the history entries that exist in the system.

Example

The following example displays all the history entries that exist in the system:

```
(host) #show rmon-config history

History index List
------------------
Name  References  Profile Status
----  ----------  --------------
1     0
10    0
Total:2
```

The following example displays history entry for a specific index entry:

```
(host) #show rmon-config history  1

History index "1"
-----------------
Parameter                   Value
---------                   -----
Number of samples           50
Interval of each sample     1800
OID to monitor              ifIndex.455
Owner of this history entry config
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

show rmon etherstat entry

```
show rmon etherstat entry <index>
```

Description

Displays the etherstat entries for a particular interface indexed by an etherstat index.

Example

```
(host) #show rmon etherstat entry 1

RMON etherstat Entry 1 is Active, and owned by config
Monitors gigabitethernet0/0/18 from 2-22-2012@03-59-01
Statistics:
    Received 0 octets, 0 packets
    0 broadcast, 0 multicast packets
    0 oversized packets, 0 fragments, 0 jabbers
    0 CRC alignment errors, 0 collisions
    Number of dropped packet events is 0
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show rmon event-table

```
show rmon event-table
```

Description

This command is used to display the event-table details.

Example

The following example lists the event-table details:

```
(host) #show rmon event-table

RMON Event Table:
-----------------
Event Index  Type            Last Seen          Description  Owner
-----------  ----            ---------          -----------  -----
1            log             -                  rmon_event   config
2            log and Trap    -                  rmon_event   config
3            trap            3-8-2012@08-54-34  rmon_event   config
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show rmon history

```
show rmon history {brief | entry <index>}
```

Description

This command is used to display the history table either briefly or detailed on history entry index basis.

Example

The following examples displays the history table either briefly or detailed on history entry index basis.

```
(host)#show rmon history brief

Total: 1 entry

RMON History Table
------------------
History Index  Interface             Octets   Pkts   Bcast Pkts  MCast Pkts  Utilization
-------------  ---------             ------   ----   ----------  ----------  -----------
1              gigabitethernet0/0/1  1323196  19594  0           19554       17

(host) #show rmon history entry 1

Entry 1 is active, and owned by config
    Monitors gigabitethernet0/0/0 every 1800 seconds
    Buckets requested 50, Buckets granted 50
    0 sample(s) created
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

show rmon history number

```
show rmon history [entry] [count]
```

Description

This command is used to display the number of latest samples for this history entry.

Example

The following example displays the number of latest samples for this history entry:

```
(host) #show rmon history entry 1 count 2

Entry 1 is active, and owned by config
    Monitors gigabitethernet0/0/1 every 8 seconds
    Requested number of timer intervals 3
    Granted number of timer intervals 3
    3 sample(s) created

Sample 509:
    Began measuring at 2-22-2012@05-06-52
    Received 1447269 octets, 21438 packets
    0 broadcast, 21398 multicast packets
    0 oversized packets, 0 fragments, 0 jabbers
    0 CRC alignment errors, 0 collisions
    Number of dropped packet events is 0
    Network utilization is estimated at 18

Sample 508:
    Began measuring at 2-22-2012@05-06-44
    Received 1453462 octets, 21502 packets
    0 broadcast, 21451 multicast packets
    0 oversized packets, 0 fragments, 0 jabbers
    0 CRC alignment errors, 0 collisions
    Number of dropped packet events is 0
    Network utilization is estimated at 18
```

Command History

Release	Modification
ArubaOS 7.1.3	Command introduced

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show rmon log-table

```
show rmon log-table
```

Description

This command is used to display the log-table details.

Example

The following example displays the log-table details:

```
(host) #show rmon log-table

RMON Log Table:
---------------
Log Id  Event Id  Creation Time       Description
------  --------  -------------       -----------
3       2         3-17-2012@20-35-33  Falling threshold log: ifInUcastPkts.455
2       2         3-17-2012@20-35-33  Falling threshold log: ifHCInOctets.455
8       3         3-17-2012@20-35-23  Rising threshold log: ifInUcastPkts.455
1       2         3-17-2012@20-35-13  Falling threshold log: ifInUcastPkts.455
7       3         3-17-2012@20-35-03  Rising threshold log: ifInUcastPkts.455
6       3         3-17-2012@20-34-53  Rising threshold log: ifHCInOctets.455
5       3         3-17-2012@20-32-07  Rising threshold log: ifInUcastPkts.455
4       3         3-15-2012@21-03-07  Rising threshold log: ifInUcastPkts.455
3       3         3-15-2012@21-02-27  Rising threshold log: ifInUcastPkts.455
2       3         3-15-2012@21-01-57  Rising threshold log: ifInUcastPkts.455
1       3         3-15-2012@21-01-17  Rising threshold log: ifInUcastPkts.455
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

show rmon log-table event

```
show rmon log-table event <event-id> log <log-id>
```

Description

This command displays the the detailed information of a log entry.

Example

The following example displays the log-table details based on an event and log index:

```
(host) #show rmon log-table event 1 log 2
Log Id: 2, Event Id: 1
    Created by alarm entry index 2, for OID : ifOutOctets.4
    Alarm value 705, with rising threshold 10
    Alarm sample type delta

(host) #show rmon log-table event 2 log 2
Log Id: 2, Event Id: 2
    Created by alarm entry index 2, for OID : ifOutOctets.4
    Alarm value 0, with falling threshold 0
    Alarm sample type delta
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platform	License	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes

show rogue-ap-containment

```
show rogue-ap-containment
```

Description

View the rogue AP containment configuration.

Example

The example below displays the default rogue AP containment configuration.

```
(host) #show rogue-ap-containment
   rogue-ap-containment "default"
   ------------------------------
   Parameter              Value
   ---------              -----
   Rogue AP Containment   Enabled
   Action                 default
   Auto Recovery Time     300
```

Related Command

Command	Description
rogue-ap-containment	Configure the rogue AP containment actions.

Command History

Release	Modification
ArubaOS 7.4	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes (config)

show router ospf

```
show router ospf
```

Description

View the global OSPF profile configuration.

Example

The example below displays the OSPF profile named “default” parameters.

```
(host) (config) #show router ospf

Global OSPF profile "default"
-----------------------------
Parameter          Value
---------          -----
State              Enabled
Area               0.0.0.0
Area               1.1.1.1
Router-id          2.2.2.2
Redistribute vlan  2
```

Related Command

Command	Description
router ospf	Configure the global OSPF parameters.
interface-profile ospf-profile	Configures a named OSPF interface profile

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Modes (config)

show running-config

```
show running-config
```

Description

Displays the current configuration of the Mobility Access Switch, 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 Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4.0.2	The probe-profile protocol information (default value is ICMP) is displayed in the output of the show running-config command

Command Information

Platforms	Licensing	Command Mode
All Mobility Access Switches	Base operating system	Enable and Configuration (config) modes.

show snmp community

```
show snmp community
```

Description

Displays the SNMP community string details.

Syntax

No parameters.

Example

The output of this command shows the community strings stored on the Mobility Access Switch.

```
(host) # show snmp community

SNMP COMMUNITIES
----------------
COMMUNITY       ACCESS     VERSION
---------       ------     -------
 no_auth_user   READ_ONLY  V1, V2C
 public READ_ONLY V1
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show snmp context

```
show snmp context
```

Description

Displays the list of context names configured on the Mobility Access Switch.

Syntax

No parameters.

Example

The output of this command shows slot details on the Mobility Access Switch.

```
(host) #show snmp context

SNMP Contexts Count: 2

SNMP Contexts
-------------
Context Name
------------
""                (Default Context)

V3_context
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show snmp engine-id

```
show snmp engine-id
```

Description

Displays the configured SNMP engine ID.

Syntax

No parameters.

Example

The output of this command shows the configured SNMP engine ID:

```
(host) #show snmp engine-id
SNMP engine ID: 000039e7000000a10a115e01 (Factory Default)
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show snmp group-snmp

```
show snmp group-snmp
```

Description

Displays the View Access Group information populated from the snmpd process.

Syntax

No parameters.

Example

The output of this command displays the configured View Access groups populated from the snmpd process:

```
host) #show snmp group-snmp

SNMP Groups Count: 11

SNMP Groups
-----------
Group Name     Security Model    Read View   Notify View   Context Name   Context Type
----------     --------------    ---------   -----------   ------------   ------------
gr1            v1-noAuthNoPriv   view1       view1         ""             -
gr1            v2-noAuthNoPriv   view1       view1         ""             -
gr1            v3-authPriv       Not Set     Not Set       ""             -
gr1            v3-noAuthNoPriv   Not Set     Not Set       abcd           exact
gr2            v1-noAuthNoPriv   ALL         Not Set       ""             -
gr3            v3-authPriv       Not Set     Not Set       ""             -
ALLPRIV        v1-noAuthNoPriv   ALL         ALL           ""             -
ALLPRIV        v2-noAuthNoPriv   ALL         ALL           ""             -
ALLPRIV        v3-noAuthNoPriv   ALL         ALL           ""             -
AUTHPRIV       v3-authPriv       ALL         ALL           ""             -
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show snmp group-trap

```
show snmp group-trap
```

Description

Displays the View Access Group information populated from the trapd process.

Syntax

No parameters.

Example

The output of this command displays the configured View Access groups populated from the trapd process:

```
host) #show snmp group-trap

SNMP Groups Count: 15

SNMP Groups
-----------
Group Name     Security Model    Read View   Notify View   Context Name   Context Type
----------     --------------    ---------   -----------   ------------   ------------
gr1            v1-noAuthNoPriv   view1       view1         ""             -
gr1            v2-noAuthNoPriv   view1       view1         ""             -
gr1            v3-authPriv       Not Set     Not Set       ""             -
gr1            v3-noAuthNoPriv   Not Set     Not Set       abcd           exact
gr2            v1-noAuthNoPriv   ALL         Not Set       ""             -
gr3            v3-authPriv       Not Set     Not Set       ""             -
abcd           v1-noAuthNoPriv   Not Set     ALL           ""             -
abcd           v2-noAuthNoPriv   Not Set     ALL           ""             -
public         v1-noAuthNoPriv   Not Set     ALL           ""             -
public         v2-noAuthNoPriv   Not Set     ALL           ""             -
ALLPRIV        v1-noAuthNoPriv   ALL         ALL           ""             -
ALLPRIV        v2-noAuthNoPriv   ALL         ALL           ""             -
ALLPRIV        v3-noAuthNoPriv   ALL         ALL           ""             -
AUTHPRIV       v3-authPriv       ALL         ALL           ""             -
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show snmp inform stats

```
show snmp inform stats
```

Description

Displays the SNMP inform statistics.

Syntax

No parameters.

Example

The output of this command shows the SNMP inform statistics.

```
(host) # show snmp inform stats

Inform queue size is 250

SNMP INFORM STATS
-----------------
HOST          PORT  VERSION  INFORMS-INQUEUE  OVERFLOW  TOTAL INFORMS
----          ----  -------  ---------------  --------  -------------
10.13.14.61   4050  V3       0                FALSE     0
10.13.14.61   162   V2C      0                FALSE     0

10.13.14.61 4050 V2C 0 FALSE 0
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show snmp notify filter profile-name

```
show snmp notify filter profile-name
```

Description

Displays the SNMP target profile names.

Syntax

No parameters.

Example

The output of this command shows the SNMP target profile names.

```
(host) #show snmp notify filter profile-name

SNMP Target Profile Count: 6

Profile Name
------------
Trap Target Profile Name
------------------------
1.1.1.1_1_162_p
10.10.10.10_1_162_p
10.13.34.150_2_4050_p
10.13.6.66_3_162_p
10.13.6.70_1_4050_p
10.13.6.70_2_4050_p
```

The following example displays the SNMP target profile details by a specific profile name:

```
(host) #show snmp notify filter profile-name 10.13.6.70_1_4050_p

Details for Target Profile:
10.13.6.70_1_4050_p
    Target IP: 10.13.6.70, UDP Port: 4050, Version: 1

    Trap Filter Included:
        risingAlarm
        fallingAlarm
        wlsxStackTopologyChangeTrap
 wlsxStackIfStateChangeTrap
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show snmp trap-group

```
show snmp trap-group
```

Description

Displays the list of trap filter groups that can be applied while configuring trap hosts. You can also view the traps associated with a specific trap filter.

Syntax

No parameters.

Example

The output of this command shows the list of trap filter groups that can be associated during trap host configuration.

```
(host) #show snmp trap-group

Trap Group Count: 8

Trap Group Name
---------------
Trap Group Name
---------------
generic
stacking
rmon
ptopo
system
snmp
auth
vlan
The following example displays the details of a specific trap group:
(host) #show snmp trap-group rmon

Supported Traps under group: rmon

    risingAlarm
 fallingAlarm
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show snmp trap-hosts

```
show snmp trap-hosts
```

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

Configured Source IP for Trap: 100.100.100.10

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

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 generated traps in the Agent.

```
(host) # show snmp trap-queue

2012-03-20 03:05:33 Switch Cold Started
2012-03-20 03:05:33 Enterprise cold start trap.
2012-03-20 03:05:33 Power supply 1 is missing

2012-03-20 03:05:33 Link 150994944 is up.  Admin status is 1; oper status is 1
...
...


Total traps in the queue : 40
Total traps generated on the device : 40
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show snmp user-table

```
show snmp user-table
```

Description

Displays the list of SNMP user entries created on the SNMP Agent.

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 users.

```
(host) # show snmp user-table

SNMP USER TABLE
---------------
User            Auth-Protocol   Priv-Protocol   Flags   Group
----            -------------   -------------   -----   -----
V3_user         MD5             AES                     gr3
allpriv_user    NONE            NONE                    ALLPRIV
version_3       NONE            NONE                    ALLPRIV
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show snmp view

```
show snmp view
```

Description

Displays the View information with the included and excluded OID details.

Syntax

No parameters.

Example

The output of this command shows the View information with the included and excluded OID details.

```
(host) # show snmp view

SNMP Views Count: 5

SNMP Views
----------
View Name  OID Tree             OID Tree Type  Storage Type  OID Mask
---------  --------             -------------  ------------  --------
ALL        iso                  included       nonVolatile   FF
view1      ifTable              included       nonVolatile   FF
view1      ifName               included       nonVolatile   FF:FF
view1      ifName.0             excluded       nonVolatile   FF:EF

view1 ifInMulticastPkts.0 excluded nonVolatile FF:EF
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode

show spanning-tree

```
show spanning-tree [detail]
```

Description

View the spanning tree information or optionally view the details of the set spanning tree.

Syntax

Parameter	Description
`detail`	Enter the keyword **detail** to view all the MSTP or PVST VLAN information.

Example

The following output is a summary of the current spanning tree.

```
(host) #show spanning-tree

MST 0
Root ID            Address: 0019.0655.3a80,  Priority: 4097
Regional Root ID   Address: 000b.866c.3200,  Priority: 16384
Bridge ID          Address: 000b.866c.3200,  Priority: 16384
External root path cost 40000, Internal root path cost 0

Interface  Role      State  Port Id   Cost   Type
---------  ----      -----  -------   ----   ----
GE0/0/1    Desg      FWD    128.2     20000  P2p
GE0/0/2    Loop-Inc  BLK    128.3     20000  P2p Bound
GE0/0/22   Root      FWD    128.23    20000  P2p
```

The example below includes more details of the current spanning tree.

```
(host)(config) #show spanning-tree detail

MST 0

vlans mapped         : 3,7
Configuration Digest : 0xED285086D33012C7D2B283FB89730D4D

Root ID            Address: 000b.866a.f240,  Priority: 32768
Regional Root ID   Address: 000b.866a.f240,  Priority: 32768
Bridge ID          Address: 000b.866a.f240,  Priority: 32768
External root path cost 0, Internal root path cost 0
Interface  Role  State  Port Id  Cost   Type
---------  ----  -----  -------  ----   ----
GE0/0/23   Desg  FWD    128.24   20000  P2p
GE1/0/22   Desg  FWD    128.167  20000  P2p
GE1/0/23   Bkup  BLK    128.168  20000  P2p
GE2/0/23   Bkup  BLK    128.312  20000  P2p

MST 4

vlans mapped         : 1
Root ID            Address: 000b.866a.f240,  Priority: 32768
Bridge ID          Address: 000b.866a.f240,  Priority: 32768
root path cost 0, remaining hops 20

Interface  Role  State  Port Id  Cost   Type
```

```
---------  ----  -----  -------  ----   ----
GE0/0/23   Desg  FWD    128.24   20000  P2p
GE1/0/22   Desg  FWD    128.167  20000  P2p
GE1/0/23   Bkup  BLK    128.168  20000  P2p
GE2/0/23   Bkup  BLK    128.312  20000  P2p
(host)(config) #
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode (config)

show spanning-tree mstp interface all

```
show spanning-tree mstp interface all [detail]
```

Description

View all the MSTP interfaces. Optionally, view all the detail of the MSTP interface.

Example 1

```
(host)#show spanning-tree mstp interface all

GE0/0/23
Instance  Role  State  Port Id  Cost   Type
--------  ----  -----  -------  ----   ----
MST 0     Desg  FWD    128.24   20000  P2p
MST 4     Desg  FWD    128.24   20000  P2p

GE1/0/22
Instance  Role  State  Port Id  Cost   Type
--------  ----  -----  -------  ----   ----
MST 0     Desg  FWD    128.167  20000  P2p
MST 4     Desg  FWD    128.167  20000  P2p

GE1/0/23
Instance  Role  State  Port Id  Cost   Type
--------  ----  -----  -------  ----   ----
MST 0     Bkup  BLK    128.168  20000  P2p
MST 4     Bkup  BLK    128.168  20000  P2p

GE2/0/23
Instance  Role  State  Port Id  Cost   Type
--------  ----  -----  -------  ----   ----
MST 0     Bkup  BLK    128.312  20000  P2p
MST 4     Bkup  BLK    128.312  20000  P2p
```

The values in the output above are detailed in the table below.

Column	Description
Instance	The MST instance number.
Role	Master (Mstr), Designated (Desg), Alternate (Altn), Root.
State	Disabled, Forwarding (FWD), or Blocking (BLK).
Port Id	Port ID number.
Cost	The cost value configured.
Type	The link type: P2p (point to point) or non-point to point (shared).

Example

```
(host)(config) #show spanning-tree detail

MST 0

vlans mapped          : 3,7
```

```
Configuration Digest : 0xED285086D33012C7D2B283FB89730D4D

Root ID            Address: 000b.866a.f240,  Priority: 32768
Regional Root ID   Address: 000b.866a.f240,  Priority: 32768
Bridge ID          Address: 000b.866a.f240,  Priority: 32768
External root path cost 0, Internal root path cost 0

Interface  Role  State  Port Id  Cost   Type
---------  ----  -----  -------  ----   ----
GE0/0/23   Desg  FWD    128.24   20000  P2p
GE1/0/22   Desg  FWD    128.167  20000  P2p
GE1/0/23   Bkup  BLK    128.168  20000  P2p
GE2/0/23   Bkup  BLK    128.312  20000  P2p

MST 4

vlans mapped         : 1
Root ID            Address: 000b.866a.f240,  Priority: 32768
Bridge ID          Address: 000b.866a.f240,  Priority: 32768
root path cost 0, remaining hops 20

Interface  Role  State  Port Id  Cost   Type
---------  ----  -----  -------  ----   ----
GE0/0/23   Desg  FWD    128.24   20000  P2p
GE1/0/22   Desg  FWD    128.167  20000  P2p
GE1/0/23   Bkup  BLK    128.168  20000  P2p
GE2/0/23   Bkup  BLK    128.312  20000  P2p
(host)(config) #
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1	Added **spanning-tree** keyword to the command.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show spanning-tree mstp interface gigabitethernet

```
show spanning-tree mstp interface gigabitethernet <slot/module/port>
```

Description

Display MSTP interface gigabitethernet settings for the slot/module/port.

Syntax

Parameter	Description
`<slot/module/port>`	Enter the slot, module, port to view details.

Example

```
(host) # show spanning-tree mstp interface gigabitethernet 0/0/1

Instance  Role  State  Port Id  Cost   Type
--------  ----  -----  -------  ----   ----
MST 0     Desg  FWD    128.2    20000  P2p
```

The values in the output above are detailed in the table below.

Column	Description
`Instance`	The instance number.
`Role`	Master (Mstr), Designated (Desg), Alternate (Altn).
`State`	Disabled, Forwarding (FWD), or Blocking (BLK).
`Port ID`	Port ID number.
`Cost`	The cost value configured.
`Type`	The link type: P2p (point to point) or non-point to point (shared).

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1	Added **spanning-tree** keyword to the command.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show spanning-tree mstp interface port-channel

```
show spanning-tree mstp interface port-channel <id>
```

Description

View MSTP port channel interface information.

Syntax

Parameter	Description	Range	Default
<id>	Port Channel identification.	0–7	—

Example (partial)

```
(host) #show spanning-tree mstp interface  port-channel 1

Instance  Role  State  Port Id   Cost   Type
--------  ----  -----  -------   ----   ----
MST 0     Altn  BLK    128.1442  10000  P2p
MST 1     Desg  FWD    128.1442  20000  P2p
MST 2     Altn  BLK    128.1442  20000  P2p
MST 3     Desg  FWD    128.1442  20000  P2p
MST 4     Altn  BLK    128.1442  20000  P2p
MST 5     Desg  FWD    128.1442  20000  P2p
MST 6     Altn  BLK    128.1442  20000  P2p
...
```

The values in the output above are detailed in the table below.

Column	Description
Instance	The instance number.
Role	Master (Mstr), Designated (Desg), Alternate (Altn).
State	Disabled, Forwarding (FWD), or Blocking (BLK).
Port Id	The Port ID number.
Cost	The cost value configured.
Type	The link type: P2p (point to point) or non-point to point (shared).

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1	Added **spanning-tree** keyword to the command.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show spanning-tree mstp msti

```
show spanning-tree mstp msti [<msti>] | all] [detail]
```

Description

Brief description of the command funtion.

Syntax

Parameter	Description	Range	Default
`<msti>`	Enter the MST instance.	0–64	0
`detail`	Enter the keyword **detail** to display details of the specified instance.	—	—
`all`	Enter the keyword **all** to view all of the msti instances.	—	—

Example

```
(host)#show spanning-tree mstp msti all

MST 0
Root ID            Address: 000b.866a.f240,  Priority: 32768
Regional Root ID   Address: 000b.866a.f240,  Priority: 32768
Bridge ID          Address: 000b.866a.f240,  Priority: 32768
External root path cost 0, Internal root path cost 0

Interface  Role  State  Port Id  Cost   Type
---------  ----  -----  -------  ----   ----
GE0/0/23   Desg  FWD    128.24   20000  P2p
GE1/0/22   Desg  FWD    128.167  20000  P2p
GE1/0/23   Bkup  BLK    128.168  20000  P2p
GE2/0/23   Bkup  BLK    128.312  20000  P2p

MST 4
Root ID            Address: 000b.866a.f240,  Priority: 32768
Bridge ID          Address: 000b.866a.f240,  Priority: 32768
root path cost 0, remaining hops 20

Interface  Role  State  Port Id  Cost   Type
---------  ----  -----  -------  ----   ----
GE0/0/23   Desg  FWD    128.24   20000  P2p
GE1/0/22   Desg  FWD    128.167  20000  P2p
GE1/0/23   Bkup  BLK    128.168  20000  P2p
GE2/0/23   Bkup  BLK    128.312  20000  P2p

(host)#
```

The values in the output above are detailed in the table below.

Column	Description
`MST 0 / MST 4`	Instance identification. MST 0 is the default instance.
`Root ID`	Root address and Pirority.
`Regional Root ID`	Regional root address and Pirority.
`Bridge ID`	Address and priority of the bridge that attaches to a LAN that is not in the same region.
`External root path cost`	External root path cost.
`Internal root path cost`	Internal root path cost.
`Interface`	Interface type plus slot number/network port/port number in *n*/*n*/*n* format. For example, GE0/0/23 is the interface gigabitethernet with a slot zero (0) on front-panel network port zero (0) at port number three (23). Interface/port numbering starts at 0.
`Role`	Master (Mstr), Designated (Desg), Alternate (Altn),
`State`	Disabled, Forwarding (FWD), or Blocking (BLK).
`Port Id`	The Port ID number.
`Cost`	The cost value configured.
`Type`	The link type: P2p (point to point) or non-point to point (shared).
`MSTP maximum age`	The configured maximum age.
`MSTP max hops`	The maximum hops.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.1	Added **spanning-tree** keyword to the command.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show spanning-tree-profile

```
show spanning-tree-profile
```

Description

View which spanning tree is enabled.

Example

The output below confirms that MSTP is the running spanning tree.

```
(host)#show spanning-tree-profile

spanning-tree
-------------
Parameter           Value
---------           -----
spanning-tree-mode  mstp
```

Related Command

Command	Description
spanning-tree mode	Set the spanning tree operational mode

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode (config)

show spanning-tree vlan

```
show spanning-tree vlan [<id>] | [all]
```

Description

View the PVST VLAN information for a specified VLAN or all VLANs.

Syntax

Parameter	Description	Range	Default
`vlan <id>`	Enter the keyword **vlan** followed by the VLAN identifier value to view details of the specified VLAN.	1 to 4094	—
`all`	Enter the keyword **all** to display all VLANs.	—	—

Example

The following example displays output for VLAN 1.

```
(host)#show spanning-tree vlan  1

VLAN 1
Root ID            Address: 000b.866a.1cc0,  Priority: 32768
Bridge ID          Address: 000b.866a.1cc0,  Priority: 32768
Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
We are the root of the spanning tree

Interface  Role  State  Port Id  Cost   Type
---------  ----  -----  -------  ----   ----
GE0/0/0    Desg  FWD    128.1    20000  P2p
```

The following example displays detail output for all VLANs. In this particular output, only one VLAN (VLAN 1) is configured.

```
(host)(config) #show spanning-tree vlan all detail

VLAN 1 Bridge ID priority: 32768, Address: 000b.866a.1cc0
We are the root of the spanning tree
Current Root ID priority: 32768, Address: 000b.866a.1cc0
Topology change flag not set, Number of topology changes: 1

(GE0/0/0) of VLAN1 is designated forwarding
Port path cost 20000, Port priority 128, Port identifier 128.1
Designated Root ID  priority: 32768, Address: 000b.866a.1cc0
Designated Bridge ID priority: 32768, Address: 000b.866a.1cc0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU sent: 9, Received: 0
Edge mode: Disabled
Root guard: Disabled
Loop guard: Disabled
```

Command History

Release	Modification
ArubaOS 7.1	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode (config)

show stacking asp-stats

```
show stacking asp-stats [all {member <id> | all}] | stack <module/port> {member <id> | all}
```

Description

Displays ASP control packet statistics for a specified interface or all stacking interfaces.

Syntax

Parameter	Description
`all`	Enter the keyword **all** to view all member information in the ArubaStack.
`member <id>`	Enter the keyword **member** followed by a member's ID number.
`<module/port>`	Enter the stacking interface details in module/port format.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show stacking generated-preset-profile

```
show stacking generated-preset-profile
```

Description

Generates a preset stack configuration from a dynamic-elected stack configuration.

Example

```
(host)(config) #show stacking generated-preset-profile

Preset-config Profile Command
-----------------------------
stack-profile
member-id 0 serial-number AU0000674 role primary-capable
member-id 1 serial-number AU0000731 role primary-capable
member-id 2 serial-number AU0000660 role line-card
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show stacking interface

```
show stacking interface
   brief [member <id>]
   member <id>
   stack <module/port> [member <id> | statistics [member <id>] | transceiver [detail | member
   <id>]]
   statistics [member <id>]
   transceiver [member <id>]
```

Description

Display the stacking interface and transceiver information.

Syntax

Parameter	Description
`brief [member <id>]`	Displays the summary of all configured stacking interface.
`member <id>`	Displays the stacking information for a particular stack member.

`stack <module/port>`
`member <id>`
`statistics [member <id>]`
`transceiver [detail | member <id>]`
	Displays the following stacking interface information:
	• **member <id>**: Stacking member.
	• **statistics [member <id>]**: Displays stacking interface statistics.
	• **transceiver [detail | member <id>]**: Displays stacking interface transceiver information.

`statistics [member <id>]`	Displays stacking interface statistics.
`transceiver [member <id>]`	Displays stacking interface transceiver information.

Example

```
(host)#show stacking interface stack 1/2 transceiver
Vendor Name                : Molex Inc.
Vendor Serial Number       : 116430722
Vendor Part Number         : 74752-1051
Cable Type                 : 10GBASE-DAC-P
Connector Type             : Copper Pigtail
Wave Length                : 0 nm
Cable Length               : 1mRelated Command
```

Related Command

Command	Description
show stacking topology	View the ArubaStack topology.
show stacking neighbors	View the ArubaStack neighbors.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.3	Introduced **detail** sub-parameter under **transceiver** parameter.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show stacking internal

```
show stacking internal [member <id> | all]
```

Description

View the internal ArubaStack information.

Syntax

Parameter	Description
`member <id>`	Enter the keyword **member** followed by a member's ID number.
`all`	Enter the keyword **all** to view all member information in the ArubaStack.

Example

```
(host)#show stacking internal

Device route table:

Route Table for Device-Id: 0

Target device-id  Interface  Next-hop device-id
----------------  ---------  ------------------
2                 stack1/2   2
4                 stack1/3   4

Multicast filter table:

Device-Id: 0

Source device-id  Unblocked-ports
----------------  ---------------
0                 stack1/3
                  stack1/2
2                 None
4                 None
```

Related Command

Command	Description
show stacking topology	View the ArubaStack topology.
show stacking neighbors	View the ArubaStack neighbors.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show stacking location

```
show stacking location
```

Description

Displays the assigned location of ArubaStack members.

Example

```
(host) (stack-profile) #show stacking location

Id    Location
--    --------
0   *  eng-building
1      eng-building
2      eng-building
```

Related Commands

Command	Description
stack-profile	Configure a member's location.

Command History

Release	Modification
ArubaOS 7.1.3	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show stacking members

```
show stacking members [member <id> | all]
```

Description

View the members of an ArubaStack.

Syntax

Parameter	Description
`member <id>`	Enter the keyword **member** followed by a member's ID number.
`all`	Enter the keyword **all** to view all member information in the ArubaStack.

Example

View details of the ArubaStack members.

```
(host)#show stacking members

Member status: Active, Stack Id: 000b866af2404e339e0a
Stack uptime: 7 minutes 10 seconds
Id    Role       MAC Address     Priority  State     Model            Serial
--    ----       -----------     --------  -----     -----            ------
0   *  Primary    000b.866a.f240  128       Active    ArubaS3500-24P   AU0000674
1      Secondary  000b.866b.0340  128       Active    ArubaS3500-24P   AU0000731
2      Linecard   000b.866b.3980  128       Active    ArubaS3500-24P   AU0000660
```

The values in the output above are detailed in the table below.

Column	Description
`Stack uptime`	The amount of time the ArubaStack has been up.
`Id`	This column contains the ID number of each member of the ArubaStack.
`Role`	This column list the role of each member; Primary, Secondary or Linecard.
`MAC Address`	This column contains the MAC address of each member.
`Priority`	Priority values for each member is listed.
`State`	The final column displays the state of each member; active or inactive.
`Model`	The model number of the Mobility Access Switch.
`Serial`	The serial number of each Mobility Access Switch.

Related Command

Command	Description
show stacking topology	View the ArubaStack topology.
show stacking neighbors	View the ArubaStack neighbors.

Command History

Release	Modification
ArubaOS 7.1	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show stacking neighbors

```
show stacking neighbors [member <id> | all]
```

Description

Displays the immediate stacking neighbors statistics.

Syntax

Parameter	Description
`member <id>`	Enter the keyword **member** followed by a member's ID number.
`all`	Enter the keyword **all** to view all neighbor information in the ArubaStack.

Example

The output below displays information on all the neighbors in the ArubaStack.

```
(host)#show stacking neighbors
Neighbor MAC Address  Interface  Adjacency  Neighbor Member-id
--------------------  ---------  ---------  ------------------
00:0b:86:6b:03:40     stack1/2   up         svl_techpubs-1
00:0b:86:6b:39:80     stack1/3   up         svl_techpubs-2
```

Related Command

Command	Description
show stacking topology	View the ArubaStack topology.
show stacking members	View the ArubaStack members.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show stacking topology

```
show stacking topology
```

Description

View the ArubaStack's topology.

Usage Guidelines

This command displays your ArubaStack's entire topology including member ID, role in the ArubaStack, MAC address, interface and neighbor.

Example

The following output details a three member ArubaStack topology.

```
(host)#show stacking topology

Member-id  Role       Mac Address       Interface  Neighbor Member-id
---------  ----       -----------       ---------  ------------------
0  *       Primary    000b.866a.f240    stack1/2   1
                                        stack1/3   2
1          Secondary  000b.866b.0340    stack1/3   0
                                        stack1/2   2
2          Linecard   000b.866b.3980    stack1/2   0
                                        stack1/3   1
```

The member with the asterisk (*) indicates that you are logged onto that member (the Primary in the example above).

The values in the output above are detailed in the table below.

Column	Description
Member-id	This column contains the ID number of each member of the ArubaStack.
Role	This column list the role of each member; Primary, Secondary or Linecard.
Mac Address	This column contains the MAC address of each member.
Interface	This column lists the interfaces attached to each member.
Neighbor Member-id	The final column displays each neighbor of each member.

Related Command

Command	Description
show stacking members	Display the ArubaStack members and ID.
show stacking neighbors	Display the ArubaStack neighbors.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show stack-profile

```
show stack-profile
```

Description

View the stack-profile settings.

Example

Dynamic-Election Stack

```
(host)(config) # show stack-profile

stack-profile "default"
-----------------------
Parameter                Value
---------                -----
MAC persistence timeout  30 Minutes
Split Detection          Enabled
Election Priority:
 Member 0                255
 Member 1                200
 Member 2                128
```

Pre-provisioned Stack

```
stack-profile "default"
-----------------------
Parameter                Value
---------                -----
MAC persistence timeout  15 Minutes
Split Detection          Enabled

Preset-profile:
---------------
Member-id        Serial-number  Role
 0               BK0000020      Primary-capable
 1               BK0000014      Primary-capable
 2               BK0000019      Line-card
 3               BK0000016      Line-card
```

Related Command

Command	Description
stack-profile	Configure the stack profile

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show station-table

```
show station-table [mac | verbose]
```

Description

This command displays the L2 internal station table on the Mobility Access Switch.

Syntax

Parameter	Description
`mac`	Display station that match the MAC address of the station.
`verbose`	Display user table in detail.

Usage Guidelines

Issue this command from the command-line interface of the Mobility Access Switch to view the L2 internal station table.

Example

This example displays the L2 internal station table on the Mobility Access Switch.

```
(host) #show station-table

Station Entry
-------------
MAC                Name         Role      Age(d:h:m)   Auth   Interface   Profile
------------       ------       ----      ----------   ----   ---------   -------
00:25:45:93:bf:d8  test-user1   emp-fin   00:02:18     Yes    3/0/44      dot1x
04:7d:7b:1e:d1:bf  test-user2   emp-eng   00:02:18     Yes    3/0/44      dot1x

Station Entries: 2
```

The output of this command includes the following information:

Column	Description
`MAC`	MAC address of the client.
`Name`	User name of the client.
`Role`	Client's assigned role.
`Age(d:h:m)`	Age of the user's current session, in the format *days:hours:minutes*.
`Auth`	Authentication method.
Interface	Interface on which the client is connected.
`Profile`	Profile assigned to the device.

Command History

Release	Modification
ArubaOS 7.0	Command introduced
ArubaOS 7.3	The **Interface** output parameters was introduced as part of this command. Following output parameters were deprecated: • **AP name** • **Essid** • **Phy** • **Remote**

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable Mode

show storage

```
show storage
   member <0-7>
```

Description

View the storage details on the Mobility Access Switch.

Syntax

Parameter	Description
`member <0-7>`	Displays the storage on the specified member.

Example

The following example displays the storage details on a member:

```
(host) #show storage member 2
Member-id: 2
------------
Filesystem                Size      Used Available Use% Mounted on
none                     300.0M     11.3M    288.7M   4% /tmp
/dev/ud3                 755.6M    176.0M    541.2M  25% /flash
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show system switchover

```
show system switchover
```

Description

View the synchronization switchover status. This command is only available on the primary.

Usage Guidelines

Use this command to confirm database synchronization before you execute the database synchronize command.

Example

The example below confirms that database synchronization to the secondary is current. That is, a database synchronize is not required.

```
(host) #show system switchover

Secondary Switchover status
---------------------------
System-state   :  synchronized to primary
Configuration :  synchronized to primary
Database       :  synchronized to primary
```

Related Command

Command	Description
system switchover	*Gracefully* switch the Secondary member to become the Primary member
database synchronize	Synchronize the Primary and Secondary databases

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

show time-range

```
show time-range [STRING | summary]
```

Description

This command displays time range information.

Syntax

Parameter	Description
`STRING`	Name of protocol service.
`summary`	Summary of time ranges.

Example

```
(ArubaS3500) #show time-range

Time-Range guest, Absolute
--------------------------
StartDate   Start-time  EndDate     End-time  Active
---------   ----------  -------     --------  ------
11/20/2012  0:00        12/20/2012  0:00      Yes
Time-Range guest1, Periodic
---------------------------
StartDay  Start-time  EndDay  End-time  Active
--------  ----------  ------  --------  ------
weekday   09:00               18:00     Yes
```

Related Commands

Command	Description
show acl ace-table	This command filters traffic based on the specified time range.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show time-range-profile

```
show time-range-profile <profile-name>
```

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 displays the periodic time range details:

```
(host) #show time-range-profile trp2

Time range profile "trp2"
-------------------------
Parameter            Value
---------            -----
Time range mode      periodic
Absolute time-range  N/A
Periodic time-range  Daily 7:00 Daily 6:00
```

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show trace

```
show trace
   chassis-manager [file <number> | member <id>]
   dhcp-snooping [file <number> | member <id>]
   igmp [file <number> | member <id>]
   igmp-snooping [file <number> | member <id>]
   interface-manager [file <number> | member <id>]
   layer2-forwarding [file <number> | member <id>]
   lldp [file <number> | member <id>]
   mstp [file <number> | member <id>]
   ospf [file <number> | member <id>]
   pim [file <number> | member <id>]
   rmon [file <number> | member <id>]
   routing [file <number> | member <id>]
   stack-manager [file <number> | member <id>]
   vrrp [file <number> | member <id>]
```

Description

Displays the content of the trace file.

Syntax

Parameter	Description
`chassis-manager [file <number> | member <id>]`	Displays the content of chassis manager trace file.
`dhcp-snooping [file <number> | member <id>]`	Displays the content of DHCP snooping trace file.
`igmp [file <number> | member <id>]`	Displays the content of IGMP trace file.
`igmp-snooping [file <number> | member <id>]`	Displays the content of IGMP snooping trace file.
`interface-manager [file <number> | member <id>]`	Displays the content of interface manager trace file.
`layer2-forwarding [file <number> | member <id>]`	Displays the content of Layer-2 forwarding trace file.
`lldp [file <number> | member <id>]`	Displays the content of LLDP trace file.
`mstp [file <number> | member <id>]`	Displays the content of MSTP trace file.
`ospf [file <number> | member <id>]`	Displays the content of OSPF trace file.
`pim [file <number> | member <id>]`	Displays the content of PIM trace file.
`rmon [file <number> | member <id>]`	Displays the content of RMON trace file.
`routing [file <number> | member <id>]`	Displays the content of routing trace file.
`stack-manager [file <number> | member <id>]`	Displays the content of stack manager trace file.
`vrrp [file <number> | member <id>]`	Displays the content of VRRP trace file.

Example

```
(host) #show trace routing file 1

Sep 13 14:00:59 trace_on: Tracing to "/var/log/traces/l3m.log" startedSep 13 14:00:59
Sep 13 14:01:49 ght_resize: table 100600e8 newsize 11
Sep 13 14:01:49 ght_resize: table 100600f4 newsize 11
Sep 13 14:01:49 ght_resize: table 10060100 newsize 11
Sep 13 14:01:49 ght_resize: table 100600d0 newsize 11
Sep 13 14:01:49 ght_resize: table 1006002c newsize 11
Sep 13 14:02:03 if_rtup: ADD route for interface vlan160 192.0.2.2/255.255.255.0
Sep 13 14:02:03 if_rtup: ADD route for interface vlan161 192.0.3.2/255.255.255.0
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3	New parameters **dhcp-snooping** and **vrrp** were introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable mode

show traceoptions

```
show traceoptions
```

Description

This command helps view the set trace option flags.

Example

```
(host) #show traceoptions
traceoptions (N/A)
------------------
Parameter                                 Value
---------                                 -----
Layer2 Forwarding trace flags
Layer2 Forwarding trace level             debugging
Layer2 Forwarding trace file size (Mb)    10
MSTP trace flags
MSTP trace port gigabitethernet           N/A
MSTP trace port port-channel              N/A
Interface manager trace flags             infrastructure configuration ethernet vlan portchannel tunnel
loopback mgmt system-information
Interface manager trace level             error
Chassis manager trace flags               fru poe-configuration interface association debug
LLDP trace flags
dhcp_snoop trace flags
igmp-snooping trace flags
pim sparse mode trace flags               all
pim sparse mode trace by vlanid 0

pim sparse mode trace by tunnel id        0

ospf trace flags                          all
OSPF trace by vlanid                      800

ospf trace by tunnel id          0

routing trace flags
igmp trace flags
vrrp trace flags
ddns trace flags
stack-manager trace flags                 primary-election route system webui configuration
Stack-manager trace level                 informational
rmon trace flags
rmon trace level                          errors
rmon trace file size (Mb)                 10
```

Related Command

Command	Description
traceoptions	Use this command to move into the trace options mode (traceoptions) and set trace option flags and values

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4.1	The following enhancements in the output of the traceoptions command are done: • Filteration of OSPF and PIM traces by interface ID. • Display of actual interface number in the place of port name (for the **mstp** command's port information)

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable mode

show trunk

```
show trunk
```

Description

This command displays the list of trunk ports.

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
----     -------------  ------------  -----------
GE0/0/0  ALL            1,10          1
```

Related Command

Command	Description
show vlan	This command displays basic or detailed VLAN information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show tunneled-node

```
show tunneled-node {config|state}
```

Description

This command displays the tunneled node configuration and state information.

Syntax

Parameter	Description
`config`	Displays the tunneled node configuration.
`state`	This command displays the state of tunneled nodes on the controller.

Example

The first command in the examples below shows the configuration of the tunneled-node profile, and the second example shows the state of the tunneled nodes on the controller

```
(host) #show tunneled-node config
Tunneled Node Client: Enabled
Tunneled Node Server: 172.16.50.2
Tunneled Node Loop Prevention: Disabled

(host) # show tunneled-node state
Tunneled Node State
-------------------
IP      MAC     Port    state   vlan    tunnel   inactive-time
--      ---             ----    -----   ----    ------   -------------
172.16.30.2     00:0b:86:6a:23:80               GE0/0/11        complete        0400    4088     0000

172.16.30.2 00:0b:86:6a:23:80 GE0/0/34 complete 0400 4091     0000.
```

The output of this command includes the following information:

Parameter	Description
`Tunneled Node Client`	Shows if the tunneled node client has been enabled or disabled.
`Tunneled Node Server`	IP address of the tunneled node server
`Tunneled Node Loop Prevention`	Shows if tunneled loop prevention has been enabled or disabled.
`IP`	IP address of the controller interface
`MAC`	MAC address of the controller interface
`Port`	Slot/Module/Port number on the switch that connects to the controller
`VLAN`	Tunneled Node VLAN
`inactive-time`	Amount of time, in seconds, that the tunneled node has been inactive.

Related Commands

Command	Description
interface-profile tunneled-node-profile	This command creates a tunneled node profile that can be applied to any interface.
show interface-profile tunneled-node-profile	This command displays the name and configuration settings of the current tunneled node profile.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show usb

```
show usb
```

Descriptions

This command displays the USB device information.

Syntax

No parameters

Examples

The following example displays the USB device information.

```
(host) #show usb
USB Device Table
----------------
Address  Product   Vendor  ProdID  Serial            Type
-------  -------   ------  ------  ------            ----
2        USB DISK  058f    6387    AA04012700008278  Storage
```

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode

show user-table

```
show user-table
   authentication-method
   blacklist
   debug
   devtype
   ip
   mac
   name
   role
   rows
   station
   unique
   verbose
```

Description

This command displays the L3 internal user table on the Mobility Access Switch.

Syntax

Parameter	Description
`authentication-table`	Display clients based on the following authentication method: • dot1x—802.1X authentication • mac—MAC authentication • web—Captive Portal authentication
`blacklist`	Display blacklisted clients.
`debug`	Display clients that are debugged.
`devtype`	Display clients that match the device type of the client.
`ip`	Display clients that match the IP address of the client.
`mac`	Display clients that match the MAC address of the client.
`name`	Display clients that match the user name of the client.
`role`	Display clients that match the role assigned to the client.
`rows`	Display certain rows.
`station`	Display station table in debug mode.
`unique`	Display unique user entries.
`verbose`	Display user table in detail.

Usage Guidelines

Issue this command from the command-line interface of the Mobility Access Switch to view the L3 internal user table.

Example

This example displays the L3 internal user table on the Mobility Access Switch.

```
(host) #show user-table

Users
-----
IP            MAC               Name        Role     Age(d:h:m)   Auth          Connection
----------    ------------      ------      ----     ----------   ----          ----------
192.0.2.11    04:7d:7b:1e:d1:bf  test-user1  emp-fin  00:02:18     802.1x-Wired  Wired
192.0.2.10    00:25:45:93:bf:d8  test-user2  emp-eng  00:02:18     802.1x-Wired  Wired

Interface  Profile  Vlan
---------  -------  ----
3/0/44     dot1x    1 (3911)
3/0/44     dot1x    1 (3913)

User Entries: 2/2
```

The output of this command includes the following information:

Column	Description
IP	IP address of the client.
MAC	MAC address of the client.
Name	User name of the client.
Role	Client's assigned role.
Age(d:h:m)	Age of the user's current session, in the format *days:hours:minutes*.
Auth	Authentication method.
Connection	Type of connection.
Interface	Interface on which the client is connected.
Profile	Profile assigned to the device.
Vlan	Initial and final VLAN.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.3	Following new output parameters were introduced: • **Connection** • **Interface** • **Vlan** Following output parameters were deprecated: • **VPN link** • **AP name** • **Roaming** • **Essid/Bssid/Phy**

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable Mode

show vlan

```
show vlan {[<id> detail|extensive]|[detail|extensive|status|summary]}
```

Description

This command displays basic or detailed VLAN information.

Syntax

Parameter	Description
`<id> detail | extensive`	Displays the details of the specified VLAN.
`detail`	Displays the details of all the VLANs.
`extensive`	Displays the details such as IGMP-snooping, MSTP instances and MAC aging time for all the VLANs.
`status`	Displays the status of all the VLANs in a table.
`summary`	Displays the summary of the VLAN information.

Example

Issue the **`show vlan`** command to show the 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 **`show vlan extensive`** command in the second example below displays the 802.11q tag, the IGMP-snooping profile associated with the VLAN, and information about MSTP instances and the configured MAC address aging time.

```
(host) #show vlan

VLAN CONFIGURATION
------------------
VLAN  Description  Ports
----  -----------  -----
1     VLAN0001     GE0/0/0-23 Pc1

(host) #show vlan extensive

Dot1q tag: 1, Description: VLAN0001
IGMP-snooping profile name: default
IGMP-snooping: Enabled
MSTP instance: 0
MAC aging time: 300
Number of interfaces: 25, Active: 2
VLAN membership:
        GE0/0/0*   Access Trusted   Untagged
        GE0/0/0*   Access Trusted   Tagged...
...
<output truncated>
(host)#show vlan status

Vlan Status
-----------
VlanId IPAddress               Adminstate  Operstate  Nat Inside  Mode     AAA Profile
------ ---------               ----------  ---------  ----------  ----     ---------
```

```
1       unassigned/unassigned   Up          Up          Disabled    Regular  N/A
11      2.2.2.1/255.255.255.0   Up          Down        Disabled    Regular  N/A

(host)#show vlan summary

Number of tunneled-node VLANs                   :2
Number of operational VLANs                     :10
```

Related Command

Command	Description
vlan	This command creates a VLAN with the specified configuration parameters.
show vlan-config	This command displays the configuration information for the specified VLAN ID.

Command History

Release	Modification
ArubaOS 7.0	Command introduced
ArubaOS 7.1	Introduced the `status` and `summary` parameters.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show vlan-config

```
show vlan-config <vlan-id>
```

Description

This command displays the configuration information for the specified VLAN ID.

Syntax

Parameter	Description
<vlan-id>	VLAN ID

Example

The example below shows configuration information for **VLAN 10**.

```
(host) #show vlan-config 10

VLAN "10"
---------
Parameter                Value
---------                -----
Description              N/A
aaa-profile              N/A
igmp-snooping-profile    N/A
MAC Aging time(Minutes)  5
```

The output of this command includes the following information:

Parameter	Description
Description	Description given to the VLAN
aaa-profile	AAA profile assigned to the VLAN
igmp-snooping-profile	IGMP Snooping profile assigned to the VLAN.
MAC Aging time (minutes)	Number of minutes after which a MAC address will be removed from the MAC address table. The default value is 5 minutes.

Related Command

Command	Description
interface vlan	This command creates the VLAN interface for the switch.
show vlan	This command displays basic or detailed VLAN information.
vlan	This command creates a VLAN with the specified configuration parameters.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration or Enable mode.

show vlan-profile dhcp-snooping-profile

```
show vlan-profile dhcp-snooping-profile [<profile-name]
```

Description

This command displays an DHCP snooping profile and the associated parameters.

Syntax

Parameter	Description
<profile-name>	Displays the profile with the specified name.

Usage Guidelines

By default, this command displays the entire list of DHCP snooping profile configurations. Include a profile name to display detailed information for that DHCP snooping profile.

Example

```
(host) (config) #show  dhcp-snooping-database  vlan 6
Total DHCP Snoop Entries : 3
Learnt Entries : 1, Static Entries : 2

DHCP Snoop Table
----------------
MAC                IP         BINDING-STATE  LEASE-TIME                 VLAN-ID  INTERFACE
---                --         -------------  ----------                -------  ---------
00:00:00:60:4a:69  6.6.6.10   Dynamic entry  2013-09-06 10:50:05 (PST)  6
gigabitethernet1/0/2
00:00:11:22:44:55  4.4.4.4    Static entry   No lease time              6
gigabitethernet1/0/2
00:00:11:33:66:77  7.7.7.7    Static entry   No lease time              6
gigabitethernet1/0/11
```

The output of this command includes the following information:

Parameter	Description
MAC	Shows the MAC address.
IP	Shows the IP address.
BINDING-STATE	Shows if the entry is dynamic or static.
LEASE-TIME	Shows the amount of time for which the ip address is allocated to the client.
VLAN-ID	Interval at which startup queries should be sent.
INTERFACE	Periodic interval at which queries are sent.

Related Command

Command	Description
vlan-profile dhcp-snooping-profile	This command creates an DHCP snooping profile that can be applied to a VLAN.

Command History

Release	Modification
ArubaOS 7.3	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show vlan-profile igmp-snooping-profile

```
show vlan-profile igmp-snooping-profile [<profile-name]
```

Description

This command displays an IGMP snooping profile and the associated parameters.

Syntax

Parameter	Description
<profile-name>	Displays the profile with the specified name.

Usage Guidelines

By default, this command displays the entire list of IGMP snooping profile configurations, including the configuration status and the number of references to each profile. Include a profile name to display detailed information for that IGMP snooping profile.

Example

The first example below shows that the switch has three IGMP snooping profiles. The **References** column lists the number of other profiles with references to the IGMP snooping profiles, 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 vlan-profile igmp-snooping-profile
igmp-snooping-profile List
--------------------------
Name                          References  Profile Status
----                          ----------  --------------
default                       0
igmp-snooping-factory-initial  1
profile123                    0
Total:3


(host) #show vlan-profile igmp-snooping-profile igmp-snooping-factory-initial
igmp-snooping-profile "igmp-snooping-factory-initial"
-----------------------------------------------------
Parameter                        Value
---------                        -----
Enable igmp snooping             Enabled
Enable igmp snooping proxy       Disabled
Enable fast leave                Disabled
startup-query-count              2
startup-query-interval(secs)     31
query-interval(secs)             125
query-response-interval(secs)    10
last-member-query-count          2
last-member-query-interval(secs) 1
robustness-variable              2
```

The output of this command includes the following information:

Parameter	Description
`Enable igmp snooping`	Shows if the IGMP snooping feature is enabled or disabled within this profile.
`Enable igmp snooping proxy`	Shows if the IGMP snooping proxy feature is enabled or disabled within this profile.
`Enable fast leave`	Shows if fast leave is enabled or disable3d.
`startup-query-count`	Number of queries to be sent at startup.
`startup-query-interval(secs)`	Interval at which startup queries should be sent.
`query-interval(secs)`	Periodic interval at which queries are sent.
`query-response-interval(secs)`	Maximum query response time.
`last-member-query-count`	Number of IGMP queries sent in response to a host leave message.
`last-member-query-interval(secs)`	Interval at which queries should be sent in response to a host leave message.
`robustness-variable`	Robustness variable.

Related Command

Command	Description
`vlan-profile igmp-snooping-profile`	This command creates an IGMP snooping profile that can be applied to a VLAN.
`show igmp-snooping`	This command lists IGMP snooping counters, groups, membership, and multicast router information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable Mode

show vlan-profile mld-snooping-profile

```
show vlan-profile mld-snooping-profile <profile-name>
```

Description

This command displays a list of the mld-snooping profiles. You can also view the details of a specific mld-snooping profile.

Syntax

Parameter	Description
<profile-name>	Displays the details of the profile with the specified name.

Example

```
(host) show vlan-profile mld-snooping-profile

mld-snooping-profile List
-------------------------
Name     References  Profile Status
----     ----------  --------------
default  2
Total:1

(host) show vlan-profile mld-snooping-profile default

mld-snooping-profile "default"
------------------------------
Parameter                       Value
---------                       -----
robustness-variable             2
last-member-query-interval(secs)  10
query-interval(secs)            125
query-response-interval(secs)   10
Enable fast leave               Enabled
Enable mld snooping             Enabled
```

Command History

Release	Modification
ArubaOS 7.1.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

show vlan-profile pvst-profile

```
show vlan-profile pvst-profile <profile name>
```

Description

Display the details of the PVST+ profile.

Syntax

Parameter	Description
`<profile name>`	Enter the name of the profile that you want to view.

Example

```
(host)(config) # show vlan-profile pvst-profile techpubs

pvst-profile "techpubs"
-----------------------
Parameter              Value
---------              -----
Enable PVST+ bridge    Enabled
bridge priority        32768
bridge hello time      5
bridge forward delay   22
bridge maximum age     25
```

Related Command

Command	Description
vlan-profile pvst-profile	Specify a name for your PVST+ profile.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable or Configuration Mode (config)

show vrrp

```
show vrrp [<id> statistics]
```

Descriptions

This command displays the VRRP interface profile state and statistics.

Syntax

Parameter	Description
`<id> statistics`	Displays the operational statistics of a specific VRRP instance.

Examples

The following example displays the VRRP interface profile state:

```
(host) #show vrrp 1

VRRP Instance Information
-------------------------
Virutal RouterId  Admin State  Vrrp State  Interface  VIP        Primary IP  Local IP
----------------  -----------  ----------  ---------  ---        ----------  --------
1                 UP           Master      vlan1      192.0.2.2  192.0.2.1   192.0.2.1
```

The following example displays the operation statistics of VRRP ID 1:

```
(host) #show vrrp 1 statistics

Virtual Router 1:
Admin State UP, VR State Master
Advertisements:
Sent:                                250   Received:                          196
Zero priority sent:                  0     Zero priority received:            0
Lower IP address received            0     Lower Priority received            0
Advertisements received errors:
Interval mismatch                 0   Invalid TTL                       0
Invalid packet type               0   Authentication failure            0
Invalid auth type                 0   Mismatch auth type                0
Invalid VRRP IP address           0   Invalid packet length             0
```

Related Commands

Command	Description
vrrp	This command enables and configures VRRP profile on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.3	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode

show vrrp-config

```
show vrrp-config [<id>]
```

Descriptions

This command displays the VRRP interface profile configuration.

Syntax

Parameter	Description
<id>	Enter the Virtual Router ID of the VRRP profile.

Examples

The following example displays the VRRP interface profile configuration:

```
(host) #show vrrp-config 1

Interface VRRP profile "1"
--------------------------
Parameter                   Value
---------                   -----
Master advertise interval   1
Router priority level       100
Virtual router IP address   192.0.2.2
Shutdown the VRRP instance  Disabled
Enable pre-emption          Enabled
pre-emption delay           10
Enable vlan Tracking        0
```

Related Commands

Command	Description
vrrp	This command enables and configures VRRP profile on the Mobility Access Switch.

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode

show web-server

```
show web-server
```

Description

Displays the configuration of the Mobility Access Switch's web server.

Syntax

No parameters.

Example

The output of this command shows the web-server configuration.

```
(host) # show web-server

  Web Server Configuration (N/A)
  ------------------------------
  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
  Enable/Disable Webserver                     Enabled
  Enable/Disable Captive portal                Enabled
```

Command History

This command was available in ArubaOS 3.0

Version	Description
ArubaOS 7.0	Command introduced.
ArubaOS 7.3.1	The output of this command displays the status of **Enable/Disable Webserver**and **Enable/Disable Captive portal**.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration or Enable mode

show ztp-boot-info

```
show ztp-boot-info
```

Description

Displays the provisioning details of the Mobility Access Switch.

Syntax

No parameters.

Example

The output of this command shows the details of provisioning of a Mobility Access Switch.

The following sample output displays the details of the TFTP method of provisioning:

```
(host) (config) #show ztp-boot-info
Zero Touch Provisioning Method: TFTP
Time of Provisioning          : Jun/18/2015 06:43:07
TFTP Config Download          : Successful
DHCP AMP Discovery            : N/A
Activate AMP Discovery        : N/A
DHCP Options Received
---------------------
Option No. Option Name  Value
---------- ------------ -------
3          Router       192.168.1.2
6          DNS Server   10.13.6.110
43         VSA
60         Vendor
67         Bootfile     AW0000161.cfg
150        TFTP Server  10.16.59.60
```

The following sample output displays the details of provisioning through Activate:

```
(host) #show ztp-boot-info
Zero Touch Provisioning Method: Activate
Time of Provisioning          : N/A
TFTP Config Download          : Failed
DHCP AMP Discovery            : Failed
Activate AMP Discovery        : Failed
DHCP/Activate provisioning aborted.
DHCP Options Received
---------------------
Option No. Option Name Value
---------- ----------- -----
3          Router      192.168.1.2
6          DNS Server  10.13.6.110
43         VSA
60         Vendor
67         Bootfile
150        TFTP Server
```

The output of this command includes the following information:

Parameter	Description
`Zero Touch Provisioning Method`	Displays TFTP or Activate. **NOTE:** Whenever ZTP fails, this still shows **Activate** as the provisioning method as the Mobility Access Switch keeps polling Activate in the background as long as it is in factory default.
`Time of Provisioning`	Displays the Timestamp of provisioning in Date and Time format. **NOTE:** This field displays N/A if not provisioned.
`TFTP Config Download`	Displays **Successful** or **Failed**. **NOTE:** If TFTP is the chosen ZTP method, it is the first method to attempt provisioning, and the output dispalys **Successful**; otherwise, the output displays **Failed**.
`DHCP AMP Discovery`	Displays **Successful** if the AMP parameters were discovered through DHCP option 43. **NOTE:** If TFTP is the chosen method of provisioning, this is not applicable.
`Activate AMP Discovery`	Displays one of the following: • **Successful**, if the AMP parameters are received through Activate. • **N/A**, if the method is not attempted. • **Failed**, if provisioning fails.
`DHCP Options Received`	Displays the various DHCP options received with the name and value in tabular format.

Command History

Version	Description
ArubaOS 7.4.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration or Enable mode

snmp-server

```
snmp-server
   community <string> view <view-name>
   context <context-name>
   enable trap
   engine-id <engineid>
   group <group-name> {v1 | v2c | [v3 {auth|no-auth|priv}] [context-prefix <name> context-
   match {exact|prefix}] notify <notify-view-name> read <read-view-name>}
   host <ipaddr> version {1 <security-string>} | {2c <security-string> | {3 <user-name>
   [engine-id <engineid>]} [inform] [interval <seconds>] [retrycount <number>]} udp-port
   <port> all auth generic ptopo rmon snmp stacking system vlan
   inform queue-length <size>
   trap enable|disable|{source <ipaddr>}
   user <name> group <name> {v1 | v2c | {v3[auth-prot {md5|sha} <password>] [priv-prot
   {AES|DES} <password>]}}
   view <view-name> oid-tree <OID> [excluded | included]
```

Description

This command configures SNMP parameters.

Syntax

Parameter	Description	Range	Default
`community`	Sets the read-only community string.	—	—
`view`	Restricts the community to the specified MIB view.	—	—
`context`	Creates a context with the specified context name.	—	—
`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	—
`group`	Creates a view access group entry with the specified name.	—	—
`v1`	Enables the SNMP V1 Security Model.	—	—
`v2c`	Enables the SNMPv2c Security Model.	—	—
`v3`	Enables the SNMPv3 Security Model.	—	—
`auth`	Enables authentication of a packet without encrypting it.	—	—
`noauth`	Enables no authentication of a packet. This authentication mechanism is used for SNMPv1 and SNMPv2c Security Model.	—	—

Parameter	Description	Range	Default
priv	Enables the authentication of a packet and then scrambles it.	—	—
read-view	Specifies the name of the view that enables only to read the contents of the Agent. **NOTE:** You must configure the read-view in the Agent to get an SNMP response.	—	—
notify-view	Specifies the name of the view that enables to specify a notification, inform, or trap. **NOTE:** You must configure the notify-view in the Agent to send SNMP trap. You must also ensure to include the trap varbinds in the notify-view along with the trap OID.	—	—
context-prefix	Configures a context prefix with the specified name which is used for the read operation using SNMP v3 Security model. **NOTE:** You must configure the context name in the Agent to get an SNMP response.	—	—
context-match	Specifies the type of context match for the SNMP request. • exact - exactly matches the context name to satisfy the SNMP request. • prefix - matches only the context prefix to satisfy the SNMP request.	exact | prefix	NULL
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 Mobility Access Switch.	—	—
version	Configures the SNMP version and security string for notification messages. For SNMPv3, the v3 user name must be specified as the security string. **NOTE:** You must configure the user name before configuring the host for SNMPv3.	—	—
inform	Sends SNMP inform messages to the configured host.	—	disabled
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
all	Allows the Trap Receiver to receive all the traps.	—	—

Parameter	Description	Range	Default
auth	Allows the Trap Receiver to receive the authentication traps.	—	—
generic	Allows the Trap Receiver to receive the generic traps.	—	—
ptopo	Allows the Trap Receiver to receive the ptopo traps.	—	—
rmon	Allows the Trap Receiver to receive the RMON traps.	—	—
snmp	Allows the Trap Receiver to receive the SNMP traps.	—	—
stacking	Allows the Trap Receiver to receive the stacking traps.	—	—
system	Allows the Trap Receiver to receive the system traps.	—	—
vlan	Allows the Trap Receiver to receive the VLAN traps.	—	—
inform queue-length <size>	Specifies the length for the SNMP inform queue.	100-350	250
trap source <ipaddr>	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.	—	—
user	Configures an SNMPv3 user 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. **NOTE:** It is recommended to provide at least eight characters in the password for security.	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. **NOTE:** It is recommended to provide at least eight characters in the password for security.	AES/DES	DES
view	Creates a view entry with the specified name. The view entry is associated with an OID. This is used for configuring groups.	—	—

Parameter	Description	Range	Default
`oid-tree`	Allows to specify an SNMP Object Identifier in ASN.1 Syntax Notation. You can also specify an OID. **NOTE:** OID can be in dotted nation, or an object name or wild card masked. You can use the wild card character *, where * indicates any value. For example, if you want to retrieve data only for the second row of of a MIB table, then the OID entry must be 1.3.6.1.2.1.31.1.1.1.*.2.	—	—
`included`	Includes the specified OID tree in the view.	—	—
`excluded`	Excludes the specified OID tree from the view.	—	—

Usage Guidelines

Use this command to configure SNMP parameters on the Mobility Access Switch.

Example

The following command configures an SNMP trap receiver:

```
(host) (config) #snmp-server host 191.168.1.1 version 2c public
```

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

spanning-tree mode

```
spanning-tree mode [mstp | pvst]
```

Description

Set the spanning tree operational mode.

Syntax

Parameter	Description
`mstp`	Enter the keyword **mstp** to set the spanning tree to MSTP.
`pvst`	Enter the keyword **pvst** to set the spanning tree to PVST+.

Usage Guidelines

Once you set the spanning tree mode, the new spanning tree mode is automatically applied to all configured VLANs, including the default VLAN 1.

Use spanning-tree **no mode** to disable running spanning trees.

Example

In the example below, PVST+ is set as the spanning tree mode.

```
(host)(config) #spanning-tree mode ?
mstp                    Multiple spanning tree mode
pvst                    Per-Vlan rapid spanning tree mode
(host)(config) #spanning-tree mode pvst
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

stack-profile

```
stack-profile
   mac-persistent-timer <value>
   member-id <id> location <locationstring>
   member-id <id> election-priority <priority>
   member-id <id> | serial-number <serial-number> role {primary-capable | line-card}
   split-detection
```

Description

Configure stacking profile parameters.

Syntax

Parameter	Description	Range	Default
`mac-persistent-timer`	Enter the keywords **mac-persistent-timer** to configure the MAC persistent timer.	—	—
`<value>`	Enter the value, in minutes, for your MAC persistent timer.	0–60 minutes	15 minutes
`member-id <id>`	Enter the keyword **member-id** followed by the member ID you want to configure for the election priority.	0–7	—
`location <locationstring>`	Enter the keyword **location** followed by a description of the ArubaStack's location (location string) such as building number or lab name.	—	—
`election-priority <priority>`	Enter the keywords **election-priority** followed by the election priority value.	0–255	128
`serial-number <serial-number> role <primary-capable | line-card>`	Enter the keywords **serial-number** followed by the serial number of the MAS. Then, enter the keyword **role** followed by the intended role of the MAS. The role options are **primary-capable** or **line-card**.	—	—
`split-detection`	Enter the keywords split-detection to enable/disable split detection. **NOTE:** Use this command on a two-member ArubaStack only.	—	enable

Usage Guidelines

When adding a Mobility Access Switch to an ArubaStack, you may need to manually set the priority value so that the switch enters the ArubaStack as a Line Card (or a Primary or Secondary). The switches priority value is one condition in the election process. The higher the election- priority the better chances that a switch is elected as Primary.

Alternatively, an ArubaStack can be created using the ArubaStack pre-provisioning feature. This allows you to configure the role and member-id of the members before the ArubaStack is created. The members are configured using their serial numbers. After the serial-number is added, the role is configured; either primary-capable or line-card. Additionally, at least two of the devices in the pre-provisioned ArubaStack must be primary-capable.

The split detect feature, which detects if a split occurs in an ArubaStack, is enabled by default. When your ArubaStack has only two members, best practices recommends that you disable the split detection feature to ensure that the Primary does not transition to a dormant state if the Secondary is powered down.

Example

The command to disable split detections is:

```
(host)(stack-profile) #no split-detection
```

The following show the steps for adding a single device to a stack profile for a pre-provisioned ArubaStack:

```
(host) (config) # stack-profile
(host) (stack-profile) #member-id 1
(host) (stack-profile) #member-id 1 serial-number AU00006600
(host) (stack-profile) #member-id 1 serial-number AU00006600 role line-card
```

Related Command

Command	Description
show stack-profile	View the stacking profile.

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.
ArubaOS 7.1.3	ArubaStack pre-provisioning and location commands introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

system switchover

```
system switchover [force]
```

Description

This command *gracefully* toggles the Primary and Secondary roles in the ArubaStack.

Syntax

Parameter	Description
`force`	Enter the keyword **force** to force the switchover without the benefit of a graceful switchover.

Usage Guidelines

Best practices recommends executing the database synchronize command before attempting a system switch over. To view the switch over status, use the show system switchover command to verify synchronization before executing the database synchronize command.

Periodic synchronization is automatically executed every two minutes.

This command is successful only when both the Primary and Secondary are configured with the same stack-priority. Once this command is executed:

- the Secondary becomes the new Primary
- the old Primary becomes the new Secondary

Example

The example below illustrates an attempt to execute the command. The system sends a message warning that the event will be without the benefit of a graceful switch over.

```
(host)#system switchover

System Not Ready for graceful Switchover, Please try again later or use force option
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Related Command

Command	Description
database synchronize	Synchronize the database between the Primary and Secondary.
show database synchronize	Display the database synchronization details.
show system switchover	View the switchover (synchorization) status.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

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_member_<member_ID>.tar
`flash`	Removes flash.tar.gz
`logs`	Removes logs.tar
`crash`	Archives the crash directory to crash_member_<member_ID>.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

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

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 filters traffic based on the specified time range.

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
```

Related Commands

Command	Description
show time-range	This command displays time range information.

Command History

Version	Modification
ArubaOS 7.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode

time-range-profile

```
time-range-profile <profile-name>
mode absolute
absolute [start-date <mm/dd/yyyy> start-time <hh:mm> end-date <mm/dd/yyyy> end-time <hh:mm>]
time-range-profile <profile-name>
mode periodic
periodic [start-day
<Daily|Weekend|Weekday|Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday> start-time
<hh:mm> end-day
<Daily|Weekend|Weekday|Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday> end-time
<hh:mm>]
no ...
```

Description

This command configures time ranges.

Syntax

Parameter	Description
`absolute`	Specifies an absolute time range, with a specific start and/or end time and date.
`clone`	Copy data from another time range profile.
`mode`	Specifies the time range profile mode (absolute | periodic).
`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.

Example

The following command configures a time range for daytime working hours:

```
(host) (config) #time-range-profile sample
(host) (config) #mode periodic
(host) (config) #periodic start-day daily start-time 7:00 end-day daily end-time 18:00
```

Command History

Release	Modification
ArubaOS 7.1.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

traceoptions

```
traceoptions
   chassis-manager
   ddns
   dhcp-snoop
   igmp
   igmp-snooping
   interface-manager
   layer2-forwarding
   lldp
   mstp
   no
   ospf
   pim
   rmon
   routing
   stack-manager
   vrrp
```

Description

Use this command to move into the trace options mode (traceoptions) and set trace option flags and values.

Syntax

Parameter	Description
`chassis-manager flags`	Enter the keyword **flags** and enable any of the following chassis manager trace options: • all • association • debug • environment-monitoring • fru • interface • interface-statistics • ipc • poe-configuration • poe-statistics • statistics-sync • system-statistics
`ddns flags`	Enter the keyword **flags** and enable any of the following ddns trace options: • all • cfg • debug • errors • receive • timer • transmit

Parameter	Description
`dhcp-snoop`	Enter the keyword flags and enable any of the following DHCP snoop trace options: • all • cfg • debug • errors • receive • timer
`igmp`	Enter the keyword **flags** and enable any of the following IGMP trace options: • all • debug • leave • query • report
`igmp-snooping`	Enter the keyword **flags** and enable any of the following IGMP snooping trace options: • all • config • errors • receive • transmit
`interface-manager`	Enter the keyword **flags** and enable any of the following interface manager trace options: • all • configuration • dhcp-client • ethernet • infrastructure • lacp • loopback • mgmt • oam • oam-pdu • port-channel • port-mirroring • system-information • tunnel • vlan Enter the keyword **level** and enable any of the following interface manager tracing levels: • debug • error • verbose

Parameter	Description
`layer2-forwarding`	Enter the keyword **flags** and enable any of the following Layer2-forwarding trace options: • all • config • fdb • gvrp • hsl • interface • ipc • learning • nexthop • port-loop-protect • sysinfo • task • timer • tunneled-node • vlan • vlan-assignment • vlan-port Enter the keyword **level** and enable any of the following Layer2-forwarding tracing levels: • debugging • errors • informational Enter the keyword **size** and specify the size of the Layer2 forwarding trace file.
`lldp`	Enter the keyword **flags** and enable any of the following LLDP trace options: • all • debug • errors • receive • system-state • transmit
`mstp`	Enter the keyword **flags** and enable any of the following MSTP trace options: • all • config • debug • port-information • received-bpdu-all • role-selection • sent-bpdu-all • state-machine-changes • system • topology-change Enter the keyword **port** followed by the port number to set MSTP traces on the specified port. The following two options are introduced under the **port** command: • gigabitethernet—Specify the actual interface number • port-channel—Specify the port-channel ID
`no`	Deletes the specified command.

Parameter	Description
`ospf`	Enter the keyword **flags** and enable any of the following OSPF trace options: • all • cnf • db • dd • debug • dr-elect • flood • hello • lsa • lsr • lsu • msm • pkt-all • spf • state
`pim`	Enter the keyword **flags** and enable any of the following PIM trace options: • adjacency • all • debug • jp-asserts • register • route • state
`rmon`	Enter the keyword **flags** and enable any of the following remote monitoring trace options: • alarm • all • cli • event • history • ifstat • log • snmp Enter the keyword **level** and enable any of the following remote monitoring tracing levels: • debugging • errors • informational Enter the keyword **size** and specify the size of the remote monitoring trace file.
`routing`	Enter the keyword **flags** and enable any of the following routing trace options: • all • arp • configuration • event • interface • route

Parameter	Description
`stack-manager`	Enter the keyword **flags** and enable any of the following stack manager trace options: • adjacency • all • asp • configuration • primary-election • route • system • webui Enter the keyword **level** and enable any of the following stack manager tracing levels: • alert • critical • debugging • emergency • errors • informational • notice • warning
`vrrp`	Enter the keyword **flags** and enable any of the following VRRP trace options: • all • debug • receive • state • transmit

Usage Guidelines

You must be in the **traceoptions** mode to set trace option flags and values.

Example

From the configuration mode execute the **traceoptions** command to move into the trace options mode.

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

The following example sets the Layer 2 forwarding level to debugging :

```
(host)(traceoptions) #layer2-forwarding level debugging
```

The sample **port** configuration commands are as follows:

```
(host) (traceoptions) #mstp port gigabitethernet 0/0/6
(host) (traceoptions) #mstp port port-channel 1
```

Related Command

Command	Description
show traceoptions	View all the trace options flags.

Command History

Release	Modification
ArubaOS 7.0	Command introduced
ArubaOS 7.3	New parameters— **dhcp-snoop** and **vrrp** parameters— were introduced.
ArubaOS 7.4.1	New options—**gigabitethernet** and **port-channel**—under **mstp** parameter are introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

traceoptions interface-manager

```
traceoptions interface-manager
   flags [all|configuration|dhcp-client|ethernet|infrastructure|lacp|loopback|mgmt|port-
   channel|port-mirroring|system-information|tunnel|vlan]
   level {debug|error|verbose}
```

Description

Enable chassis manager trace options.

Syntax

Parameter	Description
`flags`	Enter the keyword **flags** to set the interface manager trace flags.
`all`	Enter the keyword **all** to set all interface manager debug tracing.
`configuration`	Enter the keyword **configuration** to enable configuration debug tracing.
`dhcp-client`	Enter the keyword **dhcp-client** to enable DHCP client debug tracing.
`ethernet`	Enter the keyword **ethernet** to enable ethernet debug tracing.
`infrastructure`	Enter the keyword **infrastructure** to enable infrastructure debug tracing.
`lacp`	Enter the keyword **lacp** to enable LACP debug tracing.
`loopback`	Enter the keyword **loopback** to loopback debug tracing.
`mgmt`	Enter the keyword **mgmt** to enable management debug tracing.
`port-channel`	Enter the keyword **port-channel** to enable port channel debug tracing.
`port-mirroring`	Enter the keyword **port-mirroring** to enable port mirroring debug tracing.
`system-information`	Enter the keyword **system-information** to enable system debug message tracing.
`tunnel`	Enter the keyword **tunnel** to enable tunnel interface debug tracing.
`vlan`	Enter the keyword **vlan** to enable VLAN interface debug tracing.
`level`	Enter the keyword **level** to set the interface manager trace level.
`debug`	Enter the keyword **debug** to set the interface manager to trace debug messages.
`error`	Enter the keyword **error** to set the interface manager to trace debug messages.

Parameter	Description
`verbose`	Enter the keyword **verbose** to display user-friendly debug messages.

Usage Guidelines

This trace option command allows you to specify the trace flag(s) you want for the Interface Manager modules.

Example

The following example sets the interface manager to enable debug tunnel interface tracing:

```
(host) (traceoptions) #interface-manager tunnel
```

Related Command

Command	Description
`show traceoptions`	View the currently set trace flags.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

tracepath

```
tracepath <global-address>
```

Description

Traces the path of an IPv6 host.

Syntax

Parameter	Description
`<global-address>`	The IPv6 global address of the host.

Usage Guidelines

Use this command to identify points of failure in your IPv6 network.

Example

The following command traces the path of the specified IPv6 host.

```
(host) #tracepath 2005:d81f:f9f0:1001::14
```

Command History

Release	Modification
ArubaOS 7.1	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable and Configuration Mode (config)

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

Release	Modification
ArubaOS 7.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All Platforms	Base operating system	Enable

user-role

```
user-role <name>
   access-list {eth|mac|stateless} <acl> [position <number>]
   captive-portal <captive-portal-profile>
   deny-inter-user-traffic
   no ...
   policer-profile <name> [per-user]
   qos-profile <name>
   reauthentication-interval <minutes>
   vlan VLAN ID
   voip-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. **stateless:** Stateless ACL, configured with the `ip access-list stateless` command.	—	—
`<acl>`	Name of the configured ACL.	—	—
`captive-portal <captive-portal-profile>`	Name of the captive portal profile to be applied to the user-role	—	—

Parameter	Description	Range	Default
`deny-inter-user-traffic`	Enable Deny Inter-user Traffic on a role to deny the traffic between users with the same role. You can enable this option on a maximum of 7 user-roles.	—	—
`policer-profile <name>`	Name of the policer profile to be configured under this role.	—	—
`per-user`	Option to assign policer profile where granular rate limiting is required, that is per-user. **NOTE:** The default is per-role.	—	—
`qos-profile <name>`	Name of the QoS profile to be configured under this role.	—	—
`reauthentication-interval`	Time interval in minutes after which the client is required to reauthenticate.	0-4096	0 (disabled)
`vlan VLAN ID`	Identifies the VLAN ID to which the user role is mapped.	—	—
`voip-profile <name>`	Name of the VoIP profile to be configured under this role.	—	—

Usage Guidelines

Every client in a user-centric network is associated with a user role. 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
access-list stateless stl_acl
```

Command History

Release	Modification
ArubaOS 7.0	Command introduced.
ArubaOS 7.2	The **per-user** parameter for policer-profile was introduced.
ArubaOS 7.4	`The` **`deny-inter-user-traffic`** `parameter was introduced.`

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration

vlan

```
vlan <id>
   aaa-profile <profile-name>
   clone <source>
   description <name>
   igmp-snooping-profile <profile-name>
   mac-address-table static <mac-address> {gigabitethernet <slot/module/port>|port-channel<0-
   7>}
   mac-aging-time <minutes>
   no {...}
   pvst-profile <profile-name>
   exit
```

Description

This command creates a VLAN with the specified configuration parameters.

Syntax

Parameter	Description	Range	Default
`<id>`	Identification number for the VLAN.	2–4094	—
`aaa-profile <profile-name>`	Assigns a AAA profile to a VLAN to enable role-based access for wired clients connected to an untrusted VLAN or port on the Mobility Access Switch. This parameter applies to wired clients only. Note that this profile will only take effect if the VLAN and/or the port on the switch is untrusted. If both the port and the VLAN are trusted, no AAA profile is assigned.	—	—

Parameter	Description	Range	Default
`clone <source>`	Copies VLAN configuration information from another VLAN ID.	—	—
`description <name>`	Specifies a description/name for the VLAN.	1-32 characters; cannot begin with a numeric character	VLAN000x, where x is the ID number.
`igmp-snooping-profile <profile-name>`	Applies the specified IGMP snooping profile to the VLAN.	—	—
`mac-aging-time <minutes>`	Specifies the MAC aging time in minutes.	—	5 minutes
`mac-address-table static <mac-address> {gigabitethernet <slog/module/port> |port-channel<0-7>`	Adds the specified MAC address to the MAC address table.	—	—
`no {...}`	Removes the specified configuration parameter.	—	—
`pvst-profile <profile-name>`	Applies the specified PVST profile to the VLAN.	—	—

Usage Guidelines

Use the **`interface vlan`** command to configure the VLAN interface, including an IP address.

To enable role-based access for wired clients connected to an untrusted VLAN and/or port on the switch, you must use the **`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 AAA profile, traffic from clients connected to an untrusted wired port or VLAN will use the global AAA profile, if configured.

Example

```
vlan 101
   aaa-profile AAA_General
   description General
```

```
igmp-snooping-profile IGMP_General
mac-address-table static 1a:2b:3c:4d:5e:6f:7g:8h gigabitethernet 0/0/2
mac-aging-time 30
exit
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

Command History

Release	Modification
ArubaOS 7.0	Command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Config mode

vlan-profile dhcp-snooping-profile

```
vlan-profile dhcp-snooping-profile <profile-name>
```

Description

This command creates a DHCP snooping profile that can be applied to a VLAN.

Syntax

Parameter	Description	Range	Default
<profile-name>	Identification name for the IGMP snooping profile.		

Usage Guidelines

Use this command to create a dhcp-snooping profile.

Example

The following example enables and configures DHCP Snooping on a VLAN:

```
(host) ("vlan 6")# vlan-proifile dhcp-snooping-profile DHCP
(host) (dhcp-snooping-profile "DHCP")# enable
```

The following example attaches DHCP Snooping profile on the VLAN:

```
(host) ("vlan 6")# dhcp-snooping-profile DHCP
```

Related Commands

Command	Description
show vlan-profile dhcp-snooping-profile	This command displays an DHCP snooping profile and the associated parameters.

Command History

Release	Modification
ArubaOS 7.3	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

vlan-profile igmp-snooping-profile

```
vlan-profile igmp-snooping-profile {igmp-snooping-factory-initial |default|<profile-name>}
   clone <source>
   fast-leave
   last-member-query-count <1-5>
   last-member-query-interval <1-25 seconds>
   no {...}
   query-interval <1-18000 seconds>
   query-response-interval <1-25 seconds>
   robustness-variable <1-7>
   snooping [v3]
   snooping-proxy [v3]
   startup-query-count <1-10>
   startup-query-interval <1-18000 seconds>
```

Description

This command creates an IGMP snooping profile that can be applied to a VLAN.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Identification name for the IGMP snooping profile.		
`clone <source>`	Copies IGMP snooping configuration information from another IGMP snooping profile.		
`fast-leave`	Enables fast leave.		Disabled
`last-member-query-count <1-5>`	Specifies the number of IGMP queries in response to host leave message.	1–5	2
`last-member-query-interval <1-25 seconds>`	Specifies the IGMP query interval in response to host leave message.	1-25 seconds	1
`no {...}`	Disables the specified configuration parameters.		
`query-interval <1-18000 seconds>`	Specifies the periodic interval at which queries are sent.	1–18000 seconds	125
`query-response-interval <1-25 seconds>`	Specifies the maximum query response time.	1–25 seconds	10
`robustness-variable <1-7>`	Specifies the expected IGMP packet loss on a congested network.	1–7	2

Parameter	Description	Range	Default
`snooping [v3]`	Enables IGMPv2 Snooping. Specifying the v3 keyword enables IGMPv3 Snooping.		IGMPv2 Snooping Enabled
`snooping-proxy [v3]`	Enables IGMPv2 Snooping proxy. Specifying the v3 keyword enables IGMPv3 Snooping proxy.		Disabled
`startup-query-count <1-10>`	Specifies the number of queries to be sent at startup.	1–10	2
`startup-query-interval <1-18000 seconds>`	Specifies the interval at which startup queries should be sent.	1–18000 seconds	31

Usage Guidelines

Use this command to create an igmp-snooping profile. Creating an IGMP snooping profile does not apply the configuration to any VLAN. To apply the IGMP snooping profile, use the `vlan` command.

Example

The following example creates an IGMP snooping profile:

```
vlan-profile igmp-snooping-profile IGMP_General
   fast-leave
   last-member-query-count 3
   last-member-query-interval 20
   query-interval 15000
   query-response-interval 20
   robustness-variable 5
   snooping
   snooping-proxy
   startup-query-count 7
   startup-query-interval 15000
```

Related Commands

Command	Description
`show vlan-profile igmp-snooping-profile`	Displays the IGMP snooping profile information.

Command History

Release	Modification
ArubaOS 7.0	This command was introduced.
ArubaOS 7.4	The **v3** parameter was added to **snooping** and **snooping-proxy** commands.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration mode

vlan-profile mld-snooping-profile

```
vlan-profile mld-snooping-profile <profile-name>
   clone
   fast-leave
   last-member-query-interval
   no
   query-interval
   query-response-interval
   robustness-variable
   snooping
```

Description

Use this command to configure an MLD-Snooping profile.

Syntax

Parameter	Description	Range	Default
`clone`	Copies data from another mld-snooping-profile.	n/a	n/a
`fast-leave`	Enables or disables fast leave.	n/a	n/a
`last-member-query-interval`	MLD query interval in response to host leave message.	1–25	secs
`no`	Delete command.	_	_
`query-interval`	Periodic interval at which queries are sent.	1–18000	_
`query-response-interval`	Maximum query response time (1-25)secs	(1–25)	secs
`robustness-variable`	Expected MLD packet loss on a congested network.	1–7	
`snooping`	Enable or disable MLD snooping.	n/a	enabled

Usage Guidelines

To configure an MLD-Snooping profile, use the following commands in the configuration mode:

```
(host)(config) #vlan-profile mld-snooping-profile default
(host)(mld-snooping-profile "default") #snooping
(host)(mld-snooping-profile "default") #
```

Example

To display an MLD-Snooping profile, use the following command in the configuration mode:

```
(host) #show vlan-profile mld-snooping-profile default

mld-snooping-profile "default"
------------------------------
Parameter                       Value
---------                       -----
robustness-variable             2
last-member-query-interval(secs)  1
query-interval(secs)            125
```

```
query-response-interval(secs)      10
Enable fast leave                  Disabled
Enable mld snooping                Enabled
```

Command History

Release	Modification
ArubaOS 7.4	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Enable

vlan-profile pvst-profile

```
vlan-profile pvst-profile <name>
   bridge-priority
   clone
   enable
   forward-delay
   hello-time
   max-age
   no
```

Description

Creates a PVST+ profile and allows you to enable or disable the PVST+ bridge and configure the root bridge priority, forward delay time, time interval for generating PVST+ BPDUs, and the refresh time

Syntax

Parameter	Description	Range	Default
`<name>`	Name of the PVST+ profile.	—	—
`bridge-priority <value>`	The root bridge priority. Enter the bridge priority value in increments of 4096. **Valid value**s: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.	0–61440	32768
`clone`	Creates a copy of the PVST+ profile with the same configuration.	—	—
`enable`	Enables or disables the PVST+ bridge.	—	—
`forward-delay`	The amount of time, in seconds, before the port transitions to forwarding. During this delay time, data packets are not forwarded	4–30	15
`hello-time`	Sets the time interval, in seconds, between generation of PVST+ BPDUs (Bridge Protocol Data Units).	1–10	2
`max-age`	Sets the time interval for the PVST+ bridge to maintain configuration information before refreshing that information	6–40	20

Usage Guidelines

This command enters you into the PVST+ profile configuration mode. The prompt changes to include the PVST+ profile name. You can then enable or disable the PVST+ bridge, set the root bridge priority, forward delay time, time interval for generating PVST+ BPDUs, and the refresh time.

Example

The following is a sample PVST+ profile configuration:

```
(host)(config) #vlan-profile pvst-profile techpubs
(host)(pvst-profile "techpubs") #enable
```

```
(host)(pvst-profile "techpubs") #bridge-priority 12288
(host)(pvst-profile "techpubs") #forward-delay 22
(host)(pvst-profile "techpubs") #hello-time 5
(host)(pvst-profile "techpubs") #max-age 25
```

Related Command

Command	Description
show vlan-profile pvst-profile	Display the parameters and values of the pvst-profile

Command History

Release	Modification
ArubaOS 7.1	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration Mode (config)

vrrp

```
vrrp <id>
   advertise <interval>
   clone <source>
   ip <address>
   no
   preempt
   preemption delay <seconds>
   priority <level>
   shutdown
   tracking vlan <vlanId>
```

Description

Issue this command to enable and configure a VRRP profile on the Mobility Access Switch.

Syntax

Parameter	Description	Range	Default
`vrrp <id>`	Unique virtual router ID of the VRRP profile.	1–255	—
`advertise <interval>`	Specifies the VRRP advertisement interval (in seconds) after which the master Mobility Access Switch sends VRRP advertisement packets to the peers in the group.	1–3600	1
`clone <source>`	Copy configuration from another VRRP instance.	—	—
`ip <address>`	Virtual router IP address of the master and backup Mobility Access Switch. This IP address must be different from the VLAN interface IP address on which the virtual router is configured.	—	—
`no`	Deletes or negates previously entered VRRP configuration or parameter.	—	—
`preempt`	Enables preemption for the VRRP profile. If you enable preemption, VRRP determines the state of the backup Mobility Access Switch when it becomes the master. For example, if Switch A is the master and fails, VRRP selects Switch B (next in the order of priority). If Switch C comes online with a higher priority than Switch B, VRRP selects Switch C as the new master, although Switch B has not failed. When disabled, VRRP switches only if the original master recovers or the new master fails. This is the default behavior.	Enabled	—
`preemption delay <seconds>`	Delay in seconds, the backup should wait for before transitioning to master.	0–3600	0

Parameter	Description	Range	Default
`priority <level>`	Sets the VRRP router priority level. A priority of 255 indicates that the Mobility Access Switch has stopped participating in the VRRP group. The switch with highest configured priority always wins the election for master in preemptive mode of operation. For example, a switch with a priority level of 254 wins the election, but a switch with priority level 255 stops participating in the VRRP group.	1—255	100
`shutdown`	Terminates the participation of the master Mobility Access Switch in the VRRP group. The priority of the switch is set to 255 indicating that the switch has stopped participating in the VRRP group.	–	–
`tracking vlan <vlanId>`	Tracks the up-link layer-3 VLAN interface transitions. When the up-link layer-3 VLAN interface of the master Mobility Access Switch fails, the role of the master is transitioned to the backup Mobility Access Switch.	–	–

Usage Guidelines

By default, VRRP is disabled on the Mobility Access Switch. You can enable VRRP by issuing the **vrrp <id>** command in the CLI.

Example:

```
(host) (config) #vrrp 1
(host) (Interface VRRP profile "1") #advertise 10
(host) (Interface VRRP profile "1") #ip 192.0.2.2
(host) (Interface VRRP profile "1") #preempt
(host) (Interface VRRP profile "1") #preemption delay 10
(host) (Interface VRRP profile "1") #priority 200
```

Related Commands

Command	Description
show vrrp	This command displays the VRRP interface profile state and statistics.
show vrrp-config	This command displays the VRRP interface profile configuration.

Command History

Release	Modification
ArubaOS 7.3	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode

web-server

```
web-server
   captive-portal-cert <name>
   captive-portal-ports
   ciphers {high|low|medium}
   mgmt-auth [certificate] [username/password]
   mgmt-ui-ports
   no ...
   session-timeout <session-timeout>
   ssl-protocol [tlsv1] [tlsv1.1] [tlsv1.2]
   switch-cert <name>
   web-max-clients <web-max-clients>
```

Description

This command configures the Mobility Access Switch's web server.

Syntax

Parameter	Description	Range	Default
`captive-portal-cert`	Specifies the 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 Mobility Access Switch.	—	default
`captive-portal-ports`	Disable or re-enable the ports for Captive Portal.	—	enabled
`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 **NOTE:** This command is not available in FIPS software images because ciphers are pre-configured only to acceptable values.	high, low, medium	high
`mgmt-auth`	Specifies the 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
`mgmt-ui-ports`	Disable or re-enable the ports for WebUI	—	enabled
`no`	Negates any configured parameter.	—	—

Parameter	Description	Range	Default
`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`	Specifies the Transport Layer Security (TLS) protocol version used for securing communication with the Web server: **TLSv1** **TLSv1.1** **TLSv1.2**	—	tlsv1 tlsv1.1 tlsv1.2
`switch-cert`	Specifies the 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 Mobility Access Switch.	—	default
`web-max-clients <web-max-client>`	Configures the web server's maximum number of supported concurrent clients.	25–320	25

Usage Guidelines

There is a default server certificate installed in the Mobility Access Switch, 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). After importing the signed certificate into the Mobility Access Switch, 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 Mobility Access Switch:

```
(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 7.0	Command introduced.
ArubaOS 7.3.1	The **mgmt-ui-ports** and **captive-portal-ports**parameters were introduced.
ArubaOS 7.4.0.1	The **ssl-protocol** parameter is modified to include only transport layer security options: tlsv1, tlsv1.1, and tlsv1.2.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode

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 7.0.

Command Information

Platforms	Licensing	Command Mode
Mobility Access Switch	Base operating system	Configuration and Enable modes

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 tofactory 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, includingthe license key management database.

If you reset the controller to the factory default configuration, perform the Initial Setup as described in the Aruba 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.

Parameter	Description
`Q`	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.
`U`	Saves the current system configuration to memory. Any configuration changes made during this session will be made permanent.
`spacebar`	Displays the current system configuration.

Parameter	Description
/	Enter a text string for your search.
N	Repeat the text string for your search.

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

Release	Modification
ArubaOS 7.0	Thiis command was introduced.

Command Information

Platforms	Licensing	Command Mode
All Platforms	Base operating system	Enable