

ArubaOS 7.4.x



User Guide

Copyright Information

© Copyright 2017 Hewlett Packard Enterprise Development LP.

Open Source Code

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

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

Contents	3
Revision History	14
About this Guide	15
What's New In ArubaOS 7.4.x	15
Audience	18
Fundamentals	18
Related Documents	19
Conventions	19
Contacting Support	20
System Basics	21
Factory Initial Configuration	21
Zero-Touch Provisioning	23
Packet Tracing	26
Trace Options	27
Profiles Management	29
Profiles for Interfaces	30
Understanding Interface Profiles	38
Understanding Interface Group	40
Managing Controller IP	41
Using the LCD	41
Setting the System Clock	44
Managing Files on the Mobility Access Switch	45
PAPI Enhanced Security	49
Management Access	51
Management Users	51
Management Password Policy	51

Setting an Administrator Session Timeout	53
Bypassing the Enable Password Prompt	53
Resetting the Admin or Enable Password	53
Managing Ports for WebUI and Captive Portal	54
Certificate Authentication Concepts	55
Public Key Authentication for SSH Access	55
Managing Certificates	56
SSL Vulnerability Fix	59
Aruba Central	61
Overview	61
Managing Mobility Access Switch Using Aruba Central	61
Provisioning Mobility Access Switch Using Aruba Central Portal	62
Automatic Configuration with Aruba Activate	63
Activate Integration Overview	63
Activate Provisioning Service	63
Activate and AirWave	64
Network Requirements for AirWave Provisioning	65
Activate Firmware Services	65
ArubaStack	67
Important Points to Remember	67
Stacking Topology	68
Dynamic Election	73
ArubaStack Pre-Provisioning	75
ArubaStack Database	76
ArubaStack Resiliency	78
ArubaStack Member Replacement	84
Stack Member Renumbering	95
Factory Reset on Detached ArubaStack Member	95

Ethernet Interfaces and PoE	97
Configuring the Management Port	97
Gigabit Ethernet Network Interfaces	97
Small Form-factor Pluggable Diagnostics	98
Configuring Ethernet Interfaces	100
Configuring an Interface Group	102
Creating and Applying an Ethernet Link Profile to an Interface	105
Power Over Ethernet	107
Configuring Power Over Ethernet	111
Creating and Applying a PoE Profile to an Interface	111
Time-Domain Reflectometer	114
Port-Channels	117
Important Points to Remember	117
Creating a Port-Channel	117
Creating and Applying a Dynamic Port-Channel Profile to an Interface	119
Link Aggregation Control Protocol	121
Operations, Administration, and Maintenance	129
Creating an OAM Profile	129
Applying an OAM Profile	130
Applying OAM to each Port Channel Member	130
Related Show Commands	131
VLANs	133
VLANs Overview	133
Creating VLANs	133
Creating and Applying a Switching Profile to an Interface	135
Deleting Switching Profile from an Interface	137
Managing the MAC Address Table	138
VLAN Profile	141

GVRP	143
GVRP Overview	143
Enabling and Configuring GVRP Functionality	143
Sample Configurations	144
Link Layer Discovery Protocols	147
Important Points to Remember	147
LLDP	147
LLDP-MED	152
PoE Negotiation over LLDP	154
Proprietary Link Layer Discovery Protocols	156
VoIP	159
Voice VLANs	159
Creating and Applying VoIP Profile to an Interface	160
VoIP Auto-Discovery on Trusted Ports	160
VoIP Auto-Discovery on Untrusted Ports	161
MSTP	163
Important Points to Remember	163
Example MSTP Configuration	163
Loopguard and Rootguard	166
Bridge Protocol Data Unit (BPDU) Guard	168
Portfast	169
Bridge Protocol Data Unit (BPDU) Filter	170
Sample MSTP Topology and Configuration	171
Rapid PVST+	177
Important Points to Remember	177
Configuring PVST+	177
Loopguard and Rootguard	179
Bridge Protocol Data Unit (BPDU) Guard	180

Portfast	181
Hot-Standby Link	183
Important Point to Remember	183
Configuration Steps	183
Generic Routing Encapsulation	185
L2 GRE	185
L3 GRE	187
Layer 3 Routing	189
Understanding Routed VLAN Interfaces	189
Multinetting	190
Loopback Interfaces	191
Network Address Translation	191
NAT Pools	193
Session ACLs on RVI	194
Support for IP NAT Outside	196
IP Directed Broadcast	197
Static Routes	198
Equal Cost Multipath	201
IP Prefix List	202
Support for Egress ACLs on Routed VLAN Interfaces	203
Route Monitoring	204
Dynamic Domain Name Server Client	207
Static Address Resolution Protocol	209
Proxy Address Resolution Protocol	209
Virtual Router Redundancy Protocol	211
VRRP Definitions	211
VRRP Overview	211
Important Points to Remember	212

VRRP Deployment Scenarios	212
Enabling and Configuring VRRP	213
Sample Configuration	215
Policy Based Routing	217
Policy Based Routing Overview	217
Configuring Policy-Based Routing	217
Sample Configurations	219
DHCP Server and DHCP Relay	221
Understanding DHCP Server and DHCP Relay	221
Configuring DHCP Server and DHCP Relay	221
Verifying DHCP Server and DHCP Relay	224
Local DHCP Server Device Reservation	226
OSPFv2	229
OSPF Feature Overview	229
Configuring OSPF	229
OSPF MD5 Authentication	234
OSPF Route Summarization	236
IPv6	239
IPv6 Support for Mobility Access Switch	239
IGMP, PIM-SM and PIM-SSM	241
Important Points to Remember	241
Understanding IGMP, PIM-SM and PIM-SSM	241
Configuring IGMP	242
Configuring PIM Sparse Mode	244
Configuring PIM Source Specific Multicast	246
IGMP Snooping	249
Important Points to Remember	249
Multicast Support with IGMP Snooping	249

Support for IGMPv3 Snooping	250
IGMP Snooping Factory Initial and the Default Profiles	250
Creating and Applying an IGMP Snooping Profile to a VLAN	251
Monitoring IGMP Snooping	253
Mrouter	254
MLD Snooping	257
Important Points to Remember	257
Understanding MLD Snooping	257
Configuring MLD Snooping	257
Verifying MLD Snooping	258
DHCP Snooping	265
DHCP Snooping Overview	265
Configuring DHCP Snooping	265
Port Security	267
Port Security Overview	267
Configuring Port Security Functionality	269
Sample Configurations	275
Storm Control	277
Important Points to Remember	277
Configuration Steps	277
Access Control List	279
Types of ACLs	279
Configuring the ACLs	280
Verifying the ACL configuration	282
Quality of Service	283
QoS Concepts	283
Configuring QoS	285

Authentication Servers	289
Important Points to Remember	289
Server and Server Group Concepts	289
Configuring Authentication Servers	290
Internal Database Concepts	296
Configuring the Internal Database	297
Server Group Concepts	298
Assigning Server Groups	302
Authentication Timers	305
AAA Authentication	307
AAA Authentication Profile	307
Configuring Authentication End to End	312
RADIUS Fail-Open	314
Authentication Survivability	317
Preauth Role Assignment	319
Deny DHCP Role for 802.1x Authentication	321
Delay EAP Success for dot1x Authentication	321
Port Bounce	322
Roles and Policies	325
Firewall Policies	325
User Roles	331
User Role Assignments	332
Deny Inter-User Traffic	334
MAC-Based Authentication	337
MAC-Based Authentication Concepts	337
Configuring MAC-Based Authentication	337
Configuring Clients	338

802.1x Authentication	339
802.1x Authentication Concepts	339
Configuring 802.1x Authentication	341
Configuring 802.1x Authentication with Machine Authentication	343
Captive Portal	349
Captive Portal Overview	349
Captive Portal Configuration Example	351
Personalizing the Captive Portal Page	353
Creating Walled Garden Access	355
Mobility Access Switch Server Certificate	355
Tunneled Nodes	357
Important Points to Remember	357
Tunneled Nodes Overview	358
Support for Tunneled Node Back-up Server	359
Creating and Configuring Tunneled Node Profile	359
Verifying and Monitoring Tunneled Nodes	360
Verifying and Monitoring the Tunneled Nodes on the Controller	360
Aruba AP Integration	361
Aruba Instant Overview	361
Aruba AP Integration with Mobility Access Switch	361
Viewing the Blacklisted MAC Address of the Rogue APs	363
Dynamic Port Reconfiguration	365
Device-Group Configuration	365
Aruba AirGroup Integration	369
Overview	369
Configuring mDNS packet forwarding	369
Sample Configuration	370

ClearPass Policy Manager Integration	373
Introduction	373
Important Points to Remember	373
Enabling Role-Download on Mobility Access Switch	374
Deleting Downloadable Roles	375
Sample Configuration	375
Virtual Private Networks	385
Site-to-Site VPN	385
Site-to-Site VPN Interface Survivability	390
Default Route to VPN	392
Aruba VPN	393
Distributed DHCP Scopes	395
Static Route Support for VPN	397
Troubleshooting	397
Port Mirroring	399
Important Points to Remember	399
The Source Port	399
The Destination Port	399
Mirroring Sampled Ratio	399
Creating and Applying a Mirroring Profile to an Interface	400
Sample Configuration	400
Verifying Port Mirroring Configuration	400
Remote Monitoring (RMON)	403
Remote Monitoring (RMON) Overview	403
Enabling RMON Service	403
Configuring RMON Parameters	403
Viewing RMON Active Configuration	406

SNMP and Syslog	409
MIB and SNMP	409
SNMP Parameters for Mobility Access Switch	409
Logging	417
Glossary of Terms	418

Revision History

The following table provides 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: <ol style="list-style-type: none">Customer-reported issues<ul style="list-style-type: none">Bandwidth Control in MASS2S VPN—multiple subnetsBugs with Techpubs keyword<ul style="list-style-type: none">94980—Sample MSTP Topology revised106468—Central Activate Behavior After Leaving Factory Default110151—Policer-profile sub-option per-user under user
Release 04	Addressed all new features and enhancements from ArubaOS 7.4.0.1 through ArubaOS 7.4.1.7. Addressed customer-reported concern - ID 154555

This guide describes the instructions and examples for configuring the ArubaOS Mobility Access Switch.

This chapter covers:

- [What's New In ArubaOS 7.4.x on page 15](#)
- [Audience on page 18](#)
- [Fundamentals on page 18](#)
- [Related Documents on page 19](#)
- [Conventions on page 19](#)
- [Contacting Support on page 20](#)

What's New In ArubaOS 7.4.x

The following features and enhancements are introduced in ArubaOS 7.4.x:

Table 2: *New Features in ArubaOS 7.4.x*

Feature	Description
Route Monitoring	Route Monitoring enables the Mobility Access Switch to monitor the L3 uplink status using ping probes. The causes due to which the probe status of the interface is down are indicated by the Flags column in the command output.
Authentication Survivability	The authentication survivability (also called auth survivability) feature provides support for a survivable authentication framework when the link to the remote authentication server fails.
Auto-Link Aggregation Control Protocol	Auto Link Aggregation control Protocol (Auto-LACP) dynamically forms a port channel when both ports of a dual-port AP are connected to the same Mobility Access Switch.
Disabling BASH Access	In Mobility Access Switch, the BASH access is disabled for security reasons.
SSH Enhancement	Mobility Access Switches do not support the Diffie Hellman (DH) Group 1 key exchange algorithm in the Secure Shell (SSH) configuration.
Aruba VPN	Aruba VPN utilizes the factory installed certificates and the Mobility Controller whitelist to enable the rapid deployment of a secure tunnel between Mobility Access Switches and a Mobility Controller. This feature is very similar to Aruba's existing RAP and RAPNG (Instant AP) VPN capability.
AirWave ZTP VPN	Using the new Aruba VPN feature, Mobility Access Switches can receive a Mobility Controller IP address via Aruba Activate so that it may establish a VPN to AirWave for Zero-Touch Provisioning (ZTP).
PAPI Enhanced Security	Mobility Access Switch introduces an enhancement to PAPI Security feature that provides protection to Aruba devices and AirWave against malicious users sending fake messages that results in security challenges.

Table 2: New Features in ArubaOS 7.4.x

Feature	Description
Deny Inter-User Traffic	Deny Inter-User Traffic enables Mobility Access Switches to filter traffic between users with the same role.
Dynamic DNS Client	The Dynamic DNS Client enables a Mobility Access Switch to update its DHCP assigned IP address with a Dynamic DNS service provider. This helps to keep the remote devices reachable without tracking their IP address. Mobility Access Switch extends support for the myonlineportal.net dynamic DNS server in addition to the other servers
NAT Pools	Network Address Translation Pools extend the NAT capabilities of the Mobility Access Switch to support one-to-one NAT or NAT certain traffic to one IP address and the rest to another.
Session ACLs on RVI	Session Access Control Lists on Routed VLAN Interfaces provide session aware security for L3 interfaces irrespective of physical port.
IP NAT Outside	IP NAT Outside enables NAT on a specific egress Routed VLAN Interface to avoid performing NAT operations on inter-VLAN traffic when there are multiple private side VLANs.
Site-to-Site VPN Interface Survivability	Site-to-Site VPN Interface Survivability enables seamless VPN connectivity through a configured standby interface upon failure of the primary interface.
Default Route to VPN	A crypto map matching all destinations can now be used for customer applications requiring all client generated traffic (Internet and Corporate bound) to be sent over a VPN tunnel.
Distributed L3 DHCP Scopes	Distributed L3 DHCP Scopes enables remotely deployed Mobility Access Switches to be dynamically assigned unique DHCP Scopes when using Aruba VPN with a Mobility Controller.
DHCP Scope Distribution	By default, only those Mobility Access Switches with configurations received from Trusted modes can access the data center.
Device Group Configuration	Device Groups is a mechanism by which a Mobility Access Switch dynamically reconfigures interface-profiles attached to a port based on the type of device connected to it. Initial device support is for Aruba Access Points (Campus and Instant).
Configurable Rogue AP Containment	Instant APs can provide information on suspected Rogue APs that a Mobility Access Switch can act upon. For example, shutting down the port connected to the AP detected as Rogue. In earlier versions of ArubaOS, the containment options were not user configurable.
Multiple Default Gateway Support using Route Metrics	Multiple default gateways may now be configured using static routes or DHCP enabled Routed VLAN Interfaces and prioritized using metrics.
IGMPv3 Snooping	IGMPv3 Snooping and snooping proxy can now be used with clients using IGMPv3 multicast messaging.
Static ARP Support	User-defined entries may now be manually entered into the ARP table.
SSLv3 TLS Disable	SSLv3 transport layer security is now disabled from ArubaOS 7.4.0.1 onwards.

Table 2: *New Features in ArubaOS 7.4.x*

Feature	Description
New and Modified SNMP Traps	Two new Aruba Enterprise traps for linkup/linkdown status are introduced in the Mobility Access Switch. Another trap to indicate the Stack MAC change is also introduced. An existing Aruba Enterprise trap is modified.
CPPM Server Authentication	The Mobility Access Switch requires the user to provide the CPPM server admin credentials starting from ClearPass Policy Manager 6.4.3 to download roles from the CPPM server.
Personalized Captive Portal Page	The Authorization Required page appearing before the actual Captive Portal login page is removed from the Mobility Access Switch WebUI.
Sticky MAC	The Mobility Access Switch is modified to allow you configure the Sticky MAC feature with an action to take when a Sticky MAC violation occurs. The allowed actions are down and shutdown .
QoS Trust on Tunneled Node Port	When qos-trust parameter is enabled on a Tunneled Node port, the QoS markings (DSCP/dot1p) of the incoming packet are copied to the outer GRE header packet as well. This enables appropriate QoS treatment along the tunnel path.
Port Bounce	Mobility Access Switch provides support for the port bounce feature which enables a client to re-initiate a DHCP request when there is a VLAN change.
Factory-Reset on a Detached ArubaStack Member	You can reset a detached ArubaStack member that boots up as a line card to its factory defaults. This allows you to reset the password on the Mobility Access Switch if the login credentials are lost.
Global and ACL-Based Packet Tracing	Mobility Access Switch introduces a new feature to enable or disable the global packet tracing and ACL-based packet tracing functionalities.
GVRP Enhancement	Mobility Access Switch displays a warning message when you apply the GVRP profile on an interface without enabling the global GVRP functionality.
Traceoptions Enhancement	Mobility Access Switch allows you to specify the actual interface number or the port-channel instead of specifying the index number of the port. It also allows you to filter OSPF and PIM traces by interface ID.
OSPF Enhancement	Mobility Access Switch introduces options to get the OSPF details such as Interface, Instance, Area, IP/MASK, Cost, State, and Neighbors in a brief tabular format.
Troubleshooting ZTP	Mobility Access Switch introduces an enhancement to help troubleshoot any ZTP issues.
Enhancement to Switching Profile	Mobility Access Switch now allows you to remove any switching-profile applied to a tunnel and point the tunnel back to the default switching-profile.
Source Interface Support for TACACS+ Server	Mobility Access Switch introduces an enhancement to allow you select a specific source interface IP address for the outgoing TACACS+ packets.
Error Statistics Views in WebUI	The column header in the Dashboard > Interfaces page of the Mobility Access Switch WebUI is changed to Total Error Frames .

Table 2: *New Features in ArubaOS 7.4.x*

Feature	Description
Support to Delete Downloadable Roles from CPPM Server	Mobility Access Switch now allows you to delete downloadable roles from the CPPM server.
Proxy ARP	Mobility Access Switch supports proxy ARP. When you enable the proxy ARP feature, SOS traps all the ARP packets to the Proxy-ARP module in the control plane.
Stack Member Renumbering	Mobility Access Switch now allows a user to renumber any stack member except the primary and secondary stack members.
NTP Version Upgrade	Network Time Protocol (NTP) version is upgraded to ntp-4.2.8p4. With this upgrade, 13 NTP vulnerabilities are addressed; further, the server IP resolution and sync time are quicker than that in earlier versions.
LLDP-MED Enhancement	In Mobility Access Switches, the LLDP-MED option is set to auto mode. Hence the Mobility Access Switch can publish its LLDP-MED-related information to the neighbor only when it receives the LLDP-MED information from the neighbor.
Revocation of ArubaOS Default Certificate	This security update concerns revocation of ArubaOS default certificate issued by GeoTrust from ArubaOS 7.4.1.7 version. The Mobility Access Switch-issued server certificate replaces the ArubaOS default certificate issued by GeoTrust Public CA for WebUI authentication, Captive Portal, 802.1X termination, and Single Sign-On (SSO) because the default certificate is now revoked.
Applicability of logging level debugging user debug command	Users are restricted from configuring the logging level debugging user debug command for the Stack Manager process, because this is applicable only to the Auth Manager process.

Audience

This is intended for system administrators responsible for accessing networking infrastructures and assumes you are knowledgeable in Layer 2 and Layer 3 networking technologies.

Fundamentals

Throughout this document references are made to the Mobility Access Switch and configuring using the WebUI or command line interface (CLI).

WebUI

The WebUI is accessible through a standard Web browser from a remote management console or workstation. The WebUI includes a Quick Setup wizard that steps you through tasks that includes:

- Basic Information—Specify device name, domain name, password, date, and time
- Management—Specify switch management options, VLAN assignment, and static or DHCP IP address assignment
- Summary page— Displays the settings and allows you to print or save the summary from a separate window.

The WebUI also includes a post-setup Dashboard, Configuration, Diagnostic, and Maintenance screens.

WebUI Enhancement

Starting from ArubaOS 7.4.1, the column header in the **Dashboard > Interfaces** page of the Mobility Access Switch WebUI is changed from **Total Errors** to **Total Error Frames** to indicate that the error counter refers to the frames counter.

CLI

The CLI is a text-based interface accessible from a local console connected to the serial port on the S3500 or through a Telnet or Secure Shell (SSH) session.



By default, you can access the CLI from the serial port or from an SSH session. You must explicitly enable Telnet on your Mobility Access Switch in order to access the CLI using a Telnet session.

When entering commands remember that:

- commands are not case sensitive
- the space bar will complete your partial keyword
- the backspace key will erase your entry one letter at a time
- the question mark (?) will list available commands and options

Related Documents

The following documents are part of the complete documentation suite for the Aruba Mobility Access Switch:

- *Aruba S3500 Series Mobility Access Switch Installation Guide*
- *Aruba S2500 Series Mobility Access Switch Installation Guide*
- *Aruba S1500 Series Mobility Access Switch Installation Guide*
- *ArubaOS Mobility Access Switch Command Line Reference Guide*
- *ArubaOS Mobility Access Switch Quick Start Guide*
- *Release Notes*

Conventions

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

Table 3: *Typographical Conventions*

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
system items	This fixed-width font depicts the following: <ul style="list-style-type: none">• 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.

Type Style	Description
<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.

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

System basics is an introduction to the feature rich ArubaOS Mobility Access Switch and introduces functionalities that are presented in detail in the rest of this document. This chapter covers:

- [Factory Initial Configuration on page 21](#)
- [Zero-Touch Provisioning on page 23](#)
- [Trace Options on page 27](#)
- [Profiles Management on page 29](#)
- [Understanding Interface Profiles on page 38](#)
- [Understanding Interface Group on page 40](#)
- [Managing Controller IP on page 41](#)
- [Using the LCD on page 41](#)
- [Setting the System Clock on page 44](#)
- [Managing Files on the Mobility Access Switch on page 45](#)
- [PAPI Enhanced Security on page 49](#)

Security Update

This security update concerns revocation of ArubaOS default certificate issued by GeoTrust. Refer to the *ArubaOS 7.4.1.6 Release Notes*.

The Mobility Access Switch-issued server certificate replaces the ArubaOS default certificate issued by **GeoTrust Public CA** for WebUI authentication, Captive Portal, 802.1X termination, and Single Sign-On (SSO) because the default certificate is now revoked.

For more information on the **GeoTrust Public CA** certificate revocation, refer to the [advisory](#).

Using the Mobility Access Switch-issued server certificate has the following caveats:

- When MacBook or iOS devices connect to Captive Portal, the CNA (Captive Network Assistant) popup window does not appear. So, you must open a browser to get redirected to a Captive Portal page.
- When the Captive Portal custom welcome page is configured in Mac Safari 8.1, the certificate warning pops up as soon as the welcome page appears.
- EAP-TLS authentication does not work with self-signed certificates; hence Authentication Survivability fails on Windows clients with EAP-TLS authentication.
- 802.1X PEAP authentication fails on Windows 7 clients. So, you must disable the **Validate Server Certificate** option on the Windows 7 clients.



It is recommended to use custom certificates to avoid these caveats



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

Factory Initial Configuration

The Mobility Access Switch is pre-loaded with a factory initial configuration. The default username/password to log in to the Mobility Access Switch is admin/admin123.

To view the initial factory setting, execute the **show running configuration** command with the initial factory option.

```
(host) #show running-config | include factory-initial
Building Configuration...
interface-profile poe-profile "poe-factory-initial"
interface-profile lldp-profile "lldp-factory-initial"
vlan-profile igmp-snooping-profile "igmp-snooping-factory-initial"
igmp-snooping-profile "igmp-snooping-factory-initial"
lldp-profile "lldp-factory-initial"
poe-profile "poe-factory-initial"
```



By default, MSTP is enabled in the factory setting.

Restoring Factory Default Settings in S1500 Switches

Starting from ArubaOS 7.4.0.2, the S1500 Mobility Access Switch allows you to use the Mode button to restore the switch to the factory default settings. You can enable this feature by using a CLI command on a configured S1500 Mobility Access Switch. After enabling the feature, you must 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.

Configuring Mode Button in S1500 Mobility Access Switches

Execute the following commands to enable the **Mode** button for factory reset:

```
(host) (config) #mode-button
(host) (mode-button) #enable factory-default
```

Verifying Mode Button Configuration

Use the following command to verify the **Mode** button configuration:

```
(host) #show mode-button
mode-button (N/A)
-----
Parameter      Value
-----      -
factory-default enabled
```

Spanning Tree Modes

The spanning tree mode is set to MSTP in factory default.

```
(host) #show running-config | begin spanning-tree
Building Configuration...
spanning-tree
  mode mstp
```

To change spanning tree modes, use the spanning tree mode command. After you change the spanning tree mode, the new spanning tree is automatically applied to all configured VLANs, including default VLAN 1.

```
(host) (config) #spanning-tree mode ?
mstp          Multiple spanning tree mode
pvst          Per-Vlan rapid spanning tree mode
(host) (config) #spanning-tree mode pvst
```

To verify the current spanning tree mode:

```
(host) (config) #show spanning-tree-profile

spanning-tree
-----
```

Parameter	Value
-----	-----
spanning-tree-mode	pvst

For more information on spanning tree, see [MSTP on page 163](#) and [Rapid PVST+ on page 177](#).

Zero-Touch Provisioning

The Mobility Access Switch supports zero-touch provisioning (ZTP) using one of the following methods:

- By downloading a predefined configuration file from a TFTP server.
- By contacting the customer's AirWave Management Platform (AMP) server using options provided by DHCP.
- By using Aruba's cloud-based Activate service to contact the customer's AMP server.
- By using Aruba Central, Aruba's cloud-based Management service.

For any of the ZTP services, the Mobility Access Switch must receive an IP address via DHCP with the necessary options for it to query a TFTP Server or AMP Server (directly or through information provided by Activate) or Aruba Central.



NOTE

By default, the Mobility Access Switch has the DHCP client enabled on VLAN 1.

ZTP starts in the following sequence as soon as a factory default Mobility Access Switch boots up:

1. Mobility Access Switch receives an IP address and server options via DHCP.
2. It first attempts to download the configuration file from the TFTP server based on the DHCP options received.
 - a. If both option 150 and option 67 (IP and filename respectively) are received, it attempts to download the file specified in option 67 from the TFTP server whose address is defined in option 150.
 - b. If only option 150 is received, it attempts to download a file with the name, `<SERIALNUMBER>.cfg` from the TFTP server.
 - c. If none of the above methods is successful, the Mobility Access Switch moves to the next step.
3. It checks for option 60 with a value **ArubaInstantAP**. If the value does not match, it moves directly to Step 4.
 - a. If the value matches, it checks for option 43 to obtain the AirWave configuration parameters.
 - b. If the AirWave parameters are valid, it attempts to contact and register with AMP.
 - c. After successful registration, AirWave configures the Mobility Access Switch.
 - d. If any of the above fails, it moves to Step 4.
4. If DNS servers have been provided by DHCP, the Mobility Access Switch attempts to connect to Activate via <https://devices.arubanetworks.com> and gets the AMP details based on the provisioning rule defined in Activate. If no provisioning rule is defined in Activate, it moves to Step 5.
 - a. The Mobility Access Switch automatically establishes an IPsec tunnel with the Aruba Mobility Controller, if a controller IP is provisioned in the Activate server along with the AMP details. If a controller IP is not provisioned, it moves to the next step.



NOTE

A VPN tunnel is established, only if Activate is configured with the IP address of the AirWave Management Platform (AMP) and the controller IP. The use of hostnames for AirWave Management Platform (AMP) or Mobility Controller is not currently supported for VPN establishment. through ZTP.

- b. Mobility Access Switch sends registration request to AMP upon successful receipt of the AMP details.
- c. After successful registration, AirWave configures the Mobility Access Switch.

- d. If all the above steps fail, it moves to the next step.



If you have an Aruba Central license assigned to manage your device, Activate automatically directs the Mobility Access Switch to Aruba Central. For more information on provisioning a device using Aruba Central, see [Provisioning Mobility Access Switch Using Aruba Central Portal on page 62](#).

5. The Mobility Access Switch keeps polling Activate in the background as long as it is in factory-default configuration. The polling stops as soon as the switch moves out of factory-default configuration or when a user intervenes by logging in to the switch. However, the polling for firmware continues at periodic intervals until it is manually disabled by executing the following command on the Mobility Access Switch:

```
(host) (config) #activate-service-firmware
(host) (activate-service-firmware) #no enable
```

Each ZTP method is described in detail in the subsequent sections. For more details on Activate-based ZTP, see [Activate Integration Overview on page 63](#).



With a factory default configuration, all physical ports (base and uplink ports) are in VLAN 1 (untagged).

You can also configure ArubaStack using ZTP. Ensure that you connect and configure only the primary member of an ArubaStack before connecting the subsequent members. This ensures that the correct configuration is adopted by ArubaStack.

Important Points to Remember

The Mobility Access Switch must have:

- ArubaOS 7.2.1.1 or higher for TFTP-based configuration file download.
 - ArubaOS 7.3.1.0 or higher for DHCP-based AirWave detection.
 - ArubaOS 7.3.0.0 or higher for Activate service.
 - ArubaOS 7.3.2.0 or higher for Aruba Central.
 - ArubaOS 7.4.0.0 or higher for AirWave ZTP over Aruba VPN.
 - The Mobility Access Switch must be in factory default for ZTP.
- A DHCP server must be reachable through an untagged interface.
- If WebUI Startup Wizard or CLI Quick Setup is initiated, all ZTP services are disabled.
- The Mobility Access Switch blocks the WebUI and Quick-setup options in the following scenarios:
 - After the configuration file is successfully downloaded from the TFTP server.
 - After the provisioning information is downloaded from the Activate server.

However, the users can still login and configure the Mobility Access Switch.

TFTP-Based Zero-Touch Provisioning

The TFTP-based ZTP service relies on the following:

- Configuration file stored on an accessible TFTP Server—The file name can either be *<serial-number-of-device>.cfg* or *<customer-defined>.cfg*.
- Configuration file must be less than 2 MB.
- The content in the configuration file must begin with:

```
#
# Configuration file for ArubaOS
```
- The TFTP server address in the DHCP Offer—The TFTP server address can be stored in `siaddr` or `option 150` or both. If the TFTP server address is included in both, the `siaddr` takes precedence.

- (Optional) Configuration filename and path in the DHCP Offer—The filename and path can be stored in the boot-file option or option 67, or both. When using this option, you may choose any filename for the configuration as long as the file extension is *.cfg*. For example, *aruba-mas.cfg*. When not using the boot-file option or option 67, the Mobility Access Switch attempts to download a configuration file name with its serial number (*<serialnumber>.cfg*).

When these options are processed, the Mobility Access Switch downloads the new configuration file, compares it with the configuration file in use, and if they differ, the new file is copied as *default.cfg*. The Mobility Access Switch then reboots automatically and loads the new configuration file. A syslog message is logged for every failed or successful configuration download.

DHCP-Based AirWave Discovery

The Mobility Access Switch can be provisioned with the AirWave parameters through DHCP. To achieve this, DHCP options 60 and 43 are used to transmit the AirWave configuration parameters.

To avoid conflicts with Aruba Instant AP deployments, the Mobility Access Switch uses the same DHCP option 60 value (**ArubaInstantAP**), to first validate that DHCP option 43 contains AirWave configuration parameters.

Option 43 is sent in the format, **Group:Top-Folder:Sub-Folder,AMP IP,Pre shared secret** where:

- **Group** maps to Device Group in AirWave.
- **Group:Top-Folder:Sub-Folder** maps to Folder information for the device.
- **AMP IP** is the AirWave IP.
- **Pre shared secret** is the shared secret between AirWave and the device.

For example, if the option 43 string is **Acme:Store1,192.168.1.10,aruba123** the following group and folder structure is created on AMP:

- A group with the name, **Acme** is created.
- A top-level folder with the name, **Acme** is created.
- A sub-folder with the name, **Store1** is created.
- AirWave IP is **192.168.1.10**.
- Pre shared secret is **aruba123**.

The format **Group,AMP IP,Pre shared secret** is also accepted as sub-folder is not mandatory in the AMP configuration parameters.

For example, if the option 43 string is **Acme,192.168.1.10,aruba123**, the following group and folder structure is created on AMP:

- A group with the name, **Acme** is created.
- A top-level folder with the name, **Acme** is created.
- AirWave IP is **192.168.1.10**.
- Pre shared secret is **aruba123**.

Important Points to Remember

- If Mobility Access Switch receives AirWave parameters as part of option 43, it will not attempt Activate-based Zero-Touch Provisioning.
- If option 60 is not offered or does not match the value **ArubaInstantAP**, then the Mobility Access Switch ignores option 43 and initiates the Activate-based Zero-Touch Provisioning.

DHCP Scope Distribution

Starting from ArubaOS 7.4.1.3, by default, only those Mobility Access Switches with configurations received from Trusted modes can access the data center.

Configurations for VPN deployments are done through Aruba Central or AirWave as these are considered as Trusted modes. If the Mobility Access Switch received the configuration from Aruba Central, the **Trusted Branch Mode** flag is set to 1. If it received the configuration from AirWave, the **Trusted Branch Mode** flag is set to 2. When this flag value is set to 1 or 2, the registration request is sent with the value for **Trusted Branch** set to **Yes**. Otherwise, the value for **Trusted Branch** is set to No and the controller will block the Mobility Access Switch.

Troubleshooting Zero-Touch Provisioning

Starting from ArubaOS 7.4.1, Mobility Access Switch introduces the **show ztp-boot-info** command to help troubleshoot any ZTP issues.

The output of the **show ztp-boot-info** command displays the status of various methods of provisioning a Mobility Access Switch. The output details include TFTP configuration download status, DHCP AMP discovery status, Activate AMP discovery status in addition to DHCP options received.

Execute the following command to get the details of the method of provisioning for Mobility Access Switch:

```
(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
```

For details on the description of output parameters for the **show-ztp-boot-info** command, refer to the *ArubaOS 7.4.x CLI Reference Guide*.

Packet Tracing

The packet tracing feature is used to enable or disable global packet tracing and ACL-based packet tracing. Starting from ArubaOS 7.4.1, Mobility Access Switch allows you to enable global and ACL-based packet tracing options.

Two new CLI commands are introduced to enable this feature—**pkt-trace-global enable** and **pkt-trace acl <ACL-name> enable**.

Configuring Packet Tracing

You can configure either the global packet tracing option or the ACL-based packet tracing option.

Enabling and Disabling Global Packet Tracing

Execute the following CLI command to enable global packet tracing:

```
(host) # pkt-trace-global enable
```

Execute the following CLI command to disable global packet tracing:

```
(host) # pkt-trace-global disable
```

Enabling and Disabling ACL-based Packet Tracing

Execute the following CLI command to enable packet tracing for an ACL entry:

```
(host) # pkt-trace acl <ACL-name> enable
```

Execute the following CLI command to disable packet tracing for an ACL entry:

```
(host) # pkt-trace acl <ACL-name> disable
```

Sample Configuration

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
```

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
```

Verifying Packet Tracing Configuration

The following **show** command helps verify the packet tracing configuration:

```
(host) #show datapath debug trace-buffer
Datapath Trace Buffer Entries:
MacAddr( bb) 0x0 0x0 0x0 0x0 0xb86a1 0x6ac00000
MacAddr( bb) 0x0 0x0 0x0 0x0 0xb86a1 0x6ac00000
MacAddr( bb) 0x0 0x0 0x0 0x0 0xb86a1 0x6ac00000
CPDNSok( 4f) 0x0 0x1 0xa1045a2 0x37 0x1f0x0
...
```



The **show** command output may not completely imply that the packet tracing configuration is set. Enabling packet tracing might impact the throughput of the system.

Trace Options

The tracing feature is important for debugging the sequence of events that occur inside a process or protocol, for example message processing, state machine transitions, configuration change events, or timer events.

You can enable or disable trace options for various modules such as mstp, lldp, igmp, ospf, pim, rmon, layer2-forwarding, interface-manager, chassis-manager, and stack-manager using the `traceoptions` command.



The traceoption port references use the SNMP interface index number and not the X/Y/Z values.

Configuring Trace Options

You can use the following command to enable or disable the traceoptions for various modules:

```
(host) (config) #traceoptions
(host) (traceoptions) #?
chassis-manager          Control chassis manager trace options
dhcp-snoop               Control DHCP Snoop trace options
igmp                     Control igmp trace options
igmp-snooping            Control igmp-snooping trace options
interface-manager        Interface manager trace options
layer2-forwarding        Control Layer2 Forwarding trace options
lldp                     Control LLDP trace options
mstp                     Control MSTP trace options
```

```

no                Delete Command
ospf              Control ospf trace options
pim              Control pim sparse mode trace options
rmon             rmon trace options
routing          Control layer3 manager trace options
stack-manager    Control stack-manager trace options
vrrp             Control vrrp trace options

```

Use the following commands to configure the OSPF VLAN ID and Tunnel ID as filters:

```

(host) (traceoptions) #ospf vlanid <ID>
(host) (traceoptions) #ospf tunlid <ID>

```

Similarly, use the following commands to configure PIM VLAN ID and Tunnel ID as filters:

```

(host) (traceoptions) #pim vlanid <ID>
(host) (traceoptions) #pim tunlid <ID>

```

Starting from ArubaOS 7.4.1, the port command under traceoptions allows you to specify the actual interface number or the port-channel instead of specifying the index number of the port. The following two options are introduced under the **port** command:

- gigabitethernet—Specify the actual interface number
- port-channel—Specify the port-channel ID

The sample port configuration commands are as follows:

```

(host) (traceoptions) #mstp port gigabitethernet 0/0/6
(host) (traceoptions) #mstp port port-channel 1

```

Verification

The following command displays the enabled trace options:

```

(host) #show trace ?

```

```

chassis-manager    Show the contents of chassis manager trace file
dhcp-snooping      Show the contents of dhcp-snooping trace file
igmp               Show the contents of igmp trace file
igmp-snooping      Show the contents of igmp-snooping trace file
interface-manager  Show the contents of interface manager trace file
layer2-forwarding  Show the contents of layer2-forwarding trace file
lldp               Show the contents of lldp trace file
mstp               Show the contents of mstp trace file
ospf               Show the contents of ospf trace file
pim                Show the contents of pim trace file
rmon               Show the contents of RMON trace file
stack-manager      Show the contents of stack-manager trace file
vrrp               Show the contents of VRRP trace file

```

Starting from ArubaOS 7.4.1, the **show traceoptions** command output is enhanced to filter OSPF and PIM traces by interface ID.

The sample output of the **show traceoptions** command is as follows:

```

(host) (traceoptions) #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

```



Without OSPF or PIM trace configuration, no filtering is done by VLAN ID and Tunnel ID and the output of **show traceoptions** command displays **0**, by default.

Examples

The following is an example traceoption configuration:

```

(host) (traceoptions) #layer2-forwarding flags fdb learning vlan
(host) (traceoptions) #show trace layer2-forwarding 10

```

The following is a sample OSPF trace VLAN ID configuration command:

```

(host) (traceoptions) #ospf vlanid 800

```

For a complete list of trace options commands, refer to the *ArubaOS 7.4.x Command Line Reference Guide*.

Profiles Management

The Mobility Access Switch supports profile based configuration for interfaces, interface-groups, port-channels, and VLANs. You can use profiles to apply the same configuration to multiple interfaces and VLANs. It is often tedious to configure a lot of interfaces individually. For example, instead of setting the interface characteristics such as speed and duplex multiple times for multiple interfaces, you can define them in a profile and apply the profile to the interfaces. This is beneficial when you have many interfaces that share the same characteristics where you can define the parameters in a profile and then reference the name of the profile on the interfaces. When you need a change later, the change needs to be made only on the profiles and not on the individual interfaces. The profile-based configuration helps you to avoid having to manage large configurations on every interface and VLAN.

This section includes the following topics:

- [Profiles for Interfaces on page 30](#)
- [Profiles for VLANs on page 31](#)
- [Scope of the Profiles and Parameters on page 31](#)
- [Creating a Profile on page 34](#)
- [Viewing a Profile and its Parameters on page 35](#)
- [Applying and Activating a Profile on page 37](#)

- [Deleting a Profile on page 38](#)
- [Best Practices on page 38](#)

Profiles for Interfaces

The Mobility Access Switch uses profile-based configuration for the physical interfaces. You can apply the same profile to multiple interfaces that share the same characteristics such as physical specifications, type, and VLAN membership. You can also apply these profiles to an interface-group, or a port-channel.

You can create and apply the following profiles to an interface:

Table 5: *Interface Profiles*

Interface Profile	Description	Reference
dhcp-relay-profile	Specifies the dhcp relay profile for an interface.	See Configuring DHCP Relay on page 222 .
enet-link-profile	Specifies the physical properties of an interface.	See Creating and Applying an Ethernet Link Profile to an Interface on page 105 .
gvrp-profile	Specifies the gvrp profile parameters for an interface.	See Enabling and Configuring GVRP Functionality on page 143 .
igmp-profile	Specifies the igmp profile parameters for an interface.	See Configuring IGMP on page 242 .
lACP-profile	Specifies the dynamic port-channel configuration parameters for an interface.	See Creating and Applying a Dynamic Port-Channel Profile to an Interface on page 119 .
lldp-profile	Enables or disables the Link Level Discovery Protocol (LLDP) and LLDP MED extension.	See Verifying the LLDP Profile Configuration to Check LLDP-MED Status on page 154 .
mirroring-in-profile	Specifies the ingress packet mirroring properties for an interface.	See Port Mirroring on page 399
mirroring-out-profile	Specifies the egress packet mirroring properties for an interface.	See Port Mirroring on page 399
mstp-profile	Specifies the MSTP configuration parameters for an interface.	See MSTP on page 163
oam-profile	Specifies the OAM configuration parameters for an interface.	See Operations, Administration, and Maintenance on page 129
ospf-profile	Specifies the OSPF configuration parameters for an interface.	See Configuring OSPF on page 229 .
pim-profile	Specifies the PIM configuration parameters for an interface.	See Configuring PIM-SM End to End on page 244 .
poE-profile	Specifies the PoE configuration parameters for an interface.	See Creating and Applying a PoE Profile to an Interface on page 111 .

Interface Profile	Description	Reference
port-security-profile	Specifies the port security parameters for an interface.	See Configuring Port Security Functionality on page 269 .
pvst-port-profile	Specifies the parameters for PVST bridge.	See Configuring using the Interface-based Profile on page 178 .
switching-profile	Specifies the switching parameters such as VLAN and port mode for an interface.	See Creating and Applying a Switching Profile to an Interface on page 135 .
tunneled-node-profile	Specifies the controller information for a tunneled node interface.	See Support for Tunneled Node Back-up Server on page 359 .
voip-profile	Specifies the VOIP configuration parameters for an interface that is connected to the VOIP devices and/or PCs and Laptops.	See Creating and Applying VoIP Profile to an Interface on page 160 .

Profiles for VLANs

You can configure the following profiles for a VLAN:

Table 6: *VLAN Profiles*

VLAN Profile	Description	Reference
dhcp-snooping-profile	Specifies the DHCP snooping configuration parameters for a VLAN.	See Configuring DHCP Snooping on page 265 .
igmp-snooping-profile	Specifies the IGMP snooping configuration parameters for a VLAN.	See Creating and Applying an IGMP Snooping Profile to a VLAN on page 251 .
mld-snooping-profile	Specifies the MLD snooping configuration parameters for a VLAN.	See Configuring MLD Snooping on page 257 .
pvst-profile	Specifies the PVST profile configuration parameters for a VLAN.	See Configuring PVST+ on page 177 .

Scope of the Profiles and Parameters

This section includes the following topics:

- [Factory Initial vs Default vs Non-Default Profiles and Parameters on page 31](#)
- [Profiles and Parameters Assigned to the Interfaces and Groups on page 32](#)
- [AAA Profiles Assigned to the Interfaces, Groups, and VLANs on page 33](#)
- [Profiles and Parameters Assigned to the Port-Channel Members on page 34](#)

Factory Initial vs Default vs Non-Default Profiles and Parameters

There are three factory initial profiles that are effective when you set the Mobility Access Switch to run on the factory initial setup. They are the following:

- `igmp-snooping-factory-initial` assigned to VLAN 1.
- `lldp-factory-initial` assigned to the default interface-group.
- `poe-factory-initial` assigned to the default interface-group.

The `lldp-factory-initial` and the `poe-factory-initial` profiles are also part of the default interface-group configuration and work as the default profiles for all the interfaces.

Any profile that has the `default` reserved keyword as the profile name is called the default profile. Similarly, any parameter assigned to the default interface-group is called the default value for the interface. Modifying any of the default parameters within the default profiles does not make the profile non-default. Similarly, modifying the default parameters for the default interface-group does not make the parameter non-default.

Profiles that you create with names other than `factory-initial` and `default` are called non-default profiles. Similarly, interface-groups that you create using other than the `default` keyword are called non-default interface-groups.

Profiles and Parameters Assigned to the Interfaces and Groups

The effective profile or the parameter for an interface is determined by the following concurrent rules:

1. A non-default profile or parameter takes precedence over the default profile or parameter irrespective of whether it is configured under the interface or the interface-group.
2. If the interface and the interface-group have a non-default profile or parameter, then an interface configuration takes precedence over interface-group configuration.

For example, the effective configuration is selected based on the rules in the following table:

Table 7: *Scope of the Interface Parameters and Profiles*

<code>interface gigabitethernet <slot/module/port></code>	<code>interface-group gigabitethernet <group-name>/default</code>	Effective Profile/Parameter: <code>show interface-config gigabitethernet <slot/module/port></code>
default	default	default
default	A (non default)	A (non default)
B (non default)	default	B (non default)
C (non default)	D (non default)	C (non default)

By default, all the interfaces belong to a default interface-group. To view the configuration of the default interface-group, use the **show interface-group-config gigabitethernet default** command. When you create new interface-groups, the interfaces that do not belong to the new interface-groups continue to belong to the default interface-group. Note that overlapping ranges of interfaces among interface-groups is not supported.

You can view the default interface-group configuration using the following command:

```
(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

You can change the default interface-group using the following command:

```
(host) (config) # interface-group gigabitethernet default
```

For example, the following table determines the effective configuration of the `shutdown` parameter for an interface:

Table 8: *Scope of the Shutdown Parameter*

interface gigabitethernet <slot/module/port>	interface-group gigabitethernet <group-name>/default	Effective Parameter
no shutdown (default)	no shutdown (default)	no shutdown (default)
no shutdown (default)	shutdown (non default)	shutdown (non default)
shutdown (non default)	no shutdown (default)	shutdown (non default)
shutdown (non default)	shutdown (non default)	shutdown (non default)

For example, the following table determines the effective configuration of the `mtu` parameter for an interface:

Table 9: *Scope of the MTU Parameter*

interface gigabitethernet <slot/module/port>	interface-group gigabitethernet <group-name>/default	Effective Parameter
1514 (default)	1514 (default)	1514 (default)
1514 (default)	2000 (non default)	2000 (non default)
1000 (non default)	1514 (default)	1000 (non default)
2500 (non default)	3000 (non default)	2500 (non default)

AAA Profiles Assigned to the Interfaces, Groups, and VLANs

If no AAA profile is configured on the interface, interface-group, or VLAN, then, the default AAA profile is applied to the untrusted interfaces implicitly. If there are different non-default AAA profiles assigned to the interface, interface-group, and VLAN, the effective AAA profile is selected based on the rules in the following table:

Table 10: Scope of a AAA Profile

interface gigabitethernet <slot/module/port>	interface-group gigabitethernet <group- name>/default	vlan <vlan-id>	Effective AAA Profile
N/A	N/A	N/A	default
N/A	N/A	A (non default)	A (non default)
N/A	B (non default)	C (non default)	B (non default)
D (non default)	E (non default)	F (non default)	D (non default)

The default AAA profile is defined below:

```
(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
```

You can modify the default AAA profile using the following command:

```
(host) (config) # aaa profile default
```

Profiles and Parameters Assigned to the Port-Channel Members

For port-channel members, apart from the following profiles and parameters, all the other profiles and parameters are inherited from the port-channel configuration:

- shutdown
- enet-link-profile
- lacp-profile
- lldp-profile

Creating a Profile

You can create the profiles using the WebUI or the CLI.

Using the WebUI

1. Navigate to the **Configuration > Ports** page.
2. Select the **Profile** tab.
3. Click **New** under the **Profile** list.
4. Enter the details in the **Profile Name** column.
5. Complete the details of the profile.
6. Click **Apply** and then **Save Configuration**.

Using the CLI

```
(host) (config) # aaa profile <profile-name>
    {parameters}
    exit
(host) (config) # vlan-profile igmp-snooping-profile <profile-name>
    {parameters}
    exit
(host) (config) # interface-profile enet-link-profile <profile-name>
    {parameters}
    exit
(host) (config) # interface-profile lacp-profile <profile-name>
    {parameters}
    exit
(host) (config) # interface-profile lldp-profile <profile-name>
    {parameters}
    exit
(host) (config) # interface-profile mirroring-profile <profile-name>
    {parameters}
    exit
(host) (config) # interface-profile mstp-profile <profile-name>
    {parameters}
    exit
(host) (config) # interface-profile poe-profile <profile-name>
    {parameters}
    exit
(host) (config) # interface-profile switching-profile <profile-name>
    {parameters}
    exit
(host) (config) # interface-profile tunneled-node-profile <profile-name>
    {parameters}
    exit
(host) (config) # interface-profile voip-profile <profile-name>
    {parameters}
    exit
(host) (config) # policer-profile <profile-name>
    {parameters}
    exit
(host) (config) # qos-profile <profile-name>
    {parameters}
    exit
```

Example:

```
(host) (config) # interface-profile enet-link-profile 10-HALF
(Ethernet Link "10-HALF") #duplex half
(Ethernet Link "10-HALF") #speed 10
(Ethernet Link "10-HALF") #exit
```

Viewing a Profile and its Parameters

You can view the profile and profile details using the CLI.

Displaying the List of Profiles Under Each Category

```
(host)# show aaa profile
(host)# show vlan-profile igmp-snooping-profile
(host)# show interface-profile enet-link-profile
(host)# show interface-profile lacp-profile
(host)# show interface-profile lldp-profile
(host)# show interface-profile mirroring-profile
(host)# show interface-profile mstp-profile
(host)# show interface-profile poe-profile
(host)# show interface-profile switching-profile
(host)# show interface-profile tunneled-node-profile
(host)# show interface-profile voip-profile
(host)# show policer-profile
(host)# show qos-profile
```

Example:

```
(host)# show aaa profile
AAA Profile List
-----
Name                References  Profile Status
-----
default             2
default-dot1x       0          Predefined (editable)
default-mac-auth    0          Predefined (editable)
profile-new         3
```

Displaying the Parameters Assigned to Each Profile

```
(host)# show aaa profile <profile-name>
(host)# show vlan-profile igmp-snooping-profile <profile-name>
(host)# show interface-profile enet-link-profile <profile-name>
(host)# show interface-profile lacp-profile <profile-name>
(host)# show interface-profile lldp-profile <profile-name>
(host)# show interface-profile mirroring-profile <profile-name>
(host)# show interface-profile mstp-profile <profile-name>
(host)# show interface-profile poe-profile <profile-name>
(host)# show interface-profile switching-profile <profile-name>
(host)# show interface-profile tunneled-node-profile <profile-name>
(host)# show interface-profile voip-profile <profile-name>
(host)# show policer-profile <profile-name> <profile-name>
(host)# show qos-profile <profile-name>
```

Example:

```
(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

Applying and Activating a Profile

You can apply and activate the profiles created on the Mobility Access Switch using the CLI.

Applying and Activating the Profiles for an Interface

```
(host) (config) # interface gigabitethernet <slot/module/port>
  dhcp-relay-profile <profile-name>
  enet-link-profile <profile-name>
  gvrp-profile <profile-name>
  igmp-profile <profile-name>
  lacp-profile <profile-name>
  lldp-profile <profile-name>
  mirroring-in-profile <profile-name>
  mirroring-out-profile <profile-name>
  mstp-profile <profile-name>
  ospf-profile <profile-name>
  pim-profile <profile-name>
  poe-profile <profile-name>
  port-security-profile <profile-name>
  pvst-port-profile <profile-name>
  switching-profile <profile-name>
  tunneled-node-profile <profile-name>
  voip-profile <profile-name>
```

Applying and Activating the Profiles for an Interface Group

```
(host) (config) # interface-group gigabitethernet {default|<group-name>}
  dhcp-relay-profile <profile-name>
  enet-link-profile <profile-name>
  gvrp-profile <profile-name>
  igmp-profile <profile-name>
  lacp-profile <profile-name>
  lldp-profile <profile-name>
  mirroring-in-profile <profile-name>
  mirroring-out-profile <profile-name>
  mstp-profile <profile-name>
  ospf-profile <profile-name>
  pim-profile <profile-name>
  poe-profile <profile-name>
  port-security-profile <profile-name>
  pvst-port-profile <profile-name>
  switching-profile <profile-name>
  tunneled-node-profile <profile-name>
  voip-profile <profile-name>
```

Applying and Activating the Profiles for a Port-Channel

```
(host) (config) # interface port-channel <ID>
  enet-link-profile <profile-name>
  mirroring-in-profile <profile-name>
  mirroring-out-profile <profile-name>
  mstp-profile <profile-name>
  switching-profile <profile-name>
```

Applying and Activating the Profiles for a VLAN

```
(host) (config) # vlan <ID>
  pvst-profile <profile-name>
  mld-snooping-profile <profile-name>
  igmp-snooping-profile <profile-name>
```

Deleting a Profile

You can delete a profile using the following CLI commands:

```
(host) (config) # no aaa profile <profile-name>
(host) (config) # no igmp-snooping-profile <profile-name>
(host) (config) # no interface-profile enet-link-profile <profile-name>
(host) (config) # no interface-profile lacp-profile <profile-name>
(host) (config) # no interface-profile lldp-profile <profile-name>
(host) (config) # no interface-profile mirroring-profile <profile-name>
(host) (config) # no interface-profile mstp-profile <profile-name>
(host) (config) # no interface-profile poe-profile <profile-name>
(host) (config) # no interface-profile switching-profile <profile-name>
(host) (config) # no interface-profile tunneled-node-profile <profile-name>
(host) (config) # no interface-profile voip-profile <profile-name>
(host) (config) # no interface-profile dhcp-relay-profile <profile-name>
(host) (config) # no interface-profile gvrp-profile <profile-name>
(host) (config) # no interface-profile igmp-profile <profile-name>
(host) (config) # no interface-profile ospf-profile <profile-name>
(host) (config) # no interface-profile pim-profile <profile-name>
(host) (config) # no interface-profile port-security-profile <profile-name>
(host) (config) # no interface-profile pvst-port-profile <profile-name>
```

Best Practices

You can manage the profiles efficiently by applying the following guidelines:

- You can use the following process to efficiently manage the profiles:
 - a. Identify the various interface-groups that you need such as Admin, Finance, Marketing, Customer Support, Engineering, and QA.
 - b. Identify the profiles that you need to create for each interface-group.
 - c. Create and apply those profiles to the appropriate interface-groups and port-channels.
 - d. Create and apply the non common profiles to the individual interfaces.
- Use the `show references` command to find out if the profile is used or not, and then, delete all the unused profiles to keep your configuration clean and easy to understand.

Understanding Interface Profiles

There are instances when multiple interfaces share the same characteristics; for example, physical interface characteristics, type of switch interface, and/or VLAN ID. Interface profiles are used when the same configuration is defined on a profile and applied to multiple interfaces.

The parameters are defined in the functional profile(s) and the name of the profile is referenced on the interfaces. The interface profile is particularly useful when a change is required. The change can be made on the profile without updating the individual interfaces. [Table 11](#) lists the profiles and their functions.

Table 11: Interface Profiles

Profile Type	Description
ddns-profile	Configure a Dynamic DNS profile
dhcp-relay-profile	Configure a DHCP relay profile
enet-link-profile	Configure an Ethernet Link
gvrp-profile	Configure a GVRP profile
igmp-profile	Configure an Interface IGMP profile
lACP-profile	Configure an LACP
lldp-profile	Configure an LLDP Profile
mirroring-profile	Configure a Mirroring profile
mstp-profile	Configure an Interface MSTP
oam-profile	Configure an OAM profile.
ospf-profile	Configure an Interface OSPF profile
pim-profile	Configure an Interface PIM profile
poE-profile	Configure a Power over Ethernet profile
port-security-profile	Configure a Port Security profile
pvst-port-profile	Configure an Interface PVST bridge
switching-profile	Configure a switching profile
tunneled-node-profile	Configure a Tunneled Node Server profile
voip-profile	Configure a VOIP profile

Interface Numbering Convention

The Mobility Access Switch numbering convention includes three separate numbers:

- First number denotes slot number; in stacking mode, the first number is the stack member identification.
- Second number denotes the base ports; where 0 indicates the base interfaces and 1 indicates the uplink interfaces.
- Third number denotes the individual interface/port number.

For example, the interface gigabitEthernet 0/0/20 denotes the slot number zero (0), module 0 and port number 20. Note that interface/port numbering starts at 0.

Assigning an Interface Profile as an Access Port

To assign an interface as an access port belonging to a particular VLAN, configure the switching profile to reference the VLAN (for example VLAN 200). Then apply the switching profile to the interface itself (for example gigabitEthernet 0/0/10).

Configuring switching-profile that references VLAN 200:

```
(host) (config) #interface-profile switching-profile vlan_200
```

```
(host) (switching profile "vlan_200") #access-vlan 200
```

Applying the switching-profile to the gigabitethernet 0/0/10 interface:

```
(host) (config) #interface gigabitethernet 0/0/10
(host) (gigabitethernet "0/0/10") #switching-profile vlan_200
(host) (gigabitethernet "0/0/10") #exit
```

Assigning an Interface Profile as a Trunk

Similar to configuring an interface as an access port, assigning an interface profile as a trunk uses the trunk mode:

```
(host) (config) #interface-profile switching-profile TRUNK_PORTS
(host) (switching profile "TRUNK_PORTS") #switchport-mode trunk
```

Applying the switching-profile to the gigabitethernet 0/0/11 interface:

```
(host) (config) #interface gigabitethernet 0/0/11
(host) (gigabitethernet "0/0/11") #switching-profile TRUNK_PORTS
```

Native VLAN setting:

```
(host) (config) #interface-profile switching-profile TRUNK_PORTS
(host) (switching profile "TRUNK_PORTS") #native-vlan 100
```

By default, a trunk port allows all VLANs to be transported. This can be changed if necessary via the trunk parameter in the switching-profile:

```
(host) (config) #interface-profile switching-profile TRUNK_PORTS
(host) (switching profile "TRUNK_PORTS") #trunk allowed vlan all
```

Understanding Interface Group

It is often time consuming and tedious to configure multiple interfaces, which share the same configuration, via the command line. These interfaces can be grouped together so that any interface within the group can share the same configuration. When an interface is a member of an interface group, applying a specific profile to the interface will take precedence over interface group.

Configuring Interface Group

Define a group, for example `First_Floor`, which will contain the interfaces that share the same configuration. Apply valid interfaces members in ascending order; that is, from 0/0/0 through 0/0/30, and 0/0/32:

```
(host) (config) #interface-group gigabitethernet FIRST_FLOOR
(host) (gigabitethernet "FIRST_FLOOR") #apply-to 0/0/0-0/0/30,0/0/32
```

Notice there is no space in the list of interfaces.

Additionally, you can add or remove individual ports or ranges of ports without disrupting the existing port list using the following commands:

```
(host) (gigabitethernet "FIRST_FLOOR") #apply-to [add | remove] <interface-list>
```

Apply the switching-profile to the interface group:

```
(host) (gigabitethernet "FIRST_FLOOR") #switching-profile ACCESS_100
```

Verify your configuration or interface group using the **show interface-group-config** command.

```
(host) #show interface-group-config gigabitethernet FIRST_FLOOR
```

```
gigabitethernet "FIRST_FLOOR"
```

```
-----
Parameter                                     Value
-----
```

```
Interface range members          0/0/0-0/0/30,0/0/32
...
```

Managing Controller IP

The Mobility Access Switch automatically chooses the loopback IP or the first VLAN IP address as the controller IP address (also known as the Switch-IP) during the initial boot. If loopback does not exist, then the Mobility Access Switch automatically chooses the first VLAN IP as the IP address of the controller.

Aruba recommends configuring the controller IP address as the loopback interface when using Ethernet and Mobility Access Switch functionalities.

For Aruba VPN applications, you can set the controller IP as the inner IP of the VPN tunnel to source certain management traffic from that interface using the following commands:

```
(host) (config) #ip-profile
(host) (ip-profile) #controller-ip ipsec aruba-vpn
```



If a VLAN without an active member is first chosen (or configured) automatically as the controller IP address, then the controller IP will be unreachable.

1. Set the loopback interface (0 in the example) address and mask:

```
(host) (config) #interface loopback 0
(host) (loopback "0") #ip address 10.10.10.1
```

2. Set the controller-ip loopback to interface 0.

```
(host) (config) #ip-profile
(host) (ip-profile) #controller-ip loopback 0
```

3. Verify your configuration with the **show switch ip** command.

```
(host) (loopback "0") #show switch ip
```

```
Switch IP Address: 10.10.10.1
Switch IP is from Loopback Interface: 0
```

```
(host) (loopback "0") #
```

Using the LCD

The S2500/S3500 LCD panel is located on the upper right side of their respective faceplates. The LCD displays:

- Boot status
- Hostname
- Alarm
- Interface LED modes: Admin, Speed/Duplex, PoE
- ArubaOS version
- Power supply, Fan status

LCD Management

In addition to displaying current status, LCD panel supports a user-interactive maintenance mode:

- ArubaOS software image upgrade
- Configuration file upload
- Erase configuration (write erase all)
- Factory default setting (restore factory-default stacking)

- Media (external USB) eject
- System reboot (reload)
- System Halt (halt)
- GUI Quick Setup

Using the LCD and USB Drive

You can upgrade your image or upload your pre-saved configuration by using your USB drive and your LCD commands.

Upgrade an image

1. Copy MAS software image onto your USB drive into a directory named `/arubaimage`.
2. Insert the USB drive into the Mobility Access Switch's USB slot. Wait for 30 seconds for MAS to mount the USB.
3. Navigate to **Upgrade Image** in the LCD's **Maintenance** menu. Select **partition** and confirm the upgrade (Y/N) and then wait for Mobility Access Switch to copy the image from USB to the system partition.
4. Execute a system reboot either from the LCD menu or from the command line to complete the upgrade.

Upload a pre-saved configuration

1. Copy your pre-saved configuration and name the copied file **aruba_usb.cfg**.
2. Move your pre-saved configuration file onto your USB drive into a directory name **/arubaimage**.
3. Insert your USB drive into the Mobility Access Switch's USB slot. Wait for 30 seconds for MAS to mount the USB.
4. Navigate to the **Upload Config** in the LCD's Maintenance menu. Confirm the upload (Y/N) and then wait for the upload to complete.
5. Execute a system reboot either from the LCD menu or from the command line to reload from the uploaded configuration.

For detailed upgrade and upload instructions, see the *Upgrade Chapter* in the *Release Notes*.

LCD Functions with ArubaStack

[Table 12](#) lists the LED Stack mode and Maintenance mode along with each function. Some functions can be executed from any member in the ArubaStack (Primary, Secondary, or Line Card) to affect just that member. Other functions are executed from the Primary only but affect all members of the ArubaStack. For example, system reboot can be executed on a member only to reboot just that member. Or, you can execute system reboot on the Primary to reboot all members of the ArubaStack.

Table 12: LCD Functions Over Stacking

Mode	Any Stack Member (affects only local member)	Primary Only (affects all stack members)
LED Mode	Yes	—
Status (display)		
Stack	Yes	—
AOS Version	Yes	—

Mode	Any Stack Member (affects only local member)	Primary Only (affects all stack members)
PS Status	Yes	—
Fan Tray	Yes	—
Maintenance		
Upgrade Image	—	Yes
Upload Configuration	—	Yes
Erase Config	—	Yes
Media Eject	—	Yes
Factory Default	Yes	—
System Reboot	Yes	Yes
System Halt	Yes	Yes

Disabling LCD Menu Functions

For security purpose, you can disable all LCD menu functions by disabling the entire menu functionality using the following command:

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

To prevent inadvertent menu changes, you can disable LCD individual menu function using the following commands:

```
(host) (lcd-menu) #disable menu maintenance ?
erase-config Disable config erase menu
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
upload-config Disable config upload menu on LCD
upgrade-image Disable image upgrade menu on LCD
```

To display the current LCD functionality from the command line, use the following command:

```
(host) (config) #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 erase-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
```

Setting the System Clock

You can set the clock on a Mobility Access Switch manually.

In the CLI

To set the date and time, enter the following command in privileged mode:

```
(host) #clock set <year> <month> <date> <hour> <minutes> <seconds>
```

To set the time zone and daylight savings time adjustment, execute the following commands in configuration mode:

```
(host) (config) #clock timezone <WORD> <-23 - 23>
```

```
clock summer-time <zone> [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>]
```

Clock Synchronization

You can use Network Time Protocol (NTP) to synchronize the Mobility Access Switch to a central time source. Configure the Mobility Access Switch to set its system clock using NTP by configuring one or more NTP servers. For each NTP server, you can optionally specify the NTP iburst mode for faster clock synchronization. The iburst mode sends up to ten queries within the first minute to the NTP server. (When iburst mode is not enabled, only one query is sent within the first minute to the NTP server.) After the first minute, the iburst mode typically synchronizes the clock so that queries need to be sent at intervals of 64 seconds or more.



The iburst mode is a configurable option and not the default behavior for the Mobility Access Switch, as this option is considered “aggressive” by some public NTP servers. If an NTP server is unresponsive, the iburst mode continues to send frequent queries until the server responds and time synchronization starts.

Configuring NTP Authentication

The Network Time Protocol adds security to an NTP client by authenticating the server before synchronizing the local clock. NTP authentication works by using a symmetric key which is configured by the user. The secret key is shared by both the Mobility Access Switch and an external NTP server. This helps identify secure servers from fraudulent servers.



Starting from ArubaOS 7.4.1.3, the Network Time Protocol (NTP) version is upgraded from ntp-4.2.6p5 to [ntp-4.2.8p4](#). With this upgrade, 13 NTP vulnerabilities are addressed; further, the server IP resolution and sync times are quicker than those in earlier versions.

The following example enables NTP authentication, adds authentication secret keys into the database, and specifies a subset of keys which are trusted. It also enables the iburst option.

```
(host) (config) #ntp authenticate
```

```
(host) (config) #ntp authentication-key <key-id> md5 <key-secret>
(host) (config) #ntp trusted-key <key-id>
(host) (config) #ntp <server IP> iburst key <key-id>
```

Managing Files on the Mobility Access Switch

You can transfer the following types of files between the Mobility Access Switch and an external server or host:

- ArubaOS image file
- A specified file in the Mobility Access Switch's flash file system, or a compressed archive file that contains the entire content of the flash file system.



You can back up the entire content of the flash file system to a compressed archive file, which you can then copy from the flash system to another destination.

- Configuration files, either the active running configuration, startup configuration or stored configuration files.
- Log files

You can use the following protocols to copy files to or from a Mobility Access Switch:

- File Transfer Protocol (FTP): Standard TCP/IP protocol for exchanging files between computers.
- Trivial File Transfer Protocol (TFTP): Software protocol that does not require user authentication and is simpler to implement and use than FTP.
- Secure Copy Protocol (SCP): Protocol for secure transfer of files between computers that relies on the underlying Secure Shell (SSH) protocol to provide authentication and security.



The SCP server or remote host must support SSH version 2 protocol.

[Table 13](#) lists the parameters that you configure to copy files to or from a Mobility Access Switch.

Table 13: *File Transfer Configuration Parameters*

Server Type	Configuration
Trivial File Transfer Protocol (TFTP)	<ul style="list-style-type: none"> • IP address of the server • filename
File Transfer Protocol (FTP)	<ul style="list-style-type: none"> • IP address of the server • username and password to log in to server • filename
Secure Copy (SCP) You must use the CLI to transfer files with SCP.	<ul style="list-style-type: none"> • IP address of the server or remote host • username to log in to server • absolute path of filename (otherwise, SCP searches for the file relative to the user's home directory)

For example, you can copy an ArubaOS image file from an SCP server to a system partition on a Mobility Access Switch or copy the startup configuration on a Mobility Access Switch to a file on a TFTP server. You can also store the contents of a Mobility Access Switch's flash file system to an archive file which you can then copy to an FTP server. You can use SCP to securely download system image files from a remote host to the Mobility Access Switch or securely transfer a configuration file from flash to a remote host.

Transferring ArubaOS Image Files

You can download an ArubaOS image file onto a Mobility Access Switch from a TFTP, FTP, or SCP server. In addition, the WebUI allows you to upload an ArubaOS image file from the local PC on which you are running the browser.

When you transfer an ArubaOS image file to a Mobility Access Switch, you must specify the system partition to which the file is copied. The WebUI shows the current content of the system partitions on the Mobility Access Switch. You can optionally reboot the Mobility Access Switch with the transferred image file.

In the WebUI

1. Navigate to the **Maintenance > Image Management** page.
2. Select TFTP, FTP, SCP, or Local File.
3. Enter or select the appropriate values for the file transfer method.
4. Select the system partition to which the image file is copied.
5. Specify whether the Mobility Access Switch is to be rebooted after the image file is transferred, and whether the current configuration is saved before the Mobility Access Switch is rebooted.
6. Click **Upgrade**.
7. Click **Apply**.

In the CLI

```
(host) #copy tftp: <tftphost> <filename> system: partition [0|1]}
(host) #copy ftp: <ftphost> <user> <filename> system: partition {0|1}
(host) #copy scp: <scphost> <username> <filename> system: partition [0|1]
(host) #copy usb: <filename> system: partition {0|1}
```

Backing Up and Restoring the Flash File System

You can store the entire content of the flash file system on a Mobility Access Switch to a compressed archive file. You can then copy the archive file to an external server for backup purposes. If necessary, you can restore the backup file from the server to the flash file system.

Backup the Flash File System in the CLI

```
(host) #backup flash
(host) #copy flash: flashbackup.tar.gz tftp: <tftphost> <destfilename>
(host) #copy flash: flashbackup.tar.gz ftp: <ftphost> <username> <destfilename>
(host) #copy flash: flashbackup.tar.gz scp: <scphost> <username> <destfilename>
(host) #copy flash: flashbackup.tar.gz usb: <destfilename>
```

Restore the Flash File System in the WebUI

1. Navigate to the **Maintenance > Copy Files** page.
2. For **Source Selection**, specify the server to which the flashbackup.tar.gz file was previously copied.
3. For **Destination Selection**, select Flash File System.
4. Click **Apply**.

Restore the Flash File System in the CLI

```
(host) #copy tftp: <tftphost> <srcfilename> flash: flashbackup.tar.gz
(host) #copy ftp: <ftphost> <username> <srcfilename> flash: flashbackup.tar.gz
(host) #copy scp: <scphost> <username> <srcfilename> flash: flashbackup.tar.gz
(host) #copy usb: <srcfilename> flash: flashbackup.tar.gz
(host) #restore flash
```

Copying Log Files

You can store log files into a compressed archive file which you can then copy to an external TFTP or SCP server. The WebUI allows you to copy the log files to a WinZip folder which you can display or save on your local PC.

In the WebUI

1. Navigate to the **Maintenance > Copy Logs** page.
2. For **Destination**, specify the TFTP or FTP server to which log files are copied.
3. Select **Download Logs** to download the log files into a WinZip file on your local PC.
4. Click **Apply**.

In the CLI

```
(host) #tar logs
(host) #copy flash: logs.tar tftp: <tftphost> <destfilename>
(host) #copy flash: logs.tar ftp: <ftphost> <username> <destfilename>
(host) #copy flash: logs.tar scp: <scphost> <username> <destfilename>
(host) #copy flash: logs.tar usb: <destfilename>
```

Copying Other Files

The flash file system contains the following configuration files:

- startup-config: Contains the configuration options that are used when the Mobility Access Switch is rebooted. It contains all options saved by clicking the **Save Configuration** button in the WebUI or by entering the **write memory** CLI command. You can copy this file to a different file in the flash file system or to a TFTP server.
- running-config: Contains the current configuration, including changes which have yet to be saved. You can copy this file to a different file in the flash file system, to the startup-config file, or to a TFTP or FTP server.

You can copy a file in the flash file system or a configuration file between the MAS and an external server.

In the WebUI

1. Navigate to the **Maintenance > Copy Files** page.
2. Select the source where the file or image exists.
3. Select the destination to where the file or image is to be copied.
4. Click **Apply**.

In the CLI

```
(host) #copy startup-config flash: <filename>
(host) #copy startup-config tftp: <tftphost> <filename>
(host) #copy startup-config ftp: <ip-address> <username> <filename>
(host) #copy startup-config scp: <ip-address> <username> <filename>
(host) #copy startup-config usb: <filename> [usbpartition <number>]
(host) #copy startup-config member <id> usb: <filename> [usbpartition <number>]

(host) #copy running-config flash: <filename>
(host) #copy running-config ftp: <tftphost> <user> <password> <filename> [<remote-dir>]
(host) #copy running-config startup-config
(host) #copy running-config tftp: <tftphost> <filename>
(host) #copy running-config scp: <ip-address> <username> <filename>
(host) #copy running-config usb: <filename> [usbpartition <number>]
(host) #copy running-config member <id> usb: <filename> [usbpartition <number>]
```

USB Operations

The Mobility Access Switch can read and write files to an attached USB drive which can be used to upgrade software images or configurations files and also backup configurations or stored files on the local flash. Directories on the USB drive can also be created, deleted or viewed in addition to renaming and deleting files.

The Mobility Access Switch supports the following USB operations:

- Read and write files to an attached USB drive which can be used to upgrade software images or configurations files.
- Backup configurations or stored files on the local flash.
- Create, view, and delete directories in addition to renaming and deleting files.

Creating a New USB Directory

You can use the following command to create the directory in USB:

```
(host) #mkdir usb: <usbdirname>
```

You can use the following command to create the directory in member USB:

```
(host) #mkdir member id usb: <usbdirname>
```

You can use the following command to create the directory in multipartition USB:

```
(host) #mkdir usb: <usbdirname> usbpartition <number>
```

You can use the following command to create directory at multipartition member USB:

```
(host) #mkdir member id usb: <usbdirname> usbpartition <number>
```

Deleting an Existing USB Directory

You can use the following command to delete the content of USB:

```
(host) #delete usb: <usbpathname>
```

You can use the following command to delete the content of multipartitioned USB:

```
(host) #delete usb: <usbpathname> usbpartiton <number>
```

You can use the following command to delete the content of member USB:

```
(host) #delete member <id> usb: <usbpathname>
```

You can use the following command to delete the content of delete the content of multipartitioned member:

```
(host) # delete member <id> usb: <usbpathname> usbpartiton <number>
```

Renaming an Existing USB Directory

You can use the following comand to rename the path(file/directory) in USB:

```
(host) #rename usb: <oldpathname> <newpathname>
```

You can use the following command to rename the path(file/directory) in multipartition USB:

```
(host) #rename usb: <oldpathname> <newpathname> usbpartition <number>
```

You can use the following command to rename the path(file/directory) in member USB:

```
(host) #rename member <id> usb: <oldpathname> <newpathname>
```

You can use the following command to rename the path(file/directory) in multipartition in member USB:

```
(host) #rename member <id> usb: <oldpathname> <newpathname> usbpartiiton <number>
```

Uploading a Mobility Access Switch Software Image

You can use the following command to upload an image from USB:

```
(host) # copy usb: <filename> [usbpartition <number>] system: partition [0|1]
```

```
(host) # copy usb: <filename> [usbpartition <number>] member <id> system: partition [0|1]
```

Copying Files to USB:

You can use the following command to copy files from Mobility Access Switch to USB:

```
(host) #copy member: <id> flash: <filename> usb: <usbfilename> [usbpartition <number>]
(host) #copy member: <id> flash: <filename> member: <destid> usb: <usbfilename> [usbpartition
<number>]
(host) #copy flash: <filename> member: <destid> usb: <usbfilename>[usbpartition <number>]
(host) #copy flash: <filename> usb: <usbfilename> [usbpartition <number>]
(host) #copy system: partition 0 usb: snapshot
```

Copying Files to Mobility Access Switch:

You can use the following commands to copy files from USB to Mobility Access Switch:

```
(host) #copy usb: <filename> [usbpartition <number>] flash: <flashfilename>
(host) #copy usb: <filename> [usbpartition <number>] system: partition [0|1]
(host) #copy usb: <filename> [usbpartition <number>] member <destid> flash: <flashfilename>
(host) #copy usb: <filename> [usbpartition <number>] member <destid> system: partition [0|1]
(host) #copy usb: snapshot system: partition [0|1]
(host) #copy member: <id> usb: <filename> [usbpartition <number>] member: <destid> usb:
<usbfilename> [usbpartition <destnumber>]
(host) #copy member: <id> usb: <filename> [usbpartition <number>] member: <destid> flash:
<flashfilename>
```

You can use the following commands to copy files from/to a remote server:

```
(host) #copy usb: <filename> [usbpartition <number>] tftp: <tftphost> <destfilename>
(host) #copy usb: <filename> [usbpartition <number>] ftp: <ftphost> <user> <password>
(host) #copy usb: <filename> [usbpartition <number>] scp: <scphost> <username> <destfilename>
(host) #copy member: <id> usb: <filename> [usbpartition <number>] tftp: <tftphost>
<destfilename>
(host) #copy member: <id> usb: <filename> [usbpartition <number>] ftp: <ftphost> <user>
<password>
(host) #copy member: <id> usb: <filename> [usbpartition <number>] scp: <scphost> <username>
<destfilename>
```

Viewing the USB Directory

To display the USB content of the members:

```
(host) #dir member <id> usb:
```

To display the usb content of local member at one directory level:

```
(host) #dir usb:
```

To display the directory content of USB:

```
(host) #dir usb: <usbpathname>
```

To display the directory content of a member USB:

```
(host) #dir member <id> <usbpathname>
```

To display the directory content of member of a multipartitioned USB:

```
(host) #dir member <id> <usbpathname> usbpartition <number>
```

To display the directory content of local multipartitioned USB:

```
(host) #dir usb <usbpathname> usbpartition <number>
```

PAPI Enhanced Security

Starting from ArubaOS 7.4.1.5, a minor security enhancement is made to Process Application Programming Interface (PAPI) messages. With this enhancement, PAPI endpoints authenticate the sender by performing a

sanity check of the incoming messages using MD5 (hash). **All PAPI endpoints—Mobility Access Switches, APs, Controllers, AirWave, and ALE—must use the same secret key.**

The PAPI Enhanced Security configuration provides protection to Aruba devices and AirWave against malicious users sending fake messages that results in security challenges.

To implement PAPI Enhanced Security, a new CLI command is introduced in ArubaOS 7.4.1.5.

Configuring PAPI Enhanced Security

Execute the following command to enable PAPI Enhanced Security:

```
(host) (config) #papi-security
(host) (PAPI Security Profile) #?
enhanced-security      Enable or disable the use of enhanced security mode
key                    Key used to authenticate messages between systems
no                     Delete Command
```

Example Configuration

The following sample command set enables PAPI enhanced security and configures the specified key to authenticate messages exchanged between systems:

```
(host) (config) #papi-security
(host) (PAPI Security Profile) #enhanced-security
(host) (PAPI Security Profile) #key 1234567890
```

Verifying PAPI Enhanced Security Configuration

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 Enabled
```

This chapter describes management access and tasks. It contains the following topics:

- [Certificate Authentication Concepts on page 55](#)
- [Setting an Administrator Session Timeout on page 53](#)
- [Bypassing the Enable Password Prompt on page 53](#)
- [Resetting the Admin or Enable Password on page 53](#)
- [Managing Ports for WebUI and Captive Portal on page 54](#)
- [Certificate Authentication Concepts on page 55](#)
- [Public Key Authentication for SSH Access on page 55](#)
- [Managing Certificates on page 56](#)

Management Users

User authentication to the management interface (CLI or WebUI) of the Mobility Access Switch is supported using either local management user accounts or external user accounts via RADIUS/TACACS+. The Mobility Access Switch can support up to 10 local management users. The default management user is Admin and the default password is Admin123. This password must be changed before executing the **write memory** command.

To change the default password, execute the following commands:

```
(host) >enable
Password: enable
(host) #configure terminal
(host) (config) #mgmt-user admin root
Password: *****
Re-Type password: *****
```

In addition to the root role, the Mobility Access Switch supports a variety of other role types for management users:

- **guest-provisioning:** Allows the user to create guest accounts on a WebUI page. You can log in to the CLI; however, you cannot use any CLI commands.
- **location-api-mgmt:** Permits access to location API information. You can log in to the CLI; however, you cannot use any CLI commands.
- **network-operations:** Permits access to Monitoring, Reports, and Events pages in the WebUI. You can log in to the CLI; however, you can only use a subset of CLI commands to monitor the Mobility Access Switch.
- **read-only:** Permits access to CLI show commands or WebUI monitoring pages only.
- **root:** Permits access to all management functions on the Mobility Access Switch.

For more information on enabling Radius/Tacacs+ authentication for management users, see [Configuring Authentication Servers on page 290](#).

Management Password Policy

By default, the password for a new management user has no requirements other than a minimum length of six alphanumeric or special characters. However, if your company enforces a password policy for management users with root access to the network equipment, you can configure a password policy that sets requirements for management user passwords.

Defining a Management Password Policy

To define specific management password policy settings through the CLI, complete the following steps:

The table below describes the characters allowed in a management user password. The disallowed characters cannot be used by any management user password, even if the password policy is disabled.

Table 14: Allowed Characters in a Management User Password

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

In the CLI

```
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
```

Setting an Administrator Session Timeout

You can configure the number of seconds after which the WebUI or CLI session times out.

Setting a CLI Session Timeout

To define a timeout interval for a CLI session, use the command:

```
login-session timeout <value>
```

The allowed range for the **timeout** value is 5 to 60 minutes or 1 to 3600 seconds, inclusive. You can also specify a timeout value of 0 to disable CLI session timeouts.

Setting a WebUI Session Timeout

To define a timeout interval for a WebUI session, use the command:

```
web-server session-timeout <session-timeout>
```

The allowed range for the **session-timeout** value is 30 to 3600 seconds, inclusive.

Bypassing the Enable Password Prompt

The bypass enable feature lets you bypass the enable password prompt and log into the privileged commands (config) mode after logging on to the Mobility Access Switch. This is useful if you want to avoid changing the enable password due to company policy.

Use the **enable bypass** CLI command to bypass the enable prompt and log into config mode. Use the **no enable bypass** CLI command to restore the enable password prompt.

Resetting the Admin or Enable Password

This section describes how to reset the password for the default administrator user account (admin) on the Mobility Access Switch. The default password is **admin123**.

Use this procedure if the administrator user account password is lost or forgotten.

1. Connect a local console to the serial port on the Mobility Access Switch.
2. From the console, login to the Mobility Access Switch using the username **password** and the password **forgetme!**.



To recover the forgotten password in an ArubaStack, always use the local console of the primary member. Password recovery does not work on a re-directed console of the primary member or local console of the non-primary members.

3. Enter enable mode by typing in **enable**, followed by the password **enable**
4. Enter configuration mode by typing in **configure terminal**.
5. To configure the administrator user account, enter **mgmt-user admin root**. Enter a new password for this account. Retype the same password to confirm.
6. Exit from the configuration mode, enable mode, and user mode.

This procedure also resets the enable mode password to **enable**. If you have defined a management user password policy, make sure that the new password conforms to this policy.

[Figure 1](#) is a CLI example of how to reset the password.

Figure 1 *Resetting the Password*

```
(host)
User: password
Password: forgetme!
(host) >enable
Password: enable
(host) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(host) (config) #mgmt-user admin root
Password: *****
Re-Type password: *****
(host) (config) #exit
(host) #exit
(host) >exit
```

After you reset the administrator user account and password, you can login to the Mobility Access Switch and reconfigure the enable mode password. To do this, enter configuration mode and type the **enable secret** command. You are prompted to enter a new password and retype it to confirm. Save the configuration by entering **write memory**.

[Figure 2](#) details an example to reconfigure the enable mode password.

Figure 2 *Reconfigure the enable mode password*

```
User: admin
Password: *****
(host) >enable
Password: *****
(host) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(host) (config) #enable secret
Password: *****
Re-Type password: *****
(host) (config) #write memory
```

Managing Ports for WebUI and Captive Portal

Mobility Access Switch provides support for disabling or re-enabling the ports for WebUI and Captive portal. Use the following CLI options under the **web-server** command to enable or disable ports for WebUI and Captive Portal configuration. By default, these ports are enabled.

To enable WebUI port, use the following command:

```
(host) (Web Server Configuration) #mgmt-ui-ports
```

To disable WebUI port, use the following command:

```
(host) (Web Server Configuration) #no mgmt-ui-ports
```

To enable Captive Portal port, use the following command:

```
(host) (Web Server Configuration) #captive-portal-ports
```

To disable Captive Portal port, use the following command:

```
(host) (Web Server Configuration) #no captive-portal-ports
```

Certificate Authentication Concepts

The Mobility Access Switch supports client certificate authentication for users accessing the Mobility Access Switch using the CLI. You can use client certificate authentication with or without a username/password (if certificate authentication fails, the user can log in with a configured username and password). By default, the client certificate authentication is with username and password.



Each Mobility Access Switch supports a maximum of ten management users.

Configuring Certificate Authentication

To use client certificate authentication, you must do the following:

1. Obtain a client certificate and import the certificate into the Mobility Access Switch. For more information on obtaining and importing a client certificate see [Managing Certificates on page 56](#).
2. Configure certificate authentication for WebUI management. You can also optionally select username/password authentication.
3. Configure a user with a management role. Specify the client certificate for user authentication.

In the CLI

```
(host) (config) #web-server
(host) (Web Server Configuration) #mgmt-auth certificate
(host) (Web Server Configuration) #switch-cert <certificate>
(host) (Web Server Configuration) #mgmt-user webui-cacert <ca> serial <number> <username> <role>
```

Public Key Authentication for SSH Access

The Mobility Access Switch supports public key authentication for users accessing the Mobility Access Switch using SSH. When you import an X.509 client certificate into the Mobility Access Switch, the certificate is converted to SSH-RSA keys. When you enable public key authentication for SSH, the Mobility Access Switch validates the client's credentials with the imported public keys. You can specify public key authentication with or without username/password (if the public key authentication fails, the user can login with a configured username and password). By default, the public key authentication is with username and password.

To use public key authentication, follow the steps below:

1. Import the X.509 client certificate into the Mobility Access Switch using the WebUI. For more information on importing client certificates, see [Importing Certificates on page 57](#).
2. Configure SSH for client public key authentication. You can also optionally select username/password authentication.
3. Configure the username, role, and client certificate.



Starting from ArubaOS 7.4.1.5, Mobility Access Switches do not support the Diffie Hellman (DH) Group 1 key exchange algorithm in the Secure Shell (SSH) configuration.

In the CLI

```
(host) (config) #ssh mgmt-auth public-key [username/password]
(host) (config) #mgmt-user ssh-pubkey client-cert <certificate> <username> <role>
```

Managing Certificates

This section contains the following topics:

- [About Digital Certificates](#)
- [Obtaining a Server Certificate](#)
- [Obtaining a Client Certificate](#)
- [Importing Certificates](#)
- [Viewing Certificate Information](#)

The Aruba Mobility Access Switch is designed to provide secure services through the use of digital certificates. Certificates provide security when authenticating users or clients and eliminate the need for less secure password-based authentication.

There is a default server certificate installed in the Mobility Access Switch to demonstrate the authentication of the Mobility Access Switch for WebUI management access. However, this certificate does not guarantee security in production networks. Aruba strongly recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted Certificate Authority (CA). This section describes how to generate a Certificate Signing Request (CSR) to submit to a CA and how to import the signed certificate received from the CA into the Mobility Access Switch.

The Mobility Access Switch supports client authentication using digital certificates for specific user-centric network services, such as AAA FastConnect. Each service can employ different sets of client and server certificates.

During certificate-based authentication, the Mobility Access Switch provides its server certificate to the client for authentication. After validating the server certificate, the client presents its own certificate to the Mobility Access Switch for authentication. You can optionally configure the Mobility Access Switch to verify the user name in the certificate with the configured authentication server after validating the client's certificate.

About Digital Certificates

Clients and the servers to which they connect may hold authentication certificates that validate their identities. When a client connects to a server for the first time, or the first time since its previous certificate has expired or been revoked, the server requests the client to transmit its authentication certificate. The client's certificate is then verified against the CA which issued it. Clients can also request and verify the server's authentication certificate. For some authentication mechanisms such as 802.1x authentication, clients do not need to validate the server certificate.

Digital certificates are issued by a CA which can be a commercial third-party company or a private CA controlled by your organization. The CA is trusted to authenticate the owner of the certificate before issuing a certificate. A CA-signed certificate guarantees the identity of the certificate holder. This is done by comparing the digital signature on a client or server certificate with the signature on the certificate for the CA.

Digital certificates employ public key infrastructure (PKI), which requires a private-public key pair. A digital certificate is associated with a private key, known only to the certificate owner and a public key. A certificate encrypted with a private key is decrypted with its public key. For example, party A encrypts its certificate with its private key and sends it to party B. Party B decrypts the certificate with party A's public key.

Obtaining a Server Certificate

Aruba strongly recommends that you replace the default server certificate in the Mobility Access Switch with a custom certificate issued for your site or domain by a trusted CA. To obtain a security certificate for the Mobility Access Switch from a CA:

1. Generate a Certificate Signing Request (CSR) on the Mobility Access Switch using the CLI.

2. Submit the CSR to a CA. Copy and paste the output of the CSR into an email and send it to the CA of your choice.
3. The CA returns a signed server certificate and the CA's certificate and public key.
4. Install the server certificate, as described in [Importing Certificates on page 57](#)



You can have only one outstanding CSR at a time in the Mobility Access Switch.

Table 15: CSR Parameters

Parameter	Description	Range
key	Length of private/public key.	1024/2048/4096
common_name	Host and domain name, as in www.yourcompany.com.	—
country	Two-letter ISO country code for the country in which your organization is located.	—
state_or_province	State, province, region, or territory in which your organization is located.	—
city	City in which your organization is located.	—
organization	Name of your organization.	—
unit	Optional field to distinguish a department or other unit within your organization.	—
email	Email address referenced in the CSR.	—

In the CLI

1. Run the following command:

```
(host) (config) #crypto pki csr {rsa key_len <key_val> | {ec curve-name <key_val>}} common-name <value> country <country> state_or_province <state> city <city> organization <org> unit <string> email <email>
```

2. View the CSR output using the following command:

```
(host) #show crypto pki csr
```

3. Copy the CSR output between the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines, paste it into an email and send it to the CA of your choice.

Obtaining a Client Certificate

You can use the CSR generated on the Mobility Access Switch to obtain a certificate for a client. However, since there may be a large number of clients in a network, you can obtain the client certificates from a corporate CA server. For example, in a browser window, enter **http://<ipaddr>/crtserv**, where **<ipaddr>** is the IP address of the CA server.

Importing Certificates

Use the WebUI or the CLI to import certificates into the Mobility Access Switch.



You cannot export certificates from the **Mobility Access Switch**.

You can import the following types of certificates into the Mobility Access Switch:

- Server certificate signed by a trusted CA. This includes a public and private key pair.
- CA certificate used to validate other server or client certificates. This includes only the public key for the certificate.
- Client certificate and client's public key. (The public key is used for applications such as SSH which does not support X509 certificates and requires the public key to verify an allowed certificate.)

Certificates can be in the following formats:

- X509 PEM unencrypted
- X509 PEM encrypted with a key
- DER
- PKCS7 encrypted
- PKCS12 encrypted

In the CLI

Use the following command to import CSR certificates:

```
(host) (config) #crypto pki-import {der|pem|pfx|pkcs12|pkcs7}
{PublicCert|ServerCert|TrustedCA} <name>
```

The following example imports a server certificate named **cert_20** in DER format:

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

Viewing Certificate Information

In the WebUI, navigate to the **Configuration > Certificates > Upload** page. Under the **Certificate Lists** section the certificates that are currently installed in the Mobility Access Switch are listed. Click on a certificate to view its contents.

To view the contents of a certificate using the CLI, execute the following commands:

Table 16: *Certificate Show Commands*

Command	Description
<code>show crypto-local pki trustedCA [<name>][<attribute>]</code>	Displays the contents of a trusted CA certificate. If a name is not specified, all CA certificates imported into the Mobility Access Switch are displayed. If name and attribute are specified, then only the attribute in the specified certificate are displayed. Attributes can be CN, validity, serial-number, issuer, subject, or public-key.
<code>show crypto-local pki serverCert [<name>][<attribute>]</code>	Displays the contents of a server certificate. If a name is not specified, all server certificates imported into the Mobility Access Switch are displayed.
<code>show crypto-local pki publiccert [<name>][<attribute>]</code>	Displays the contents of a public certificate. If a name is not specified, all public certificates imported into the Mobility Access Switch are displayed.



All certificates on Primary node get synchronized with Secondary node only. Line Cards do not have these certificates synchronized. However, the certificates get synchronized to the node when increasing the priority of the Line Card to make it primary.

SSL Vulnerability Fix

As part of [CVE-2014-3566](#) security vulnerabilities and exposures, SSLv3 transport layer security is disabled from ArubaOS 7.4.0.1 onwards.



Clients exclusively using SSLv3 will fail to access Captive Portal or Mobility Access Switch WebUI. It is recommended to use TLSv1, TLSv1.1, or TLSv1.2 transport layer security.

To address this, the following changes are introduced under the **web-server ssl-protocol** command.

Table 17: Changes in the **web-server ssl-protocol** command

Parameter	Description	Range	Default
ssl-protocol tlsv1 tlsv1.1 tlsv1.2	Specifies the Transport Layer Security (TLS) protocol version used for securing communication with the Web server. <ul style="list-style-type: none">● tlsv1● tlsv1.1● tlsv1.2	—	tlsv1 tlsv1.1 tlsv1.2

This chapter describes provisioning and managing Mobility Access Switch using Aruba Central.

Overview

Starting from ArubaOS 7.3.2, the Mobility Access Switches can be managed and/or monitored through Aruba Central. When you order a Mobility Access Switch and a Central subscription from Aruba, you will receive a welcome email with instructions on how to activate your Central account. For more information on activating your Central account, see *Aruba Central User Guide*.

Important Points to Remember

- Mobility Access Switch must be able to reach the Internet either using a static IP address and default-gateway or information obtained from DHCP.
- DNS servers must be configured using the **ip name-server** commands or obtained from DHCP.
- A Central License

Managing Mobility Access Switch Using Aruba Central

Mobility Access Switch can be monitored and managed using Aruba Central in a seamless manner.

Enabling Mobility Access Switch for Aruba Central Management

For Managing Mobility Access Switch using Aruba Central, you must enable Aruba Central on the Mobility Access Switch. By default, Aruba Central is enabled on the Mobility Access Switch. Once Aruba Central is enabled on the Mobility Access Switch, the switch keeps polling Activate to obtain the URL of Central portal to connect to it.

You can use the following CLI commands to disable or re-enable Aruba Central on the Mobility Access Switch:

To disable

```
(host) (Aruba Central) #no enable
```

To re-enable

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

Viewing Aruba Central Status

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      central.arubanetworks.com  
Connection Status         Up  
Mode                       Monitor  
Time of last disconnect   Sun Aug 24 13:16:47 2014
```

Provisioning Mobility Access Switch Using Aruba Central Portal

If you have subscribed to Aruba Central:

1. Go to <https://portal.central.arubanetworks.com> and log in with your user credentials.
2. Connect your Mobility Access Switch to the wired network.
3. Navigate to the **Maintenance > Device Management** page of the Central UI. A list of available Mobility Access Switches will be displayed.
4. To manually add the Mobility Access Switch, click **Add Devices** and enter the MAC Address and the cloud activation key.



You can use the **show inventory | include HW** command on the Mobility Access Switch to retrieve the MAC address (lowest on the system) and the **show version** command to view the cloud activation key. The activation key is enabled only if the Mobility Access Switch has Internet access. If you have interrupted the ZTP process using the console or quick-setup, you must apply an IP address (static or DHCP), routing information, and name-servers for the Mobility Access Switch to connect to Activate to enable the activation key. If you have trouble retrieving the activation key, see Aruba Central User Guide.

5. To assign a license, select the switches and click **Assign License(s)**.
6. Complete the Mobility Access Switch configuration through the Aruba Central portal.

Limitation

The current limit for the size of the configuration file is 150 KB. When the Mobility Access Switch is in **managed** mode, the configuration received or sent from Aruba Central is NOT processed and applied properly, if the size of the running configuration file exceeds 150KB.

This chapter describes the following topics:

- [Activate Integration Overview on page 63](#)
- [Activate Provisioning Service on page 63](#)
- [Activate and AirWave on page 64](#)
- [Network Requirements for AirWave Provisioning on page 65](#)
- [Activate Firmware Services on page 65](#)

Activate Integration Overview

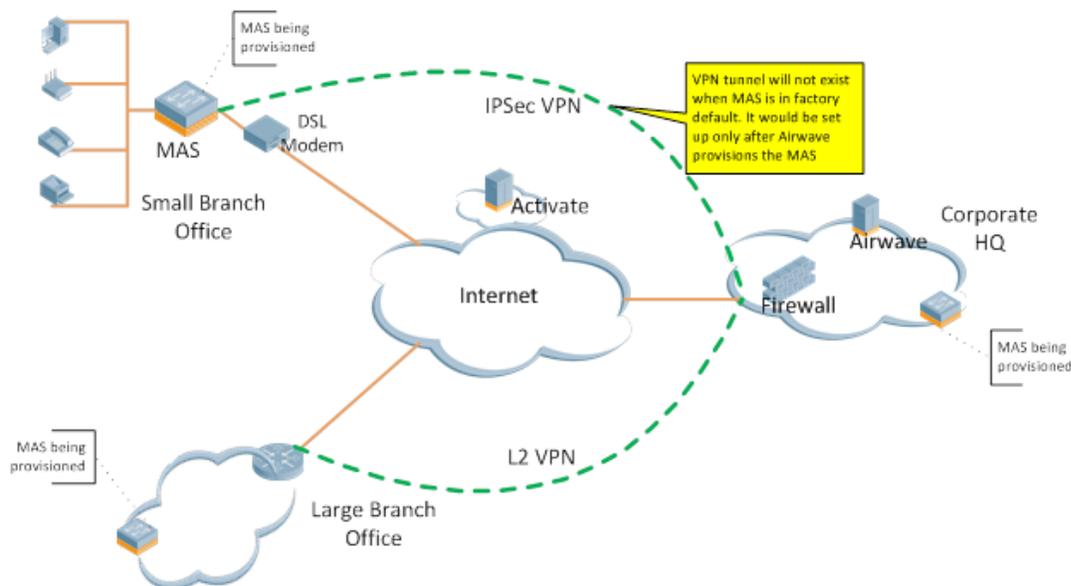
Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise. When your company orders a new Mobility Access Switch from Aruba, that device is automatically added to your inventory in Activate. Once a device is in your inventory, it can be automatically or manually associated to a folder and provisioning rule. A remote technician only needs to connect the Mobility Access Switch to the Internet, and that device will securely connect to Activate, retrieve its provisioning information, then use the provisioning information to connect to the AirWave server that has the desired Mobility Access Switch configuration.

Activate Provisioning Service

Activate customers must configure Activate with a provisioning rule for a Mobility Access Switch that provides each Mobility Access Switch with the IP address of the AirWave Management Platform and the AirWave group containing the switch configuration.

When an Activate-enabled ArubaOS 7.3.0.0 or higher Mobility Access Switch with a factory-default configuration becomes active on the network, it automatically contacts the Activate server, which responds with the AirWave server IP address and shared-secret-key, and the AirWave group and folder that contain its provisioning information.

Figure 3 Activate/AirWave/Switch flow



If your management VLAN does not have Internet access and you want to manually point your Mobility Access Switch to your local AirWave, you can provide your AirWave information via quick setup. Zero-Touch Provisioning (via Activate or DHCP) is disabled if the Mobility Access Switch enters quick-setup mode, even if quick setup is later canceled. If the Mobility Access Switch is manually configured, it will no longer attempt to use the Zero-Touch Provisioning feature.

A configuration manually defined using the quick setup wizard or WebUI takes precedence over the autoconfiguration settings downloaded from an AirWave server. If the Mobility Access Switch is manually configured, it will no longer download configuration updates from Activate.



A best practice is to avoid making any configuration changes directly on a Mobility Access Switch whose configuration is managed through an AirWave. If login credentials or connectivity settings are changed directly on the Mobility Access Switch, AirWave may no longer be able to manage that device. Any required configuration changes should be managed through AirWave.

Activate and AirWave

Activate allows you to create rules to automatically provision devices with information about their configuration master. When a Mobility Access Switch in a factory-default mode sends its MAC address and serial number to Aruba Activate, Activate will respond with the AirWave IP address, shared secret, and the AirWave group and folder defined in the provisioning rule. Activate will only respond to a device when the device is associated with a customer that has enabled Activate and configured a provisioning rule.

When the Mobility Access Switch connects to the AirWave server, the device will either be automatically assigned to the specified group, or it will be available in the AirWave New Devices List (**APs/Devices > New** page).

- **Automatically Assigned Devices:** A factory default device provisioned from Activate will be automatically added to the group in AirWave only if at least one device already exists in the same group with the same shared secret.
- **Adding Devices from the New Devices List:** A factory default device that is not provisioned from Activate with the same shared secret and group will be added to the New Devices List in AirWave. For non-factory devices, AirWave will prompt you for the Community String, Telnet/SSH Username and Password, and the Enable Password. This information allows AirWave to import the configuration immediately when the device is added to the group.

The first device that is added to an AirWave group is added manually through the New Devices List and becomes the "golden" configuration for all subsequent devices that are added to the group. Ensure the stability of this configuration before pushing it to subsequent devices in the group. In addition, when adding this first device to AirWave, you must log in as an Admin user or provide the admin password in the device's Management profile. This is required in order to change the admin password of the factory default switch so that the configuration can be written and pushed to AirWave.

Additional devices can be added in either Monitor Only mode or Manage Read/Write mode. Devices that are added in Monitor Only mode will display with a mismatch in AirWave because the group configuration cannot be pushed in this mode. The group configuration will only be pushed if the Automatically Authorized Switch Mode option in **AMP Setup > General** is set to **Manage Read/Write**.



The first device that is added and whose configuration is imported will display with a "Good" configuration state regardless of the Automatically Authorized Switch setting.

After a Mobility Access Switch appears as an associated device on the AirWave server, future configuration changes on the device must be made through AirWave. A caution message will display in the Mobility Access Switch WebUI if you attempt to make configuration changes directly on a switch that was provisioned with

Activate and AirWave and that is managed by AirWave. In some cases, if settings are changed through the Mobility Access Switch WebUI, AirWave may no longer be able to manage that device.

Network Requirements for AirWave Provisioning

The Mobility Access Switch cannot use Activate/AirWave provisioning unless it has L3 access to the Activate server through the Internet. This connectivity must be available even when the Mobility Access Switch boots up with factory default settings, so the network into which the Mobility Access Switch is installed has the following requirements:

- Connectivity to the Internet is available over an untagged interface.
- DHCP-based address assignment.
- DNS entries via DHCP to resolve activate.arubanetworks.com.

AirWave uses SNMP polling to verify that the Mobility Access Switch is active on the network.

Activate Firmware Services

By default, the Mobility Access Switch contacts the Activate server upon initial bootup and then periodically every seven days to see if there is a new image version to which that switch can upgrade. If a new version is available, Activate prompts you to download and upgrade to the new image. The download process is not triggered automatically and requires admin intervention.

This feature is enabled by default. To disable the activate firmware services, issue the command **activate-service-firmware no enable**.

The ArubaStack feature enables simplified management by presenting a set of Mobility Access Switches as one entity, and reduces the operational complexity of managing multiple redundant links between access and distribution layer switches. Since the ArubaStack appears as one network node, loop prevention protocols are not required.

An ArubaStack is a set of interconnected Mobility Access Switches using stacking ports to form an ArubaStack. A stacking port is a physical port configured to run the stacking protocol. In factory default settings for Mobility Access Switches, uplink ports 2 and 3 (24/48 port models) and port 1 (12 port model) are pre-provisioned to be ArubaStack link ports. Once a port is provisioned for stacking, it is no longer available to be managed as a network port. A stacking port can only be connected to other Mobility Access Switches running the Aruba Stacking Protocol (ASP).

You can also configure the base ports as ArubaStack ports for specific topologies. You can use the following command to configure the base ports as ArubaStack:

```
(host) (config)# add stacking interface stack <module/port>
```

To delete a stacking port, execute the following command locally under executive mode:

```
(host) #delete stacking interface stack <module/port>
```

To delete a stacking port from the primary, execute the following command under executive mode:

```
(host) #delete stacking interface stack <module/port> member <id>
```

Use module=0 for base ports. For more information on adding a stacking interface, see ArubaOS 7.4.x *Command Line Interface Guide*.

This chapter contains the following sections:

- [Important Points to Remember on page 67](#)
- [Stacking Topology on page 68](#)
- [Dynamic Election on page 73](#)
- [ArubaStack Pre-Provisioning on page 75](#)
- [ArubaStack Database on page 76](#)
- [ArubaStack Resiliency on page 78](#)
- [Management User Authentication on page 83](#)
- [ArubaStack Member Replacement on page 84](#)
- [Stack Member Renumbering on page 95](#)
- [Factory Reset on Detached ArubaStack Member on page 95](#)

Important Points to Remember

- Dynamic Election—An ArubaStack is formed and roles are assigned based on Auto Discovery.
- ArubaStack Pre-provisioning—ArubaStack members and roles are configured before the ArubaStack is formed.



Dynamic-election and Pre-provisioning cannot be configured together. You must choose one or the other for each ArubaStack.

- S2500s and S3500s can form an ArubaStack with other S2500s and S3500s.
- S1500s can form an ArubaStack with other S1500s,

- The ArubaStack members are Primary, Secondary and Line Card. A valid ArubaStack contains at least a Primary and a Secondary member.
 - Member—a collective term that includes Primary, Secondary, and Line Cards. All valid members run Aruba Stack Protocol (ASP) to discover each other.
 - Primary—runs all Layer2/Layer 3 functions and controls the ArubaStack. All configurations are performed on the Primary and then “pushed” to other members of the ArubaStack.
 - Secondary—back up for the Primary in the event of a hardware or software failure.
 - Line Card—a member of the ArubaStack that is neither a Primary or Secondary. The Line Card includes all interfaces required to *switch* traffic.
- The connection between the Mobility Access Switches cannot go over a Layer 2/Layer 3 cloud.
- One or more stacking ports might be connected between two Mobility Access Switches. The interconnection between the switches can form common topologies; chain, ring, hub-and-spoke etc.
- A port provisioned for stacking can not be managed as a network port.

Stacking Topology

ArubaOS provides support for the following use cases:

- ArubaStack connected in a ring topology
- ArubaStack using base port links
 - Creating an ArubaStack with 10/100/1000 base ports
 - Creating an ArubaStack with S3500-24F base ports
 - Creating an ArubaStack across multiple wiring closets
- ArubaStack distributed wiring closet with redundancy
 - Creating an ArubaStack across two wiring closets with two layer redundancy

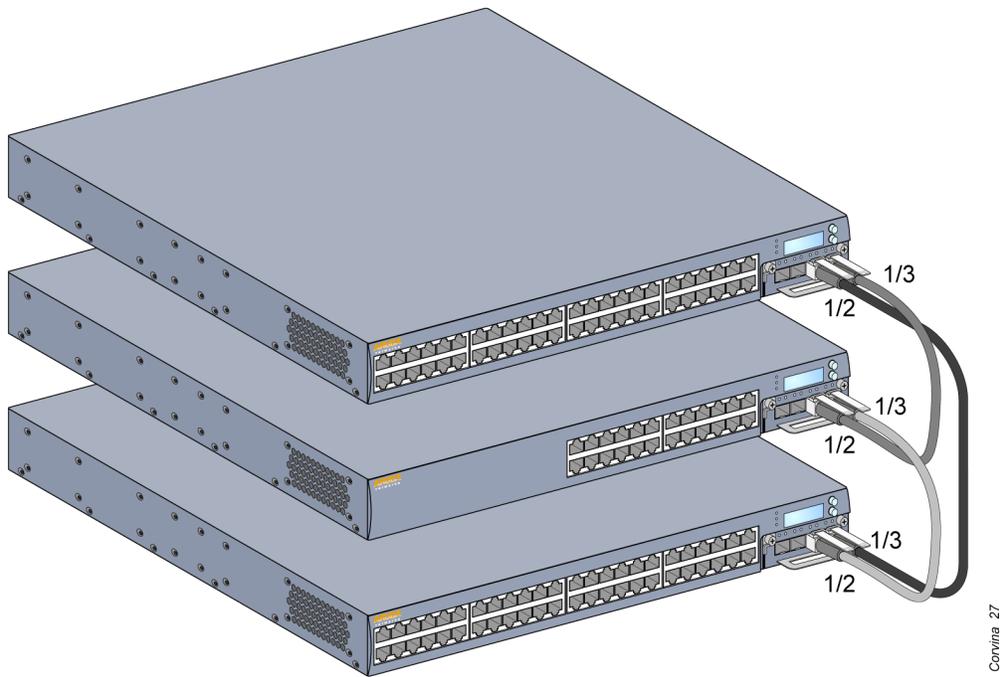


All the use cases are supported only with the exact interconnections as illustrated in the figures 1 to 5 provided in this document..

ArubaStack connected in a Ring Topology

[Figure 4](#) displays an ArubaStack connected in a ring topology. After the election process (see [Primary Election on page 74](#)), member 0 is the Primary, member 1 is the Secondary, and member 2 is a Line Card.

Figure 4 ArubaStack Ring Topology



ArubaStack using Base Port Links

The following use-cases are supported under ArubaStack using base port links:

- Creating an ArubaStack with 10/100/1000 base ports
- Creating an ArubaStack with S3500-24F base ports
- Creating an ArubaStack across multiple wiring closets

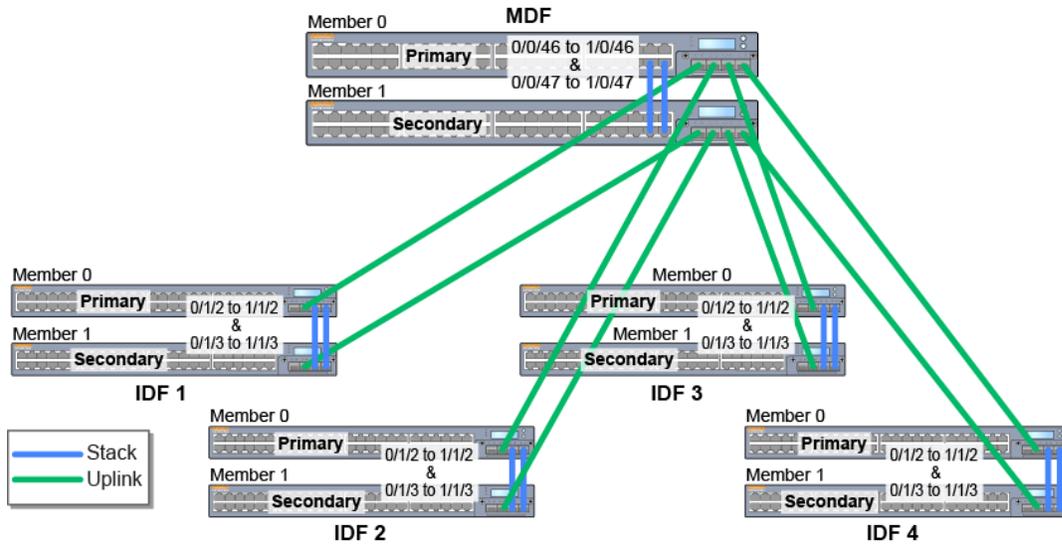


All the ArubaStack using base port links support reduced ArubaStack bandwidth in MDF.

Creating ArubaStack with 10/100/1000 Base Ports

[Figure 5](#) illustrates how to create an ArubaStack with 10/100/1000 base ports. This is useful when all the uplink ports are used for interconnecting with devices in the other locations.

Figure 5 ArubaStack with 10/100/1000 Base Ports



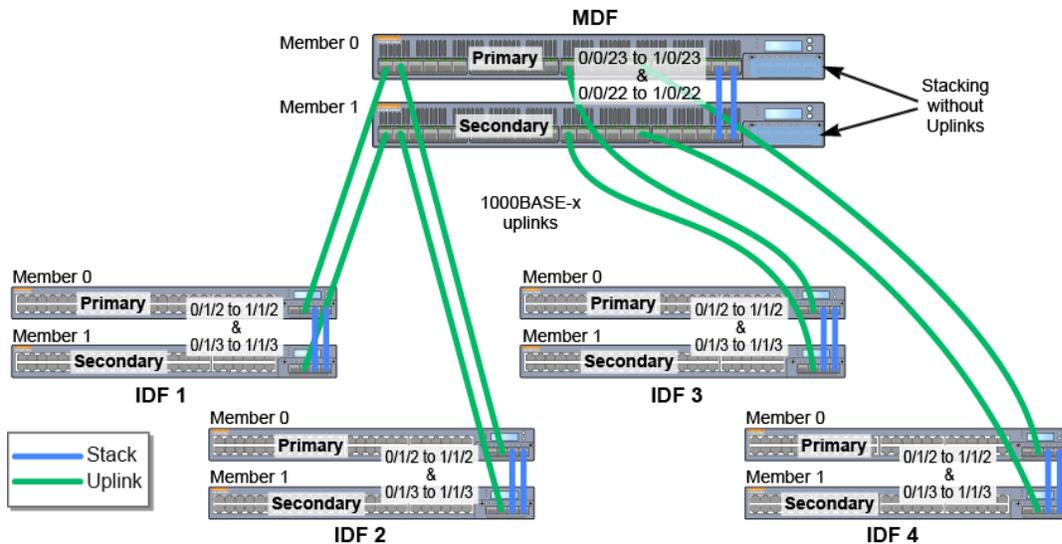
The characteristics of this topology are described below:

- Full redundancy is provided between every ArubaStack.
- Provides 1000BASE-T PoE on every ArubaStack.
- 1000Base-X (fiber) uplinks to MDF connect to the uplink ports.
- MDF stack is completed by 1000BASE-T base port links.
- x/0/x ports are stacked only with other x/0/x ports at MDF.

Creating ArubaStack with S3500-24F Base Ports

Figure 6 illustrates how to create an ArubaStack with S3500-24F base ports. This physical configuration is used to create a redundant S3500-24F aggregation layer without an uplink module.

Figure 6 ArubaStack with S3500-24F Base Ports



The characteristics of this topology are described below:

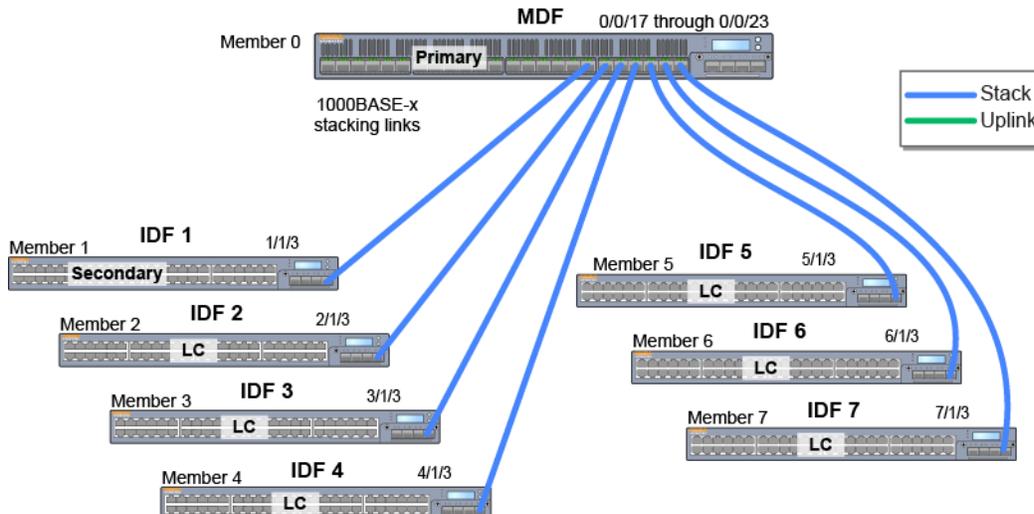
- Full redundancy is provided between every ArubaStack.
- No uplink module is required at MDF.
- 1000Base-X (fiber) uplinks to MDF connect to 1000Base-X base ports.

- MDF stack is completed by 1000BASE-X base port links.
- x/0/x ports are stacked only with other x/0/x ports at MDF.

Creating ArubaStack across Multiple Wiring Closets

[Figure 7](#) illustrates how to create an ArubaStack across multiple wiring closets. This is an alternative star topology used for multiple remote wiring closets instead of the traditional ring topology.

Figure 7 ArubaStack across Multiple Wiring Closets



The characteristics of this topology are described below:

- MDF and IDFs are integrated as one ArubaStack for simplified management.
- 1000Base-X Fiber extends ArubaStack to a longer distance.
- No uplink module is required at MDF.
- 1000Base-X (fiber) uplinks to MDF connect to 1000Base-X base ports.
- A maximum of seven ArubaStack ports are allowed at MDF (S3500-24F shown).



This topology does not provide ArubaStack redundancy for stack members.

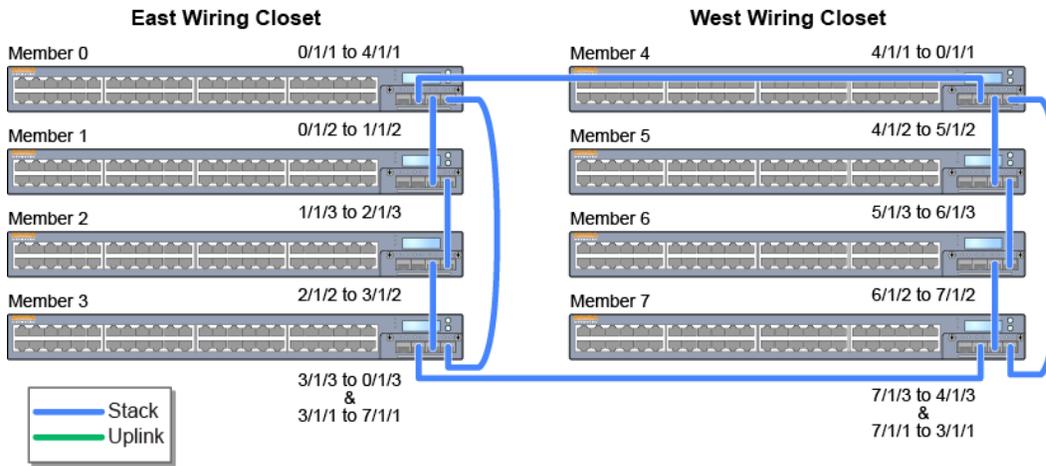
ArubaStack Distributed Wiring Closet with Redundancy

You can create an ArubaStack across two wiring closets with two layer redundancy. This use case provides redundancy through the traditional ring topology between the members within the wiring closet. It also provides a redundant ring between the members across the distributed wiring closets.

Creating ArubaStack across Two Wiring Closets with Two Layer Redundancy

[Figure 8](#) illustrates how to create an ArubaStack across two wiring closets with two layer redundancy.

Figure 8 ArubaStack across Two Wiring Closets with Two Layer Redundancy



The characteristics of this topology are described below:

- Primary member is in one closet and the secondary is in the other.
- DAC is provided between the members within the closet and 10GE is provided between the closets.
- Full redundancy is provided in each wiring closet
- Full redundancy is provided between closets
- Provides simplified management.
- Redundant uplink interfaces are available to core.

Viewing the ArubaStack Information

There are several commands available that allow you to view ArubaStack information such as topology, members, routes, interface and neighbors to name a few.

```
(host)#show stacking ?
asp-stats          Show asp stats on stacking interfaces
generated-preset-profile  Generate preset stack config from dynamic config
interface          Show configured stacking interfaces
internal           Show stacking internal details
location          Show stacking location
members           Show stacking members
neighbors          Show directly connected stacking neighbors
topology          Show stacking topology
```

For example, to view the ArubaStack topology, use the **show stacking topology** command.

```
(host)#show stacking topology
```

Member-id	Role	Mac Address	Interface	Neighbor	Member-id
0	*	Primary	000b.866a.f240	stack1/2	1
			stack1/3	stack1/3	2
1		Secondary	000b.866b.0340	stack1/3	0
			stack1/2	stack1/2	2
2		Linecard	000b.866b.3980	stack1/2	0
			stack1/3	stack1/3	1

Another example, to view the ArubaStack topology, use the **show stacking members** command.

```
(host) (config) #show stacking members

Member status: Active, Stack Id: 000b866af2404e339e0a
Stack uptime: 13 days 6 hours 3 minutes 52 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	*	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

[S] - Split
[V] - Version Mismatch
[D] - Depleted Slots
[C] - Preset Configuration Mismatch
[I] - Preset Independent Stack



The member with the asterisk (*) indicates that you are logged onto that member (the Primary in the example above).

Dormant State

An ArubaStack member will enter the dormant state if it cannot contact a valid primary member. A member can become dormant for one of the following reasons:

- Split [S]—This member cannot connect to the primary member after an ArubaStack split.
- Version Mismatch [V]—This member's version of ArubaOS does not match that of the primary member.
- Depleted Slots [D]—The number of ArubaStack members has exceeded the maximum.
- Preset Configuration Mismatch [C]—This member's pre-provisioned configuration does not match the configuration of the primary member.
- Preset Independent Stack [I]—This member is part of a pre-provisioned ArubaStack that has not completely merged with another pre-provisioned ArubaStack.

Dynamic Election

Dynamic election is a stack-formation process that is completed automatically with only optional configuration (setting the priority value) done before the Mobility Access Switches are physically connected. The stacking protocol sends information between the ArubaStack members and the election process is completed to determine the primary and secondary members. The primary then assigns member-IDs and roles to the remaining members.

Configuring Priority

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 (see [Primary Election on page 74](#)). In the example below, the priority value (election-priority) is set to the default 128 assuring that the switch enters the ArubaStack as a Line Card.



In the example, the switch entering the ArubaStack has a previous member identification (member-id 2).

Using the WebUI

1. Navigate to the **Configuration > Stacking** page.
2. Click the **Add** button to add a MAS to the ArubaStack.
3. Enter the **Member ID**.
4. Enter the **Election Priority**.
5. Click **OK**.

6. Repeat this process until you have added all the necessary MAS's.
7. Set the **MAC persistence timeout** value.
8. Enable or disable **Split Detection** as required for your deployment.
9. Click **Apply** and **Save Configuration**.

Using the CLI

```
(host) (stack-profile) #member-id 1 election-priority 128
WARNING!! This profile will not be applied till the configuration is saved.
```

```
(host) (stack-profile) #member-id 1 location eng-building
WARNING!! This profile will not be applied till the configuration is saved.
```

```
(host) (stack-profile) #write memory
Saving Configuration.....
```

Configuration Saved.



The command `member-id <member ID> location` is only available through CLI.

The Stacking Protocol

Each Mobility Access Switch runs an ArubaStack manager process that is responsible for running the stacking protocol. The stacking protocol is responsible for automatically:

- Identifying the ArubaStack neighbors and determining the ArubaStack topology.
- Assigning the switch's member ID to each member of the ArubaStack.
- Assigning each member of the ArubaStack a role; Primary, Secondary or Line Card.
- Setting up optimized communication path/channel between the ArubaStack members. This path/channel transports user data packets and the switch's own control packets.
- Converges the stacking topology during a ArubaStack link or ArubaStack member failure event; users and traffic are automatically re-routed via a different path.

Auto Discovery

The Stacking protocol exchanges information between Mobility Access Switches that are connected to each other and without any prior stacking related configuration. The protocol exchanges information between the different ArubaStack members, runs distributed election algorithm, and elects a Primary and Secondary members among the ArubaStack members. The Primary then assigns ArubaStack member IDs to all the members.

Primary Election

The ArubaStack manager discovers the ArubaStack topology. A Primary is elected based on the following in the order of priority.

1. Configured Priority (0-255). Priority is configured by administrator. Higher the priority, better the chances are for the MAS to become Primary. Default priority is 128.
2. Current Role (Primary, Secondary, LC). Weight associated with current role will be in descending order from Primary to LC. If the switch boots up in Dormant state it does not participates in election.
3. Uptime. Uptime for the switch in 100s of seconds.
4. Hardware Priority (0-31). Priority of becoming Primary if all of the above are same. This priority will be hardcoded based on the switch's hardware.
5. MAC Address of the switch. In Primary election, lower MAC wins.

Election Anatomy

The synchronization of the link state database also triggers a primary election task on all the ArubaStack members. This algorithm chooses one primary and one secondary amongst all the ArubaStack members based on the priority list in [The Stacking Protocol on page 74](#).

The system's MAC address of the ArubaStack members is the final tiebreaker. The ArubaStack member selected as a Primary asks for an explicit acknowledgment from the remaining ArubaStack members. Upon success, it assigns a ArubaStack unit ID and ArubaStack role for the remaining ArubaStack members and then conveys this information to each ArubaStack member. The ArubaStack unit ID and the chassis-role assigned by the Primary is persistent on a stacking database on all the ArubaStack members. Reboots, therefore, do not result in changes in ArubaStack unit IDs or roles.

Only a Mobility Access Switch that has an un-assigned ArubaStack ID or the same ArubaStack ID as the Primary is allowed to participate fully in the ArubaStack election. In addition, the ArubaStack members must be running the same software version. A Mobility Access Switch with a different software version is admitted into the ArubaStack for the purpose of administration but cannot participate in forwarding network traffic.

Interfaces for such a Mobility Access Switch is not created in the Primary. In the case of incompatible software versions, you can manually upgrade the ArubaStack members, or if configured, the Primary can automatically upgrade the ArubaStack members.

ArubaStack Pre-Provisioning

The ArubaStack pre-provisioning feature allows you to configure the role and member-id of the members before the ArubaStack is created. In preset config the members are configured using their serial numbers, which can be found on the purchase order or can be located on the back of the Mobility Access Switch. Additionally, the CLI commands `show inventory` or `show stacking-profile` displays the serial number.

Configuring ArubaStack Pre-Provisioning

All configuration for ArubaStack pre-provisioning is completed on a single Mobility Access Switch. Configuration consists of setting all parameters of all eventual members of the ArubaStack. This can be configured using the WebUI or the CLI. These parameters are:

- Serial number: The switch's serial number is used to identify the unit for ArubaStack formation. This is located on the purchase order, the rear of the unit, or the commands `show inventory` or `show stacking members` or `show stacking generated-preset-profile`.
- ArubaStack-unit number: The member-ID (or slot number) assigned to the switch.
- Chassis-role: The role assigned to the switch when configuring the ArubaStack. The roles are primary-capable or line card. Primary-capable switches can become a primary, secondary, or line card.



At least two Mobility Access Switches in the ArubaStack must be assigned as primary-capable.

After the configuration has been saved, all Mobility Access Switches are physically connected. The ArubaStack then forms a chassis as specified in the configuration.

After the preset ArubaStack configuration is applied to the connected switches, primary-capable members choose one primary and one secondary by running the Primary-Election algorithm. The switches configured as line-card capable will become line cards and receive the configured slot number defined in the preset config after the primary election algorithm.

Using the WebUI

1. Navigate to the **Configuration > Stacking** page.

2. Click the **Enable pre-provisioning** check box.
3. Click the **Add** button to add a MAS to the ArubaStack.
4. Enter the **Member ID**.
5. Enter the **Serial Number**.
6. Select the device **Role** from the drop-down menu.
7. Click **OK**.
8. Repeat this process until you have added all the necessary MAS's.
9. Set the **MAC persistence timeout** value.
10. Enable or disable **Split Detection** as required for your deployment.
11. Click **Apply** and **Save Configuration**.

Using the CLI

```
(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
(host) (stack-profile) #member-id 1 location eng-building
```



The command `member-id <member ID> location` is only available through CLI.

ArubaStack Database

Information related to the ArubaStack is kept in persistent storage so that the ArubaStack's Primary election procedure converges faster after subsequent reboots. This ArubaStack information includes:

- ArubaStack ID
- MAC address, role and member ID of all the members

When the switch boots using the ArubaStack database, it assumes the last role it had according to the ArubaStack database.

To accommodate any change in the ArubaStack topology since the last boot, the Mobility Access Switch uses a count down timer and then it verifies as follows:

- If I was the Primary and...
 - I see the Secondary which means that both the previous Primary and previous Secondary are present in the ArubaStack. I continue as Primary.
 - I do not see the Secondary, however, I can see more than half of the ArubaStack members in the database. I continue as Primary.
 - I do not see the Secondary and I can only see less than half of the ArubaStack members in the database. I transition into dormant state. The network interfaces of the switch will remain down.
- If I was the Secondary and...
 - I see the Primary which means that both the previous Primary and previous Secondary are present in the ArubaStack. I continue as Secondary.
 - I do not see the Primary, however, I can see more than half of the ArubaStack members in the database. I change to Primary.
 - I do not see the Primary and I can only see less than half of the ArubaStack members in the database. I transition into dormant state. The network interfaces of the switch will remain down.
- If I was a Line Card and...

- I do not see Primary nor Secondary. I move to dormant state.
- I do see both Primary and Secondary, The Primary will assign me my appropriate role and member-id.
- I see either the Primary or the Secondary. I will wait for instructions from the member I see (Primary or Secondary).

Removing an ArubaStack Database

An ArubaStack database can be removed at each individual ArubaStack member to return the device to factory default settings. Use the command below to remove an ArubaStack database. Once removed, the device will be automatically reboot.

```
(host) #restore factory-default stacking
```

```
All configuration and stack settings will be restored to
factory default on this member after reload.
Press 'y' to proceed with reload: [y/n]: y
System will now restart
.....
```

Booting without an ArubaStack Database

When Mobility Access Switches boot without the ArubaStack database, various timers are launched to assure that ArubaStack ports are brought up and RTMs (Routing Topology Messages) are exchanged with other members before deciding on its role. These timers are used to avoid unnecessary transition in roles and changes in member-id. Because of these timers, the switch's boot up time is longer than with the ArubaStack database.

Primary Switchover

Best practices recommend executing the **database synchronize** command before attempting a system switchover. To view the switchover status, use the **show system switchover** command and 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. When this command is executed, the following changes take place:

- The Secondary becomes the new Primary
- The old Primary becomes the new Secondary

The example below confirms that database synchronization to the secondary is current.

```
(host) #show system switchover
```

```
Secondary Switchover status
-----
System-state   : synchronized to primary
Configuration  : synchronized to primary
Database       : synchronized to primary
```

Important Note

- ArubaStack does not support synchronization of network control protocols among the members of the stack.
- A member of the stack in Secondary mode or Linecard mode does not run full network control protocols.

- Primary-to-Secondary switchover may lead to traffic disruption as the new Primary has to resynchronize L2/L3 protocol states with the neighboring devices.

ArubaStack Resiliency

When a member(s) of an ArubaStack exits the ArubaStack unexpectedly (due to hardware or software error for example) or members are removed from one ArubaStack to create another ArubaStack, it is known as a “stack split.” Keep-alive packets are exchanged among all the ArubaStack ports at regular intervals. When a member(s) of the ArubaStack exits the ArubaStack thereby isolating the remaining ArubaStack member(s), each ArubaStack member independently calculates the resultant state of the stack split.

Some rules governing the stack split are:

- After a stack split, members may transition to a dormant line card state regardless of their previous role.
- After a stack split, several members may form an inactive sub-stack of dormant line card switches.
- After a stack split if the Primary and Secondary members are within the same sub-stack, then that sub-stack is active and passing traffic.
- After a stack split if the Primary is in a different sub-stack than the Secondary, the active sub-stack is determined by the sub-stack with the most members.
- After a stack split if the Primary is in a different sub-stack than the Secondary *and* both sub-stacks contain the same number of members, the sub-stack with the Secondary becomes the active sub-stack. The Secondary rightly assumes that the Primary is completely offline.



An ArubaStack (or sub-stack) can never have two Primaries. The ArubaStack is designed to transition to an inactive state to avoid a collision of two Primaries.

Split Detect

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. The command to disable split detections is shown below; note that you must save your configuration.

```
(host)(stack-profile) #no split-detection
WARNING!! This profile will not be applied till the configuration is saved.
```

```
(host)(stack-profile) #write memory
Saving Configuration.....
```

The **no split-detection** command is applied to a 2 member ArubaStack only. If you apply this command to an ArubaStack with more than 2 members, save the command, then execute the **show stack member** command, a warning notice is displayed.

```
(host)(stack-profile) #show stacking members
```

```
Member status: Active, Stack Id: 000b866af2404e339e0a
Id   Role      MAC Address      Priority  State   Model          Serial
--   ---      -
0   *   Primary    000b.866a.f240  255     Active  ArubaS3500-24P  AU0000674
1     Secondary 000b.866b.0340  200     Active  ArubaS3500-24P  AU0000731
2     Linecard  000b.866b.3980  128     Active  ArubaS3500-24P  AU0000660
```

Note: no-split-detect configured but not in effect



Split detect is not supported on pre-provisioned ArubaStacks.

Stack Join

Stack join occurs when a stack split creates two sub-stacks; an active sub-stack (includes the Primary and Secondary) and an inactive sub-stack with dormant Line Card members. The stack join pulls these two sub-stacks back together again as one active ArubaStack. The stack join is just resolving the broken connection between switches. There is no software command to issue. Once the connection is made, the stacking protocol will auto discover the ArubaStack topology. Original roles of the switches are maintained because all the switches in the ArubaStack know the identity of the ArubaStack Primary and Secondary and share the same ArubaStack ID.

Additionally, a stack join occurs when two or more Mobility Access Switches with factory default settings are connected via a stack port and then booted up. Those devices will join and the stack protocol will auto discover the stack topology. Each member's role is determined using the primary election algorithm ([Primary Election on page 74](#)).

Stack Merge—Dynamic Election

Stack merge takes place when two independently running ArubaStacks (with unique ArubaStack IDs) are connected to each other. Rules to determine which ArubaStack wins the merge are:

- A pre-provisioned ArubaStack wins over a dynamic-election ArubaStack
- An active ArubaStack wins over an inactive ArubaStack
- The ArubaStack with a higher stack priority (priority of the primary) wins
- The ArubaStack with more members wins over an ArubaStack with fewer members
- The ArubaStack with the lower ArubaStack uptime will merge into a higher uptime ArubaStack
- The tie breaker is the Stack ID; the ArubaStack with the lower Stack ID wins

The losing ArubaStack members perform an automatic software reset to clear any previous software states and then those members join their place in the “winning” ArubaStack.

The following describes a merge scenario in which two Mobility Access Switches with less than 100 seconds of uptime are combined and the device with the lowest MAC becomes the primary. In this scenario, Device-A is the 48-port S3500 and Device-B is the 24-port S3500.

- On Device-A:

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 000b866a5ac04f7a3a6c
```

```
Stack uptime: 1 minutes 3 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	*	000b.866a.5ac0	128	Active	ArubaS3500-48P	AW0000155

- On Device-B:

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 000b866a75004f7a3a41
```

```
Stack uptime: 1 minutes 51 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	*	000b.866a.7500	128	Active	ArubaS3500-24T	AU0000229

- On Device-A, now acting as the primary for the ArubaStack:

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 000b866a5ac04f7a3a6c
```

```
Stack uptime: 22 minutes 20 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial	
0	*	Primary	000b.866a.5ac0	128	Active	ArubaS3500-48P	AW0000155
1		Secondary	000b.866a.7500	128	Active	ArubaS3500-24T	AU0000229

Stack Merge—Pre-Provisioning

Unlike ArubaStacks created by dynamic election, there is no automatic stack merge for deployments that include pre-provisioned ArubaStacks. If two ArubaStacks must be merged, the process of merging the members must be completed manually.

Pre-provisioned and Dynamic ArubaStacks Merge

In case of merge of one pre-provisioned ArubaStack and one dynamic-election ArubaStack, the pre-provisioned ArubaStack takes precedent. The two ArubaStacks will merge to form a single ArubaStack but the members from dynamic ArubaStack will become dormant if their config is not present in preset config. These members will remain dormant unless the pre-provisioned ArubaStack is modified to include members from dynamic ArubaStack. Complete the merge by taking the following steps.

1. The pre-provisioned ArubaStack will discover the new members and the members of the dynamic-election ArubaStack will become dormant.

After merge:

Member status: Active, Stack Id: 000b866b4a804f3f01c6
Stack uptime: 17 minutes 3 seconds

Id	Role	MAC Address	Priority	State	Model	Serial	
0	*	Primary	000b.866b.4a80	Preset	Active	ArubaS3500-48P	AW0000257
1		Secondary	000b.866c.2640	Preset	Active	ArubaS3500-48P	AW0000625
?		Linecard	000b.866a.6280	255	Dormant [C]	ArubaS3500-24T	AU0000183
?		Linecard	001a.1e08.7d80	255	Dormant [C]	ArubaS2500-48P	BL0000028

2. Add the former members of the dynamic-election ArubaStack to the stack-profile of the pre-provisioned ArubaStack.

After stack-profile update:

Member status: Active, Stack Id: 000b866b4a804f3f01c6
Stack uptime: 23 minutes 22 seconds

Id	Role	MAC Address	Priority	State	Model	Serial	
0	*	Primary	000b.866b.4a80	Preset	Active	ArubaS3500-48P	AW0000257
1		Secondary	000b.866c.2640	Preset	Active	ArubaS3500-48P	AW0000625
2		Linecard	000b.866a.6280	Preset	Active	ArubaS3500-24T	AU0000183
3		Linecard	001a.1e08.7d80	Preset	Active	ArubaS2500-48P	BL0000028

Pre-provisioned ArubaStacks Merge

If two pre-provisioned ArubaStacks are physically connected via a stack port, they will not merge automatically.



Aruba recommends that you remove the stack-profile configuration or execute `restore factory-default stacking` on each member of the joining ArubaStack before physical connection.

The following is an example of how to remove the pre-provisioned settings from a ArubaStack that will be merged with another pre-provisioned ArubaStack:

```
(Stack-B) #show stacking members
```

Member status: Active, Stack Id: 000b866a76c04f877710
Stack uptime: 1 minutes 56 seconds

Id	Role	MAC Address	Priority	State	Model	Serial
----	------	-------------	----------	-------	-------	--------

```

--      ----      -----      -----      -----      -----      -----
1      Linecard  000b.866b.e300  Preset   Active   ArubaS3500-24P  AU0001357
4 *    Primary   000b.866c.0ac0  Preset   Active   ArubaS3500-24P  AU0001517
7      Secondary 000b.866a.76c0  Preset   Active   ArubaS3500-24T  AU0000228

(Stack-B) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Stack-B) (config) #stack-profile
(Stack-B) (stack-profile) #no member-id 1 serial-number AU0001357 role line-card
WARNING!! This profile will not be applied till the configuration is saved.

(Stack-B) (stack-profile) #no member-id 4 serial-number AU0001517 role primary-capable
WARNING!! This profile will not be applied till the configuration is saved.

(Stack-B) (stack-profile) #no member-id 7 serial-number AU0000228 role primary-capable
WARNING!! This profile will not be applied till the configuration is saved.

(Stack-B) (stack-profile) #end
(Stack-B) #
(Stack-B) #write memory
Saving Configuration.....

(Stack-B) #show stacking members

```

```

Member status: Active, Stack Id: 000b866a76c04f877710
Stack uptime: 16 minutes 3 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   ----      -
1    Linecard  000b.866b.e300  128     Active  ArubaS3500-24P AU0001357
4 *  Primary   000b.866c.0ac0  128     Active  ArubaS3500-24P AU0001517
7    Secondary 000b.866a.76c0  128     Active  ArubaS3500-24T AU0000228

```

In the case that two pre-provisioned ArubaStacks are physically connected before the stack-profile is removed from one of them, no merge will occur automatically. The following steps describe how to complete the merge without removing the physical connection:

Before Merge (primary ArubaStack, Stack-A):

```

(Stack-A) #show stacking members

Member status: Active, Stack Id: 000b866a75004f846b14
Stack uptime: 15 hours 25 minutes 2 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   ----      -
4    Linecard  001a.1e08.8140  Preset   Active  ArubaS2500-24P BJ0000025
5    Secondary 000b.866a.7500  Preset   Active  ArubaS3500-24T AU0000229
7 *  Primary   000b.866a.5ac0  Preset   Active  ArubaS3500-48P AW0000155

```

Before Merge (joining ArubaStack, Stack-B):

```

(Stack-B) #show stacking members

Member status: Active, Stack Id: 000b866a76c04f875627
Stack uptime: 22 minutes 51 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   ----      -
1    Linecard  000b.866b.e300  Preset   Active  ArubaS3500-24P AU0001357
4    Secondary 000b.866c.0ac0  Preset   Active  ArubaS3500-24P AU0001517
7 *  Primary   000b.866a.76c0  Preset   Active  ArubaS3500-24T AU0000228

```

1. The two ArubaStacks are physically connected using the stacking interfaces.



In this case, both ArubaStacks remain still independent, denoted by [I] but can see the members of the other ArubaStack.

After Physical Connection (primary ArubaStack, Stack-A):

```
(Stack-A) #show stacking members
```

```
Member status: Active, Stack Id: 000b866a75004f846b14
Stack uptime: 15 hours 27 minutes 31 seconds
Id   Role      MAC Address      Priority  State      Model          Serial
--   -
4    Linecard  001a.1e08.8140  Preset   Active     ArubaS2500-24P BJ0000025
5    Secondary 000b.866a.7500  Preset   Active     ArubaS3500-24T AU0000229
7    * Primary   000b.866a.5ac0  Preset   Active     ArubaS3500-48P AW0000155
?    Linecard  000b.866c.0ac0  Preset   Dormant [I] ArubaS3500-24P AU0001517
?    Linecard  000b.866a.76c0  Preset   Dormant [I] ArubaS3500-24T AU0000228
?    Linecard  000b.866b.e300  Preset   Dormant [I] ArubaS3500-24P AU0001357
```

After Physical Connection (joining ArubaStack, Stack-B):

```
(Stack-B) #show stacking members
```

```
Member status: Active, Stack Id: 000b866a76c04f875627
Stack uptime: 26 minutes 59 seconds
Id   Role      MAC Address      Priority  State      Model          Serial
--   -
1    Linecard  000b.866b.e300  Preset   Active     ArubaS3500-24P AU0001357
4    Secondary 000b.866c.0ac0  Preset   Active     ArubaS3500-24P AU0001517
7    * Primary   000b.866a.76c0  Preset   Active     ArubaS3500-24T AU0000228
?    Linecard  001a.1e08.8140  Preset   Dormant [I] ArubaS2500-24P BJ0000025
?    Primary   000b.866a.5ac0  Preset   Dormant [I] ArubaS3500-48P AW0000155
?    Linecard  000b.866a.7500  Preset   Dormant [I] ArubaS3500-24T AU0000229
```

2. Remove the configured stack-profile from the joining ArubaStack (Stack-B).

```
(Stack-B) #configure terminal
```

```
Enter Configuration commands, one per line. End with CNTL/Z
```

```
(Stack-B) (config) #stack-profile
```

```
(Stack-B) (stack-profile) #no member-id 1 serial-number AU0001357 role line-card
WARNING!! This profile will not be applied till the configuration is saved.
```

```
(Stack-B) (stack-profile) #no member-id 4 serial-number AU0001517 role primary-capable
WARNING!! This profile will not be applied till the configuration is saved.
```

```
(Stack-B) (stack-profile) #no member-id 7 serial-number AU0000228 role primary-capable
WARNING!! This profile will not be applied till the configuration is saved.
```

```
(Stack-B) (stack-profile) #end
```

```
(Stack-B) #write memory
```

3. The members of the joining ArubaStack now merge with the primary ArubaStack.

```
(Stack-A) #show stacking members
```

```
Member status: Active, Stack Id: 000b866a75004f846b14
Stack uptime: 15 hours 44 minutes 33 seconds
Id   Role      MAC Address      Priority  State      Model          Serial
--   -
0    Linecard  000b.866a.76c0  Preset   Active     ArubaS3500-24T AU0000228
1    Linecard  000b.866b.e300  Preset   Active     ArubaS3500-24P AU0001357
2    Linecard  000b.866c.0ac0  Preset   Active     ArubaS3500-24P AU0001517
```

4	Linecard	001a.1e08.8140	Preset	Active	ArubaS2500-24P	BJ0000025
5	Secondary	000b.866a.7500	Preset	Active	ArubaS3500-24T	AU0000229
7	* Primary	000b.866a.5ac0	Preset	Active	ArubaS3500-48P	AW0000155

Console Redirect

Logging onto the ArubaStack using a console connection, from any member, redirects the session to the Primary. You can use a control sequence to redirect between the Primary command line and the ArubaStack's local member's (secondary or line card) command line.



If there is a disconnect between the Primary and its members, for example during an ArubaStack split or primary down, the console automatically redirects to a member command line until the new primary is elected.

Use the following control sequence to redirect console session:

- **Esc Ctrl-I** — redirects the console session from the Primary to a Secondary or Line Card member's command line.
- **Esc Ctrl-r** — redirects the Primary console session from a Secondary or Line Card member's session. This key sequence also enables the console redirect.

To verify the status of the console connection, execute the **show console status** command. In the example below, the ArubaStack has a Primary and a Secondary members only.

Management User Authentication

In an ArubaStack, management users are authenticated by a Primary member. The local user authentication credentials synchronize to all the members so that if the Primary becomes unreachable from other members, the authentication is performed locally. Apart from local admin users, you can configure an external authentication server.

From the Primary member console connection:

```
User:admin
Password: *****

(Primary) >enable
Password:*****

(Primary) #show console status

Redirect State: Idle
Member Id: 0
```

From a Non-primary member console connection:

```
User:admin
Password: *****

(Primary) >enable
Password:*****

(Primary) #show console status

Redirect State: Active
Member Id: 1
```

Enter **Esc Ctrl-I** to move to the local console. You will be required to login again.

```
*** CONNECTING TO LOCAL SLOT ***
```

```
(LC-1) #
User:admin
Password: *****

(LC-1) >enable
Password:*****

(LC-1) #show console status

Redirect State: Disabled
Member Id: 1
```

ArubaStack Member Replacement

The ArubaStack features allows the user to replace one or more members of a ArubaStack without bringing down the complete ArubaStack. Following are best practices, based on dynamic and preset ArubaStack configurations.



When replacing a unit with another unit that is not factory default, it is recommended to restore the unit to factory default as shown below.

```
(Aruba) (config) #restore factory_default stacking
```

```
All configuration and stack settings will be restored to
factory default on this member after reload.
Press 'y' to proceed with reload: [y/n]: y
System will now restart
```

Dynamic ArubaStack Configuration

The following section describes how to replace a member of a dynamic ArubaStack.

Replacing a Linecard Member

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 3 minutes 55 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	* Primary	001a.1e08.7b00	128	Active	ArubaS2500-48T	BK0000016
1	Linecard	001a.1e08.7b80	128	Active	ArubaS2500-48T	BK0000018
2	Secondary	001a.1e08.7c00	128	Active	ArubaS2500-48T	BK0000015
3	Linecard	001a.1e08.7c80	128	Active	ArubaS2500-48T	BK0000014

In the above ArubaStack of four members, if Linecard member 1 is down and to be replaced, complete the following steps:

1. Verify stacking members. Member 1 is down and the status will be displayed as Away and the role will be Unknown.

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 11 minutes 16 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	* Primary	001a.1e08.7b00	128	Active	ArubaS2500-48T	BK0000016
1	Unknown	001a.1e08.7b80	128	Away	ArubaS2500-48T	BK0000018
2	Secondary	001a.1e08.7c00	128	Active	ArubaS2500-48T	BK0000015

```
3 Linecard 001a.1e08.7c80 128 Active ArubaS2500-48T BK0000014
```

- To replace member 1, clear the stacking database from the ArubaStack using the clear command as shown below.

```
(host) #clear stacking member-id 1
```

```
Member-id: 0
```

```
-----
```

```
Deleting Member-id: 1
```

```
Member-id: 2
```

```
-----
```

```
Deleting Member-id: 1
```

```
Member-id: 3
```

```
-----
```

```
Deleting Member-id: 1
```

- Stacking database will be cleared and member 1 will not be visible in the show stacking command as shown below.

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
```

```
Stack uptime: 18 minutes 29 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	* Primary	001a.1e08.7b00	128	Active	ArubaS2500-48T	BK0000016
2	Secondary	001a.1e08.7c00	128	Active	ArubaS2500-48T	BK0000015
3	Linecard	001a.1e08.7c80	128	Active	ArubaS2500-48T	BK0000014

- Physically replace member with a new unit. The new unit will transition from an invalid unit Id shown by (?) and eventually be assigned the lowest stack-id available in the existing ArubaStack. In this case the new unit will be assigned unit ID 1.

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
```

```
Stack uptime: 29 minutes 15 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	* Primary	001a.1e08.7b00	128	Active	ArubaS2500-48T	BK0000016
2	Secondary	001a.1e08.7c00	128	Active	ArubaS2500-48T	BK0000015
3	Linecard	001a.1e08.7c80	128	Active	ArubaS2500-48T	BK0000014
?	Linecard	001a.1e08.7ac0	128	Active	ArubaS2500-48T	BK0000019

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
```

```
Stack uptime: 29 minutes 17 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	* Primary	001a.1e08.7b00	128	Active	ArubaS2500-48T	BK0000016
1	Linecard	001a.1e08.7ac0	128	Active	ArubaS2500-48T	BK0000019
2	Secondary	001a.1e08.7c00	128	Active	ArubaS2500-48T	BK0000015
3	Linecard	001a.1e08.7c80	128	Active	ArubaS2500-48T	BK0000014

Replacing a Secondary Member



The new member joining the ArubaStack will assume the role of Secondary only if the priority is configured to be higher than the Linecard members. If the priority is the same for all the members an existing member of the ArubaStack will be elected as the secondary and the new member joining the ArubaStack will be a Linecard.

In this scenario, member-ID 1 is configured for a higher priority.

```
(host) #show stack-profile
```

```
stack-profile "default"
-----
Parameter          Value
-----
MAC persistence timeout 15 Minutes
Split Detection      Enabled
Election Priority:
  Member 0           250
  Member 1           250
```

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 42 minutes 40 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   -
0 *  Primary   001a.1e08.7b00  250     Active  ArubaS2500-48T BK0000016
1   Secondary 001a.1e08.7ac0  250     Active  ArubaS2500-48T BK0000019
2   Linecard  001a.1e08.7c00  128     Active  ArubaS2500-48T BK0000015
3   Linecard  001a.1e08.7c80  128     Active  ArubaS2500-48T BK0000014
```

In the above ArubaStack of four members, if the Secondary member 1 is down and needs to be replaced, here are the steps:

1. Verify stacking members. Secondary member 1 is down and the status will be displayed as Away and the role will be Unknown. An existing member will be elected as the secondary unless the secondary role is configured for a higher priority.

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 43 minutes 50 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   -
0 *  Primary   001a.1e08.7b00  250     Active  ArubaS2500-48T BK0000016
1   Unknown   001a.1e08.7ac0  250     Away    ArubaS2500-48T BK0000019
2   Secondary 001a.1e08.7c00  128     Active  ArubaS2500-48T BK0000015
3   Linecard  001a.1e08.7c80  128     Active  ArubaS2500-48T BK0000014
```

2. To replace member 1, clear the stacking database from the ArubaStack using the clear command as shown below.

```
(host) #clear stacking member-id 1
```

```
Member-id: 0
-----
Deleting Member-id: 1

Member-id: 2
-----
Deleting Member-id: 1

Member-id: 3
-----
Deleting Member-id: 1
```

3. Stacking database will be cleared and member 1 will not be visible in the show stacking command as shown below.

```
(host) #show stacking members
```

```

Member status: Active, Stack Id: 001ale087b004fcee152
Stack uptime: 44 minutes 46 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   ---      -
0   *   Primary    001a.1e08.7b00  250     Active  ArubaS2500-48T BK0000016
2   Secondary 001a.1e08.7c00  128     Active  ArubaS2500-48T BK0000015
3   Linecard  001a.1e08.7c80  128     Active  ArubaS2500-48T BK0000014

```

4. Physically replace member with a new unit. The new unit will transition from an invalid unit Id shown by (?) and eventually be assigned the lowest stack-id available in the existing ArubaStack. In this case the new unit will be assigned unit ID 1 and since member 1 is configured with higher priority it will be elected as secondary.

```
(host) #show stacking members
```

```

Member status: Active, Stack Id: 001ale087b004fcee152
Stack uptime: 47 minutes 6 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   ---      -
0   *   Primary    001a.1e08.7b00  250     Active  ArubaS2500-48T BK0000016
2   Secondary 001a.1e08.7c00  128     Active  ArubaS2500-48T BK0000015
3   Linecard  001a.1e08.7c80  128     Active  ArubaS2500-48T BK0000014
?   Unknown   001a.1e08.7a80  128     Away    ArubaS2500-48T BK0000017

```

```
(host) #show stacking members
```

```

Member status: Active, Stack Id: 001ale087b004fcee152
Stack uptime: 48 minutes 53 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   ---      -
0   *   Primary    001a.1e08.7b00  250     Active  ArubaS2500-48T BK0000016
1   Secondary 001a.1e08.7a80  250     Active  ArubaS2500-48T BK0000017
2   Linecard  001a.1e08.7c00  128     Active  ArubaS2500-48T BK0000015
3   Linecard  001a.1e08.7c80  128     Active  ArubaS2500-48T BK0000014

```

Replacing a Primary Member

The new member joining the ArubaStack will assume the role of Primary only if the priority is configured to be higher than the Secondary member. If the priority of the primary and secondary are same, the existing Secondary member of the ArubaStack will be elected as the Primary and the new member joining the ArubaStack will be elected as Secondary.

If the priority is the same for all the members an existing secondary will take over the role of Primary member, and an existing Linecard member will assume the role of Secondary. The new member joining the ArubaStack will be a Linecard. In this scenario member-id 0 and 1 are configured for a higher priority

```
(host) #show stack-profile
```

```

stack-profile "default"
-----
Parameter          Value
-----
MAC persistence timeout 15 Minutes
Split Detection      Enabled
Election Priority:
  Member 0           255
  Member 1           250

```

```
(host) #show stacking members
```

```

Member status: Active, Stack Id: 001ale087b004fcee152
Stack uptime: 1 hours 10 minutes 12 seconds
Id   Role      MAC Address      Priority  State   Model          Serial

```

```

--      ----      -----      -----      -----      -----      -----
0 * Primary  001a.1e08.7b00  255      Active   ArubaS2500-48T  BK0000016
1 Secondary  001a.1e08.7a80  250      Active   ArubaS2500-48T  BK0000017
2 Linecard  001a.1e08.7c00  128      Active   ArubaS2500-48T  BK0000015
3 Linecard  001a.1e08.7c80  128      Active   ArubaS2500-48T  BK0000014

```

In the above stack of four members, if the Primary member 0 is down and needs to be replaced, here are the steps:

1. Verify stacking members. Primary member 0 is down and the status will be displayed as Away and the role will be Unknown. An existing Secondary member will be elected as the Primary and an existing Linecard member will be elected as Secondary.

```
(host) # show stacking members
```

```

Member status: Active, Stack Id: 001a1e087b004fcee152
Id   Role      MAC Address      Priority  State   Model          Serial
--   ----      -
0    Unknown   001a.1e08.7b00  255     Away    ArubaS2500-48T  BK0000016
1    Primary   001a.1e08.7a80  250     Active  ArubaS2500-48T  BK0000017
2 *  Secondary  001a.1e08.7c00  128     Active  ArubaS2500-48T  BK0000015
3    Linecard  001a.1e08.7c80  128     Active  ArubaS2500-48T  BK0000014

```

2. To replace member 0, clear the stacking database from the ArubaStack using the clear command as shown below.

```
(host) #clear stacking member-id 0
```

```

Member-id: 1
-----
Deleting Member-id: 0

Member-id: 2
-----
Deleting Member-id: 0

Member-id: 3
-----
Deleting Member-id: 0

```

3. Stacking database will be cleared and member 0 will not be visible in the show stacking command as shown below.

```
(host) #show stacking members
```

```

Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 1 hours 17 minutes 13 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   ----      -
1 *  Primary   001a.1e08.7a80  250     Active  ArubaS2500-48T  BK0000017
2    Secondary  001a.1e08.7c00  128     Active  ArubaS2500-48T  BK0000015
3    Linecard  001a.1e08.7c80  128     Active  ArubaS2500-48T  BK0000014

```

4. Physically replace member with a new unit. The new unit will transition from an invalid unit Id shown by (?) and eventually be assigned the lowest stack-id available in the existing ArubaStack. In this case the new unit will be assigned unit ID 0 and since member 0 is configured with highest priority it will be elected as Primary.

```
(host) # show stacking members
```

```

Member status: Active, Stack Id: 001a1e087b004fcee152
Id   Role      MAC Address      Priority  State   Model          Serial
--   ----      -
1    Primary   001a.1e08.7a80  250     Active  ArubaS2500-48T  BK0000017
2 *  Secondary  001a.1e08.7c00  128     Active  ArubaS2500-48T  BK0000015
3    Linecard  001a.1e08.7c80  128     Active  ArubaS2500-48T  BK0000014

```

```
?      Unknown      001a.1e08.7b00 255      Away      ArubaS2500-48T  BK0000016
```

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001ale087b004fcee152
```

```
Stack uptime: 47 minutes 6 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	* Primary	001a.1e08.7b00	255	Active	ArubaS2500-48T	BK0000016
1	Secondary	001a.1e08.7a80	250	Active	ArubaS2500-48T	BK0000017
2	Linecard	001a.1e08.7c00	128	Active	ArubaS2500-48T	BK0000015
3	Linecard	001a.1e08.7c80	128	Active	ArubaS2500-48T	BK0000014



To avoid another switchover happened when the new unit becomes the primary, you may want to modify ArubaStack profile to keep member-1 as primary and new unit as secondary.

```
(host) #show stack-profile
```

```
stack-profile "default"
```

Parameter	Value
MAC persistence timeout	15 Minutes
Split Detection	Enabled
Election Priority:	
Member 0	250
Member 1	255

Preset ArubaStack Configuration

The following section describes how to replace a member of a preset ArubaStack.

In a preset ArubaStack configuration, the units are assigned role and slot number using the stack-profile configuration. Here is a ArubaStack of four members configured as below

```
(host) #show stack-profile
```

```
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	BK0000017	Primary-capable
2	BK0000015	Line-card
3	BK0000014	Line-card

Replacing a Linecard Member

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001ale087b004fcee152
```

```
Stack uptime: 2 hours 19 minutes 26 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	* Primary	001a.1e08.7bc0	Preset	Active	ArubaS2500-48T	BK0000020
1	Secondary	001a.1e08.7a80	Preset	Active	ArubaS2500-48T	BK0000017
2	Linecard	001a.1e08.7c00	Preset	Active	ArubaS2500-48T	BK0000015

In the above ArubaStack of four members, if Linecard member 2 is down and to be replaced, here are the steps:

1. Verify stacking members. Member 2 is down and the status will be displayed as Away and the role will be Unknown.

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 2 hours 33 minutes 56 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   -
0   *   Primary   001a.1e08.7bc0  Preset   Active   ArubaS2500-48T  BK0000020
1   Secondary 001a.1e08.7a80  Preset   Active   ArubaS2500-48T  BK0000017
2   Unknown   001a.1e08.7c00  Preset   Away     ArubaS2500-48T  BK0000015
3   Linecard  001a.1e08.7c80  Preset   Active   ArubaS2500-48T  BK0000014
```

2. To replace member 2, clear the stacking database from the ArubaStack using the clear command as shown below.

```
(host) #clear stacking member-id 2
```

```
Member-id: 0
```

```
-----
```

```
Deleting Member-id: 2
```

```
Member-id: 1
```

```
-----
```

```
Deleting Member-id: 2
```

```
Member-id: 3
```

```
-----
```

```
Deleting Member-id: 3
```

3. Stacking database will be cleared and member 2 will not be visible in the show stacking command as shown below.

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 2 hours 36 minutes 10 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   -
0   *   Primary   001a.1e08.7bc0  Preset   Active   ArubaS2500-48T  BK0000020
1   Secondary 001a.1e08.7a80  Preset   Active   ArubaS2500-48T  BK0000017
3   Linecard  001a.1e08.7c80  Preset   Active   ArubaS2500-48T  BK0000014
```

4. Delete the serial number of member 2.

```
(host) (stack-profile) #no member-id 2 serial-number BK0000018 role line-card
```

5. Physically replace member with a new unit. The unit will not be an active part of the ArubaStack until the serial number is added to the stack-profile and will be displayed as Dormant

```
(host) (stack-profile) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 4 hours 24 minutes 50 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   -
0   *   Primary   001a.1e08.7bc0  Preset   Active   ArubaS2500-48T  BK0000020
1   Secondary 001a.1e08.7a80  Preset   Active   ArubaS2500-48T  BK0000017
2   Linecard  001a.1e08.7b80  128      Dormant [C] ArubaS2500-48T  BK0000018
3   Linecard  001a.1e08.7c80  Preset   Active   ArubaS2500-48T  BK0000014
```

```
[S] - Split
[V] - Version Mismatch
[D] - Depleted Slots
[C] - Preset Configuration Mismatch
[I] - Preset Independent Stack
```

6. Add the serial number of the new unit to the ArubaStack using the following command and save the configuration.

```
(host) (stack-profile) #member-id 2 serial-number BK0000018 role line-card
WARNING!! This profile will not be applied till the configuration is saved.
```

```
(host) (stack-profile) #write memory
Saving Configuration.....
```

```
Configuration Saved.
```

```
(host) #
```

7. The new unit will now be part of the ArubaStack

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 3 hours 14 minutes 49 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   -
0   * Primary   001a.1e08.7bc0   Preset   Active  ArubaS2500-48T BK0000020
1   Secondary 001a.1e08.7a80   Preset   Active  ArubaS2500-48T BK0000017
2   Linecard  001a.1e08.7b80   Preset   Active  ArubaS2500-48T BK0000018
3   Linecard  001a.1e08.7c80   Preset   Active  ArubaS2500-48T BK0000014
```

Replacing a Secondary Member

In a stack-preset configuration at least two members in a ArubaStack must be configured as primary capable.

- An existing Linecard member will be elected as the Secondary if there is a unit that has a role as primary-capable
- If all other units are configured as Linecard, no Secondary member will be elected.
- If the Secondary unit needs to be replaced, the best practices are listed below.

```
(host) #show stack-profile
```

```
stack-profile "default"
-----
Parameter          Value
-----
MAC persistence timeout 14 Minutes
Split Detection     Enabled
```

```
Preset-profile:
```

```
-----
Member-id   Serial-number  Role
0           BK0000020     Primary-capable
1           BK0000017     Primary-capable
2           BK0000018     Line-card
3           BK0000014     Line-card
```

In the above ArubaStack of four members, if the Secondary member 1 is down and needs to be replaced, here are the steps:

1. Verify stacking members. Secondary member 1 is down and the status will be displayed as Away and the role will be Unknown.

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001ale087b004fcee152
```

```
Stack uptime: 4 hours 17 minutes 39 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	* Primary	001a.1e08.7bc0	Preset	Active	ArubaS2500-48T	BK0000020
1	Unknown	001a.1e08.7a80	Preset	Away	ArubaS2500-48T	BK0000017
2	Linecard	001a.1e08.7b80	Preset	Active	ArubaS2500-48T	BK0000018
3	Linecard	001a.1e08.7c80	Preset	Active	ArubaS2500-48T	BK0000014

- To replace member 1, clear the stacking database from the ArubaStack using the clear command as shown below.

```
(host) #clear stacking member-id 1
```

```
Member-id: 0
```

```
-----
```

```
Deleting Member-id: 1
```

```
Member-id: 2
```

```
-----
```

```
Deleting Member-id: 1
```

```
Member-id: 3
```

```
-----
```

```
Deleting Member-id: 1
```

- Stacking database will be cleared and member 1 will not be visible in the show stacking command as shown below.

```
((host) #show stacking members
```

```
Member status: Active, Stack Id: 001ale087b004fcee152
```

```
Stack uptime: 4 hours 20 minutes 18 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	* Primary	001a.1e08.7bc0	Preset	Active	ArubaS2500-48T	BK0000020
2	Linecard	001a.1e08.7b80	Preset	Active	ArubaS2500-48T	BK0000018
3	Linecard	001a.1e08.7c80	Preset	Active	ArubaS2500-48T	BK0000014

- Delete the serial number of member 1 from the stack-profile.

```
(host) (stack-profile) #no member-id 1 serial-number BK0000017 role line-card
```

- Physically replace member with a new unit.

- The unit will not be an active part of the ArubaStack until the serial number is added to the stack-profile and will be displayed as Dormant.

```
(host) (stack-profile) #show stacking members
```

```
Member status: Active, Stack Id: 001ale087b004fcee152
```

```
Stack uptime: 4 hours 34 minutes 57 seconds
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	* Primary	001a.1e08.7bc0	Preset	Active	ArubaS2500-48T	BK0000020
1	Linecard	001a.1e08.7b00	128	Dormant [C]	ArubaS2500-48T	BK0000016
2	Linecard	001a.1e08.7b80	Preset	Active	ArubaS2500-48T	BK0000018
3	Linecard	001a.1e08.7c80	Preset	Active	ArubaS2500-48T	BK0000014

```
[S] - Split
```

```
[V] - Version Mismatch
```

```
[D] - Depleted Slots
```

```
[C] - Preset Configuration Mismatch
```

```
[I] - Preset Independent Stack
```

7. Add the serial number of the new unit to the ArubaStack using the following command and save the configuration

```
(host) (config) #stack-profile member-id 1 serial-number BK0000016 role primary-capable
WARNING!! This profile will not be applied till the configuration is saved.
```

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

Configuration Saved.

8. The new unit will now be part of the ArubaStack

```
(host) (config) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 4 hours 47 minutes 18 seconds
Id   Role      MAC Address      Priority  State   Model          Serial
--   ---      -
0   *   Primary    001a.1e08.7bc0  Preset   Active  ArubaS2500-48T  BK0000020
1     Secondary 001a.1e08.7b00  Preset   Active  ArubaS2500-48T  BK0000016
2     Linecard  001a.1e08.7b80  Preset   Active  ArubaS2500-48T  BK0000018
3     Linecard  001a.1e08.7c80  Preset   Active  ArubaS2500-48T  BK0000014
```

Replacing a Primary Member

In a stack-preset configuration at least two members in a ArubaStack must be configured as primary capable.

- The Secondary member will be elected as a Primary.
- An existing Linecard member will be elected as the Secondary if there is a unit that has a role as primary-capable
- If all other units are configured as Linecard, no Secondary member will be elected.
- If the Primary unit needs to be replaced, the best practices are listed below.

In this scenario member-id 0 and 1 are configured as primary capable

```
(host) #show stack-profile
```

```
stack-profile "default"
-----
Parameter          Value
-----
MAC persistence timeout 14 Minutes
Split Detection      Enabled
```

```
Preset-profile:
```

```
-----
Member-id      Serial-number  Role
0              BK0000020     Primary-capable
1              BK0000016     Primary-capable
2              BK0000018     Line-card
3              BK0000014     Line-card
```

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Id   Role      MAC Address      Priority  State   Model          Serial
--   ---      -
0     Primary    001a.1e08.7bc0  Preset   Active  ArubaS2500-48T  BK0000020
1     Secondary 001a.1e08.7a80  Preset   Active  ArubaS2500-48T  BK0000017
3   *   Linecard  001a.1e08.7c80  Preset   Active  ArubaS2500-48T  BK0000014
4     Linecard  001a.1e08.7b80  Preset   Active  ArubaS2500-48T  BK0000018
```

In the above ArubaStack of four members, if the Primary member 0 is down and needs to be replaced, here are the steps:

1. Verify stacking members. Primary member 0 is down and the status will be displayed as Away and the role will be Unknown. An existing Secondary member will be elected as the Primary.

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 4 hours 52 minutes 32 seconds
Id   Role      MAC Address      Priority  State      Model          Serial
--   ---      -
0    Unknown   001a.1e08.7bc0   Preset   Away       ArubaS2500-48T BK0000020
1    * Primary   001a.1e08.7b00   Preset   Active     ArubaS2500-48T BK0000016
2    Linecard  001a.1e08.7b80   Preset   Active     ArubaS2500-48T BK0000018
3    Linecard  001a.1e08.7c80   Preset   Active     ArubaS2500-48T BK0000014
```

2. To replace member 0, clear the stacking database from the ArubaStack using the clear command as shown below.

```
(host) #clear stacking member-id 0
```

```
Member-id: 1
-----
Deleting Member-id: 0

Member-id: 2
-----
Deleting Member-id: 0

Member-id: 3
-----
Deleting Member-id: 0
```

3. Stacking database will be cleared and member 0 will not be visible in the show stacking command as shown below.

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 5 hours 12 minutes 55 seconds
Id   Role      MAC Address      Priority  State      Model          Serial
--   ---      -
1    * Primary   001a.1e08.7b00   Preset   Active     ArubaS2500-48T BK0000016
2    Linecard  001a.1e08.7b80   Preset   Active     ArubaS2500-48T BK0000018
3    Linecard  001a.1e08.7c80   Preset   Active     ArubaS2500-48T BK0000014
```

4. Delete the serial number of member 0 from the stack-profile.

```
(host) (stack-profile) #no member-id 0 serial-number BK0000020 role line-card
```

5. Physically replace member with a new unit.

6. The unit will not be an active part of the ArubaStack until the serial number is added to the stack-profile and will be displayed as Dormant

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152
Stack uptime: 5 hours 24 minutes 32 seconds
Id   Role      MAC Address      Priority  State      Model          Serial
--   ---      -
0    Linecard  001a.1e08.7ac0   128     Dormant [C] ArubaS2500-48T BK0000019
1    * Primary   001a.1e08.7b00   Preset   Active     ArubaS2500-48T BK0000016
2    Linecard  001a.1e08.7b80   Preset   Active     ArubaS2500-48T BK0000018
3    Linecard  001a.1e08.7c80   Preset   Active     ArubaS2500-48T BK0000014
```

```
[S] - Split
```

[V] - Version Mismatch
[D] - Depleted Slots
[C] - Preset Configuration Mismatch
[I] - Preset Independent Stack

7. Add the serial number of the new unit to the ArubaStack using the following command and save the configuration.

```
(host) (config) #stack-profile member-id 0 serial-number BK0000019 role primary-capable  
WARNING!! This profile will not be applied till the configuration is saved.
```

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

Configuration Saved.

8. The new unit will now be part of the ArubaStack and be elected as Secondary

```
(host) #show stacking members
```

```
Member status: Active, Stack Id: 001a1e087b004fcee152  
Stack uptime: 5 hours 29 minutes 51 seconds  
Id    Role      MAC Address      Priority  State   Model          Serial  
--    -
```

Id	Role	MAC Address	Priority	State	Model	Serial
0	Secondary	001a.1e08.7ac0	Preset	Active	ArubaS2500-48T	BK0000019
1	* Primary	001a.1e08.7b00	Preset	Active	ArubaS2500-48T	BK0000016
2	Linecard	001a.1e08.7b80	Preset	Active	ArubaS2500-48T	BK0000018
3	Linecard	001a.1e08.7c80	Preset	Active	ArubaS2500-48T	BK0000014

Stack Member Renumbering

Starting from ArubaOS 7.4.1.1, the **set stacking renumber** command in the Mobility Access Switch allows you to renumber any stack member in the ArubaStack except the primary and secondary stack members.

In the CLI

To renumber a stack member (except the primary or the secondary stack member), execute the following command:

```
(host) #set stacking renumber 1 4
```

The Mobility Access Switch displays the following error message if you try to renumber the primary and secondary stack members:

ERROR: Renumber involving Primary or Backup member-id is not allowed

Factory Reset on Detached ArubaStack Member

Starting from ArubaOS 7.4.0.3, you can reset a detached ArubaStack member to its factory defaults as it boots up as a line card. This allows you to reset the password on the Mobility Access Switch if the login credentials are lost.

To reset a line card to its factory defaults:

1. Connect a local console to the serial port on the Mobility Access Switch.
2. From the console, log in to the Mobility Access Switch using the following username and password:
 - Username: **password**
 - Password: **forgetme!**
3. Execute the following commands:

```
(LC-1) #restore factory_default stacking  
(LC-1) #reload
```



Similar to resetting line cards to factory default settings, factory reset can be done on ArubaStack as well. For more information on factory reset for ArubaStack, refer to the [ArubaStack Member Replacement](#) section.

After detaching the member from ArubaStack, remove the member from the stack. Otherwise, the member shows up in *Away* state always.

To remove a member (say, member 1) from the stack, execute the following command:

```
(Aruba) (config) #delete member 1
```

The Mobility Access Switch family includes platforms that support 12, 24 or 48 gigabit ethernet network interfaces, up to four 10-gigabit ethernet (S2500/S3500), four gigabit ethernet (S1500-24/48) or two gigabit ethernet (S1500-12P) uplink interfaces and an out of band ethernet management port (S2500/S3500 only).

This chapter includes the following topics:

- [Configuring the Management Port on page 97](#)
- [Gigabit Ethernet Network Interfaces on page 97](#)
- [Time-Domain Reflectometer on page 114](#)
- [Small Form-factor Pluggable Diagnostics on page 98](#)
- [Configuring an Interface Group on page 102](#)
- [Creating and Applying an Ethernet Link Profile to an Interface on page 105](#)
- [Power Over Ethernet on page 107](#)
- [Configuring Power Over Ethernet on page 111](#)
- [Creating and Applying a PoE Profile to an Interface on page 111](#)

Configuring the Management Port

The management interface is located above the console port on the rear panel of the Mobility Access Switch. It is labeled as *mgmt*. The management port is a dedicated interface for out-of-band management purpose. 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.

You can configure the management port using the CLI.

Using the CLI

```
(host) (config) # interface mgmt
  description <name>
  ip address <ip-address> <mask>
  ipv6 [ <prefix> prefix_len <prefix_len> | link-local <link-local-address> ]
  no {...}
  shutdown
```

Sample Management Port Configuration

```
(host) (config) # interface mgmt
  description MGMT_PORT
  ip address 10.1.13.1 255.255.255.0
  no shutdown
```

Gigabit Ethernet Network Interfaces

The Mobility Access Switch supports 12, 24, or 48 port gigabit ethernet interfaces of 10/100/1000 Mbps speeds. The S3500-24F supports 24 small form-factor pluggable (SFP) gigabit ethernet interfaces (SFPs sold separately).

A network gigabit ethernet interface is referred by its *<slot>/<module>/<port>*.

- Slot—The member ID of the stack.

- **Module**—There are two modules where the first one is the front-panel network module (0), while the other one is the uplink network module (1).
- **Port**—The individual port number.

For example, interface `gigabitethernet 0/0/20` refers to the first stack member (0) on the front-panel network module (0) at port number (20).



The Mobility Access Switch also supports two/four Gigabit Ethernet (S1500s) or four 10-Gigabit Ethernet interfaces (S2500/S3500) for stacking and uplink purposes. See the Hardware Installation Guide for more information on the uplink ports.

Small Form-factor Pluggable Diagnostics

A Small Form-factor Pluggable (SFP) module is a compact, hot-pluggable transceiver used for both telecommunication and data communications applications. Diagnostic information related to signal strength, temperature, etc can be polled from SFPs installed in the Mobility Access Switch.

This chapter includes the following topics:

- [Important Points to Remember on page 98](#)
- [Viewing SFP Diagnostic Information on page 98](#)
- [Sample Configuration on page 99](#)

Important Points to Remember

- SFP diagnostic is not supported on copper transceivers. Only fiber transceivers are supported.
- SFP diagnostic is supported on 1 Gbit/s and 10 Gbit/s fiber transceivers.
- Aruba supports most 1 Gbit/s and 10 Gbit/s transceivers. However, the following list is tested by Aruba:
 - 1 Gbit/s transceivers
 - OpNext TRF2716AALB400 (SFP-SX)
 - OpNext TRF2716AALB465 (SFP-SX)
 - Fiberxon, Inc. FTM-3012C-SLG (SFP-LX)
 - 10 Gbit/s transceivers
 - Finisar FTLX1371D3BCL (SFP-10GE-LRM)
 - OpNext TRS2001EN-0065 (SFP-10GE-SR)
 - OpNext TRS5020EN-S002 (SFP-10GE-LR)

Viewing SFP Diagnostic Information

You can view the SFP diagnostic information by issuing the following CLI commands.

Using the CLI

To display detailed interface transceiver diagnostic information, issue the following command:

```
(host) #show interface gigabitethernet 0/1/1 transceiver detail
```

To display detailed stacking interface transceiver diagnostic information, issue the following command:

```
(host) #show stacking interface stack 0/1 transceiver detail
```

To display basic transceiver information, issue the following command:

```
(host) #show interface transceiver brief
```

Sample Configuration

The following example displays detailed interface transceiver diagnostic information.

```
(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	
Module	Low Warning	Low Alarm	High Warning	High Alarm
Laser Bias 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	
Module	Low Warning	Low Alarm	High Warning	High Alarm
Laser TX 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	
Module	Low Warning	Low Alarm	High Warning	High Alarm
Laser RX 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	

The following example displays the stacking interface transceiver diagnostic information.

```
(host) #show stacking interface stack 0/1 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    : 1 min 44 sec
Module      Low Warning      Low Alarm      High Warning      High Alarm
Temperature Threshold      Threshold      Threshold      Threshold      Threshold
-----
40 C /      -10 C /      -15 C /      80 C /      85 C /
104.00 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

```

The following example displays transceiver diagnostic information in a tabular format.

```

(host) # show interface transceivers brief
Port      VendorName      VendorSN      ArubaSupported  CableType
-----
GE0/1/0   OPNEXT INC     L12J55161    YES             1000BASE-SX

```

Configuring Ethernet Interfaces

To set up your network, you can configure the various parameters for each ethernet network and uplink interfaces individually. You can also configure the parameters for a range of interfaces in case of identical configuration.

Using the CLI

To configure one interface at a time, use the following command :

```
(host)(config)# interface gigabitethernet <slot/module/port>
  aaa-profile <profile_name>
  backup interface {gigabitethernet <slot/module/port> | port-channel <0-7>}
  clone <source>
  description <description>
  enet-link-profile <profile_name>
  igmp-snooping mrouter-vlan {add | delete} <vlan-id>
  ip access-group in <in>
  lacp-profile <profile_name>
  lldp-profile <profile_name>
  mac-limit <limit>
  mirroring-in-profile <profile_name>
  mirroring-out-profile <profile_name>
  mstp-profile <profile_name>
  mtu <64-9216>
  no {...}
  poe-profile <profile_name>
  policer-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>
  exit
```

To configure a range of interfaces at the same time, use the following command:

```
(host)(config) #interface range gigabitethernet <interface-list>
(host)(config-range)#?
  aaa-profile          Apply AAA profile to interface
  description          Interface description
  enet-link-profile    Apply ethernet link profile to interface
  gvrp-profile         Apply GVRP profile to interface
  ip                  Apply IP access control list
  lacp-profile         Apply LACP profile to interface
  lldp-profile         Apply lldp profile to interface
  mirroring-in-profile Apply ingress mirroring profile to interface
  mirroring-out-profile Apply egress mirroring profile to interface
  mstp-profile         Apply MSTP profile to interface
  mtu                  Set MTU on interface between 64 and 9216
  no                  Delete Command
  oam-profile          Apply OAM profile to interface
  poe-profile          Apply POE profile to interface
  policer-profile      Apply policer profile to interface
  port-security-profile Apply security profile to interface
  pvst-port-profile    Apply PVST profile to interface
  qos                  Interface QoS
  qos-profile          Apply QOS profile to interface
  shutdown             Shut down the selected interface
  switching-profile    Apply switchport profile to interface
  trusted              Set trusted mode for the interface
  tunneled-node-profile Apply Tunneled Node profile to interface
  voip-profile         Apply VOIP profile to interface
```

Configuring Jumbo Frame Size

The Mobility Access Switch supports jumbo frames. You can enable jumbo frames on a per-interface basis with sizes from 64 to 9216 bytes. The default size is 1514 bytes.

```
(host)(config)# interface gigabitethernet 0/0/6
    mtu 9216
exit
```

Verifying Jumbo Frame Size

You can verify the jumbo frame size on an interface using the following command:

```
(host)# show interface gigabitethernet 0/0/6
GE0/0/6 is administratively Up, Link is Down, Line protocol is Down
Hardware is Gigabit Ethernet, Address is 00:0b:86:6a:42:03
Encapsulation ARPA, Loopback not set
Configured: duplex (Auto), Speed (Auto), FC (Off), Autoneg (On)
Auto negotiation in progress
Interface index: 2
MTU 9216 bytes
Flags: Access, Trusted
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
<output truncated>
```

Displaying Interface Counters and Statistics

```
(host)# show interface gigabitethernet 0/0/1 counters
Port                InOctets   InUcastPkts  InMcastPkts  InBcastPkts
GE0/0/1             0          0            0            0
Port                OutOctets   OutUcastPkts  OutMcastPkts  OutBcastPkts
GE0/0/1             0          0            0            0
```

```
(host)# show interface gigabitethernet 0/0/1 statistics
Last update of counters:      0d 00:00:00 ago
Last clearing of counters:     0d 00:00:00 ago
Received Statistics:
  0 frames, 0 octets
  0 unicast, 0 multicast, 0 broadcast
  0 error frames, 0 error octets, 0 CRC events, 0 runs, 0 giants, 0 throttles
  0 drop events
Transmitted Statistics:
  0 frames, 0 octets
  0 unicast, 0 multicast, 0 broadcast
  0 throttles, 0 deferred
  0 collisions, 0 multiple collisions, 0 late collisions
Received and Transmitted Frame Size Statistics:
0 64 octet, 0 65-127 octet, 0 128-255 octet, 0 256-511 octet, 0 512-1023 octet, 0 1024-max octet
```

Configuring an Interface Group

In the CLI configuration, it is often tedious to individually configure interfaces when there are multiple interfaces that have the same configuration. In such scenarios, you can group the interfaces together so that any interface within the group has the same configuration. When you configure an interface that is a member of an interface-group, applying a non-default profile or a parameter to the interface takes precedence over the interface-group configuration. By default, all the interfaces belong to a default interface-group.

To view the configuration of the default interface-group, use the `show interface-group-config gigabitethernet default` command. When you create non-default interface-groups, the excluded interfaces continue to belong to the default interface-group.



Interface-group and port-channel are not the same. Interface group assigns the configuration to individual interfaces whereas the port-channel makes a group of interfaces to work as a single logical interface.



You cannot have overlapping ranges of interfaces when you have multiple interface-groups. For more information about the scope of an interface and interface-group profiles, see [Scope of the Profiles and Parameters on page 31](#).

Using the CLI

```
(host) (config) # interface-group gigabitethernet {default|<group-name>}
  aaa-profile <profile_name>
  apply-to <interface range> add | remove
  clone <source>
  enet-link-profile <profile_name>
  igmp-snooping mrouter-vlan {add | delete} <vlan-id>
  ip access-group in <in>
  lACP-profile <profile_name>
  lldp-profile <profile_name>
  mac-limit <limit>
  mirroring-in-profile <profile_name>
  mirroring-out-profile <profile_name>
  mld-snooping mrouter-vlan {add | delete} <vlan-list>
  mstp-profile <profile_name>
  mtu <64-9216>
  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
  voip-profile <profile_name>
```

Sample Interface Group Configuration

```
(host) (config) # interface-group gigabitethernet FINANCE
  apply-to 0/0/0-0/0/20,0/0/32
```



Ensure that you do not add blank spaces between the ranges or multiple interfaces, and there must be three tuples in the individual, starting, and ending ranges. Also, the interface numbers should be in ascending order from start to finish of the range value. For example, 0/0, 0/1/0-1/1 is not a valid range because there is a space and the interface number format is not of slot/module/port in all the occurrences.

Verifying the Interface Group Configuration

You can use the following commands to view details about an interface-group.

```
(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 IGMP Multicast Router port for VLANs N/A
Static MLD Multicast Router port for VLANs N/A
Interface Trusted/Untrusted          Trusted
MAC-Limit (Action)                  N/A

```

(host)# show interface-group-config gigabitethernet FINANCE

gigabitethernet "FINANCE"

```

-----
Parameter                               Value
-----
Interface group members                  0/0/0-0/0/20,0/0/32
Interface MSTP profile                   default
Interface Tunneled Node profile          N/A
Interface VOIP profile                   N/A
Interface LLDP profile                   default
Interface PoE profile                    default
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

```

(host)# show interface-group-config gigabitethernet

gigabitethernet List

```

-----
Name           References  Profile Status
-----
default        0
FirstFloor    0
SecondFloor   0
Total:3

```



In the case of LLDP and PoE profiles, the default interface-group has lldp-factory-initial and poe-factory-initial profiles applied, whereas a non-default interface-group that you create has the LLDP and PoE default profiles applied. The default LLDP and PoE profiles have LLDP and PoE disabled, while they are enabled in the factory-initial profiles.

You can view the differences in the LLDP and PoE factory-initial and default profiles using the following commands:

```
(host)# show interface-profile poe-profile poe-factory-initial
```

```
Power over Ethernet profile "poe-factory-initial"
```

```
-----  
Parameter                               Value  
-----  
Enable PoE interface                     Enabled  
Max Power on PoE port milliwatts        30000  
PoE port priority                         low  
time-range-profile                       N/A
```

```
(host)# show interface-profile poe-profile default
```

```
Power over Ethernet profile "default"
```

```
-----  
Parameter                               Value  
-----  
Enable PoE interface                     Disabled  
Max Power on PoE port milliwatts        30000  
PoE port priority                         low  
time-range-profile                       N/A
```

```
(host)# show interface-profile lldp-profile lldp-factory-initial
```

```
LLDP Profile "lldp-factory-initial"
```

```
-----  
Parameter                               Value  
-----  
LLDP pdu transmit                       Enabled  
LLDP protocol receive processing         Enabled  
LLDP transmit interval (Secs)           30  
LLDP transmit hold multiplier           4  
LLDP-MED protocol                       Enabled
```

```
(host)# show interface-profile lldp-profile default
```

```
LLDP Profile "default"
```

```
-----  
Parameter                               Value  
-----  
LLDP pdu transmit                       Disabled  
LLDP protocol receive processing         Disabled  
LLDP transmit interval (Secs)           30  
LLDP transmit hold multiplier           4  
LLDP-MED protocol                       Disabled
```

Creating and Applying an Ethernet Link Profile to an Interface

You can use the ethernet link profile to configure the gigabit ethernet switching and uplink ports. The ethernet interfaces support auto negotiation from 10BaseT to 1000BaseT as per IEEE 802.3u/z standards. When you enable auto negotiation, the device that is connected to the port is automatically configured to the highest speed supported by the device in the following order (highest to lowest):

- 10000 Mbps full duplex (supported only on the S2500/S3500 uplink interfaces)

- 1000 Mbps full duplex
- 100 Mbps full duplex
- 100 Mbps half duplex
- 10 Mbps full duplex
- 10 Mbps half duplex



The 10000 Mbps ports (10 gigabit uplink interfaces) cannot scale down to less than 1000 Mbps (1 gigabit speed).

Auto negotiation also supports the pause capabilities, automatic Media Detection Interface (MDI), and Media Detection Interface Crossover (MDIX) cable detection. The devices exchange information using the Fast link Pulse (FLP) bursts. The auto negotiation on the link is performed when you perform any of the following activities:

- Connect the device.
- Power on or reset the device at either end of the link.
- Make a negotiation request.

You can configure the ethernet link profile either using the CLI or the WebUI.

Using the WebUI

1. Navigate to the **Configuration > Ports > Ethernet** page.
2. Click **New** under the Profiles list, and enter a name for the Ethernet profile.
3. Click on the **Speed/Duplex** column and select the Speed and Duplex from the popup window.
4. Select a **Flow Control** option from the next column.
5. Select whether you need **Autonegotiation** enabled or disabled.
6. Click on the **Association** column and move the ports to the **Selected** list to apply this profile to selected ports.
7. Click **Apply**.

Using the CLI

```
(host) (config) # interface-profile enet-link-profile <profile-name>
  autonegotiation
  duplex {auto|full|half}
  speed {auto|10|100|10m_100m|1000|10000}
  flowcontrol {auto|on|off}
  no {...}
  exit
(host) (config) # interface gigabitethernet <slot/module/port>
  enet-link-profile <profile-name>
```



When the port speed is explicitly configured, the autonegotiation is disabled.

Ethernet Link Default Profile

```
(host) # show interface-profile enet-link-profile default
Ethernet Link "default"
-----
Parameter      Value
-----
Speed          auto
```

```
Duplex          auto
Autonegotiation Enabled
Flowcontrol     off
```

Sample Ethernet Link Profile Configuration

```
(host)(config)# interface-profile enet-link-profile intspd
duplex full
speed 1000
(host)(config)# interface gigabitethernet0/0/0
enet-link-profile intspd
```

Verifying Ethernet Link Profile Configuration

```
(host)# show interface gigabitethernet 0/0/0
GE0/0/0 is administratively Up, Link is Down, Line protocol is Down
Hardware is Gigabit Ethernet, Address is 00:0b:86:6a:42:02
Encapsulation ARPA, Loopback not set
Configured: duplex (Auto), Speed (Auto), FC (Off), Autoneg (On)
Auto negotiation in progress
Interface index: 1
MTU 1514 bytes
Flags: Access, Trusted
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 0 frames, 0 octets
  0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 error octets, 0 CRC frames
  0 multicast, 0 unicast
  Transmitted 0 frames, 0 octets
  0 broadcasts, 0 throttles
  0 errors octets, 0 deferred
  0 collisions, 0 late collisions
PoE Information:
  Interface: GE0/0/0, Administratively Disable, Port status: On
  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: On
```

Ethernet Flow Control

Ethernet flow control prevents loss of frames by providing a back pressure. When an ethernet port receives frames faster than it can handle, it sends a PAUSE frame to stop the transmission from the sender for a specific period of time. The PAUSE frame has a destination group address of 01-80-c2-00-00-01.

Use the following command in the ethernet link profile to configure flow control for an ethernet port:

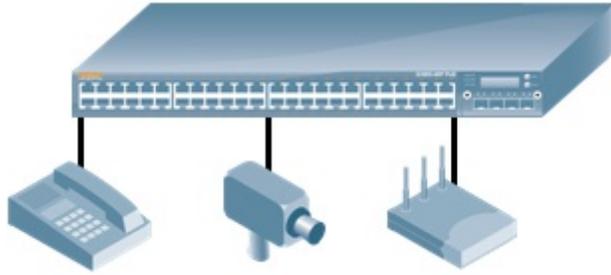
```
(host)( Ethernet Link " intspd")# [no] flow-control {on|off|auto}
```



When flow control frames are received, only pausing the transmit is supported. Sending flow control frames are not supported. This means that the system can only respond to PAUSE frames and cannot generate them. The flow-control can be enabled or disabled to respond to incoming PAUSE frames.

Power Over Ethernet

Power over Ethernet (PoE) as per IEEE 802.3at is a technology for wired Ethernet LANs to carry the electric-power required for the device in the data cables. You can use this technology to power IP phones, wireless LAN access points, cameras, embedded computers, thin clients, and LCDs.



The IEEE standard defined in IEEE 802.3af allows network equipment (power sourcing equipment) to provide up to 15.4 Watts of power at the output for powered devices (PDs). In addition, the IEEE 802.3at (PoE+) standard provides more power to PDs where up to 30.0 Watts of power on output is delivered on the standard copper cable. The Mobility Access Switch supports both PoE standards.

Power Management Modes

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.

Power Pools

The Mobility Access Switch family use a variety of power supply units (PSUs), some are integrated and some are modular depending on the platform

- **Integrated 150W PSU**—This power supply is used in the S1500-12P and provides 120W for PoE.
- **Integrated 180W PSU**—This power supply is used in the non-PoE models of the S2500.
- **Integrated 580W PSU**—This power supply is used in the 24 and 48 port PoE models of the S1500 and S2500 and provides 400W for PoE.
- **Modular 350W PSU**—This power supply is used in the non-PoE models of the S3500. You can also install two 350W PSUs for system redundancy.
- **Modular 600W PSU**—This power supply is used in the 24 and 48 port PoE models of the S3500 and provides 400W for PoE. You can also install two 600W PSUs for system redundancy and an increased PoE budget.
- **Modular 1050W PSU**—This power supply is used in the 48 port PoE model of the S3500 and provides 850W for PoE. You can also install two 1050W PSUs for system redundancy and an increased PoE budget.

Table 18: Power Supply Pools

Power Supply Capacity	System Power Redundancy	Power Available for PoE and PoE+Pool
350W	No	—
350W+350W	Yes	—
600W	No	400W
600W+600W	Yes	689W
1050W	No	850W
1050W+1050W	Yes	1465W

Mixed Mode PSUs

You can mix and match PSU models. The [Table 19](#) describes the various mixed mode PSU models.

Table 19: Mixed Mode PSUs

	350W	600W	1050W
350W	No PoE	PoE with 400W budget Not redundant for PoE	PoE with 850W budget Not redundant for PoE
600W	PoE with 400W budget Not redundant for PoE	PoE with 666W budget	PoE with 666W budget
1050W	PoE with 850W budget Not redundant for PoE	PoE with 666W budget	PoE with 1440W budget

PoE Priority

When you have 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. Priority can be either low (default), high, or critical. When there is a power shortage, the Mobility Access Switch stops power to the low priority ports, then high priority ports, until there is enough PoE power available in the pool. If the ports have the same priority, PoE is stopped for ports with higher interface numbers and then the lower interface numbers. For example, when there is an interface 0/0/4 and an interface 0/0/10 with the same priority, the Mobility Access Switch will stop power to the interface 0/0/10 before stopping power to the interface 0/0/4.

PoE Guard-Band

The PoE guard-band can provide protection when there is a sudden spike in the consumed power of PDs that could potentially impact other PoE enabled ports. When the guard-band is configured, the Mobility Access Switch reserves the specified amount of power to prevent other PoE enabled ports from powering off and then on again. The default value for guard-band is 11,000mW. You can specify the guard-band value in steps of 1000 starting from 1000 to 30,000 milliwatts.

PoE Compatibility with CISCO Legacy Devices

The Mobility Access Switch supports the IEEE 802.3af and 802.3at Power over Ethernet detection standards by default. Certain older CISCO PoE devices require a pre-standard Power over Ethernet detection method to be recognized and powered up. The Mobility Access Switch can power these devices in addition to standards based devices by enabling **cisco-compatibility** mode.

Execute the following commands to enable this functionality under the PoE management profile:

```
(host) (config)# poe-management-profile slot <slot_number 0-7>
(host) (poe-management profile "<slot number 0-7>")cisco-compatibility
```

Execute the following command to disable this functionality:

```
(host) (poe-management profile "<slot number 0-7>") #no cisco-compatibility
```

Limitations

- The **cisco-compatibility** option is per stack member (slot) and not per port, i.e. if you configure this option it applies to the entire slot.
- When **cisco-compatibility** is disabled, the Mobility Access Switch continues to provide power to the CISCO legacy devices until that device is unplugged or the Mobility Access Switch is reloaded.
- When cisco-compatibility is enabled, Mobility Access Switch may provide PoE to any detected CISCO legacy switch with pre-standard PoE. It is recommended not to connect a CISCO legacy phone and legacy switch on the same slot.

PoE Configuration Delay Timer

The Mobility Access Switch allows you to configure a time delay while applying the PoE configuration 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. You can configure the delay time using the CLI.

Configuring Delay Time

Execute the following commands to configure the delay time for applying the PoE configuration between ports:

```
(host) (config) #poe-management-profile slot <0-7>
(host) (poe-management profile "<0-7>") #config-delay <config-delay>
```

Sample Configuration

```
(host) (config) #poe-management-profile slot 0
(host) (poe-management profile "0") #config-delay 3000
```

Verifying Delay Configuration

Execute the following command to verify the configured delay time for applying the PoE configuration between ports:

```
(host) #show poe-management-profile slot 0
poe-management profile "0"
-----
Parameter Value
-----
Power Management Algorithm dynamic
Guard band for PoE controller 11000
Cisco Pre-Standard compatibility Disabled
Delay in applying config for PoE controller 3000
```

Configuring Power Over Ethernet

PoE/PoE+ is enabled on the Mobility Access Switch by default. It supports plug-and-play capability for 802.3af/802.3at capable devices. You can configure PoE either using the CLI or the WebUI.

Using the WebUI

1. Navigate to the **Configuration > Ports > PoE** page.
2. Select a mode from the **Power Management Mode** drop-down list.
3. Click **Apply** and **Save Configuration**.



You can configure only one PoE management mode for the stack.

Using the CLI

```
(host) (config)# poe-management-profile slot <slot_num>
  clone<source>
  poe-powermanagement {class|dynamic|static}
  poe-guardband <1000-30000 milliwatts>
  no {...}
```



You can configure different PoE management modes (class/dynamic/static) on each stack member.

Sample PoE Configuration

```
(host) (config)# poe-management-profile slot 0
  poe-powermanagement static
  poe-guardband 15000
```

Creating and Applying a PoE Profile to an Interface

You can configure the PoE profile either using the CLI or the WebUI.

Using the WebUI

1. Navigate to the **Configuration > Ports > PoE** page.
2. Click **New** under the Profiles list, and enter a name for the PoE profile.
3. Click on the **Priority** column and select the priority from the drop-down list.
4. Enter the power in milliwatts in the **Power(/mW) Port** column.
5. Select whether the PoE state is enabled or disabled in the **State** column.
6. Click on the **Association** column and move the ports to the **Selected** list to apply this profile to the selected ports.
7. Click **Apply** and **Save Configuration**.

Using the CLI

```
(host) (config)# interface-profile poe-profile <profile-name>
  close <source>
  enable
  poe-maxpower <milliwatts>
  poe-priority {critical|high|low}
  time-range-profile <name>
(host) (config)# interface gigabitethernet <slot/module/port>
  poe-profile <profile-name>
```

Sample PoE Profile Configuration

```
(host) (config) # interface-profile poe-profile CAMERAS
  poe-priority high
  poe-maxpower 15000
  enable
(host) (config) # interface gigabitethernet 0/0/15
  poe-profile CAMERAS
```

Time Range Support for PoE

The PoE supports time range for controlling the mode of the PoE power (enable/disable) to the PoE port. The PoE port mode is enabled by the administrator.



By default, the time range profile is disabled in the poe-profile.

The PoE time range can be configured in two modes: **absolute** and **periodic**. In absolute mode, the time parameters correspond to a specific time range: start date, start time, end date, and the end time. The PoE port is enabled if the current system time is within this range. In periodic mode, the user can specify start day, start time, end day, and end time. The start day or end day can be daily, weekend, weekday, or any day of the week. The PoE port is enabled if the current day and time falls within the range.

The following are the invalid combinations for start and end values for the time range parameters in the periodic mode:

- **start-day:** daily, **end-day:** any other day other than daily
- **start-day:** weekend, **end-day:** any other day other than than weekend. (Here weekend refers to Saturday or Sunday)
- **start-day:** weekday, **end-day:** any other day other than weekday



Both the **start-time** and the **end-time** should not have identical time values if the **start-day** and the **end-day** are same.

You can configure the PoE time-range-profile using the following CLI :

```
(host) (config) # time-range-profile <profile_name>
```



As a best practice, avoid configuring the PoE time-of-day when the connected devices are in the process of being upgraded or when a power loss has rendered the connected device inoperable. In the case of an Aruba wireless Access Point, the PoE time-of-day should not be configured when an AP flash memory upgrade is in progress as it may result in potential corruption of the flash.

PoE Factory-Initial and Default Profiles

When the Mobility Access Switch is booted as factory-default and when it is booted for the first time, the poe-factory-initial profile is associated to all the ports.

```
(host) # show interface-profile poe-profile poe-factory-initial
Power over Ethernet profile "poe-factory-initial"
-----
Parameter                               Value
-----
Enable PoE interface                     Enabled
Max Power on PoE port milliwatts         30000
PoE port priority                         low
time-range-profile                       N/A
(host) # show interface-profile poe-profile default
Power over Ethernet profile "default"
-----
```

Parameter	Value
-----	-----
Disable PoE interface	Disabled
Max Power on PoE port milliwatts	30000
PoE port priority	low
time-range-profile	N/A

Monitoring Power-over-Ethernet

You can use the following commands to verify the PoE configuration and monitor the PoE usage:

```
(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 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>
```

```
(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
```

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

(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>

```

(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>

Time-Domain Reflectometer

Time-Domain Reflectometer (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.

Use this command to execute a TDR diagnostic test on a specific gigabitethernet interface.

```
(host) (config)# run diagnostics interface gigabitethernet <slot/module/port> cable
```

Use the following command to view the test results for the Time-Domain Reflectometer (TDR) cable diagnostics:

```
(host)# show diagnostics interface gigabitethernet
```


A port-channel is a bundle of multiple physical interfaces that form a single logical interface. You can use port-channels to provide additional bandwidth or link redundancy between two devices. This chapter describes how to configure port-channels using the static Link Aggregation Group (LAG) and the dynamic Link Aggregation Control Protocol (LACP) methods.

This chapter includes the following topics:

- [Important Points to Remember on page 117](#)
- [Creating a Port-Channel on page 117](#)
- [Link Aggregation Control Protocol on page 121](#)
- [Creating and Applying a Dynamic Port-Channel Profile to an Interface on page 119](#)

Important Points to Remember

- A port-channel is always trusted. Any network that extends beyond the port-channel on the Mobility Access Switch must be a trusted network.
- The maximum port-channels supported per system is 8 groups for the S1500s and 64 groups for the S2500/S3500s; each group can be created statically or dynamically (via LACP).
- Each port-channel can have up to 8 member ports.
- The port-channel group identification (ID) range is 0 to 7 (S1500) or 0 to 63 (S2500/S3500s) for both static and dynamic port-channels.
- The static and dynamic methods must use different group IDs and different port-channel members.
- When a port is added to a port-channel, it inherits the port-channel's properties such as VLAN membership and trunk status.
- Ports that are already assigned a feature profile cannot be part of a static or dynamic port-channel.
- Aruba recommends that all the port-channel members have the same port speed and duplex for proper operation. Configuring dissimilar speed and duplex on the port-channel members will result in a syslog error message.
- There is no default LACP profile.
- For port-channel members, apart from the following profiles and parameters, all the other profiles and parameters are inherited from the port-channel configuration:
 - shutdown
 - lacp-profile
 - lldp-profile

Creating a Port-Channel

You can create port channels using the static method or the dynamic method.

- In the static method, you must first create the port-channel interface, and then add the physical interfaces to the port-channel.
- In the dynamic method, you must first create the lacp-profile and then apply the lacp-profile to the member interfaces.

Using the WebUI

1. Navigate to the **Configuration > Ports > Port Channel** page.
2. Select the **Group ID** for the port channel.
3. Select Static or LACP from the **Type** popup window and click **OK**.
4. Click on the **Membership** column and move the ports to the **Selected** list to include the selected ports to the port channel.
5. Click **Apply** and **Save Configuration**.

Using the CLI

```
(host) (config) #interface port-channel <0-63>
  backup [gigabitethernet <slot/module/port> | port-channel <0-63>]
  clone <source>
  description <description>
  enet-link-profile <profile-name>
  gvrp-profile <profile-name>
  igmp-snooping [ mrouter-vlan [ <vlan-list> | add <vlan-list> | delete <vlan-list>]]
  ip [access-group [in <ingress-acl> | out <egress-acl>]]
  mirroring-in-profile <profile-name>
  mirroring-out-profile <profile-name>
  mld-snooping [mrouter-vlan [<vlan-list> | add <vlan-list> | delete <vlan-list>]]
  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 <10-300s> | mode [forced | off]]
  pvst-port-profile <profile-name>
  qos [trust [auto | dot1p | dscp | none]
  qos-profile <profile-name>
  shutdown
  switching-profile <profile-name>
```



For all Mobility Access Switches except the S1500 Mobility Access Switch, you can configure up to 64 (0-63) port channels. For the S1500 Mobility Access Switch, you can configure only up to 8 (0-7) port channels.

Default Enet-Link Profile for Port-Channels

If you do not assign any enet-link-profile to the static or dynamic port-channel, the hidden **pc_default** profile is applied by default:

```
(show)# show interface-profile enet-link-profile pc_default
Ethernet Link "pc_default" (Predefined (editable))
-----
Parameter      Value
-----
Speed          1000
Duplex         full
Autonegotiation Enabled
Flowcontrol    off
```

Sample Static Port-Channel Configuration

```
(host) (config) # interface port-channel 1
  port-channel-members gigabitethernet0/0/4,gigabitethernet0/0/5
  [or]
  port-channel-members add gigabitethernet 0/0/4
```

```
port-channel-members add gigabitethernet 0/0/5
exit
```

Verifying the Port-Channel Configuration

You can use the following command to verify the port-channel configuration:

```
(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
```

Creating and Applying a Dynamic Port-Channel Profile to an Interface

Using the WebUI

1. Navigate to the **Configuration > Ports > Port Channel** page.
2. Select the **Group ID** for the port channel.
3. Select LACP from the **Type** popup window.
4. Choose whether you want to select the LACP profile from a list of existing LACP profiles or you want to specify a new profile.
5. Select the LACP Profile name from the drop-down list or enter the name for the new LACP profile in the **Profile Name** text box.
6. Select the mode as passive or active from the **Mode** drop-down list.
7. Enter the priority in the **Priority** text box.
8. Select the timeout as long or short from the **Timeout** drop-down list.
9. Click on the **Membership** column and move the ports to the **Selected** list to include the selected ports to the port channel.
10. Click **Apply** and **Save Configuration**.

Using the CLI

```
(host) (config) # interface-profile lacp-profile <profile-name>
  group-id <0-63>
  mode {active|passive}
  port-priority <1-65535>
```

```

timeout {long|short}
no {...}
exit
(host)(config)# interface gigabitethernet <slot/module/port>
lacp-profile <profile-name>

```



For all Mobility Access Switches except the S1500 Mobility Access Switch, you can configure up to 64 (0-63) port channel group-ids. For the S1500 Mobility Access Switch, you can configure only up to 8 (0-7) port channel group ids.

Sample Dynamic Port-Channel Configuration

```

(host)(config)# interface-profile lacp-profile LACP_2
group-id 2
mode active
exit
(host)(config)# interface gigabitethernet 0/0/0
lacp-profile LACP_2
exit
(host)(config)# interface gigabitethernet 0/0/1
lacp-profile LACP_2
exit

```

Verifying Port-Channel Configuration

(host)# show interface port-channel 2

```

port-channel 0 is administratively Up, Link is Down, Line protocol is Down
Hardware is Port-Channel, LACP enabled, Address is 00:0b:86:6a:25:40
Description: Link Aggregate
Member port(s):
  GE0/0/0 is administratively Up, Link is Down, Line protocol is Down
  GE0/0/1 is administratively Up, Link is Down, Line protocol is Down
Speed: 0 Mbps
Interface index: 1443
MTU 1514 bytes
Flags: Access, Trusted
Link status last changed: 0d 04h:10m:27s ago
Last clearing of counters: 0d 00h:00m:02s ago
Statistics:
  Received 0 frames, 0 octets
  0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 error octets, 0 CRC frames
  0 multicast, 0 unicast
  Transmitted 0 frames, 0 octets
  0 broadcasts, 0 throttles
  0 errors octets, 0 deferred
  0 collisions, 0 late collisions

```

Verifying Port-Channel Neighbor Information

(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
GE0/0/0	SP	0	0x0	0x0	0x0	00:00:00:00:00:00
GE0/0/1	SP	0	0x0	0x0	0x0	00:00:00:00:00:00

Verifying Port-Channel Internal (Local) Information

(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
GE0/0/0	SA	255	0x3	0x3	0x5	0x7	down
GE0/0/1	SA	255	0x3	0x3	0x5	0x8	down

Verifying Port-Channel Counters Information

```
(host) #show lacp 2 counters
```

```
LACP Counter Table
-----
```

Port	LACPDUTx	LACPDURx	MrkrTx	MrkrRx	MrkrRspTx	MrkrRspRx	ErrPktRx
GE0/0/0	0	0	0	0	0	0	0
GE0/0/1	0	0	0	0	0	0	0

Link Aggregation Control Protocol

The Mobility Access Switch supports Link Aggregation Control Protocol (LACP) based on the IEEE 802.3ad standard. LACP provides a standardized means for exchanging information with partner systems, to form a dynamic link aggregation group. LACP avoids port channel misconfiguration. You can define the LACP parameters in a `lacp-profile`, and then reference the profile in the ports to form a dynamic port-channel. A port-channel will be operationally down if all the ports in the port-channel are down.

LACP Port Modes

The dynamic port-channel member interfaces can operate in the following modes:

- Active mode—the interface is in active negotiating state. LACP runs on any link that is configured to be in the active state. The port in an active mode automatically initiates negotiations with other ports by initiating LACP packets.
- Passive mode—the interface is *not* in an active negotiating state and does not initiate negotiations. LACP runs on any link that is configured in a passive state. The port in a passive mode only responds to negotiations requests from other ports that are in an active state. .



A port in a passive state cannot set up a port-channel with another port in a passive state. Hence, to form a port-channel group between two ports, one port must be an active participant.

LACP Session Timeout and Port Priority

You can set the timeout for a LACP session. The timeout value is the amount of time that a port-channel interface waits for a LACPDU from the remote system before terminating the LACP session. The default time out value is long (90 seconds); short is 3 seconds. You can also set the port priority. The higher the value the lower the priority. The priority range is 1 to 65535 and the default is 255.

When a port in a port-channel is misconfigured (that is, the partner port is different from the other ports) or if the neighbor experiences time out or if it cannot exchange LACPDUs with the partner, then the port operational status is displayed as DOWN.



The port priority is used to dynamically select the ports that have the highest priority to form the port-channel when there are unspecified number of ports. As Mobility Access Switch provides support for a maximum of only 8 ports per port-channel, configuring the port priority does not have any effect.

LACP—Independent State

Mobility Access Switch allows the users to configure the ethernet ports in 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.

By default, this feature is enabled on the Mobility Access Switch. You can enable or disable this feature on the LACP profile using the CLI.

Important Points to Remember

- An LACP Independent state enabled interface falls to Independent state in the following scenarios:
 - When LACPDUs are not received from the peer. This is determined by the LACP timeout timer configured in the LACP profile .
 - When both the peers connected are in passive mode.
- Any LACP enabled interface in Independent state has the following behavior:
 - It continues to send the LACPDUs periodically.
 - It inherits all configuration parameters from the parent port-channel (Example: switching-profile).
 - It supports only those features supported on a LAG member (mstp-profile and poe-profile) if enabled on the parent port-channel.
 - It bundles back into port-channel and behaves as a LAG member upon receiving LACPDUs from the peer.
 - It clears the LLDP neighbor entries learnt (after timeout) upon joining the bundle to form a port-channel .

Configuring LACP 'I' state

You can configure the LACP Independent state using the following CLI command:

```
(host) (config) #interface-profile lACP-profile lACP
(host) (LACP "lACP") # independent-state
```

Verifying LACP 'I' State Configuration

You can verify the LACP Independent state configuration using the following CLI command:

```
(host) #show interface port-channel 5

port-channel 5 is administratively Up, Link is Up, Line protocol is Down
Hardware is Port-Channel, LACP enabled, Address is 00:0b:86:6a:c1:c0
Description: Link Aggregate
Member port(s):
GE1/0/12 is administratively Up, Link is Up, Line protocol is UP (LACP-I)

Speed: 0 Mbps
Interface index: 1446
MTU 1514 bytes
Flags: Access, Trusted
Link status last changed: 1d 21h:49m:36s ago
Last clearing of counters: 1d 21h:49m:36s ago
Statistics:
Received 118368 frames, 19215896 octets
0 pps, 1.775 Kbps
0 broadcasts, 0 runts, 0 giants, 0 throttles
0 error octets, 0 CRC frames
118368 multicast, 0 unicast
Transmitted 5502 frames, 704256 octets
0 pps, 509 bps
```

```

0 broadcasts, 0 throttles
0 errors octets, 0 deferred
0 collisions, 0 late collisions
GE1/0/12:
Statistics:
Received 118368 frames, 19215896 octets
0 pps, 1.775 Kbps
0 broadcasts, 0 runts, 0 giants, 0 throttles
0 error octets, 0 CRC frames
118368 multicast, 0 unicast
Transmitted 5502 frames, 704256 octets
0 pps, 509 bps
0 broadcasts, 0 throttles
0 errors octets, 0 deferred
0 collisions, 0 late collisions

```

The I flag in the following command output indicates that the corresponding interface is in Independent state:

```

(host) (config) #show interface brief
Interface      Admin      Link      Line Protocol      Speed/Duplex
-----      -
GE1/0/12      Enable     Up        Up (LACP-I)        1 Gbps / Full
Pc5           Enable     Up        Down                N/A
MGMT         Enable     Up        Up                  1 Gbps / Full

```

Execute the following command to check the number of LACPDUs sent or received on an interface in Independent state:

```

(host) (config) # show lacp 5 counters
LACP Counter Table
-----
Port          LACPDUTx  LACPDURx  MrkrTx  MrkrRx  MrkrRspTx  MrkrRspRx  rrPktRx
-----
GE1/0/12     26        30        0        0        0          0          0

```

Auto Link Aggregation Control Protocol

Starting from ArubaOS 7.4.1.1, the Mobility Access Switch supports Auto Link Aggregation Control Protocol (Auto-LACP). Based on the device-group configuration, the Auto-LACP forms port-channels automatically. It helps automatic detection of the neighboring devices with port-channels when AP is connected to the Mobility Access Switch.

Auto-LACP is disabled by default on the Mobility Access Switch. You can enable Auto-LACP on the Mobility Access Switch using the CLI.

APs, IAPs, and ArubaOS Versions Supporting Auto-LACP

The following table lists the supporting access points and Mobility Access Switch- ArubaOS versions categorized by controller version.

Table 20: APs, IAPs, and ArubaOS versions supporting Auto-LACP

Controller Version	Supported APs	Mobility Access Switch-ArubaOS Version
6.4.4.0	AP-224, AP-225, AP-274, AP-275, AP-325	ArubaOS 7.4.1.1
6.4.3.1	AP-224, AP-225, AP-274, AP-275	ArubaOS 7.4.1.1
6.4.3.4-4.2.1.0	IAP-225	ArubaOS 7.4.1.1

Important Points to Remember

- Auto-LACP is supported only for AP-224, AP-225, AP-274, AP-275, AP-325, and IAP-225 access points.
- Auto-LACP is supported on S1500, Mobility Access Switch S2500/S3500 platforms.
- All Auto-LACP port-channels share the same device group configuration for AP device type.
- Configuration is blocked for Auto-LACP port-channels and port members.
- Alteration and deletion in the Auto-LACP profile is blocked.
- The maximum number of supported port-channels on S1500 is eight and that for S2500/S3500 is sixty-four. Auto LACP uses the LAG IDs from these limits only.
- Auto-LACP is functional only if **device-group** configuration is enabled.

Configuring Auto LACP

To configure Auto-LACP, you should enable device configuration and Auto-LACP on the Mobility Access Switch.

To enable device configuration, execute the following commands:

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

To enable Auto-LACP, execute the following commands:

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

Verifying Auto-LACP

To verify the Auto-LACP configuration on the Mobility Access Switch, execute the following command:

```
(host) # show device-group-config ap
device-group access-point (N/A)
-----
Parameter                               Value
-----
Enable Device Config                   true
Enable Auto LACP                       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                    N/A
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



The **Enable Device Config** and **Enable Auto LACP** parameters display a true value.

To view Auto-LACP port-channel interfaces, execute the following command:

```
(host) # show interface port-channel auto-lacp
port-channel 1 is administratively Up, Link is Up, Line protocol is Up
Hardware is Port-Channel, LACP enabled, Address is 00:0b:86:6a:bd:80
Description: Link Aggregate
Created by Auto-LACP Link Aggregate
Member port(s) :
GE1/0/16 is administratively Up, Link is Up, Line protocol is Up
GE2/0/16 is administratively Up, Link is Up, Line protocol is Up

Speed: 2 Gbps
Interface index: 1442
MTU 1514 bytes
Flags: Access, Trusted
Link status last changed: 0d 00h:27m:32s ago
Last clearing of counters: 0d 00h:27m:32s ago
Statistics:
Received 15172 frames, 3183154 octets
5 pps, 7.979 Kbps
7 broadcasts, 0 runts, 10 giants, 0 throttles
15220 error octets, 0 CRC frames
3410 multicast, 11755 unicast
Transmitted 6605 frames, 721121 octets
1 pps, 844 bps
1867 broadcasts, 0 throttles
0 errors octets, 0 deferred
0 collisions, 0 late collisions
GE1/0/16:
Statistics:
Received 13470 frames, 2960782 octets
5 pps, 6.966 Kbps
2 broadcasts, 0 runts, 10 giants, 0 throttles
15220 error octets, 0 CRC frames
1713 multicast, 11755 unicast
Transmitted 2265 frames, 190374 octets
0 pps, 0 bps
1867 broadcasts, 0 throttles
0 errors octets, 0 deferred
0 collisions, 0 late collisions
GE2/0/16:
Statistics:
Received 1714 frames, 224436 octets
0 pps, 1.013 Kbps
7 broadcasts, 0 runts, 0 giants, 0 throttles
0 error octets, 0 CRC frames
1707 multicast, 0 unicast
Transmitted 4372 frames, 534065 octets
1 pps, 844 bps
0 broadcasts, 0 throttles
0 errors octets, 0 deferred
0 collisions, 0 late collisions
```

To view if a gigabit Ethernet port is a member of a port-channel, execute the following command:

```
(host) # show interface gigabitethernet 1/0/16
GE1/0/16 is administratively Up, Link is Up, Line protocol is Up
Hardware is Gigabit Ethernet, Interface is GE1/0/16, Address is 00:0b:86:6c:19:52
Port is the member of port-channel1
Encapsulation ARPA, Loopback not set
Configured: duplex (Full), Speed (1 Gbps), FC (Off), Autoneg (On)
Negotiated: duplex (Full), Speed (1 Gbps)
Interface index: 161
MTU 1514 bytes
Link flaps: 28
Flags: Port is a member of port-channel4
Link status last changed:      0d 00:15:08 ago
Last update of counters:      0d 00:00:07 ago
Last clearing of counters:     0d 01:36:13 ago
Statistics:
Received 41557 frames, 5669988 octets
6 pps, 7.912 Kbps
35928 unicast, 5605 multicast, 24 broadcast
0 runts, 19 giants, 0 throttles
28918 error octets, 0 CRC frames
Transmitted 1133140920 frames, 82607799007 octets
1 pps, 1.428 Kbps
43422 unicast, 626358842 multicast, 506738656 broadcast
0 throttles, 0 errors octets, 0 deferred
0 collisions, 0 late collisions
PoE Information:
Administratively Enable, Port status: On, Power consumption: 12000 mW
PSE port status: On
```

To view all Auto-LACP port-channel interface status in brief, execute the following command:

```
(host) # show interface brief port-channel auto-lacp
Interface      Admin   Link   Line Protocol   Speed/Duplex
-----
port-channel1  Enable Up     Up              1 Gbps / Full
port-channel2  Enable Up     Up              2 Gbps / Full
port-channel3  Enable Up     Up              2 Gbps / Full
port-channel4  Enable Up     Up              2 Gbps / Full
port-channel5  Enable Up     Up              2 Gbps / Full
```

To view all neighboring devices, execute the following command:

```
(host) (config) #show lldp neighbor
Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone, (S)Station (r)Repeater, (O)
Other
LLDP Neighbor Information
-----
Local Intf Chassis ID          Capability Remote Intf
-----
GE0/0/1    18:64:72:c8:1e:40 B:A      18:64:72:c8:1e:40
GE0/0/3    18:64:72:c8:1e:40 B:A      18:64:72:c8:1e:40
GE0/0/6    9c:1c:12:c0:9f:e4 B:A      9c:1c:12:c0:9f:e4
GE0/0/7    9c:1c:12:c0:9f:e4 B:A      9c:1c:12:c0:9f:e4
Expiry (Secs) System Name
-----
103          18:64:72:c8:1e:40
102          18:64:72:c8:1e:40
107          9c:1c:12:c0:9f:e4
105          9c:1c:12:c0:9f:e4
Number of neighbors: 4
```

Triggers on Disabling Auto LACP Port-Channels

When you disable Auto-LACP port-channels, keep the following points in mind:

- When you disable **auto-lACP** parameter from **device-group ap**, all Auto-LACP port-channels are deleted.
- When you disable **device-group ap**, all Auto-LACP port-channels are deleted.
- If an AP is deleted from one of the member interfaces or if there is an LLDP timeout, the corresponding Auto-LACP port-channel is deleted.
- In case a member is plugged out of one port and inserted into another, a new port-channel will be formed with updated member interfaces.

Operations, Administration, and Maintenance (OAM) refers to the tools and utilities to install, monitor, and troubleshoot a network. This implementation of OAM complies with the IEEE 802.3ah standard and is able to report layer-2 network behavior. This helps network administrators monitor troubleshoot a network without sending technicians into the field to diagnose problems on location. OAM provides mechanisms to monitor link operation and health, and improve fault isolation.

The Mobility Access Switch OAM supports the following Link Fault Management Functionalities:

- Discovery – OAM-enabled local interface discovers remote interface enabled with OAM and notifies each other of own capabilities. After discovery, both sides send OAM PDUs periodically to monitor the link.
- Remote fault detection – Detection and handling of faulty link such as not receiving OAM PDU from the other peer within configured time-out or OAM PDU with “link-fault” flag.
- Remote loopback – Link segment testing controlled remotely using test frames. Usually remote loopback used during installation or for troubleshooting.

OAM is disabled by default. To enable OAM, you must create an OAM profile and apply it to a physical interface.

Creating an OAM Profile

OAM parameters are set by creating an OAM profile, which is a new type of interface profile.

```
(host) (config) # interface-profile oam-profile <oam-profile-name>
(host) (OAM profile "<oam-profile-name>") # ?
allow-loopback          Support OAM local loopback
clone                   Copy data from another OAM profile
discovery-mode          OAM discovery mode
link-fault-action       Action taken on link-fault detection
link-timeout            Timeout in seconds to declare link fault
no                       Delete Command
pdu-rate                Maximum OAM PDUs sent per second
remote-loopback        Put remote device into loopback mode
```

Table 21: OAM Profile Parameters Default Values

Parameter	Possible Values	Default Value
discovery-mode	Active, Passive	Active
remote-loopback	Enable, Disable	Disable
allow-loopback	Enable, Disable	Disable
pdu-rate	1 to10	5
link-timeout	2 to10	5
link-fault-action	Syslog, Error-disable	Error-disable

Sample Configuration

```
(host) (OAM profile "oam1") #allow-loopback
```

```
(host) (OAM profile "oam1") #link-fault-action syslog
(host) (OAM profile "oam1") #link-timeout 3
(host) (OAM profile "oam1") #pdu-rate 8

(host) (OAM profile "oam1") #show interface-profile oam-profile oam1

OAM profile "oam1"
-----
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
```

Applying an OAM Profile

Once you've created an OAM profile, you must apply it to physical interfaces.

```
(host) (config) #interface gigabitethernet 0/0/1
(host) (gigabitethernet "0/0/1") #oam-profile <oam-profile-name>
(host) (config) #interface gigabitethernet 0/0/2
(host) (gigabitethernet "0/0/2") #oam-profile <oam-profile-name>
```



You cannot simultaneously apply both OAM and tunneled node settings to an interface.



An OAM profile must be applied to each port channel member interface.

Applying OAM to each Port Channel Member

In this first example, the output of the **show interface port channel** command identifies **GE0/0/12** and **GE0/0/13** as member ports of port channel 4:

```
(host) (config) #show interface port-channel 4
port-channel 4 is administratively Up, Link is Up, Line protocol is Up
Hardware is Port-Channel, LACP enabled, Address is 00:0b:86:6a:70:c0
Description: Link Aggregate
Member port(s):
  GE0/0/12 is administratively Up, Link is Up, Line protocol is Up
  GE0/0/13 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
0 errors octets, 0 deferred
0 collisions, 0 late collisions

```

The commands in the example below apply an OAM profile to Port Channel Members **GE0/0/12** and **GE0/0/13**:

```

(host) (config) #interface gigabitethernet 0/0/12
(host) (gigabitethernet "0/0/12") #oam-profile oam1
(host) (gigabitethernet "0/0/12") #interface gigabitethernet 0/0/13
(host) (gigabitethernet "0/0/13") #oam-profile oam1
(host) (gigabitethernet "0/0/13") #

```

Related Show Commands

The following show commands display the status of OAM on your Mobility Access Switches.

The **show oam brief** command displays a quick overview of the ports on which OAM is enabled.

OAM Interface	Link-fault Mode	Loopback Action	Link Local	Oper 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

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 Interface	Error PDU Received	Unknown PDU Received	Total PDU Received	Transmit Transmitted	Discarded
GE0/0/1	295	0	0	295	0
GE0/0/2	295	0	0	295	0

Use the **clear counters oam** command to clear any OAM counters:

```
(host) #clear counters oam
```

The **show oam interface gigabitethernet** command displays the OAM profile and status on a specific port:

```

show oam interface gigabitethernet <slot/port/module>
GE0/0/1 is operationally Up, Link is Up
  OAM link-fault action is syslog
  Local loopback is Enable, Remote loopback is Disable
  OAM PDU rate is 8, Link timeout is 3
Local:
  MAC address is 00:0b:86:6a:4f:03, PDU size is 64
  MUX state is Forward, Parser state is Forward
  Discovery mode is Active, Discovery state Completed
  Local is stable, Locat is satisfied
Remote:
  MAC address is 00:0b:86:6a:4f:04, PDU size is 64
  MUX state is Forward, Parser state is Forward
  Discovery mode is Active
  Remote is stable, Remote is valid

```


The Mobility Access Switch supports IEEE 802.1Q VLANs. It supports MAC-based VLANs, tag-based VLANs, port-based VLANs, and voice VLANs. You can optionally configure an IP address and netmask for a VLAN for inband management.

This chapter includes the following topics:

- [VLANs Overview on page 133](#)
- [Creating VLANs on page 133](#)
- [Creating and Applying a Switching Profile to an Interface on page 135](#)
- [Deleting Switching Profile from an Interface on page 137](#)
- [Managing the MAC Address Table on page 138](#)
- [VLAN Profile on page 141](#)

VLANs Overview

The Mobility Access Switch supports the following types of VLANs:

- **MAC-based VLANs**—In the case of untrusted interfaces, you can associate a client to a VLAN based on the source MAC of the packet. Based on the MAC, you can assign a role to the user after authentication. For more information about how to assign MAC-based VLANs, see [MAC-Based Authentication on page 337](#).
- **Port-based VLANs**—In the case of trusted interfaces, all untagged traffic is assigned a VLAN based on the incoming port.
- **Tag-based VLANs**—In the case of trusted interfaces, all tagged traffic is assigned a VLAN based on the incoming tag.
- **Voice VLANs**—You can use the voice VLANs to separate voice traffic from data traffic when the voice and data traffic are carried over the same ethernet link. For more information on Voice VLANs, see [Voice VLANs on page 159](#).

Creating VLANs

By default, all the ports in the Mobility Access Switch are assigned to VLAN 1. You can create VLANs and assign ports to them.

Using the WebUI

1. Navigate to the **Configuration > VLANs** page.
2. Click **New** under the VLANs list.
3. Enter the **VLAN ID**.
4. Enter a Description for the VLAN.
5. Click **Apply** and **Save Configuration**.

Using the CLI

```
(host) (config) # 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>
mac-aging-time <minutes>
mld-snooping-profile <profile-name>
no {...}
pvst-profile <profile-name>
exit

```

Sample VLAN Configuration

```

(host)(config)# vlan 100
  description Faculty
  exit
(host)(config)# vlan 200
  description Students
  exit

```

Verifying VLAN Configuration

You can verify the VLANs created and the ports assigned to the VLANs using the following commands:

```
(host)# show vlan
```

```
VLAN CONFIGURATION
```

```

-----
VLAN  Description          Ports
----  -
1      All                    GE0/0/0-1 GE0/0/7 GE0/0/9-29 GE0/0/33
                                GE0/0/35-41 GE0/0/44-47
100    Faculty                GE0/0/0
101    Student                 GE0/0/0
102    Admin                    GE0/0/0
103    Finance                  GE0/0/0
104    HR                       GE0/0/0
105    Engineering              GE0/0/0
106    QA                       GE0/0/0
107    Support                  GE0/0/0
108    Marketing                GE0/0/0
109    Management                GE0/0/0

```

```
(host)# show vlan detail
```

```
U - Untagged member, T - Tagged member
```

```
* - Active interface
```

```
Dot1q tag: 1, Description: VLAN0001
```

```
Number of interfaces: 36, Active: 5
```

```
VLAN membership:
```

```
Access:
```

```

GE0/0/1(U) GE0/0/7(U) GE0/0/9*(U) GE0/0/10*(U)
GE0/0/11(U) GE0/0/12(U) GE0/0/13(U) GE0/0/14(U)
GE0/0/15(U) GE0/0/16(U) GE0/0/17(U) GE0/0/18(U)
GE0/0/19(U) GE0/0/20(U) GE0/0/21(U) GE0/0/22(U)
GE0/0/23(U) GE0/0/24(U) GE0/0/25(U) GE0/0/26(U)
GE0/0/27(U) GE0/0/28(U) GE0/0/29(U) GE0/0/33(U)
GE0/0/35(U) GE0/0/36(U) GE0/0/37(U) GE0/0/38(U)
GE0/0/39(U) GE0/0/40(U) GE0/0/41(U) GE0/0/44(U)
GE0/0/45*(U) GE0/0/46*(U) GE0/0/47*(U)

```

```
Trunk:
```

```
GE0/0/0(U) GE0/0/0(T)
```

```
Dot1q tag: 100, Description: Faculty
```

```
Number of interfaces: 1, Active: 0
```

```
VLAN membership:
```

```
Trunk:
```

```
GE0/0/0(T)
```

```
(host)# show vlan extensive
```

```

Dot1q tag: 1, Description: VLAN0001
IGMP-snooping profile name: igmp-snooping-factory-initial
IGMP-snooping: Enabled
IGMP-snooping proxy: Disabled
MSTP instance: 0
MAC aging time: 5 minutes
Number of interfaces: 36, Active: 5
VLAN membership:
  GE0/0/0    Trunk  Trusted  Untagged
  GE0/0/0    Trunk  Trusted  Tagged
  GE0/0/1    Access Trusted  Untagged
  GE0/0/7    Access Trusted  Untagged
  GE0/0/9*   Access Trusted  Untagged
  ....
Dot1q tag: 100, Description: Faculty
MSTP instance: 0
MAC aging time: 300
Number of interfaces: 1, Active: 0
VLAN membership:
  GE0/0/0    Trunk  Trusted  Tagged

```

(host)#show vlan summary

```

Number of tunneled-node VLANs      :2
Number of operational VLANs        :10

```

Creating and Applying a Switching Profile to an Interface

You can assign VLAN membership to the interface using the switching profile. The switching profile has the following types of configurations for a port:

- **Switch-Port Mode**—Specifies whether the port is an access port connected to an end device or a trunk port for uplink connectivity.
- **Access VLAN**—Specifies the VLAN ID for the port, when the switch-port mode is access.
- **Native VLAN**—Specifies the VLAN for incoming untagged packets, when the switch-port mode is trunk. When a packet goes out of a trunk interface in native VLAN, it will be untagged. By default, VLAN 1 is the native VLAN. The native VLAN should be part of the trunk allowed VLANs.
- **Trunk Allowed VLANs**—Identifies the VLAN IDs for which the trunk carries the traffic.

Using the WebUI

1. Navigate to the **Configuration > Ports > Switching** tab.
2. Under the profiles list, click **New**.
3. Enter a name for the new switching profile under the **Name** column.
4. Select a mode from the drop-down list. It can be either trunk or access.
5. If you selected the mode as access, select the Access VLAN from the drop-down list. Only the VLANs created already are listed.
6. If you selected the mode as trunk, select the Native VLAN from the drop-down list. Only the VLANs created already are listed.
7. If you selected the mode as Trunk, select the trunk allowed VLANs from the Allowed VLAN column.
8. Select the interfaces that are part of this VLAN in the Association column.
9. Click **Apply** and **Save Configuration**.

Using the CLI

```
(host)(config)# interface-profile switching-profile <profile-name>
```

```

access-vlan <VLAN-ID>
clone <source>
native-vlan <VLAN-ID>
switchport-mode {access|trunk}
trunk allowed vlan [add|all|except|remove] <VLANs-List>
storm-control-bandwidth <1-100>
storm-control-broadcast
storm-control-multicast
storm-control-unknown-unicast
no {...}
exit
(host)(config)# interface gigabitEthernet <slot/module/port>
switching-profile <profile-name>

```



If you do not specify a switch-port mode, the port will be in switch-port mode access implicitly. In the case of switchport-mode trunk, the native vlan has to be in the allowed vlan list if you want the port to receive and transmit on the native vlan.

Default Switching Profile

```
(host)# show interface-profile switching-profile default
```

```
switching profile "default"
```

```

-----
Parameter                               Value
-----
Switchport mode                          access
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

```

Sample Access Port Configuration

You can use the following steps to configure an interface as an access port that belongs to a particular VLAN:

1. Create a switching profile.
2. Apply the switching profile to the interface.

To configure a switching profile with access VLAN 200, use the following commands:

```

interface-profile switching-profile Student
access-vlan 200

```

To apply the switching-profile to the interface (gigabitEthernet 0/0/10), use the following commands:

```

interface gigabitEthernet 0/0/10
switching-profile Student
exit

```

Verifying the Switching Profile Configuration for the Interface

To verify the configuration, use one of the following commands:

```
(host) #show vlan
```

```
VLAN CONFIGURATION
```

```
-----
```

```
VLAN Description Ports
```

```

-----
1   VLAN0001   GE 0/0/0 GE 0/0/1 GE 0/0/11 GE 0/0/12
      GE 0/0/13 GE 0/0/14 GE 0/0/15 GE 0/0/16
      GE 0/0/17 GE 0/0/18 GE 0/0/19 GE 0/0/2

```

```
100 Faculty
200 Student GE 0/0/10
```

```
(host) #show interface gigabitethernet 0/0/0 switchport extensive
GE0/0/0
Link is Up
Flags: Access, Trusted
```

VLAN membership:

```
VLAN tag  Tagness  STP-State
-----  -
1          Untagged  FWD
```

Sample Trunk Port Configuration

To configure a trunk port, the switch-port mode should be set as trunk. To define the switching profile, use the following commands:

```
interface-profile switching-profile Upstream
  switchport-mode trunk
```

To apply the switching profile to the trunk ports, use the following commands:

```
interface gigabitethernet 0/0/11
  switching-profile Upstream
```

For trunk ports, there are times when the other side of the link requires traffic to be sent without any tags. This functionality is commonly referred as native VLAN. For this purpose, you can use the native-vlan parameter in the switching-profile:

```
interface-profile switching-profile Upstream
  native-vlan 100
```

By default, a trunk port allows all VLANs to be transported. You can change the allowed VLANs using the trunk allowed vlan parameter in the switching profile:

```
interface-profile switching-profile Upstream
  trunk allowed vlan all
```

Verifying the Trunk Configuration

You can use the following command to view the trunk configuration:

```
(host)# show trunk
Trunk Port Table
-----
Port          Vlans Allowed  Vlans Active  Native Vlan
----          -
GE 0/0/11 ALL          1,100,200    100
GE 0/0/12 2-45        2,30         45
```

Deleting Switching Profile from an Interface

Starting from ArubaOS 7.4.1, Mobility Access Switch introduces the **no switching-profile** command inside a tunnel to remove any switching-profile applied to the tunnel and point the tunnel back to the default switching-profile.

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
```

Verification of Switching-Profile Deletion

Execute the following **show interface tunnel** command to verify if any switching-profile applied to the tunnel is removed:

```
(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 output of **show interface tunnel** command displays the switching-profile as **default** when no switching profile is applied to the interface tunnel.

Managing the MAC Address Table

The Mobility Access Switch populates the MAC address table as a result of dynamic learning, static addition, Sticky MAC, and authentication process. These MACs are referred to as learnt, static, sticky, and auth MACs respectively. You can manage the MAC address table using the following tasks:

- [Adding Static MAC Addresses on page 138](#)
- [Displaying the MAC Address Table on page 139](#)
- [Displaying Sticky MAC Addresses on page 139](#)
- [Deleting the Static MACs on page 140](#)
- [Clearing the Learnt MACs on page 140](#)
- [Clearing Sticky MAC Addresses on page 140](#)
- [Configuring the MAC Aging Time on page 140](#)

Adding Static MAC Addresses

You can add static MAC addresses to a VLAN and thus to the MAC address table.

```
(host) (config) # vlan <vlan-id>
    mac-address-table static <mac-address> gigabitethernet <slot/module/port>
```

Example Configuration

```
(host) (config) # vlan 700
    description "vlan 700"
    aaa-profile default
    mac-aging-time 10
    mac-address-table static 00:01:02:03:04:05 gigabitethernet 0/0/14
    mac-address-table static 0a:0b:0c:0d:4e:0f gigabitethernet 0/0/16
(host) (config) # show vlan-config 700
VLAN "700"
-----
Parameter                Value
-----                -
Description                vlan 700
aaa-profile                default
igmp-snooping-profile     N/A
```

```

mld-snooping-profile      N/A
pvst-bridge-profile      predefinedprofile
MAC Aging time(Minutes)  10
Static mac address        00:01:02:03:04:05 gigabitethernet 0/0/14
Static mac address        0a:0b:0c:0d:4e:0f gigabitethernet 0/0/16

```

Displaying the MAC Address Table

```
(host)# show mac-address-table
```

```

Total MAC address: 3
Learnt: 1, Static: 1, Auth: 0, sticky: 1
MAC Address Table
-----

```

Destination Address	Address Type	VLAN	Destination Port
00:0b:86:0f:0a:80	Learnt	0226	GE0/0/42
00:10:db:00:00:11	Static	0201	GE0/0/0
00:00:cc:aa:1c:00	Sticky	0001	GE0/0/12

```
(host)# show mac-address-table interface gigabitethernet 0/0/19
```

```

Total MAC address: 1
Learnt: 1, Static: 0, Auth: 0
MAC Address Table
-----

```

Destination Address	Address Type	VLAN	Destination Port
00:0c:34:46:f2:52	Learnt	0100	GE0/0/19

```
(host)#show mac-address-table summary
```

```

Total MAC address: 3
Learnt: 3, Static: 0, Auth: 0, sticky: 0

```

```
(host)# show mac-address-table vlan 700
```

```

Total MAC address: 5
Learnt: 0, Static: 5, Auth: 0, sticky: 0

```

```
MAC Address Table
```

Destination Address	Address Type	VLAN	Destination Port
00:01:02:03:04:05	static	700	GE0/0/14
00:01:02:03:44:05	static	700	GE0/0/16
00:00:02:03:44:05	static	700	GE0/0/16
00:00:00:03:44:05	static	700	GE0/0/16
00:00:00:03:54:05	static	700	GE0/0/16

Displaying Sticky MAC Addresses

The following example displays Sticky MAC addresses on a switch:

```
(host) #show mac-address-table sticky
```

```

Total MAC address: 5
MAC Address Table
-----

```

Destination Address	Address Type	VLAN	Destination Port
00:00:cc:aa:1c:00	Sticky	0001	GE0/0/12
00:00:cc:aa:1c:01	Sticky	0001	GE0/0/12
00:00:cc:aa:1c:02	Sticky	0001	GE0/0/12
00:00:cc:aa:1c:03	Sticky	0001	GE0/0/12
00:00:cc:aa:1c:04	Sticky	0001	GE0/0/12

The following example displays Sticky MAC addresses on a VLAN

```
(host) #show mac-address-table vlan 2 sticky

Total MAC address: 5
MAC Address Table
-----
Destination Address  Address Type  VLAN  Destination Port
-----
00:00:cc:aa:1c:00   Sticky       0002  GE0/0/12
00:00:cc:aa:1c:01   Sticky       0002  GE0/0/12
00:00:cc:aa:1c:02   Sticky       0002  GE0/0/12
00:00:cc:aa:1c:03   Sticky       0002  GE0/0/12
00:00:cc:aa:1c:04   Sticky       0002  GE0/0/12
```

The following example displays Sticky MAC addresses on an interface:

```
(host) #show mac-address-table interface gigabitethernet 0/0/12 sticky
Total MAC address: 5
MAC Address Table
-----
Destination Address  Address Type  VLAN  Destination Port
-----
00:00:cc:aa:1c:00   Sticky       0001  GE0/0/12
00:00:cc:aa:1c:01   Sticky       0001  GE0/0/12
00:00:cc:aa:1c:02   Sticky       0001  GE0/0/12
00:00:cc:aa:1c:03   Sticky       0001  GE0/0/12
00:00:cc:aa:1c:04   Sticky       0001  GE0/0/12
```

Deleting the Static MACs

You can use the following command to delete the static MAC addresses from the MAC address table:

```
(host) (config) # vlan <vlan-id>
    no mac-address-table static <mac-address>
```

Clearing the Learnt MACs

You can use the following commands to clear the learnt MACs from the MAC address table:

```
(host) (config) # clear mac-address-table
(host) (config) # clear mac-address-table interface gigabitethernet 0/0/5
(host) (config) # clear mac-address-table vlan 20
(host) (config) # clear mac-address-table vlan 20 interface gigabitethernet 0/0/0
```

Clearing Sticky MAC Addresses

You can use the following commands to clear the Sticky MAC addresses from the MAC address table:

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

Configuring the MAC Aging Time

In the case of learnt MACs, you can configure the system to prune the MAC address if it does not get refreshed within the specified MAC aging time. The default value is 5 minutes. Use the following command to specify the MAC aging interval per VLAN:

```
(host) (config) # vlan <vlan-id>
```

```
mac-aging-time <minutes>
```

VLAN Profile

A VLAN Profile (as opposed to interface profile) can be created to enable/modify IGMP-Snooping, MLD-Snooping and PVST settings. You can use the `vlan-profile` command followed by the particular feature.

```
(host) (config) #vlan-profile
    dhcp-snooping-profile
    igmp-snooping-profile
    mld-snooping-profile
    pvst-profile
```

For more information on configuring and applying DHCP Snooping profile to a VLAN, see [Configuring DHCP Snooping on page 265](#).

For more information on configuring and applying IGMP Snooping profile to a VLAN, see [Creating and Applying an IGMP Snooping Profile to a VLAN on page 251](#).

For more information on configuring and applying MLD Snooping profile to a VLAN, see [Configuring MLD Snooping on page 257](#).

For more information on configuring and applying PVST profile to a VLAN, see [Configuring PVST+ on page 177](#).

The GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP) is an application defined in the IEEE 802.1Q standard that allows for the control of 802.1Q VLANs.

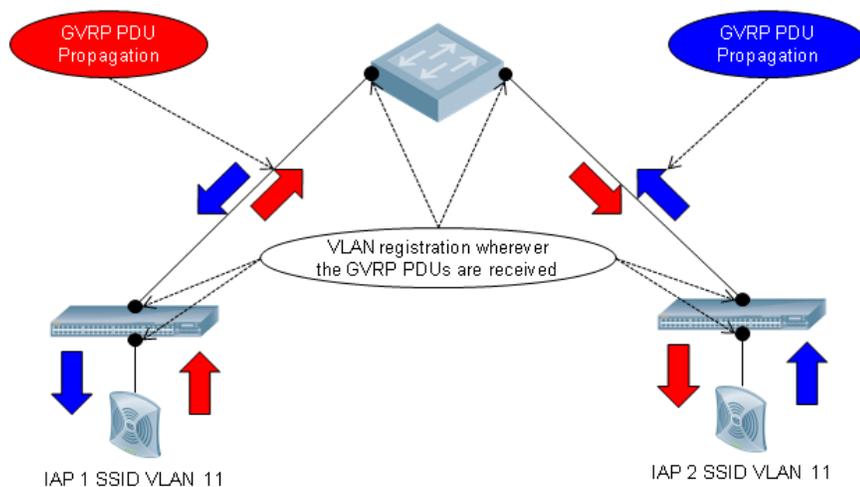
This chapter includes the following topics:

- [GVRP Overview on page 143](#)
- [Enabling and Configuring GVRP Functionality on page 143](#)
- [Sample Configurations on page 144](#)

GVRP Overview

Configuring GVRP in the Mobility Access Switch enables the switch to register/de-register the dynamic VLAN information received from a GVRP applicant such as an IAP in the network. GVRP support also enables the switch to propagate the registered VLAN information to the neighboring bridges in the network.

Figure 9 GVRP Overview



Limitation

The Mobility Access Switch does not register a GVRP VLAN on the STP blocked ports. When there is a change in the STP topology and the blocked ports become forward, the ports first register the VLAN and then the data traffic flow continues. In such conditions, there is a long delay in resuming the traffic.

Enabling and Configuring GVRP Functionality

To enable GVRP in the Mobility Access Switch, you must configure the following two profiles and attach them to a trunk port:

- `gvrp`—To enable GVRP globally.

- gvrp-profile—To enable GVRP on an interface.



You can enable GVRP only on trunk ports.

You can use the following CLI commands to define the GVRP global profile settings.

```
(host) (config) # gvrp
(host) (Global GVRP configuration) # enable
(host) (Global GVRP configuration) # join-time <milliseconds>
```

The join period timer controls the interval between the transmit PDU events that are applied to the applicant state machine. Default is 200 milliseconds.

```
(host) (Global GVRP configuration) # leave-time <milliseconds>
```

The leave period timer controls the period of time that the registrar state machine waits in the leaving state before transmitting to the empty state. Default is 600 milliseconds.

```
(host) (Global GVRP configuration) # leave-all-time <milliseconds>
```

The leave all period timer controls the frequency with which the leave all state machine generates LeaveAll PDUs. Default is 10000 milliseconds.

You can use the following CLI commands to define the interface specific gvrp-profile:

```
(host) (config) # interface-profile gvrp-profile <profile_name>
(host) (Interface GVRP profile <profile_name>) # registrar-mode [normal|forbidden]
```

In normal registrar mode, the Mobility Access Switch registers and de-registers VLANs to or from its connected switches and IAPs. In forbidden registrar mode, the Mobility Access Switch cannot register nor de-register VLANs to or from its connected switches and IAPs. The default registrar-mode is normal.

Sample Configurations

To enable and configure GVRP globally:

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

To enable and configure GVRP profile on an interface:

```
(host) (config) # interface-profile gvrp-profile Enable-GVRP
(host) (Interface GVRP profile "Enable-GVRP") # enable
(host) (Interface GVRP profile "Enable-GVRP") # registrar-mode normal
```

To attach GVRP profile to the interface:

```
(host) (config) # interface gigabitethernet 0/0/10
(host) (gigabitethernet "0/0/10") # gvrp-profile Enable-Gvrp
```

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 following example displays the interfaces in which gvrp is enabled:

```
(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

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 the global GVRP functionality: **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.

The Mobility Access Switch supports Link Layer Discovery Protocol (LLDP) to advertise identity information and capabilities to other nodes on the network, and store the information discovered about the neighbors. LLDP is also used to implement Voice VLAN configurations. For more information on Voice VLAN configuration, see [VoIP on page 159](#).

This chapter contains the following major sections:

- [Important Points to Remember on page 147](#)
- [LLDP on page 147](#)
- [LLDP-MED on page 152](#)
- [PoE Negotiation over LLDP on page 154](#)
- [Proprietary Link Layer Discovery Protocols on page 156](#)

Important Points to Remember

- Inventory-management, and Location TLVs are not currently supported.
- LLDP-MED must be enabled to advertise a VOIP VLAN.

LLDP

This section contains the following sections:

- [Understanding LLDP on page 147](#)
- [Configuring LLDP on page 149](#)

Understanding LLDP

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 a LAN. The Mobility Access Switch supports a simple one-way neighbor discovery protocol with periodic transmissions of LLDP PDU.

- LLDP frames are constrained to a local link.
- LLDP frames are TLV (Type-Length-Value) form.
- LLDP Multicast address is 01-80-C2-00-00-0E.

LLDP provides support for a set of attributes used to discover neighbor devices. These attributes are referred as TLVs which contain type, length, and value descriptions. LLDP supported devices use TLVs to receive and send information such as configuration information, device capabilities, and device identity to their neighbors.

The Mobility Access Switch supports the following optional basic management TLVs which are enabled by default:

- Aggregation status TLV
- MAC Phy configuration TLV
- Management address TLV
- Maximum frame size TLV
- Port-description TLV
- Port VLAN ID TLV
- Power management TLV

- System capabilities TLV
- System description TLV
- System name TLV
- VLAN name TLV

LLDP Factory Initial and Default Profiles

This section contains the following sections:

- [LLDP Factory Initial Profile on page 148](#)
- [Default LLDP Profile on page 148](#)

LLDP Factory Initial Profile

When the Mobility Access Switch is booted as factory-default for the first time, the "lldp-factory-initial" profile is associated to all the ports.

To display this information, use the following command:

```
(host)# show interface-profile lldp-profile lldp-factory-initial
LLDP Profile "lldp-factory-initial"
```

```
-----
```

Parameter	Value
-----	-----
LLDP pdu transmit	Enabled
LLDP protocol receive processing	Enabled
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	Enabled
Control proprietary neighbor discovery	Disabled

Default LLDP Profile

To display the default lldp profile information, use the following command:

```
(host)# show interface-profile lldp-profile default
```

```
LLDP Profile "default"
```

```
-----
```

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



When you use the default LLDP profile, the RX and TX parameters are disabled. You have to explicitly enable them for LLDP to work.

Configuring LLDP

- [Configuring an LLDP Profile on page 149](#)
- [Applying LLDP Profile to an Interface on page 149](#)

Configuring an LLDP Profile

To configure an LLDP profile, use the following command:

```
(host)(config)# interface-profile lldp-profile <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>}
no {...}
exit
```

Applying LLDP Profile to an Interface

To apply an LLDP profile to an interface, use the following command:

```
(host)(config)# interface gigabitethernet <slot/module/port>
  lldp-profile <profile-name>.
```



In the case of static and dynamic port-channels, the LLDP profile must be applied to the member interfaces.

Verifying LLDP Profile Configuration

```
(host)# show interface-profile lldp-profile <profile-name>
LLDP Profile "<profile-name>"
-----
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

Monitoring LLDP

This section describes commands for monitoring LLDP. It contains the following sections:

- [Display LLDP Interface on page 150](#)
- [Display LLDP Interface <interface> on page 150](#)
- [Display LLDP Neighbor on page 151](#)
- [Display LLDP Neighbor Interface Detail on page 151](#)
- [Display LLDP Statistics on page 152](#)
- [Display LLDP Statistics Interface on page 152](#)

Display LLDP Interface

To display all LLDP information for all interfaces, use the following command:

```
(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
GE0/0/6    Enabled  Enabled  Enabled    30            120
GE0/0/7    Enabled  Enabled  Enabled    30            120
GE0/0/8    Enabled  Enabled  Enabled    30            120
GE0/0/9    Enabled  Enabled  Enabled    30            120
GE0/0/10   Enabled  Enabled  Enabled    30            120
<output truncated>
```

Display LLDP Interface <interface>

To display LLDP information for a specific interface, use the following command:

```
(host) #show lldp interface gigabitethernet 0/0/1

Interface: gigabitethernet0/0/1
LLDP Tx: Enabled, LLDP Rx: Enabled
Proprietary Neighbor Discovery: Disabled
LLDP-MED: Enabled
```

Fast Transmit interval: 1, Fast Transmit message counter: 4
Transmit interval: 30, Hold timer: 120

Display LLDP Neighbor

```
(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

To view proprietary neighbors, use the **show neighbor-devices** command.



Display LLDP Neighbor Interface Detail

```
(host) (gigabitethernet "0/0/2") #show lldp neighbor interface gigabitethernet 0/0/1 detail
Interface: gigabitethernet0/0/1, Number of neighbors: 1
```

```
-----
Chassis id: 24.1.1.253, Management address: 24.1.1.253
Interface description: SW PORT, ID: 04C5A44C3485:P1
Device MAC: 04:c5:a4:4c:34:85
Last Update: Thu Oct 3 17:01:41 2013
Time to live: 180, Expires in: 179 Secs
System capabilities : Bridge,Phone
Enabled capabilities: Bridge,Phone
System name: SEP04C5A44C3485
System description:
Cisco IP Phone 7962G,V10, SCCP42.9-2-1S
Auto negotiation: Supported, Enabled
Autoneg capability:
100Base-X, HD: no, FD: yes
1000Base-T, HD: yes, FD: yes
Media attached unit type: 100BaseTXFD - 2 pair category 5 UTP, full duplex mode (16)
802.3 Power:
PortID:      local 04C5A44C3485:P1
PortDescr:   SW PORT
LLDP-MED:
Device Type: Communication Device Endpoint (Class III)
Capability:  LLDP-MED capabilities, Network policy, Extended power via MDI/PD, Inventory
LLDP-MED Network Policy for: AppType: 1, Defined: yes
Descr:      Voice
VLAN:      204
Layer 2 Priority: 5
DSCP Value: 46
LLDP-MED Network Policy for: AppType: 2, Defined: yes
Descr:      Voice Signaling
VLAN:      204
Layer 2 Priority: 4
DSCP Value: 32
Extended Power-over-Ethernet:
Power Type & Source: PD Device
```

```

Power Source: unknown
Power Priority: unknown
Power Value: 6300
Inventory:
Hardware Revision: 10
Software Revision: SCCP42.9-2-1S
Firmware Revision: tnp62.8-3-1-21a.bin
Serial Number: FCH1529F57D
Manufacturer: Cisco Systems, Inc.
Model: CP-7962G

```

Display LLDP Statistics

```
(host)# show lldp statistics
```

```

LLDP Statistics
-----
Interface  Received  Unknow TLVs  Malformed  Transmitted
-----
GE0/0/0    0         0             0           0
GE0/0/1    0         0             0           0
GE0/0/2    0         0             0           0
GE0/0/3    0         0             0           0
GE0/0/4    0         0             0           0
GE0/0/5    4         2             0           4
GE0/0/6    0         0             0           0
GE0/0/7    0         0             0           0
GE0/0/8    0         0             0           0
GE0/0/9    0         0             0           0
GE0/0/10   0         0             0           0
<output truncated>

```

Display LLDP Statistics Interface

```
(host)# show lldp statistics interface gigabitethernet 0/0/0
```

```

LLDP Statistics
-----
Interface                Received  Unknow TLVs  Malformed  Transmitted
-----
gigabitethernet0/0/0    0         0             0           0

```

LLDP-MED

This section contains the following sections:

- Understanding LLDP-MED
- Configuring LLDP-MED
- Verifying LLDP-MED



Starting from ArubaOS 7.4.1.5, the Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED) option in Mobility Access Switches is set to **auto** mode. This makes the Mobility Access Switch publish its LLDP-MED-related information to the neighbor only when it receives the LLDP-MED information from the neighbor. With this modification to LLDP-MED, the **med enable** and **no med enable** commands under **interface-profile lldp-profile <profile-name>** command remain deprecated from ArubaOS 7.4.1.5 release.

Understanding LLDP-MED

LLDP-MED (media endpoint devices) is an extension to LLDP developed by TIA (ANSI/TIA-1057) to support interoperability between VoIP endpoint devices and other networking end-devices. LLDP-MED is focused mainly on discovery running between network devices and endpoints such as IP phones.

LLDP-MED supports the following optional TLVs that are enabled by default:

- Network policy TLV
- Power management TLV

Configuring LLDP-MED

LLDP-MED network policy discovery lets endpoints and network devices advertise their VLAN IDs (e.g., voice VLAN), IEEE 802.1p, and DSCP values. The Mobility Access Switch can instruct end-devices to modify their settings to match VoIP requirements.

To configure the LLDP profile to enable LLDP-MED, use the following command:

```
(host)(config)# interface-profile lldp-profile <profile-name>
  lldp transmit
  lldp receive
  med enable
  med-tlv-select
(host)(config)# interface gigabitethernet 0/0/18
  lldp-profile <profile-name>
```



If the end devices connected to the Mobility Access Switch sends LLDP MED packets, then the Mobility Access Switch automatically responds with the LLDP MED packets irrespective of the LLDP MED configuration.

LLDP-MED Usage

In a converged network, LLDP-MED provides the following benefits:

- **Interoperability**
LLDP-MED offers vendor-independent management capabilities, enabling different convergence endpoints to interoperate on one network.
- **Automatic deployment of network policies**
With LLDP-MED, administrators can automatically deploy voice VLAN.



The default transmit interval time is 30 seconds and the default transmit hold timer is 120 seconds. You can change the transmit-interval and transmit-hold timer in the lldp-profile.

- **Location services**
LLDP-MED allows deploying location services.
- **Detailed inventory management capabilities**
For each converged device, LLDP-MED can supply model, manufacturer, firmware and asset information.
- **Advanced PoE**
LLDP-MED enables advanced Power over Ethernet capabilities.
- **IP telephony network troubleshooting**
LLDP-MED enables detection of speed and duplex mismatches, and of improper static voice policy configurations.
- **More security**
LLDP-MED runs after 802.1X to prevent unauthenticated devices from gaining access to the network.
- **Hardware Information**
For each converged device, LLDP-MED can supply model, manufacturer and firmware.
- **IP Telephony Network Troubleshooting**

The information from the device attached and information from our own device is available for the user to take corrective action.

Verifying the LLDP Profile Configuration to Check LLDP-MED Status

To verify the LLDP profile configuration and check LLDP-MED status, use the following command:

```
(host) (config) #show interface-profile lldp-profile <profile-name>
```

```
LLDP Profile "<profile-name>"
-----
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
```

PoE Negotiation over LLDP

Mobility Access Switch supports Power over Ethernet (PoE) negotiation over LLDP. By default, PoE negotiation is enabled on all the PoE interfaces of the Mobility Access Switch. The PoE negotiation happens either through LLDP or via LLDP MED packets.

To enable this feature on an interface not using default settings, you must configure the power management TLVs on both LLDP and LLDP MED packets.



Ensure that the LLDP transmit and receive processing is enabled on the LLDP profile.

Enabling PoE Negotiation on LLDP

You can use the following CLI commands to enable PoE negotiation on an LLDP profile:

```
(host) (config) # interface-profile lldp-profile PoE
(host) (LLDP Profile "PoE") #lldp transmit
(host) (LLDP Profile "PoE") #lldp receive
(host) (LLDP Profile "PoE") #lldp tlv-select power-management
(host) (LLDP Profile "PoE") #lldp med-tlv-select power-management
(host) (LLDP Profile "PoE") #interface gigabitethernet 0/0/26
(host) (gigabitethernet "0/0/26") #lldp-profile PoE
```

Verifying the Configuration

To verify if the PoE is enabled on the LLDP Profile, execute the following command:

```
(host) #show interface-profile lldp-profile PoE
LLDP Profile "PoE"
-----
Parameter                               Value
-----
LLDP pdu transmit                        Enabled
LLDP protocol receive processing         Enabled
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
```

Viewing PoE negotiation on a device

Use the following commands to view the power negotiated on a device through LLDP or LLDP MED:

```
(host) #show lldp neighbor interface gigabitethernet 0/0/26 detail
...
100Base-X, HD: no, FD: yes
1000Base-T, HD: yes, FD: yes
Media attached unit type: 100BaseTXFD - 2 pair category 5 UTP, full duplex mode (16)
802.3 Power:
PortID:      local D0574CF7E2FB:P1
PortDescr:   SW PORT
MDI Power:   supported: no, enabled: no
Power Port Class: PD
Port Power Classification: class 4
Power type:  2
Power Source: Primary power source
Power Priority: unknown
PD requested power Value: 10600
PSE allocated power Value: 20000
LLDP-MED:
Device Type: Communication Device Endpoint (Class III)
Capability:  LLDP-MED capabilities, Network policy, Extended power via MDI/PD, Inventory
LLDP-MED Network Policy for: AppType: 1, Defined: no
Descr:       Voice
Layer 2 Priority: 5
DSCP Value:  46
...

(host) # show neighbor-devices interface gigabitethernet 0/0/26 detail
Interface: gigabitethernet0/0/26, Number of neighbors: 1
-----
```

```
...
MDI Power:      supported: no, enabled: no
Power Port Class: PD
Port Power Classification: class 4
Power type:     2
Power Source:   Primary power source
Power Priority:  unknown
PD requested power Value: 10600
PSE allocated power Value: 20000
LLDP-MED:
Device Type:    Communication Device Endpoint (Class III)
Capability:     LLDP-MED capabilities, Network policy, Extended power via MDI/PD, Inventory
LLDP-MED Network Policy for: AppType: 1, Defined: no
Descr:         Voice
Layer 2 Priority: 5
DSCP Value:    46
LLDP-MED Network Policy for: AppType: 2, Defined: no
Descr:         Voice Signaling
Layer 2 Priority: 4
DSCP Value:    32
Extended Power-over-Ethernet:
Power Type & Source: PD Device
Power Source:   PSE
Power Priority:  unknown
Power Value:    2000
Inventory:
Hardware Revision: 1
Software Revision: sip9971.9-2-1
Firmware Revision: sboot9971.031610R1-9-2-1.sebn
Serial Number:  FCH142990H9
...
```

Proprietary Link Layer Discovery Protocols

This section contains the following sections:

- [Understanding Proprietary Link Layer Discovery Protocol on page 156](#)
- [Configuring Proprietary LLDP Receive Processing on page 157](#)
- [Verifying Proprietary LLDP Receive Processing on page 157](#)
- [Monitoring the Proprietary Neighbor Discovery on page 158](#)

Understanding Proprietary Link Layer Discovery Protocol

Network companies can also define their proprietary data link layer discovery protocol. For instance, Cisco Discovery Protocol (CDP) is a proprietary data link layer discovery protocol. CDP is similar to LLDP and is used to share information about other directly connected vendor-specific equipment. CDP runs on many of vendor-specific devices including routers, switches, and VoIP phones.

When there are devices in the network that do not support LLDP, you can use the `proprietary-neighbor-discovery` knob in the LLDP interface profile to turn on the ability to receive proprietary discovery protocol packets and identify the neighbors. Mobility Access Switch supports only CDP (Cisco Discovery Protocol) under proprietary protocols. You can use the `show neighbor-devices` command to display the neighbors identified using LLDP and CDP protocols.

CDP Receive Processing

The Mobility Access Switch processes CDP frames that are received from CDP-supported devices. However, the Mobility Access Switch only receives CDP frames and does not forward CDP frames to other connected

neighbors/devices. When new CDP information is received from an existing neighbor, the Mobility Access Switch updates the information and discards the existing information.

CDP Frame Information

The CDP frame contains the following information:

- Device ID
- IP Address
- Port ID
- Capabilities
- Software Version
- Platform
- Native VLAN

Configuring Proprietary LLDP Receive Processing

Priority LLDP receive processing is configured under LLDP profile:

```
(host) (config) #interface-profile lldp-profile CDP-PROC
(host) (LLDP Profile "CDP-PROC") #proprietary-neighbor-discovery
(host) (LLDP Profile "CDP-PROC") #exit
```

The configured LLDP/CDP-PROC profile needs to be applied to the interface:

```
(host) (config) #interface gigabitethernet 2/0/23
(host) (gigabitethernet "2/0/23") #lldp-profile CDP-PROC
(host) (gigabitethernet "2/0/23") #exit
```

Verifying Proprietary LLDP Receive Processing

Proprietary LLDP receive processing configuration profile can be verified with the following command:

```
(host) #show interface-profile lldp-profile CDP-PROC
LLDP Profile "CDP-PROC"
```

```
-----
Parameter                               Value
-----
LLDP pdu transmit                        Disabled
LLDP protocol receive processing         Disabled
LLDP transmit interval (Secs)           30
LLDP transmit hold multiplier            4
LLDP fast transmit interval (Secs)       30
LLDP fast transmit counter                1
LLDP-MED protocol                        Disabled
Control proprietary neighbor discovery    Enabled
```

CDP-enabled neighboring devices can be viewed by following CLI command:

```
(host) #show neighbor-devices
Neighbor Devices Information
```

```
-----
Local Intf  Chassis ID          Protocol  Remote Intf          Expiry-Time (Secs)
-----
GE2/0/22    SEP002414B211B3     CDPv2    GigabitEthernet0/22  44
GE2/0/23    SEP00254593BFD8     CDPv2    Port 1                166
```

```
System name
```

```
-----
SEP002414B211B3.cisco.com
SEP00254593BFD8.cisco.com
```

```

Number of neighbors: 2
(host) #show neighbor-devices interface gigabitethernet 2/0/23
Neighbor Devices Information
-----
Local Intf   Chassis ID           Protocol  Remote Intf  Expiry-Time (Secs)
-----
GE2/0/23    SEP00254593BFD8     CDPv2    Port 1       137

System name
-----
SEP00254593BFD8.cisco.com

```

```

Number of neighbors: 1
(host) #show neighbor-devices interface gigabitethernet 2/0/23 detail

```

```

Interface: GE2/0/23, Number of neighbors: 1
-----
Chassis id: SEP00254593BFD8, Protocol: CDPv2
Management address: 5.5.5.21
Interface description: Port 1, ID: Port 1
Last Update: Sat Oct 1 14:24:43 2011
Time to live: 180, Expires in: 170 Secs
System capabilities :
Enabled capabilities:
System name: SEP00254593BFD8
System description:
  SCCP41.8-4-4S
Duplex: full

```

Monitoring the Proprietary Neighbor Discovery

You can use the following commands to display the neighbors discovered using the proprietary protocols such as CDP:

```

(host)# show neighbor-devices
(host)# show neighbor-devices interface gigabitethernet 0/0/1
(host)# show neighbor-devices interface gigabitethernet 0/0/1 detail

```

The Mobility Access Switch supports certain Voice functionalities.

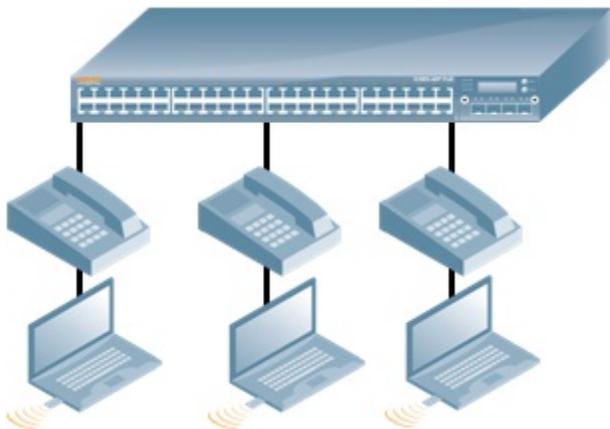
This chapter includes the following topics:

- [Voice VLANs on page 159](#)
- [Creating and Applying VoIP Profile to an Interface on page 160](#)
- [VoIP Auto-Discovery on Trusted Ports on page 160](#)
- [VoIP Auto-Discovery on Untrusted Ports on page 161](#)

Voice VLANs

The VoIP VLAN feature enables access ports to accept both untagged (data) and tagged (voice) traffic from IP phones connected directly to the Mobility Access Switch and separate these traffic into different VLANs (namely data VLAN and voice VLAN). You can configure a voice VLAN using the `voip-profile`.

The dot1p and DSCP values in the VoIP profile are communicated to the phone using LLDP. VoIP profile does not affect the QoS behavior on the switch. The QoS behavior depends on the QoS configuration on the port.



The following guidelines and limitations must be considered before creating a VoIP profile:

- If the port is configured as QoS trusted then the phone is expected to mark the DSCP and dot1p fields accordingly.
- To enable separate QoS treatment for the voice traffic ingressing an interface, you can either enable QoS Trust on the interface or apply the QoS-profile to the interface/access-list/user-role. For more information, see [Quality of Service on page 283](#).
- Voice VLAN can be applied only to the access ports.
- Trunk ports and port-channels are not allowed to be part of a voice VLAN.
- You cannot assign a VoIP profile to untrusted interfaces. In the case of untrusted interfaces, the phone derives the voip-vlan from the role that is assigned to the phone after authentication.
- LLDP-MED instructs the attached VoIP phones to use the specified voice VLAN ID, 802.1p, and DSCP values. For details about configuring an LLDP profile, refer to [Link Layer Discovery Protocols on page 147](#).

Creating and Applying VoIP Profile to an Interface

You can create and apply a VoIP profile to an interface using the following set of commands:

```
(host) (config) # interface-profile voip-profile <profile-name>
  clone <source>
  no{...}
  voip-dot1p <priority>
  voip-dscp <value>
  voip-vlan <VLAN-ID>
(host) (config) # interface gigabitethernet <slot/module/port>
  voip-profile <profile-name>
```

VoIP Auto-Discovery on Trusted Ports

ArubaOS provides support for VoIP Auto-discovery (also referred as CDP Fingerprinting) to discover the VoIP phones using neighbor discovery protocols (such as LLDP-MED and CDP) and assign Voice VLAN to the traffic originating from the phone. For more information on LLDP-MED, see [Link Layer Discovery Protocols on page 147](#).

You can configure VoIP either in static mode or auto-discover mode. By default, VoIP is configured in static mode. When VoIP operates in static mode, the phone is expected to know the Voice VLAN to be used and send the Voice traffic with the Voice VLAN tag. This is achieved, only if the Voice VLAN is configured statically on the phone or propagated to the phone using LLDP-MED.

In auto-discover mode, when LLDP-MED or CDP discovers a phone, the switch creates a rule to associate all the traffic originating from the phone to the Voice VLAN. Hence, the Voice VLAN need not be configured statically on the phone. The Voice VLAN can be tagged or untagged depending on the LLDP-MED configuration.

VoIP configured in auto-discover mode applies the Voice VLAN only to the first neighbor discovered in an interface. If both LLDP-MED and CDP neighbors are discovered, the preference is always given to the first LLDP-MED neighbor even if a CDP neighbor is already associated.

Enabling VoIP Auto-Discovery

You can use the following CLI command to enable VoIP in auto-discover mode:

```
(host) (config) #interface-profile voip-profile VOIP-1
(host) (VOIP profile "VOIP-1") #voip-mode auto-discover
(host) (VOIP profile "VOIP-1") #voip-vlan 5
```



You must enable the LLDP-profile with proprietary-neighbor-discovery/LLDP on the respective interface to identify the CDP/LLDP enabled phones.

You can enable proprietary-neighbor-discovery on an LLDP profile:

```
(host) (config) #interface-profile lldp-profile LLDP-1
(host) (LLDP Profile "LLDP-1") #lldp transmit
(host) (LLDP Profile "LLDP-1") #lldp receive
(host) (LLDP Profile "LLDP-1") #med enable
(host) (LLDP Profile "LLDP-1") #proprietary-neighbor-discovery
```

You can apply the configured LLDP-1 profile to an interface:

```
(host) (config) #interface gigabitethernet 0/0/0
(host) (gigabitethernet "0/0/0") #lldp-profile LLDP-1
(host) (gigabitethernet "0/0/0") # voip-profile VOIP-1
```

Verifying VoIP Mode Configuration

You can use the following command to verify the VoIP mode configuration on a VoIP profile:

```
(host) (config) #show interface-profile voip-profile VOIP-1

VOIP profile "VOIP-1"
-----
Parameter  Value
-----  -
VOIP VLAN  5
DSCP       46
802.1 UP   6
VOIP Mode auto-discover
```

Viewing Neighboring Phones

You can use the following command to view the neighboring phones in the network and the Voice VLAN associated with the phones:

```
(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
```

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.

VoIP Auto-Discovery on Untrusted Ports

Mobility Access Switch automatically discovers the Cisco Discovery Protocol (CDP) phones on an untrusted interface and assigns a VoIP VLAN to the phone.

Complete the following steps to place a non-802.1x CDP phone in a VoIP VLAN by using a user derivation rule (UDR) to match **device-type**:

1. Create an LLDP profile.

```
(host) (config) #interface-profile lldp-profile ciscophones
(host) (LLDP Profile "ciscophones") #proprietary-neighbor-discovery
```

2. Create a VoIP profile.

```
(host) (config) #interface-profile voip-profile phone
(host) (VOIP profile "phone") #voip-vlan 100
```

3. Create a user-role and add the previously created VoIP profile to that role.

```
(host) (config-role) #user-role phonerole
(host) (config-role) #access-list stateless allowall-stateless
(host) (config-role) #voip-profile phone
```

4. Create a UDR and add the phone role.

```
(host) (config) #aaa derivation-rules user phoneudr
(host) (user-rule) #set role condition device-type equals "phone" set-value phonerole
```

5. Add the UDR to a AAA profile.

```
(host) (config) #aaa profile phone_client
(host) (AAA Profile "phone_client") #user-derivation-rules phoneudr
```

6. Attach the LLDP profile and AAA profile to a port.

```
(host) (config) #interface gigabitethernet 0/0/2
(host) (gigabitethernet "0/0/2") #lldp-profile ciscophones
(host) (gigabitethernet "0/0/2") #aaa-profile phone_client
```

Alternatively, you can define the UDR for a VLAN assignment using the following command:

```
(host) (config) #aaa derivation-rules user <rule-name>
(host) (user-rule) #set vlan condition device-type equals phone set-value <vlan-id>
[position <priority> | description <descr>]
```



It is recommended to configure the UDR for the CDP phones that do not support LLDP or 802.1x authentication on an untrusted interface.

The implementation of Multiple Spanning Tree Protocol (MSTP) is based on the IEEE Standard 802.1D-2004 and 802.1Q-2005. In addition, MSTP supports the loopguard, rootguard, bpduguard, and portfast features.



To enable MSTP, use the spanning tree mode command.

MSTP maps a group of Virtual Local Area Networks (VLANs) to a reduced number of spanning tree instances. This allows VLAN bridges to use multiple spanning trees. This protocol enables network traffic from different VLANs to flow through different potential paths within a bridged VLAN. Because most networks do not need more than a few logical topologies, MSTP provides design flexibility as well as better overall network resource utilization.

Layer 2 networks typically use multiple paths and link redundancies to handle node and link failures. By definition, spanning tree uses a subset of the available physical links in its active logical topology to provide complete connectivity between any pair of end hosts. This chapter covers:

- [Important Points to Remember on page 163](#)
- [Example MSTP Configuration on page 163](#)
- [Loopguard and Rootguard on page 166](#)
- [Bridge Protocol Data Unit \(BPDU\) Guard on page 168](#)
- [Portfast on page 169](#)
- [Bridge Protocol Data Unit \(BPDU\) Filter on page 170](#)
- [Sample MSTP Topology and Configuration on page 171](#)

Important Points to Remember

- Configure MSTP using the command line only.
- Portfast, Loopguard, BPDUGuard, and Rootguard are disabled by default.
- MSTP allows users to map a set of VLANs to a MSTP instance.
- MSTP allows formation of multiple spanning tree regions and each region can run multiple instances.
- For two switches to be in the same MSTP region, they must share the same name, the same version, and the same VLAN instance mapping.
- If a Mobility Access Switch receives RSTP/STP control packets from a neighbor, the neighbor is considered to be in a different region. For the RSTP/STP neighbor, the entire MSTP region looks like a single bridge.
- You can perform proper load balancing across redundant links using MSTP instances. The ability to configure the port cost and port priority values also provides you with the flexibility to determine the links that are chosen to carry the traffic.
- State machines (SM), as defined by the IEEE, get the port and instance information as input. As output, SMs provide the port-state for each port in every instance.

Example MSTP Configuration

Basic MSTP configuration includes setting the spanning tree mode to MSTP, entering the global MSTP mode, and assigning a region name.

1. Set the spanning tree mode:

```
(host) (config) #spanning-tree mode mstp
```

2. Verify the spanning tree mode:

```
(host) (config) #show spanning-tree-profile
```

```
spanning-tree
-----
Parameter          Value
-----
spanning-tree-mode mstp
```

3. Assign a region name:

```
(host) (Global MSTP) #region-name mstpotechpubs
```

There are, of course, other MSTP options you can configure (such as forward delay, hello time). You can view the current MSTP configuration values using the **show mstp-global-profile** command.

```
(host) # show mstp-global-profile
```

```
Global MSTP
-----
Parameter          Value
-----
MSTP region name   mstpotechpubs
MSTP revision      0
Instance bridge priority 1 4096
Instance vlan mapping 1 801-802
MSTP hello time    2
MSTP forward delay 15
MSTP maximum age   20
MSTP max hops      20
```

To view the interface MSTP configuration values, use the **show interface-profile mstp-profile** command:

```
(host) (config) #show interface-profile mstp-profile
```

```
Interface MSTP List
-----
Name           References  Profile Status
-----
default        14
mstp_cost      3
techpubs       2
Total:4
```

To view the interface-profile named 'mstp_cost', use the **show interface-profile mstp_cost** command:

```
(config) #show interface-profile mstp-profile mstp_cost
```

```
Interface MSTP "mstp_cost"
-----
Parameter          Value
-----
Instance port cost 0 100
Instance port cost 1 200
Instance port cost 2 300
Instance port priority N/A
Enable point-to-point Disabled
Enable portfast     Disabled
Enable rootguard    Disabled
Enable loopguard    Disabled
```

Viewing Operational Information

To view MSTP operational information, use the **show spanning-tree interface all detail** command (the following is a partial output)

```
(host) #show spanning-tree mstp interface all detail

(GE0/0/23) of MST 0 is designated forwarding
Port path cost 20000, Port priority 128, Port identifier 128.24
Designated Root ID priority: 32768, Address: 000b.866a.f240
Designated Bridge ID priority: 32768, Address: 000b.866a.f240
Number of transitions to forwarding state: 1
Link type is point-to-point by default, Internal
BPDU sent: 108, Received: 9
Edge mode: Disabled
Root guard: Disabled
Loop guard: Disabled
(GE0/0/23) of MST 4 is designated forwarding
Port path cost 20000, Port priority 128, Port identifier 128.24
Designated Root ID priority: 32768, Address: 000b.866a.f240
Designated Bridge ID priority: 32768, Address: 000b.866a.f240
Number of transitions to forwarding state: 1
Link type is point-to-point by default, Internal
BPDU sent: 104, Received: 5

(GE1/0/22) of MST 0 is designated forwarding
Port path cost 20000, Port priority 128, Port identifier 128.167
Designated Root ID priority: 32768, Address: 000b.866a.f240
Designated Bridge ID priority: 32768, Address: 000b.866a.f240
Number of transitions to forwarding state: 1
Link type is point-to-point by default, Internal
BPDU sent: 107, Received: 8
Edge mode: Disabled
Root guard: Disabled
Loop guard: Disabled
(GE1/0/22) of MST 4 is designated forwarding
Port path cost 20000, Port priority 128, Port identifier 128.167
Designated Root ID priority: 32768, Address: 000b.866a.f240
Designated Bridge ID priority: 32768, Address: 000b.866a.f240
Number of transitions to forwarding state: 1
Link type is point-to-point by default, Internal
BPDU sent: 104, Received: 4
...
```

Or use the **show spanning-tree msti all detail** command (partial).

```
(host) #show spanning-tree mstp msti all 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

For a more complete listing of MSTP commands, refer to the *ArubaOS 7.4.x Command Line Reference Guide*.

Loopguard and Rootguard

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).



Loopguard configuration is mutually exclusive with Rootguard configuration.

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



Best practices is that loopguard be used on non-designated ports.

Configuring Loopguard

Below is a basic configuration for loopguard using the profile name *techpubs*.

```
(host) (config) #interface-profile mstp-profile techpubs
(host) (Interface MSTP "techpubs") #loopguard
(host) (Interface MSTP "techpubs") #
```

Associate the above mstp-profile to the interface:

```
(host) (config) #interface gigabitethernet 0/0/2
(host) (gigabitethernet "0/0/2") #mstp-profile techpubs
(host) (gigabitethernet "0/0/2") #
```

Verify the loopguard configuration:

```
(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 <-- loopguard on GE0/0/2
GE0/0/22  Root      FWD    128.23  20000  P2p

```

Verify that loopguard is applied to the interface:

```

(host) #show spanning-tree mstp interface gigabitethernet 0/0/2 detail

(GE0/0/2) of MST 0 is loop inconsistent blocking
Port path cost 20000, Port priority 128, Port identifier 128.3
Designated Root ID priority: 4097, Address: 0019.0655.3a80
Designated Bridge ID priority: 16384, Address: 000b.866c.3200
Number of transitions to forwarding state: 1
Link type is point-to-point by default, Boundary
BPDU sent: 15, Received: 36
Edge mode: Disabled
Root guard: Disabled
Loop guard: Enabled <-- loopguard enabled

```

Configuring Rootguard

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 rootguard be used on designated ports.

Below is a basic configuration for rootguard using the profile name **techpubs**.

```

(host) (config) #interface-profile mstp-profile techpubs
(host) (Interface MSTP "techpubs") #rootguard
(host) (Interface MSTP "techpubs") #

```

Associate the above mstp-profile to the interface:

```

(host) (config) #interface gigabitethernet 0/0/1
(host) (gigabitethernet "0/0/1") #mstp-profile techpubs
(host) (gigabitethernet "0/0/1") #

```

If a downstream bridge starts advertising itself as root without rootguard enabled, MSTP will accept that bridge as root. With rootguard enabled, it guards the root and prevents bridges from neighboring networks from becoming the root.

Verify the rootguard configuration:

```

(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    Altn(Root-Inc) BLK    128.22   20000  P2p <---rootguard on GE0/0/1
GE0/0/2    Desg          FWD    128.301  20000  P2p
GE0/0/22   Root          FWD    128.23   20000  P2p

```

Use the **show interface-profile mstp-profile** command to view the status of loopguard and rootguard.

```
(host) #show interface-profile mstp-profile techpubs
Interface MSTP "techpubs"
-----
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
```

Bridge Protocol Data Unit (BPDU) Guard

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.

Enabling and Configuring BPDU Guard Functionality

BPDU guard can be enabled or disabled at an interface level. By default, the BPDU is disabled. The BPDU guard functionality is configured as part of the `mstp-profile` configuration.

You can use the following command to configure the BPDU guard by using the MSTP profile:

```
(host) (config) #interface-profile mstp-profile <profile-name>
    bpduguard
    auto-recovery-time <recovery-time>
```

The following example shows how to enable and configure BPDU guard :

```
(host) (config) # interface-profile mst-profile BPDU-Guard1
    bpduguard auto-recovery-time 60
```



You can configure BPDU guard with or without the **auto-recovery-time** option.

You can disable BPDU guard by using the following command:

```
(host) (config) #interface-profile <profile-name> no bpduguard
```

You can disable the auto recovery time by using the following command:

```
(host) (Interface MST "profile-name") #bpduguard no auto-recovery-time
```

Verifying the BPDU Guard Configuration

```
(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 ←——BPDU guard is enabled
Enable bpduguard auto recovery time N/A
```

Sample Configuration

To enable and configure BPDU guard using the MSTP profile:

```
(host) (config) # interface-profile mstp-profile BPDU-Guard1
  bpduguard auto-recovery-time 60
```

To attach the MSTP profile to the interface:

```
(host) (config) # interface gigabitethernet <0/0/6>
  mstp-profile BPDU-Guard1
```

Portfast

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 “speak” 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.



The portfast is mutually exclusively with the Loopguard feature.

Configuring Portfast

To immediately transition the bridge port into the forwarding state upon linkup, enable the MSTP Portfast feature.

```
(host) (config) #interface-profile mstp-profile portfast_techpubs
(host) (Interface MSTP "portfast_techpubs") #portfast
```

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



The portfast is operational on both access ports and trunk ports.

Associate the above mstp-profile to the interface:

```
(host) (config) #interface gigabitethernet 0/0/1
(host) (gigabitethernet "0/0/1") #mstp-profile portfast_techpubs
(host) (gigabitethernet "0/0/1")
```

Use the following command to enable the portfast support on a trunk port:

```
(host) (config) #interface-profile mstp-profile portfast_techpubs
(host) (Interface MSTP "portfast_techpubs") #portfast trunk
```

Use the **show interface-profile** command to view the status of Portfast.

```
(host) (config) #show interface-profile mstp-profile portfast_techpubs
```

```
Interface MSTP "portfast_techpubs"
-----
Parameter          Value
-----
Instance port cost  N/A
Instance port priority N/A
Enable point-to-point Disabled
Enable portfast     Enabled
Enable rootguard    Disabled
Enable loopguard    Disabled
```

Bridge Protocol Data Unit (BPDU) Filter

The Mobility Access Switch provides support for Bridge Protocol Data Units (BPDU) filtering. By default, BPDU filter is disabled on all interfaces. You can configure the BPDU filter in one of the following modes:

- **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.



The default BPDU filter is applicable only for portfast enabled interfaces.

- **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.



If the ports configured with unconditional BPDU filter are connected to hubs, concentrators, switches, or bridges, it may cause bridging loops. Hence, it is recommended to connect the ports only to single hosts when unconditional BPDU filter is enabled.

Configuring BPDU Filter

You can configure the BPDU filter on an MSTP or a PVST profile and apply it to an interface using the CLI.

Use the following CLI commands to enable the BPDU filter on an MSTP profile:

```
(host) (config) # interface-profile mstp-profile <profile-name>
```

To enable default BPDU Filter, execute the following command:

```
(host) (Interface MSTP "<profile-name>") # portfast
(host) (Interface MSTP "<profile-name>") # bpdufilter default
```

To enable unconditional BPDU Filter, execute the following command:

```
(host) (Interface MSTP "<profile-name>") # bpdufilter unconditional
```



You can also configure the BPDU filter on a PVST profile similar to the MSTP profile.

Sample configuration

To enable default BPDU filter on the interface 0/0/1, execute the following commands:

```
(host) (config) # interface-profile mstp-profile profile-1
(host) (Interface MSTP "profile-1") # portfast
(host) (Interface MSTP "profile-1") # bpdufilter default
(host) (Interface MSTP "profile-1") # exit
(host) (config) # interface gigabitethernet 0/0/1
(host) (gigabitethernet "0/0/1") # mstp-profile profile-1
```

Verifying BPDU Filter Configuration

Use the following CLI command to verify the BPDU filter configuration:

```
(host) (config) #show interface-profile mstp-profile profile-1
Interface MSTP "profile-1"
-----
Parameter                               Value
-----
Instance port cost                       N/A
Instance port priority                   N/A
```

```

point-to-point           Disabled
portfast                 Enabled
portfast on trunk       Disabled
rootguard                Disabled
loopguard                Disabled
bpduguard                Disabled
bpduguard auto recovery time N/A
bpdufilter unconditional disabled
bpdufilter default      Enabled

```

Viewing Spanning Tree Information

Use the following command to view the spanning tree information on a BPDU filter enabled interface:

```

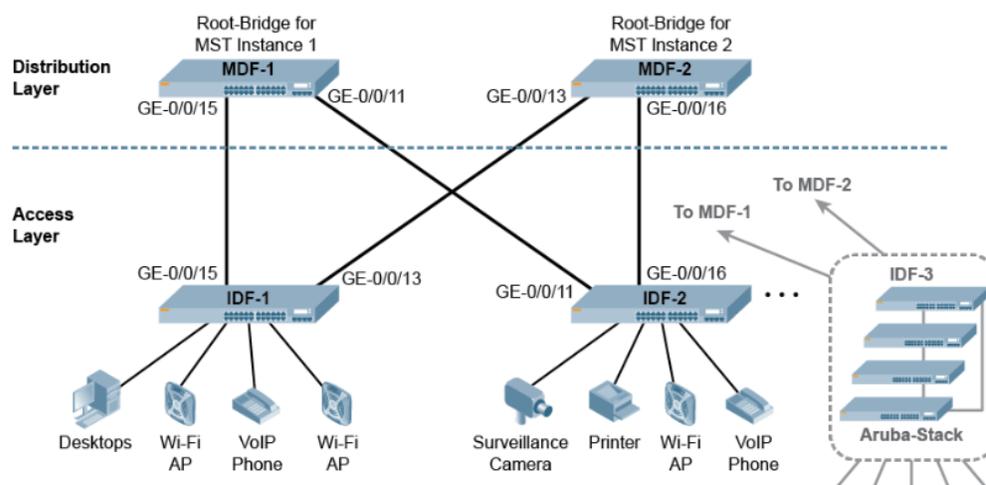
(host) (config) # show spanning-tree mstp interface gigabitethernet 0/0/1 detail
(GE0/0/1) of MST 0 is root forwarding
Port path cost 20000, Port priority 128, Port identifier 128.1
Designated Root ID priority: 4096, Address: 000b.866a.4000
Designated Bridge ID priority: 32768, Address: 001a.1e0e.1880
Number of transitions to forwarding state: 1
Link type is point-to-point by default, Internal
BPDU sent: 11, Received: 0
Port Fast: OperEdge
Root guard: Disabled
Loop guard: Disabled
Bpdu guard: Disabled
Bpdu guard auto recovery time: 0
Bpdu filter (unconditional): Disabled
Bpdu filter: Enabled

```

Sample MSTP Topology and Configuration

The following figure shows a sample topology reference to explain how multiple MST instances can be used to load-balance multiple VLANs across redundant links, which results in effectively increasing the bandwidth availability.

Figure 10 *MSTP Topology*



In [Figure 10](#), there are two switches in “Distribution Layer” labelled MDF-1 and MDF-2. Two switches are in the “Access layer” labelled IDF-1 and IDF-2. Access switches are connected to Distribution switches in a redundant, dual-homed fashion to provide high-availability. However, this potentially creates loops in this network.

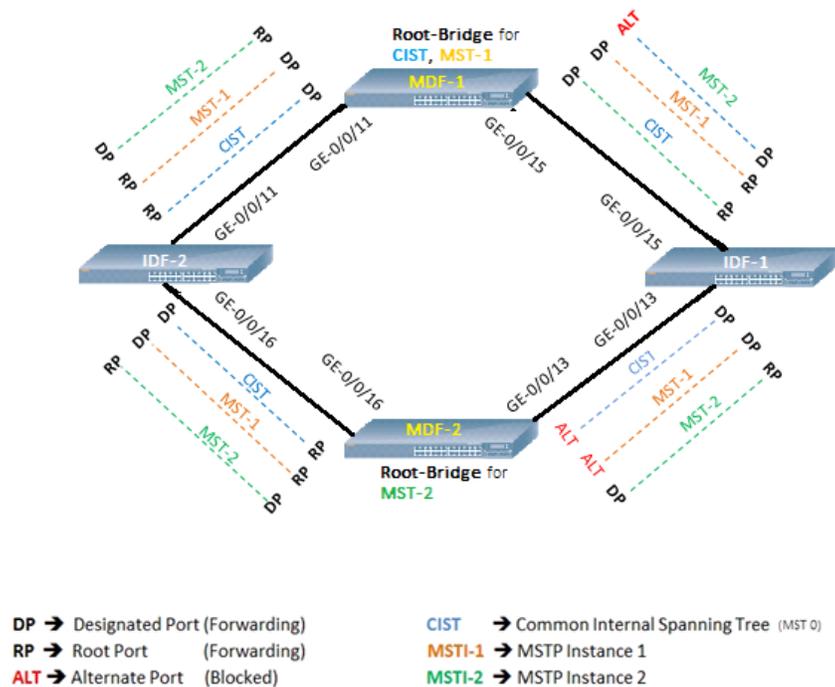
But from further examination of the diagram, one can find that all the loops are broken. Each MST instance forms its own "Logical Tree" ensuring there is no loop in its logical tree. Basically, same physical port which could be in 'forwarding' state for some MST instances can become 'blocking' for some other instance. That is, MST instances provide different paths for different VLANs, thus facilitating better load-sharing across redundant links.

For simplicity, this example is restricted to 'Single Region' and 'two MST-instances' encompassing 'four VLANs'. The preceding four-box topology that includes MDF-1, MDF-2, IDF-1, IDF-2 can be represented as follows:



To get clarity and for easy understanding of loops in CIST, MST-1, MST-2, ports and connections remain exactly the same as in the previous figure.

Figure 11 MSTP Topology - Alternative Representation



Configuration

The following configuration is a common configuration that can be copied to all the switches.

Create four VLANs and switching profile:

- VLAN 100 -> EMPLOYEE-VLAN
- VLAN 200 -> GUEST-VLAN
- VLAN 300 -> PHONE-VLAN
- VLAN 400 -> AP-VLAN

The configuration for all four switches is as follows:

```
(host) (config) #vlan 100 description EMPLOYEE-VLAN
(host) (config) #vlan 200 description GUEST-VLAN
(host) (config) #vlan 300 description PHONE-VLAN
(host) (config) #vlan 400 description AP-VLAN
(host) (config) #
(host) (config) #interface-profile switching-profile Trunk
(host) (switching profile "Trunk") #switchport-mode trunk
```

```
(host) (switching profile "Trunk") #trunk allowed vlan 100,200,300,400
```

Individual Switch Configuration

The individual switch configuration is as follows:

- Apply the previously created 'switching profile' to all the trunk-ports (inter-connecting switches)
Instead of configuring on individual ports, create an interface-group to include all the applicable ports and then apply the switching profile.
- Configure 'MSTP' global configuration. Mention the following:
 - provide region-name (REG-1)
 - create two MST-instances (1 and 2)
 - perform instance-VLAN mapping (instance-1 mapped to VLANs 100,200. And instance-2 mapped to VLANs 300,400.)
- Configure bridge-priority for each of the instances, possibly such that physically separate switches become 'root-bridge' for different instances.
 - This needs substantial planning that ensures higher port-bandwidth utilization

In the following sample, MDF-1 and MDF-2 are configured in the following fashion:

- MDF-1 becomes root-bridge for MSTI-1 and MSTI-0 (CIST)
- MDF-2 becomes root-bridge for MSTI-2

MDF-1

```
(MDF-1) (config) #interface-group gigabitethernet Trunk-Ports
(MDF-1) (gigabitethernet "Trunk-Ports") #apply-to 0/0/11,0/0/15
(MDF-1) (gigabitethernet "Trunk-Ports") #switching-profile Trunk
(MDF-1) (gigabitethernet "Trunk-Ports") # !
```

```
(MDF-1) (config) #mstp
(MDF-1) (Global MSTP) #region-name REG-1
(MDF-1) (Global MSTP) #instance 0 bridge-priority 4096
(MDF-1) (Global MSTP) #instance 1 bridge-priority 4096
(MDF-1) (Global MSTP) #instance 2 bridge-priority 8192
(MDF-1) (Global MSTP) #instance 1 vlan 100,200
(MDF-1) (Global MSTP) #instance 2 vlan 300,400
```

MDF-2

```
(MDF-2) (config) #interface-group gigabitethernet Trunk-Ports
(MDF-2) (gigabitethernet "Trunk-Ports") #apply-to 0/0/13,0/0/16
(MDF-2) (gigabitethernet "Trunk-Ports") #switching-profile Trunk
(MDF-2) (gigabitethernet "Trunk-Ports") #!
```

```
(MDF-2) (config) #mstp
(MDF-2) (Global MSTP) #region-name REG-1
(MDF-2) (Global MSTP) #instance 0 bridge-priority 8192
(MDF-2) (Global MSTP) #instance 1 bridge-priority 8192
(MDF-2) (Global MSTP) #instance 2 bridge-priority 4096
(MDF-2) (Global MSTP) #instance 1 vlan 100,200
(MDF-2) (Global MSTP) #instance 2 vlan 300,400
```

IDF-1

```
(IDF-1) (config) #interface-group gigabitethernet Trunk-Ports
(IDF-1) (gigabitethernet "Trunk-Ports") #apply-to 0/0/13,0/0/15
(IDF-1) (gigabitethernet "Trunk-Ports") #switching-profile Trunk
(IDF-1) (gigabitethernet "Trunk-Ports") #!
```

```
(IDF-1) (config) #mstp
(IDF-1) (Global MSTP) #region-name REG-1
```

```
(IDF-1) (Global MSTP) #instance 0 bridge-priority 16384
(IDF-1) (Global MSTP) #instance 1 bridge-priority 32768
(IDF-1) (Global MSTP) #instance 2 bridge-priority 16384
(IDF-1) (Global MSTP) #instance 1 vlan 100,200
(IDF-1) (Global MSTP) #instance 2 vlan 300,400
```

IDF-2

```
(IDF-2) (config) #interface-group gigabitethernet Trunk-Ports
(IDF-2) (gigabitethernet "Trunk-Ports") #apply-to 0/0/11,0/0/16
(IDF-2) (gigabitethernet "Trunk-Ports") #switching-profile Trunk
(IDF-2) (gigabitethernet "Trunk-Ports") #!
```

```
(IDF-2) (Global MSTP) #region-name REG-1
(IDF-2) (Global MSTP) #instance 0 bridge-priority 16384
(IDF-2) (Global MSTP) #instance 1 bridge-priority 32768
(IDF-2) (Global MSTP) #instance 2 bridge-priority 16384
(IDF-2) (Global MSTP) #
(IDF-2) (Global MSTP) #instance 1 vlan 100,200
(IDF-2) (Global MSTP) #instance 2 vlan 300,400
```

Verifying the MSTP Configuration on All Switches

The following samples illustrate the verification for MSTP configuration on all switches:

MDF-1

```
(MDF-1) #show spanning-tree
```

```
MST 0
Root ID          Address: 000b.868f.b8b7, Priority: 4096
Regional Root ID Address: 000b.868f.b8b7, Priority: 4096
Bridge ID        Address: 000b.868f.b8b7, Priority: 4096
External root path cost 0, Internal root path cost 0 << Root-Bridge for CIST (MST-0)
Last TC received on intf GE0/0/11, on 2014-02-10 02:52:10 (PST)
```

Interface	Role	State	Port Id	Cost	Type
GE0/0/11	Desg	FWD	128.12	20000	P2p
GE0/0/15	Desg	FWD	128.16	20000	P2p

```
MST 1
Root ID          Address: 000b.868f.b8b7, Priority: 4096
Bridge ID        Address: 000b.868f.b8b7, Priority: 4096
root path cost 0, remaining hops 20 << Root-Bridge for MST-1
Last TC received on intf GE0/0/11, on 2014-02-10 02:52:10 (PST)
```

Interface	Role	State	Port Id	Cost	Type
GE0/0/11	Desg	FWD	128.12	20000	P2p
GE0/0/15	Desg	FWD	128.16	20000	P2p

```
MST 2
Root ID          Address: 001a.1e0d.1280, Priority: 4096
Bridge ID        Address: 000b.868f.b8b7, Priority: 8192
root path cost 40000, remaining hops 18
Last TC received on intf GE0/0/11, on 2014-02-10 02:52:10 (PST)
```

Interface	Role	State	Port Id	Cost	Type
GE0/0/11	Root	FWD	128.12	20000	P2p
GE0/0/15	Altn	BLK	128.16	20000	P2p

MDF-2

(MDF-2) #show spanning-tree

MST 0

Root ID Address: 000b.868f.b8b7, Priority: 4096
Regional Root ID Address: 000b.868f.b8b7, Priority: 4096
Bridge ID Address: 001a.1e0d.1280, Priority: 8192
External root path cost 0, Internal root path cost 40000
Last TC received on intf GE0/0/13, on 2014-02-10 16:31:09 (PST)

Interface	Role	State	Port Id	Cost	Type
GE0/0/13	Altn	BLK	128.14	20000	P2p
GE0/0/16	Root	FWD	128.17	20000	P2p

MST 1

Root ID Address: 000b.868f.b8b7, Priority: 4096
Bridge ID Address: 001a.1e0d.1280, Priority: 8192
root path cost 40000, remaining hops 18
Last TC received on intf GE0/0/13, on 2014-02-10 16:31:09 (PST)

Interface	Role	State	Port Id	Cost	Type
GE0/0/13	Altn	BLK	128.14	20000	P2p
GE0/0/16	Root	FWD	128.17	20000	P2p

MST 2

Root ID Address: 001a.1e0d.1280, Priority: 4096
Bridge ID Address: 001a.1e0d.1280, Priority: 4096
root path cost 0, remaining hops 20 << Root-Bridge for MST-2
Last TC received on intf GE0/0/13, on 2014-02-10 16:31:09 (PST)

Interface	Role	State	Port Id	Cost	Type
GE0/0/13	Desg	FWD	128.14	20000	P2p
GE0/0/16	Desg	FWD	128.17	20000	P2p

IDF-1

(IDF-1) #show spanning-tree

MST 0

Root ID Address: 000b.868f.b8b7, Priority: 4096
Regional Root ID Address: 000b.868f.b8b7, Priority: 4096
Bridge ID Address: 001a.1e11.a780, Priority: 16384
External root path cost 0, Internal root path cost 20000
Last TC received on intf GE0/0/15, on 2014-02-10 11:40:09 (PST)

Interface	Role	State	Port Id	Cost	Type
GE0/0/13	Desg	FWD	128.14	20000	P2p
GE0/0/15	Root	FWD	128.16	20000	P2p

MST 1

Root ID Address: 000b.868f.b8b7, Priority: 4096
Bridge ID Address: 001a.1e11.a780, Priority: 32768
root path cost 20000, remaining hops 19
Last TC received on intf GE0/0/15, on 2014-02-10 11:40:09 (PST)

Interface	Role	State	Port Id	Cost	Type
GE0/0/13	Desg	FWD	128.14	20000	P2p

```
GE0/0/15   Root   FWD    128.16   20000   P2p << MST-1 traffic towards MDF-1
```

```
MST 2
```

```
Root ID           Address: 001a.1e0d.1280, Priority: 4096
```

```
Bridge ID         Address: 001a.1e11.a780, Priority: 16384
```

```
root path cost 20000, remaining hops 19
```

```
Last TC received on intf GE0/0/15, on 2014-02-10 11:40:09 (PST)
```

Interface	Role	State	Port Id	Cost	Type
-----	----	-----	-----	-----	-----
GE0/0/13	Root	FWD	128.14	20000	P2p << MST-2 traffic towards MDF-2
GE0/0/15	Desg	FWD	128.16	20000	P2p

IDF-2

```
(IDF-2) #show spanning-tree
```

```
MST 0
```

```
Root ID           Address: 000b.868f.b8b7, Priority: 4096
```

```
Regional Root ID Address: 000b.868f.b8b7, Priority: 4096
```

```
Bridge ID         Address: 001a.1e11.8900, Priority: 16384
```

```
External root path cost 0, Internal root path cost 20000
```

```
Last TC received on intf GE0/0/16, on 2014-02-10 10:36:41 (PST)
```

Interface	Role	State	Port Id	Cost	Type
-----	----	-----	-----	-----	-----
GE0/0/11	Root	FWD	128.12	20000	P2p
GE0/0/16	Desg	FWD	128.17	20000	P2p

```
MST 1
```

```
Root ID           Address: 000b.868f.b8b7, Priority: 4096
```

```
Bridge ID         Address: 001a.1e11.8900, Priority: 32768
```

```
root path cost 20000, remaining hops 19
```

```
Last TC received on intf GE0/0/16, on 2014-02-10 10:36:41 (PST)
```

Interface	Role	State	Port Id	Cost	Type
-----	----	-----	-----	-----	-----
GE0/0/11	Root	FWD	128.12	20000	P2p << MST-1 traffic towards MDF-1
GE0/0/16	Desg	FWD	128.17	20000	P2p

```
MST 2
```

```
Root ID           Address: 001a.1e0d.1280, Priority: 4096
```

```
Bridge ID         Address: 001a.1e11.8900, Priority: 16384
```

```
root path cost 20000, remaining hops 19
```

```
Last TC received on intf GE0/0/16, on 2014-02-10 10:36:41 (PST)
```

Interface	Role	State	Port Id	Cost	Type
-----	----	-----	-----	-----	-----
GE0/0/11	Desg	FWD	128.12	20000	P2p
GE0/0/16	Root	FWD	128.17	20000	P2p << MST-2 traffic towards MDF-2

The implementation of Rapid PVST+ (Per-VLAN Spanning Tree Plus) is based on the IEEE Standards 802.1D-2004 and 802.1Q-2005 ensuring interoperability with industry accepted PVST+ protocols. In addition, Rapid PVST+ supports the loopguard, rootguard, bpduguard, and portfast features.



To enable PVST+ , use the spanning tree mode command.

Rapid PVST+ runs a separate spanning tree instance for each Virtual Local Area Network (VLAN). This allows the port to forward some VLANs while blocking other VLANs. PVST+ provides for load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

Convergence occurs rapidly with Rapid PVST+. By default, each designated port in the spanning tree protocol sends out a BPDUs (Bridge Protocol Data Units) every 2 seconds. On a designated port in the topology, if hello messages are missed three consecutive times, or if the maximum age expires, the port immediately flushes all protocol information from the table. A port considers that it loses connectivity to its direct neighbor designated port when it misses three BPDUs or if the maximum age expires. This rapid aging of the protocol information allows for quick failure detection.

Rapid PVST+ provides for rapid recovery of connectivity following the failure of a device, a device port, or a LAN. It provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links.

This chapter covers:

- [Important Points to Remember on page 177](#)
- [Configuring PVST+ on page 177](#)
- [Loopguard and Rootguard on page 179](#)
- [Bridge Protocol Data Unit \(BPDU\) Guard on page 180](#)

Important Points to Remember

- Configure Rapid PVST+ using the command line only.
- If your Mobility Access Switch is terminated on a router/switch spanning tree environment running PVST+, your Mobility Access Switch must be in PVST mode (**spanning-tree mode pvst** command).
- Once in Rapid PVST+ mode, a predefined non-editable PVST profile automatically associates all configured VLANs (including default VLAN 1) and PVST+ starts running on all configured VLANs.
- Rapid PVST+ inter-operates seamlessly with IEEE and PVST bridges when the Mobility Access Switch is placed in a network.

Configuring PVST+

You configure Rapid PVST+ via two profiles; the VLAN profile that enables you to configure the Rapid PVST+ properties and the interface-based profile that enables you to configure your Rapid PVST+ port properties.

Configuring using the VLAN Profile

Set the spanning tree mode to PVST+, assign a profile name, attach the profile to a VLAN, then configure PVST+ properties.

1. Set the spanning tree mode to PVST+.

```
(host) (config) #spanning-tree mode pvst
```

Verify the spanning tree mode:

```
(host) (config) #show spanning-tree-profile
```

```
spanning-tree
-----
Parameter          Value
-----
spanning-tree-mode pvst
```

2. Assign a PVST+ profile name; in the example below the profile name is "techpubs":

```
(host) (config) #vlan-profile pvst-profile techpubs
(host) (pvst-profile "techpubs") #
```

3. Attach the named profile to a VLAN; in the example below the profile name "techpubs" is attached to VLAN 1:

```
(host) (config) #vlan 1#
(host) (VLAN "1") #pvst-profile techpubs
```

4. View the other PVST+ options settings (such as forward delay, hello time and maximum age).

```
(host) (pvst-profile "techpubs") # ?
bridge-priority      Bridge-priority [0-61440 in steps of 4096]. Default:
                    32768
clone                Copy data from another pvst-profile
enable               Enable or disable PVST+ bridge.
forward-delay        Forward-delay in seconds [4-30]. Default: 15 seconds
hello-time           Hello-time in seconds [1-10]. Default: 2 seconds
max-age              Maximum age in seconds [6-40]. Default: 20 seconds
no                   Delete Command
```

5. To change one of the value, for example bridge hello time, execute the following command:

```
(host) (pvst-profile "techpubs") #hello-time 5
```

6. Then verify your change:

```
(host) (pvst-profile "techpubs") #show vlan-profile pvst-profile techpubs
```

```
pvst-profile "TechPubs"
-----
Parameter          Value
-----
Enable PVST+ bridge Enabled
bridge priority    32768
bridge hello time  5                ←forward delay changed from 2 to 5 seconds
bridge forward delay 15
bridge maximum age 20
```

Disable PVST+ on a VLAN

The following example disables the PVST+ profile "techpubs" and then removes the PVST profile from VLAN 1.

```
(host) (config) #vlan-profile pvst-profile techpubs
(host) (pvst-profile "techpubs") #no enable
(host) (pvst-profile "techpubs") #exit
(host) (config) #vlan 1
(host) (VLAN "1") #pvst-profile techpubs
(host) (VLAN "1") #
```

Configuring using the Interface-based Profile

The interface-based Rapid PVST+ profile allows you to configure PVST+ port parameters.

1. Name the interface and view the configuration options.

```
(host) (config) #interface-profile pvst-port-profile techpubs
(host) (Interface PVST bridge "techpubs") #?
```

bpduguard	Enable or disable bpduguard
clone	Copy data from another Interface PVST bridge
loopguard	Enable or disable loopguard
no	Delete Command
point-to-point	Enable or disable point-to-point
portfast	Enable or disable portfast
rootguard	Enable or disable rootguard
vlan	spanning tree [1-4094]

2. Use any of the command options to further configure your interface-based profile.

```
(host) (Interface PVST bridge "techpubs") #vlan 3 cost 8
(host) (Interface PVST bridge "techpubs") #vlan 3 priority 240
```

Then verify your configuration. Notice that the cost and priority values include the original default value and the current value.

```
(host) (Interface PVST bridge "techpubs") #show interface-profile pvst-port-profile techpubs
```

```
Interface PVST bridge "techpubs"
-----
Parameter                Value
-----
spanning tree port cost   3 8 <-----new value is displayed
spanning tree port priority 3 240 <-----new value is displayed
Enable point-to-point     Enabled
Enable portfast           Disabled
Enable rootguard          Disabled
Enable loopguard          Disabled
```

Loopguard and Rootguard

Rapid PVST+ supports the loopguard and rootguard features.

Configuring Loopguard

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.

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
```

Configuring Rootguard

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.

Enable rootguard:

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

Associate to the interface:

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

Verifying the Configuration

Use the show interface-profile command to view the status of loopguard and rootguard.

```
(host) #show interface-profile pvst-port-profile techpubs
```

```
Interface PVST bridge "techpubs"
-----
Parameter                               Value
-----
Instance port cost                       3 8
Instance port priority                   3 240
Enable point-to-point                    Enabled
Enable portfast                          Enabled
Enable rootguard                         Enabled ← rootguard is enabled
Enable loopguard                         Disabled
Enable bpduguard                         Enabled
Enable bpduguard auto recovery time     60
```

Bridge Protocol Data Unit (BPDU) Guard

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.

Enabling and Configuring BPDU Guard Functionality

The BPDU Guard functionality can be enabled or disabled at an interface level. By default, the BPDU is disabled. The BPDU guard functionality can now be configured as part of the `pvst-port-profile` configuration.

You can use the following command to configure the BPDU guard by using the PVST profile:

```
(host) (config) #interface-profile pvst-port-profile <profile-name>
  bpduguard
  auto-recovery-time <recovery-time>
```

The following example shows how to enable and configure the BPDU guard functionality:

```
(host) (config) # interface-profile pvst-port-profile BPDUGuard1
  bpduguard auto-recovery-time 60
```



You can configure BPDU guard with or without the **auto-recovery-time** option.

You can disable the BPDU guard functionality by using the following command:

```
(host) (config) #interface-profile <profile-name> no bpduguard
```

You can disable the auto recovery time by using the following command:

```
(host) (Interface PVST bridge "profile-name") #bpduguard no auto-recovery-time
```

Verifying the BPDUGuard Configuration:

```
(host) (config) #show interface-profile pvst-port-profile bpdu
```

```
Interface PVST bridge "bpdu"
-----
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 ← BPDUGuard is enabled
Enable bpduguard auto recovery time     N/A
```

Sample Configuration

To enable and configure BPDUGuard using the PVST profile:

```
(host) (config) # interface-profile pvst-port-profile BPDUGuard1
  bpduguard auto-recovery-time 60
```

To attach the PVST profile to the interface:

```
(host) (config) # interface gigabitethernet <0/0/6>
  pvst-port-profile BPDUGuard1
```

Portfast

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.



The portfast is mutually exclusively with the Loopguard feature.

Configuring Portfast

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
(host) (Interface PVST bridge "techpubs") #portfast
```

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



Portfast is operational on both access ports and trunk ports.

Use the following command to enable the portfast support on a trunk port:

```
(host) (config) #interface-profile mstp-profile portfast_techpubs
(host) (Interface "portfast_techpubs") #portfast trunk
```

Verify the Configuration

Use the show interface-profile command to view the status of the portfast.

```
(host) (config) #show interface-profile pvst-port-profile bpdu
```

```
Interface PVST bridge "bpdu"
```

```
-----
```

Parameter	Value
-----	-----
Instance port cost	N/A
Instance port priority	N/A
Enable point-to-point	Disabled
Enable portfast	Enabled ← portfast is enabled
Enable rootguard	Disabled
Enable loopguard	Disabled
Enable bpduguard	Enabled
Enable bpduguard auto recovery time	N/A

The Hot-Standby Link (HSL) feature is a simplified failover mechanism. HSL 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.

HSL consists of a pair of redundant links. One is the *primary* for traversing traffic, and the other is the *backup*. When the primary fails, a rapid traffic failover occurs to the awaiting backup.

One of the primary use cases for HSL is in an enterprise topology where each access switch is dual-homed to two distribution/core switches for redundancy purpose.

Important Point to Remember

- Spanning tree (MSTP and PVST+) must be disabled before configuring HSL. HSL and spanning tree can not be configured on the same system at the same time.
- HSL is a 1:1 ratio for primary and backup pairs. One backup interface can not be the backup of multiple primary interfaces. An interface can be part of only one HSL pair.
- HSL links are always trusted.
- Primary and backup interfaces must have the same switching profiles.
- Primary and backup interfaces cannot be members of the same port-channel.
- The interfaces cannot be Tunneled Node interfaces.

Configuration Steps

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. You can force the primary interface to become active by enabling preemption.

Configure HSL directly in the interface. First, on the primary interface (for example 0/0/10), then specify the back-up interface (for example 0/0/11). Use the following steps, from the command line, to configure and verify HSL.

1. Configure the primary and backup interfaces.

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

2. Configure pre-emption if necessary (it is off by default).

```
(host) (gigabitethernet "0/0/10") #preemption mode forced
```

3. If pre-emption is configured, best practices recommends configuring *delay*. The range is 10 seconds to 5 minutes (300 seconds); default is 100 seconds.

```
(host) (gigabitethernet "0/0/10") #preemption delay 10
```

4. Verify the HSL configuration. The following show command is a partial output.

```
(host) #show interface-config gigabitethernet 0/0/10
```

```
gigabitethernet "0/0/10"
```

```
-----
```

Parameter	Value
-----	-----
Interface MSTP Profile	disabled
...	
Interface Trusted Mode	Enabled

```
HSL backup interface          gigabitethernet0/0/11
HSL preemption mode          Forced
HSL preemption delay         10
...
```

To view details of HSL on an interface, use the following show commands.

```
(host) #show hot-standby-link gigabitethernet 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: 10
Last Switchover Time: NEVER            Flap Count: 0
```

To view details of all HSL links, use the following show 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

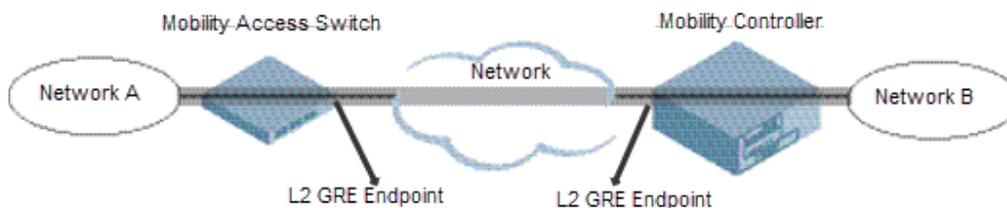
Generic Routing Encapsulation (GRE) is an Aruba proprietary tunnel across Mobility Access Switches, Aruba Controllers, and Aruba APs. This chapter describes the following topics related to GRE:

- [L2 GRE on page 185](#)
- [L3 GRE on page 187](#)

L2 GRE

ArubaOS Mobility Access Switch supports L2 connectivity through GRE tunnel. L2-GRE tunnel extends VLANs across Mobility Access Switches and Aruba controllers. GRE encapsulates Layer-2 frames with a GRE header and transmit through an IP tunnel over the cloud. Following figure shows how L2-GRE tunnel fits into network operations.

Figure 12 L2-GRE Tunnel Network Topology



Configuring an L2-GRE Tunnel

To configure an L2-GRE tunnel, see the following procedure.

```
(host) (config) #interface tunnel ethernet <tunnel-id>
(host) (Tunnel "tunnel-id") #description <interface-description>
(host) (Tunnel "tunnel-id") #source-ip <source-tunnel-ip>
(host) (Tunnel "tunnel-id") #destination-ip <destination-tunnel-ip>
(host) (Tunnel "tunnel-id") #switching-profile <profile-name>
(host) (Tunnel "tunnel-id") #keepalive <Tunnel heartbeat interval in seconds (1-86400)>
<Tunnel Heartbeat Retries (1-1024)>
```

Inter-tunnel flooding

There can be multiple L2-GRE tunnels terminating on the same device, either ArubaOS Mobility Access Switch or Mobility Controller. If the tunnels carry same VLANs, this may cause inter-tunnel flooding resulting in loops within the network. To avoid this scenario, disable inter-tunnel flooding in the switch and the controller.

```
(host) (config) #interface tunnel ethernet <tunnel-id>
(host) (Tunnel "tunnel-id") #no inter-tunnel-flooding
```

For additional parameters, refer to *ArubaOS 7.4.x Command Line Interface Guide*.

Understanding the VLAN Membership of Existing L2 GRE Tunnel

You can use the following commands to understand the VLAN membership of L2 GRE tunnel which is already configured.

Use the following command to check the VLAN membership of the existing L2 GRE tunnel:

```
(host) #show interface tunnel <tunnel-id>
```

```
tunnel 10 is administratively Up, Line protocol is Down
Description: GRE Interface
Internet address is unassigned
Source <source_IP>
Destination <destination_IP>
Protocol number 0
Tunnel mtu is set to 1100
Tunnel is an L2 GRE Tunnel
Tunnel is Trusted
Inter Tunnel Flooding is enabled
Tunnel keepalive is enabled
Tunnel keepalive interval is 3 seconds, retries 3
  Heartbeats sent 51347, Heartbeats lost 51346
  Tunnel is down 4 times
Switching-profile "100"
```

```
(host) #show interface-config tunnel <tunnel-id>
```

```
Tunnel "10"
-----
Parameter                Value
-----                -
Tunnel Description        N/A
Tunnel Source IP          <source_IP>
Tunnel Destination IP     <destination_IP>
Inter-Tunnel-Flooding    Enabled
Tunnel Mode               L2
Tunnel Protocol           0
Tunnel Keepalive          3/3
Tunnel MTU                1100
Tunnel Shutdown           Disabled
Tunnel Switching Profile  100
Tunnel Trusted            Enabled
```

This shows that Switching-Profile "100" is applied in L2 GRE tunnel interface. You can use the **show interface-profile switching-profile 100** command to view the VLAN configuration.

```
(host) #show interface-profile switching-profile 100
```

```
switching profile "100"
-----
Parameter                Value
-----                -
Switchport mode          access
Access mode VLAN         100
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
```

You can use the **show vlan** command to view the port associated with the vlan:

```
(host) #show vlan
```

```
VLAN CONFIGURATION
-----
VLAN  Description  Ports
----  -
1     VLAN0001         GE0/0/1-19 GE0/0/21-26 GE0/0/28-33 GE0/0/35-36
                                GE0/0/38-47 GE0/1/0-3 GRE-TUN30
10    VLAN0010         GE0/0/34 Pcl
```

```

11    VLAN0011    GE0/0/34
20    VLAN0020    GE0/0/20
100   VLAN0100    GE0/0/0 GE0/0/27 GRE-TUN10 GRE-TUN20

```



MAC address learned on L2 GRE tunnel does not honor `mac-aging-timer` configuration, and ages out at 270 seconds.

Sample Configuration

To configure an L2-GRE tunnel and apply the switching profile:

```

(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

```

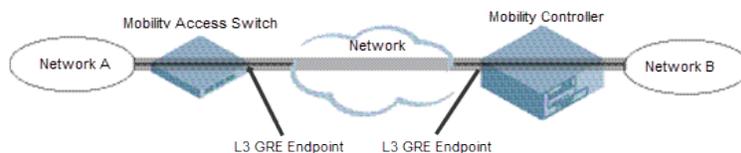


In the above example, `mDNS_vlan_200` was previously defined.

L3 GRE

ArubaOS Mobility Access Switch supports L3 connectivity through GRE tunnel. L3 GRE tunnel extends VLANs across Mobility Access Switches and Aruba controllers. GRE encapsulates Layer-3 frames with a GRE header and transmits through an IP tunnel over the cloud. Following figure shows how L3-GRE tunnel fits into network operations.

Figure 13 L3-GRE Tunnel Network Topology



Configuring an L3 GRE Tunnel

To configure an L3-GRE tunnel, see the following procedure.

```

(host) (config) #interface tunnel ip <tunnel-id>
(host) (Tunnel "tunnel-id") #description <interface-description>
(host) (Tunnel "tunnel-id") #source-ip <source-tunnel-ip>
(host) (Tunnel "tunnel-id") #destination-ip <destination-tunnel-ip>
(host) (Tunnel "tunnel-id") #keepalive <Tunnel heartbeat interval in seconds (1-86400)>
<Tunnel Heartbeat Retries (1-1024)>
(host) (Tunnel "tunnel-id") #mtu <Set MTU between 1024 and 1500 (Default 1100)>
(host) (Tunnel "tunnel-id") #ip address <addr> <mask>
(host) (Tunnel "tunnel-id") #ospf-profile <profile-name>

```

Sample Configuration

To configure an L3 GRE tunnel:

```

(host) (config) #interface tunnel ip 1
(host) (Tunnel "1") #description L3-GRE_Interface
(host) (tunnel "1") #source-ip 192.0.2.10
(host) (tunnel "1") #destination-ip 192.0.2.12
(host) (tunnel "1") #keepalive 30 5
(host) (tunnel "1") #mtu 1100
(host) (Tunnel "1") #ip address 192.0.2.1 255.255.255.0

```

```
(host) (Tunnel "1") #ospf-profile TechPubs
```

Verification

Use the following command to verify the L3 GRE tunnel configuration:

```
(host) #show interface tunnel <tunnel-id>
```

The following example shows L3 GRE tunnel configuration on tunnel 1:

```
(host) #show interface tunnel 1
tunnel 1 is administratively Up, Line protocol is Up
Description: L3-GRE_Interface
Source 192.0.2.10
Destination 192.0.2.12
Tunnel mtu is set to 1100
Tunnel keepalive is enabled
Tunnel keepalive interval is 30 seconds, retries 5
Heartbeats sent 4, Heartbeats lost 3
Tunnel is down 0 times
Tunnel is an L3 GRE Tunnel
Internet address is 192.0.2.1, Netmask is 255.255.255.0
```

This chapter describes the Layer 3 Routing features available on the Mobility Access Switch. It contains the following sections:

- [Understanding Routed VLAN Interfaces on page 189](#)
- [Multinetting on page 190](#)
- [Network Address Translation on page 191](#)
- [NAT Pools on page 193](#)
- [Support for IP NAT Outside on page 196](#)
- [IP Directed Broadcast on page 197](#)
- [Static Routes on page 198](#)
- [Equal Cost Multipath on page 201](#)
- [IP Prefix List on page 202](#)
- [Support for Egress ACLs on Routed VLAN Interfaces on page 203](#)
- [Route Monitoring on page 204](#)
- [Dynamic Domain Name Server Client on page 207](#)
- [Static Address Resolution Protocol on page 209](#)

Understanding Routed VLAN Interfaces

Routed VLAN Interfaces (RVI) are logical interfaces that enable routing and bridging between VLANs. You can route and bridge a protocol on the same interface. The traffic that remains in the bridge group (the bridged traffic) will be bridged among the bridged interfaces, and the traffic that needs to go out to another network (the routed traffic) will be routed internally to the appropriate output routed interface.

There can be an IPv4 address to each VLAN interface. You can also configure IGMP and PIM interface profiles to the VLAN interfaces. You can configure up to 4094 routed VLAN interfaces. VLAN interface 1 is configured by default.

Important Points to Remember

- The maximum number of VLAN interfaces supported are 4094.
- The Layer 2 VLAN must be configured before configuring the corresponding RVIs.
- The protocol status of a RVI is in up state only when the protocol status of at least one member port in the corresponding VLAN is in up state.

To assign member ports to a VLAN, create a switching profile with the corresponding VLAN, and assign the switching profile to the member interfaces.

Configuring Routed VLAN Interfaces

You can configure routed VLAN interfaces using the CLI.

Using the CLI

To configure routed VLAN interfaces, follow these steps:

1. Create the required VLANs.

```
(host) (config) # vlan <vlan-id>
```

2. Create the switching profiles and reference the existing VLANs.

```
(host) (config) # interface-profile switching-profile <profile-name>
    switchport-mode {access|trunk}
    access-vlan <vlan-id>
    trunk allowed vlan <vlan-list>
    native-vlan <vlan-id>
    exit
```

3. Apply the switching profiles to the physical interfaces.

```
(host) (config) # interface gigabitethernet <slot/module/port>
    switching-profile <profile-name>
    exit
```

4. Create the VLAN interfaces.

```
(host) (config) # interface vlan <vlan-id>
    description <vlan-interface-description>
    dhcp-relay-profile <profile-name>
    igmp-profile <profile-name>
    ip {address {{<ip-address> netmask <subnet-mask>}} | dhcp-client} | directed-broadcast |
    nat {inside}}
    ipv6 address {{<prefix> netmask <subnet-mask>}} | link-local <link-local>}
    mtu <64-9216>
    shutdown
    no {...}
    ospf-profile <profile-name>
    pim-profile <profile-name>
    exit
```

Multinetting

ArubaOS supports multiple IP addresses per VLAN and loopback interface. This allows the user to specify any number of secondary IP addresses. Secondary IP address can be used in a variety of situations, such as the following:

- If an insufficient number of host addresses are available on a particular network segment. Using secondary IP addresses on the routers or access devices allows you to have two logical subnets using one physical subnet
- If the an older network is built using Layer 2 bridges and has no subnetting. Secondary addresses can aid in the transition to a subnetted, router-based network.
- Two subnets of a single network might be otherwise separated by another network. You can create a single network from subnets that are physically separated by another network using a secondary address.

Important Points to Remember

- OSPF advertises the secondary IP address in the router LSA but it does not form adjacency on the secondary IP address.
- PIM will not send hello packets on the secondary IP address.
- DHCP servers identify the subnets associated with secondary IP addresses used for allocation.

Configuring Secondary IP

To configure a secondary IP address, use the following command:

```
(host) (vlan "1") #ip address 1.1.1.1 255.255.255.0 ?
secondary          Make this IP address a secondary address
```

Sample Configuration

```
(host) (config) #interface vlan 2
(host) (vlan "2") #ip address 1.1.1.1 255.255.255.0 secondary

(host) (vlan "2") #show interface vlan 2
```

```
VLAN2 is administratively Up, Line protocol is Up
Hardware is CPU Interface, Address is 00:0b:86:6a:1c:c0
Description: 802.1Q VLAN
Internet address is 20.20.20.1, Netmask is 255.255.255.0
Internet address is 1.1.1.1, Netmask is 255.255.255.0 secondary
IPV6 link-local address is fe80::b:8600:26a:1cc0
Global Unicast address(es):
Routing interface is enable, Forwarding mode is enable
Directed broadcast is disabled, BCMC Optimization disabled
```

Loopback Interfaces

The Mobility Access Switch supports a maximum of 64 (0 to 63) loopback interfaces. You can configure the loopback interfaces using the CLI. Additionally, you can assign a secondary IP address to a loopback interface by using the **secondary** parameter.

Using the CLI

```
(host) (config) # interface loopback <0-63>
  clone <source>
  description <description>
  ip address <address> [secondary]
  no {...}
  ospf-profile
  exit
```

Sample Loopback Interface Configuration

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

Network Address Translation

Aruba Mobility Access Switches support source Network Address Translation (NAT) with Port Address Translation (PAT) on VLAN interfaces. When source NAT is enabled on a VLAN interface, the IP address of the egress VLAN interface as determined by the routing table will be used as the source IP. For example, if "ip nat inside" is enabled on interface VLAN X and traffic will be routed out interface vlan Y, the IP address of interface VLAN Y will be used as the source IP for traffic from VLAN X

```
(host) (config) #interface vlan <vlan_id>
(host) (vlan "vlan_id") #ip nat inside
```



No packet fragmentation is supported by NATing.

To verify source NAT is enabled on a VLAN interface, use **show interface vlan <vlan-id>**. In the following example, source NAT has been enabled on interface VLAN 6. As a result, the output of **show interface vlan**

<vlan-id> will include the bolded section below. If the bolded section is not displayed, source NAT has not been enabled.

```
(host) # show interface vlan 6

VLAN6 is administratively Up, Line protocol is Up
Hardware is CPU Interface, Address is 00:0b:86:6a:5d:c0
Description: 802.1Q VLAN
Internet address is 6.1.1.1, Netmask is 255.255.255.0
IPV6 link-local address is fe80::b:8600:66a:5dc0
Global Unicast address(es):
Routing interface is enabled, Forwarding mode is enabled
Interface is source NAT'ed
Directed broadcast is disabled, BCMC Optimization disabled
Encapsulation 802, Loopback not set
Interface index: 50331654
MTU 1700 bytes
```

Additionally, you can use the **show datapath vlan** command to verify that source NAT has been enabled.

```
(host) #show datapath vlan

Datapath VLAN Table Entries
-----
Flags: N - Nat Inside, M - Route Multicast, R - Routing
      S - Snoop MLD, G - Snoop IGMP, P - Proxy IGMP
      B - BCMC Optimization, A - Proxy ARP, U - Suppress ARP
      1(cert-id) - 8021X Term-PEAP, 2(cert-id) - 8021X Term-TLS
VLAN  Flags          Ports
----  -
6      NRU          1/0/14
100   RU             0/0/14
```

The **show datapath session** command can be used to verify the packet flows that are being NAT'ed. This output however will not indicate the interface VLAN the flow(s) are using. To determine that information use the **show ip interface brief** command.

```
(host) #show datapath session
Datapath Session Table Entries
-----
Flags: F - fast age, S - src NAT, N - dest NAT
      D - deny, R - redirect, Y - no syn
      H - high prio, P - set prio, T - set ToS
      C - client, M - mirror, V - VOIP
      Q - Real-Time Quality analysis
      I - Deep inspect, U - Locally destined
      E - Media Deep Inspect, G - media signal
      u - User Index
Source IP      Destination IP  Prot  SPort  DPort  Cntr  Prio  ToS  Age  Destination  TAge  UsrIdx
-----
6.1.1.5        100.1.1.6     61   0      0      0/0   0 0   0   1/0/14      1    0
100.1.1.6      100.1.1.7     61   0      0      0/0   0 0   0   1/0/14      1    0

UsvrVer  Flags
-----
0        FSC
0        FNY
```

```
(host) #show ip interface brief

Interface          IP Address / IP Netmask      Admin  Protocol
```

```

vlan 100          100.1.1.7 / 255.255.255.0    Up      Up
vlan 6           6.1.1.1 / 255.255.255.0    Up      Up

```

NAT Pools

Mobility Access Switch provides support for NAT pools to protect private IPs behind the switch. It also gives the flexibility to support source NAT and dual NAT without using the switch IP. Support for applying session ACLs on RVI enables software processing of the packets that require a NAT action.

NAT Pools extend the NAT capabilities of the Mobility Access Switch to support one-to-one NAT or NAT certain traffic to one IP address and the rest to another.

The following samples illustrate Source NAT and Destination NAT:

Figure 14 Source NAT



Figure 15 Destination NAT



Creating NAT Pools

You can create a NAT pool associated with source NAT option or dual NAT option. When a pool is created with dual NAT option, both source IP and destination IP of the packet are changed. To allow the reverse traffic, a session ACL must be present on the Egress RVI to perform destination NAT on the packets.

You can execute the following CLI command to configure a NAT pool with only source NAT option:

```
(host) (config) #ip nat pool <pool_name> <start_ip_src_nat_range> <end_ip_src_nat_range>
```

You can execute the following command to create a NAT pool with dual NAT option:

```
(host) (config) #ip nat pool <pool_name> <start_ip_src_nat_range> <end_ip_src_nat_range>
<dest_ip>
```

Sample Configuration

The following samples illustrate 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
```

Verifying NAT Pool Configuration

You can use the following command to view NAT pools configured on the Mobility Access Switch:

```
(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 output of the following command displays if a NAT operation is performed on a session:

```
(host) # show datapath session
```

```
Datapath Session Table Entries
```

```
-----
```

```
Flags: F - fast age, S - src NAT, N - dest NAT
```

Source IP/ Destination MAC	Destination IP	Prot	SPort	DPort	Cntr	Prio	ToS	Age	Destination	TAge	UsrIdx
-------------------------------	----------------	------	-------	-------	------	------	-----	-----	-------------	------	--------

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

Troubleshooting NAT

You can use the following commands for troubleshooting NAT operations using DPA logs:

```
(host) #set traceflags dpa nat
(host) #set traceflags dpa-dpe vlan
(host) #set traceflags dpa-sos vlan
(host) #set traceflags dpa-sos acl
```

Limitations

- User defined NAT through Session ACLs takes precedence over NAT inside.
- Dynamic source NAT is not supported in this release. You can use the **ip nat outside** command as an alternative.

Session ACLs on RVI

ArubaOS provides support for applying session ACLs on Routed VLAN interfaces (RVI) of the Mobility Access Switch to enable software processing of the packets.

You can create and configure session ACLs on RVI using the CLI.

Creating Session ACL with NAT Pools

You can create session ACLs with source NAT pool, dual NAT pool, or destination NAT rule. For more information on creating NAT pools, see [NAT Pools on page 193](#).

Execute the following command to create a session ACL:

```
(host) (config) #ip access-list session <acl-name>
(host) (config-sess-<acl-name>)# <source> <dest> <service> <action>
```

The **<action>** can be **dst-nat**, **src-nat**, or **dual-nat** for configuring NAT operations.

Sample Configuration

Session ACL with Source NAT pool

```
(host) (config) #ip access-list session POS-ACL
(host) (config-sess-POS-ACL)#host 192.168.5.10 any any src-nat pool NAT_pool1
```

Session ACL with dual NAT pool

```
(host) (config) #ip access-list session DUAL-NAT-ACL
(host) (config-sess-DUAL-NAT-ACL)#network 192.168.1.0 255.255.255.0 any any dual-nat pool
dual_nat_pool1
```

Session ACL with destination NAT rule

```
(host) # ip access-list session OUTSIDE-ACL
(host) (config-sess-OUTSIDE-ACL)#any host 192.168.1.10 any dst-nat ip 192.168.5.10 log
(host) (config-sess-OUTSIDE-ACL)#any host 192.168.1.11 any dst-nat ip 192.168.5.11 log
```

Configuring Session ACLs on RVI

Execute the following command to configure a session ACL on a routed VLAN interface:

```
(host) (config) #interface vlan <id>
(host) (vlan "id") #ip access-group session <acl-name>
```

Sample Configuration

Session ACL on Ingress RVI:

```
(host) (config) #interface vlan 100
(host) (vlan "100") #ip access-group session POS-ACL
```

Session ACL on Egress RVI:

```
(host) (config) #interface vlan 200
(host) (vlan "200") #ip access-group session OUTSIDE-ACL
```

Verifying the Configuration for Session ACL on RVI

You can use the following commands to verify the NAT pool configuration on the Ingress and Egress RVI:

Ingress RVI

```
(host) #show interface-config vlan 100
vlan "100"
-----
Parameter                               Value
-----
Interface description                    N/A
Interface OSPF profile                   N/A
Interface PIM profile                    N/A
Interface IGMP profile                   N/A
Interface DDNS profile                   N/A
Interface VRRP profile                   N/A
Probe Profile                            test
Directed Broadcast Enabled               Disabled
Interface shutdown                       Disabled
Session-processing                       Disabled
metric                                   10
mtu                                       1500
IP Address                               192.168.5.1/255.255.255.0
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	POS-ACL

Egress RVI

```
(host) #show interface-config vlan 200
vlan "200"
```

```
-----
Parameter                               Value
-----
Interface description                    N/A
Interface OSPF profile                   N/A
Interface PIM profile                    N/A
Interface IGMP profile                   N/A
Interface DDNS profile                   N/A
Interface VRRP profile                   N/A
Probe Profile                            test
Directed Broadcast Enabled               Disabled
Interface shutdown                       Disabled
Session-processing                       Disabled
metric                                   10
mtu                                       1500
IP Address                               192.168.5.1/255.255.255.0
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                               OUTSIDE-ACL
```

Limitations

- Session ACL and stateless Ingress ACL cannot co-exist on an RVI.
- Intended use of session ACL with NAT pools is for trusted ports. If there is a configuration of session ACL on RVI with untrusted ports, Session ACL on RVI takes precedence over user-role ACLs.

Support for IP NAT Outside

Mobility Access Switch provides support for IP NAT outside on egress VLAN interface. The IP NAT outside feature changes the source IP of all the egressing packets to the IP of the egress VLAN interface. You can configure IP NAT outside using the CLI.

Important Points to Remember

- User defined ACLs take precedence over IP NAT configuration.
- IP NAT outside takes precedence over IP NAT inside.

Configuring IP NAT outside

You can use the following command to configure IP NAT on an egress VLAN interface:

```
(host) (config) #interface vlan 10
(host) (vlan "10") #ip nat outside
```

Verifying IP NAT Outside

You can use the following command to verify the IP NAT outside configuration on the egress VLAN:

```
(host) (config) #show interface vlan 10
VLAN100 is administratively Up, Line protocol is Up
Hardware is CPU Interface, Address is 00:1a:1e:0c:72:40
Description: 802.1Q VLAN
Internet address is 192.168.100.1, Netmask is 255.255.255.0
IPV6 link-local address is fe80::1a:1e00:640c:7240
Global Unicast address(es):
Routing interface is enabled, Forwarding mode is enabled
Interface is source NAT'ed
Interface is egress source NAT'ed
Directed broadcast is disabled
Encapsulation 802, Loopback not set
Interface index: 50331658
MTU 1500 bytes
Metric 10
Probe Name: test, Probe Status: Down
```

IP Directed Broadcast

An IP directed broadcast is typically used by network management systems (NMS) for features like Wake On LAN to broadcast packets on a local subnet even though the source of that broadcast is located on a remote subnet. When the source device initiates this broadcast packet, it is routed through the network as a unicast packet until it reaches the target subnet. Other than the router directly attached to the target subnet, all routers across the network view it as a unicast packet. The router directly attached to the target subnet identifies the packet as a directed broadcast, converts it to a link-layer broadcast packet and propagates it across the target subnet.

This feature is disabled by default. When disabled, the directed broadcast packets are dropped unconditionally without generating an ICMP error packet. Due to the nature of propagating broadcast, Aruba does not recommend enabling this parameter as it can result in Denial of Service (DoS) attacks, if not used correctly. When absolutely necessary, you can enable this feature on a subnet by subnet basis. You can enable this feature on the Routed VLAN Interfaces (RVI) in the CLI.

Configuring IP Directed Broadcast

```
(host) (config) #interface vlan <id>
(host) (vlan) #ip directed-broadcast
```

Sample Configuration

The following example shows how to configure a routed VLAN interface and enable IP directed broadcast:

```
(host) (config) #interface vlan 10
(host) (vlan "10") #ip address 10.10.10.10 netmask 255.255.255.0
(host) (vlan "10") #ip directed-broadcast
(host) (vlan "10") #description layer 3
(host) (vlan "10") #mtu 1500
(host) (vlan "10") #exit
```

You can verify the preceding configuration using the following command:

```
(host) #show interface vlan 10
VLAN10 is administratively Up, Line protocol is Up
Hardware is CPU Interface, Address is 00:0b:86:6a:f2:40
Description: layer3
Internet address is 10.10.10.10, Netmask is 255.255.255.0
IPV6 link-local address not assigned
Global Unicast address(es):
```

```
Routing interface is enable, Forwarding mode is enable
Directed broadcast is enabled, BCMC Optimization disabled
Encapsulation 802, Loopback not set
Interface index: 50331658
MTU 1500 bytes
```

Static Routes

The Mobility Access Switch supports static routes configuration. You can configure multiple default gateways and multiple static routes within the global IP-profile to route packets outside the local network. The static routes are inserted in to the Forwarding Information Base (FIB), only when the nexthop matches the subnet of any of the RVI interfaces or the management interface. If the nexthop becomes unreachable, the Routing Information Base (RIB) gets purged but the static route is still retained. The static routes are active or added to the routing table only when the next hop is reachable, and can be removed from the static routes list only by using the `no` command.

Important Points to Remember

- You can have multiple static routes and default gateways.
- You can have both IPv4 and IPv6 default gateways simultaneously.
- Static routes become active only when the nexthop is reachable.
- Nexthops have to be within the local network.

Route Metrics

The Mobility Access Switch includes support for route metrics. For a given route destination, there can be multiple nexthops. A route metric enables the Mobility Access Switch to prefer one route over another or load balance when the metric is the same. For more details on load balancing across multiple nexthops, see [Equal Cost Multipath on page 201](#).

A route destination with a lower metric is added to the route manager. The higher metric routes are added only when the lower metric routes are removed.

Default Gateway

Default gateway is a special case of static route where the destination mask and prefix is 0/0. The next hop in a default gateway can be any valid IP address which can be reached through a routable or the management interface.

Multiple Default Gateway Support

Mobility Access Switch allows you to configure multiple default gateways using the metrics option. Lower metric takes precedence when both routes co-exist. The second gateway with higher metrics takes over when the first route is down.

The multiple default gateways can be configured in two different ways:

- When DHCP import is not configured for the default gateway, you can configure multiple routes with metrics under the IP profile to support multiple default gateways.
- When DHCP import is configured for the default gateway, you can configure the metrics value under the VLAN interface used for the uplinks to support multiple default gateways. This can be configured only from the CLI.

Configuring Multiple Default Gateways and Static Routes

You can configure the static routes and default gateways within the global IP-profile. Each static route needs a destination, netmask and nexthop addresses.

You can configure the static routes using the WebUI or CLI.

Using the WebUI

1. Navigate to the **Configuration > Routing** page.
2. Click **New** under the static routes list.
3. Click on the **Destination IP** column and enter the destination IP address. For default gateway configuration, specify the destination IP as 0.0.0.0
4. Click on the **Destination Mask** column and enter the destination netmask address. For default gateway configuration, specify the destination mask as 0.0.0.0.
5. Click on the **Next Hop** column and enter the nexthop IP address.
6. Click on the **Metric** column and enter the metric.
7. Press **Enter**.

Using the CLI

You can use the following command to configure the static routes with metrics (optional):

```
(host) (config) #ip-profile
(host) (ip-profile) #route <dest-ip> <dest-mask> <next-hop>
(host) (ip-profile) #route 20.20.32.0 255.255.255.0 10.10.10.32
```

Use the following command to configure multiple default gateways with different nexthop IP addresses when DHCP import is not configured:

```
(host) (config) #ip-profile
(host) (ip-profile) #route 0.0.0.0 0.0.0.0 <next-hop> <metrics>
```

Use the following commands to support multiple default gateways when DHCP import is configured for the default gateway:

```
(host) (ip-profile) #default-gateway import dhcp
(host) (ip-profile) #exit
(host) (config) #interface vlan <id>
(host) (vlan "<id>") #metric <cost>
```

Sample Configuration

The following samples configure static routes with multiple next hops and multiple default gateways:

IP Route Configuration

```
(host) (config) #ip-profile
(host) (ip-profile) #default-gateway 2.2.2.2
(host) (ip-profile) #no default gateway
(host) (ip-profile) #default-gateway import dhcp
(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
```

Verifying the IP Routes

```
(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

```

(host) #**show ip route summary**

```

Route Source  Total
-----
connected    6
static       5
ospf-intra   0
ospf-inter   0
ospf-ext1    0
ospf-ext2    0
ospf-nssa    0

```

(host) #**show arp**

```

IPV4 ARP Table
-----
Protocol  IP Address      Hardware Address  Interface
-----
Internet  40.40.40.252    00:0b:86:64:a8:c0  vlan40

```

Default Gateway Configuration

The following example configures multiple default gateways under the IP profile as static routes:

```

(host) (config) #ip-profile
(host) (ip-profile) #route 0.0.0.0 0.0.0.0 200.36.36.36 10
(host) (ip-profile) #route 0.0.0.0 0.0.0.0 142.42.42.42 20

```

The following example configures multiple default gateways under the VLAN interface when the default gateway is obtained from DHCP:

```

(host) (config) #ip-profile
(host) (ip-profile) #default-gateway import dhcp
(host) (ip-profile) #exit
(host) (config) #interface vlan 10
(host) (vlan "10") #metric 10
(host) (config) #interface vlan 20
(host) (vlan "20") #metric 20

```

Verifying Multiple Default Gateway Configuration

Use the following command to view the configuration under the IP profile:

```

(host) #show ip-profile
ip-profile "default"
-----
Parameter          Value
-----
Default Gateway     N/A
Import              DHCP Gateway      Disabled          controller-ip    loopback1
route              0.0.0.0 0.0.0.0    192.168.1.1 10

```

```
route      0.0.0.0 0.0.0.0          172.168.1.1 20
```

Use the following command to verify the VLAN interface configuration:

```
(host) #show running-config | begin ip-profile
Building Configuration...
ip-profile
  default-gateway import dhcp
  controller-ip loopback 1
!
interface vlan "10"
  metric 10
  ip address dhcp-client
!
interface vlan "20"
  metric 20
  ip address dhcp-client
!
```

Route Configuration Limits

The following table specifies the maximum number of routes and nexthops you can have in a Mobility Access Switch:

Table 22: *Route Configuration Limits*

Type of Route/Nexthop	Maximum Routes Supported
IPv4 Unicast + IPv4 Multicast Groups	6912
IPv4 Multicast Sources	1024
IPv6 Unicast + IPv6 Multicast Groups + IPv6 Multicast Sources	320
Address Resolution Protocol	4096 (3k distinct MACs)
Multicast downstream interface table	4096

Equal Cost Multipath



No commands are necessary to enable ECMP.

Equal Cost Multipath (ECMP) enables Mobility Access Switch to forward the data packets to any of the multiple nexthops of a routing destination. The route manager identifies the best routing destination based on the priority of the protocol. After the route manager identifies the best route, all the nexthops of that route are used for datapath forwarding. ECMP is auto-enabled and does not require any command to enable it.

ECMP provides flow-based load balancing for the chosen routing destination. For a given flow same nexthop is used to forward all the packets. For multiple flows, load balancing happens across multiple nexthops. ECMP uses the source IP and destination IP to define a flow. For TCP/UDP packets, it also uses the source and destination ports to define the flow. ECMP automatically load balances the traffic when multiple nexthops with equal cost exist

Apart from multiple nexthops, ECMP also enables addition of metric for a route. ECMP nexthops are per metric basis. For a given metric, there can be multiple nexthops (up to 4). A route with a lower metric is added to the route manager. The higher metric routes are added only when the lower metric routes are deleted.



ECMP is not supported across different nexthop-types.

IP Prefix List

The ip prefix-list 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. The prefix list consists of an IP address and a bit mask. The IP address can be classful network, a subnet, or a single host route.



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

```
(host) (config) #ip-profile
(host) (ip-profile) #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>
(host) (ip-profile) #prefix-list test seq 1 permit 5.5.5.0 255.255.255.0 ge 32
```

Parameter	Description
prefix-list	Prefix list name.
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.

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 can be described as follows:

$$\text{network/length} < \text{ge-length} \leq \text{le-length} \leq 32$$


The ge and le values are optional parameters.

Once you have configured the desired prefix-list entries, you apply them to the global OSPF profile using the following command.

```
(host) (Global OSPF profile) #distribute-list prefix-list <prefix-list name>
```

The following is a sample configuration:

```
(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
(host) (Global OSPF profile) #distribute-list test
```

Verify the IP Prefix List configuration by using the **show ip-profile** command.

```
(host) (ip-profile) #show ip-profile

ip-profile "default"
-----
Parameter          Value
-----
Default Gateway    10.18.7.254
Import DHCP Gateway Disabled
controller-ip      N/A
prefix-list test seq 1 permit 5.5.5.0 255.255.255.0 ge 32
prefix-list test seq 2 deny 6.6.6.0 255.255.255.0 ge 32
prefix-list test seq 3 permit 10.10.0.0 ge 24 le 32
```

Support for Egress ACLs on Routed VLAN Interfaces

The Mobility Access Switch provides support for configuring egress ACLs on the Routed VLAN interfaces (RVI). The Mobility Access Switch supports only permit and deny options on the egress ACL. If both port egress ACL and router egress ACL are applicable, then by default the port egress ACL takes precedence over the RVI egress ACL. However, you can choose to configure the RVI egress ACL or the port egress ACL to have a higher priority globally.

Configuring Egress ACL on a RVI

Use the following command to configure egress ACLs on an RVI:

```
(host) (config) #interface vlan <id>
(host) (vlan "<id>") #ip access-group out <acl-name>
```



You can only apply the standard, stateless, and extended ACLs on an RVI.

Sample Configuration

```
(host) (config) #interface vlan 25
(host) (vlan "25") #ip access-group out egr-acl
```

Verifying the configuration for egress ACL on RVI

Use the following command to verify the egress ACL configuration on the RVI:

```
(host) #show interface-config vlan 25
vlan "25"
-----
Parameter          Value
-----
Interface OSPF profile    N/A
Interface PIM profile     N/A
Interface IGMP profile    N/A
Interface VRRP profile    N/A
Directed Broadcast Enabled Disabled
Interface shutdown        Disabled
Session-processing        Disabled
mtu                       1500
IP Address               25.0.0.1/255.255.255.0
IP NAT Inside             Disabled
IPv6 Address              N/A
```

IPv6 link local Address	N/A
DHCP client	Disabled
DHCP relay profile	N/A
Ingress ACL	N/A
Egress ACL	egr-acl
Interface description	N/A

Configuring Priority for Egress ACLs

Execute the following command to configure the egress ACL priority to RVI globally:

```
(host) (config) #ip egress-acl-priority rvi
```

Execute the following command to configure the egress ACL priority to port globally:

```
(host) (config) #ip egress-acl-priority port
```



If **session-processing** is enabled on an RVI, the configured egress ACL priority is not effective. In such cases, both ACLs are applied and the packets are forwarded only when both ACLs permit.

Verifying Egress ACL Priority Configuration

Execute the following command to verify the egress ACL priority configuration:

```
(host) (config) #show ip egress-acl-priority
ACL with highest egress priority: RVI
```

Route Monitoring

Route Monitoring enables the Mobility Access Switch to monitor the L3 uplink status using ping probe. Route monitoring is deployed on the outer most uplink of branch office where default routes or static routes are installed. Ping probe destined to a server IP address is sent on the uplink interface which is under monitoring. Based on the status of ping reply, probe status of the interface is updated to up or down. Interface probe status is changed from up to down, when there are consecutive unacknowledged pings. Similarly, interface probe status is changed from down to up when there is an acknowledged ping. When the probe status of the interface is down, the Mobility Access Switch removes the network routes from the routing table. When the probe status of the interface is up network routes are added back. However, the directly connected routes and the dynamic routes (that are managed by the respective protocols) are not affected by the probe status. For example OSPF routes are not deleted when the probe status goes down.

This feature is useful for branch deployments where a branch office Mobility Access Switch has two WAN uplinks (primary and standby). When the Mobility Access Switch detects an L3 failure in an established VPN over a primary uplink, it removes the network routes from the routing table and establishes the VPN tunnel through the configured standby uplink. The Mobility Access Switch detects when the primary uplink comes back up and re-establishes the VPN tunnel through the same.



By default Route Monitoring is disabled on the Mobility Access Switch.

Enabling Route Monitoring

You can enable Route Monitoring on the Mobility Access Switch using the following steps in the CLI:

1. Configure a probe profile.
2. Apply the profile to the uplink VLAN interface.

Important Points to Remember

- You can associate only one probe-profile per VLAN interface.

- You can associate the same probe-profile for multiple VLAN interfaces.
- You can configure up to four probe-profiles on the Mobility Access Switch.
- You can configure up to two host IP addresses in a probe-profile. When there are multiple hosts, probe status of the interface is changed to up if ping succeeds to at least one of the configured hosts.
- Only one instance of **pkt-lost-cnt** and **pkt-send-freq** is allowed in a probe-profile.
- In the following scenarios, the probe status is marked as down and is independent of the packet lost count:
 - IP address is not assigned for the interface where the probe is applied. The probe statistics is cleared in this case.
 - Protocol is down for the interface. The probe statistics is cleared in this case.
 - Route is not present for the probe destination.
 - MAC is not resolved for the route next-hop.

Configuring the Probe profile

You can use the following CLI commands to create and configure the probe profile:

Use the following CLI command to create a probe profile:

```
(host) (config) #probe-profile <profile-name>
```

Execute the following command to configure the destination server IP address to be probed using ping:

```
(host) (probe profile "<profile-name>") #destination <ip-address>
```

To configure the minimum number of ping responses to keep the probe status up, execute the following command:

```
(host) (probe profile "<profile-name>") #pkt-found-cnt <pkt-found-cnt>
```

The default value is 6 and the allowed range is 2-32.

To configure the minimum number of packet loss in the ping to mark the interface probe status as down:

```
(host) (probe profile "<profile-name>") #pkt-lost-cnt <pkt-lost-cnt>
```

The default value is 6 and the allowed range is 2-32.

To configure the frequency at which you want to send the ping packets, execute the following command:

```
(host) (probe profile "<profile-name>") #pkt-send-freq <pkt-send-freq>
```

The default value is 5 seconds and the allowed range is 1-32 seconds.

To configure the protocol used for the probe operation, execute the following command:

```
(host) (probe profile "<profile-name>") #protocol icmp
```

This release provides support only for ping probe and hence the only option available to choose is ICMP.

Execute the following commands to apply the probe profile to the uplink interface:

```
(host) (config) # interface vlan <vlan>
(host) (vlan "<vlan>") # probe-profile <profile-name>
```

Configuring metric is optional.

Sample Configuration

```
(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
```

Verifying Route Monitoring Configuration

Use the following command to view the configuration on a probe-profile:

```
(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
```

Use the following command to view 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
```

In addition, starting from 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.

The following sample displays the probe-profile protocol in the output of the **show running-config** command:

```
(host) (config) #show running-config | include icmp
Building Configuration...
netsservice svc-icmp 1
ip access-list stateless icmp-acl-stateless
any any svc-icmp permit
any any svc-icmp permit
access-list stateless icmp-acl-stateless
.
.
.
protocol icmp
```

Viewing Probe Status of Interfaces

Use the following **show** commands to check the probe status of the interfaces where the probe profile is attached.

From ArubaOS 7.4.0.3, the **show probe** command output displays a new **Flags** column, which indicates the cause due to which the probe status of the interface is down.

```
(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
```

(host) #show ip interface brief

```
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
```

(host) #show ip interface vlan 1

```
vlan 1 is Up, protocol is Up
Internet address is 10.16.4.1 /255.255.255.0
Address is statically configured
MTU is 1500
Metric 10
Probe Name: L3Monitoring, Probe Status: Up
```

(host) #show interface vlan 1

```
VLAN1 is administratively Up, Line protocol is Up
Hardware is CPU Interface, Address is 00:0b:86:6b:39:80
Description: Management Interface
Internet address is 10.16.4.1, Netmask is 255.255.255.0
IPV6 link-local address is fe80::b:8600:16b:3980
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: 50331649
MTU 1500 bytes
Metric 10
Probe Name: L3Monitoring, Probe Status: Up
```



When the probe destination is set to the switch's own IP, the probe status is always marked as Up and the status is displayed as **U/O**

Viewing Route Monitoring Logs

To view the logs related to route monitoring such as **route not present** and **MAC not resolved**, enable the probe flag using the following commands:

```
(host) (config) #traceoptions
(host) (traceoptions) #routing flags probe
```

When there is no route present the probe status goes down and displays the following log:

No nexthop via <vlanid> for probe destination <destip>

If probe status is down due to MAC address not resolved, the following log is displayed:

Mac address is not resolved for nexthop

Dynamic Domain Name Server Client

The Mobility Access Switch supports Dynamic Domain Name System (DDNS) protocol to update the public facing IP address of the client with the public domain DDNS server. The client associated with a domain name, which gets a dynamic IP address from the DHCP server ensures that its IP address is always kept up to date.

The Dynamic DNS servers supported by Mobility Access Switch are:

- no-ip.com (free)
- dnsdynamic.org (free)
- changeip.com (free)

- sitelutions.com (free)
- dyn.com (paid)
- myonlineportal.net (from ArubaOS 7.4.0.1 onwards)



Ensure that **ip-name-server** is configured for the feature to be functional.

Configuring DDNS

You can configure the DDNS client on the Mobility Access Switch using the CLI.

```
(host)(config)# interface-profile ddns-profile <profile-name>
(host) (DDNS profile "<profile-name>") #username <username>
(host) (DDNS profile "<profile-name>") password <password>
(host) (DDNS profile "<profile-name>") service-url <url>
(host) (DDNS profile "<profile-name>") interval <days:hours:minutes>
(host) (DDNS profile "<profile-name>") hostname <name>
```



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: dynupdate.no-ip.com/nic/update.

Use the following command to attach DDNS profile to an interface VLAN:

```
(host)(config) #interface vlan <id>
(host) (vlan "id") #ddns-profile <profile-name>
```



You can create only two DDNS profiles and only one profile can be attached on an interface VLAN. When you try to create a third DDNS profile, the Error: Cannot create more than two DDNS profiles message is displayed.

Sample Configuration

```
(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
```

To attach ddns1 to interface vlan 4:

```
(host)(config) #interface vlan 4
(host) (vlan "4") #ddns-profile ddns1
```

Verifying DDNS

You can use the following command to verify if DDNS is configured on a client:

```
(host) # show interface-profile ddns-profile <profile-name>
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
```

You can use the following command to verify the updates being sent to the server:

```
(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

Static Address Resolution Protocol

The static ARP entries are address resolutions that are manually added to the cache table for a device and are retained in the cache on a permanent basis. Mobility Access Switch allows you to add static Address Resolution Protocol (ARP) entries using the CLI.

Configuring Static ARP

Use the following command to configure an ARP entry:

```
(host) (config) #arp <ipaddr> <macaddr>
```

- <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.

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.

Sample Configuration

The following command configures an ARP entry:

```
(host) (config) #arp 10.73.7.222 ac:7f:3e:e6:cc:05
```

Verifying Configuration

Use the following command to view the list of ARP entries configured:

```
(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
```

Clearing the ARP Table

You can use the following command to clear the ARP table:

```
(host) #clear arp {<all>|<ip-address>}
```

Proxy Address Resolution Protocol

Starting from ArubaOS 7.4.1.1, the Mobility Access Switch provides proxy ARP support. If the proxy ARP feature is enabled, SOS traps all the ARP packets to the Proxy-ARP module in the control plane.

Configuring Proxy ARP

To configure a port security profile (for example, "PARP"), execute the following command:

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

To enable the proxy-arp, execute the following command:

```
(host) (Port security profile "<profile name>") #proxy-arp
```

Execute the following command to enter the port mode:

```
(host) (Port security profile "<profile name>") #interface gigabitethernet <slot>/<module>/<port>
```

To apply the port-security-profile to the interface, execute the following command:

```
(host) (gigabitethernet "<port>") #port-security-profile "PARP"
```

Sample Configuration

The following commands configures a proxy ARP and help enter the port mode to apply the port-security profile:

```
(host) (config) #interface-profile port-security-profile "PARP"
(host) (Port security profile "PARP") #proxy-arp
(host) (Port security profile "PARP") #interface gigabitethernet 0/0/10
(host) (gigabitethernet "0/0/10") #port-security-profile "PARP"
```

Verifying Configuration

Use the following command to view the Proxy ARP configuration:

```
(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
```

The following are the commands to unconfigure proxy ARP:

```
(host) (Port security profile "PARP") #interface gigabitethernet 0/0/10
(host) (gigabitethernet "0/0/10") #no port-security-profile
(host) (gigabitethernet "0/0/10") #no interface-profile port-security-profile "PARP"
```

Virtual Router Redundancy Protocol (VRRP) enables a group of layer 3 configured Mobility Access Switches to form a single virtual router. LAN clients may be configured with the virtual router IP as the default gateway.

This chapter includes the following topics:

- [VRRP Definitions on page 211](#)
- [VRRP Overview on page 211](#)
- [Important Points to Remember on page 212](#)
- [VRRP Deployment Scenarios on page 212](#)
- [Enabling and Configuring VRRP on page 213](#)
- [Sample Configuration on page 215](#)

VRRP Definitions

Table 23: Common VRRP Terms

Term	Definition
VRRP Router	A Mobility Access Switch running the Virtual Router Redundancy Protocol. It may participate in one or more virtual routers.
Virtual Router	An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP address(es) across a common LAN. A VRRP Router may backup one or more virtual routers.
Primary IP Address	In an active-standby scenario, the IP address of the master Mobility Access Switch is the primary IP address.
Virtual Router Master	The VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router, and answering ARP requests for these IP addresses.

VRRP Overview

The underlying mechanism for the Aruba redundancy solution is the Virtual Router Redundancy Protocol (VRRP). VRRP is used to create various redundancy solutions, including:

- pairs of Mobility Access Switches acting in an active-active mode or a hot-standby mode.
- a master Mobility Access Switch backing up a set of backup Mobility Access Switches.
- a pair of Mobility Access Switches acting as a redundant pair of master Mobility Access Switches in a hot-standby mode.

VRRP eliminates a single point of failure by providing an election mechanism, among the Mobility Access Switches, to elect a VRRP master Mobility Access Switch. If VRRP preemption is disabled and all Mobility Access Switches share the same priority, the first Mobility Access Switch that comes up becomes the master. However, if VRRP preemption is enabled (the default setting) and all the Mobility Access Switches share the same priority, the Mobility Access Switch with the highest IP address becomes the master. This helps in achieving high-availability in Mobility Access Switch.

The master Mobility Access Switch owns the configured virtual IP address for the VRRP instance. When the master Mobility Access Switch becomes unavailable, a backup Mobility Access Switch steps in as the master and takes ownership of the virtual IP address. All network elements (APs and controllers) can be configured to access the virtual IP address, thereby providing a transparent redundant solution to your network.

Following are the advantages of enabling VRRP:

- Redundancy on a cluster of virtual-interfaces: Alternate paths can be configured for the hosts in the network without any explicit configuration by creating redundancy. This eliminates single point of failure.
- Load sharing in a cluster of virtual interfaces: To eliminate under-utilization of a backup Mobility Access Switch in a cluster, you can configure an active-active VRRP deployment, This way the hosts can share the traffic amongst the Mobility Access Switches in the cluster.

Important Points to Remember

- The Mobility Access Switch implementation of VRRP adheres to RFC 2338.
- VRRP is disabled by default and should be enabled manually on a layer-3 VLAN interface.
- For VRRP to be operational, you should have at least one IP address configured on a layer-3 VLAN interface.
- You can configure a maximum of two VRRP profiles on a layer-3 VLAN interface.

VRRP Deployment Scenarios

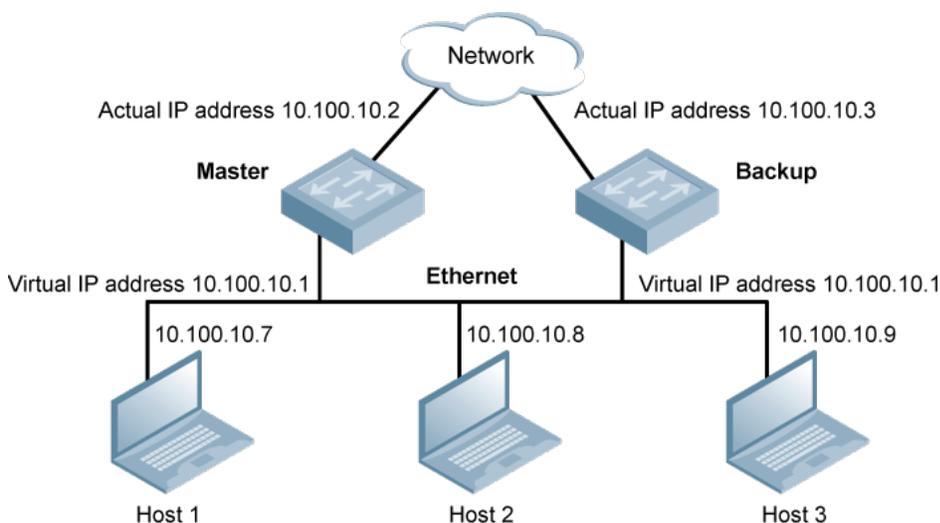
The following VRRP deployment scenarios are described in this section:

- [Active-Standby Deployment on page 212](#)
- [Active-Active Deployment on page 213a](#)

Active-Standby Deployment

In an active-standby deployment, one Mobility Access Switch is configured as the active or master and the other as standby or backup. If the master Mobility Access Switch fails or should become unavailable at any point of time, the backup Mobility Access Switch takes over from the master Mobility Access Switch by the use of dynamic fail-over and the network state is maintained. [Figure 16](#) shows a simple active-standby deployment.

Figure 16 *Active-Standby Deployment*

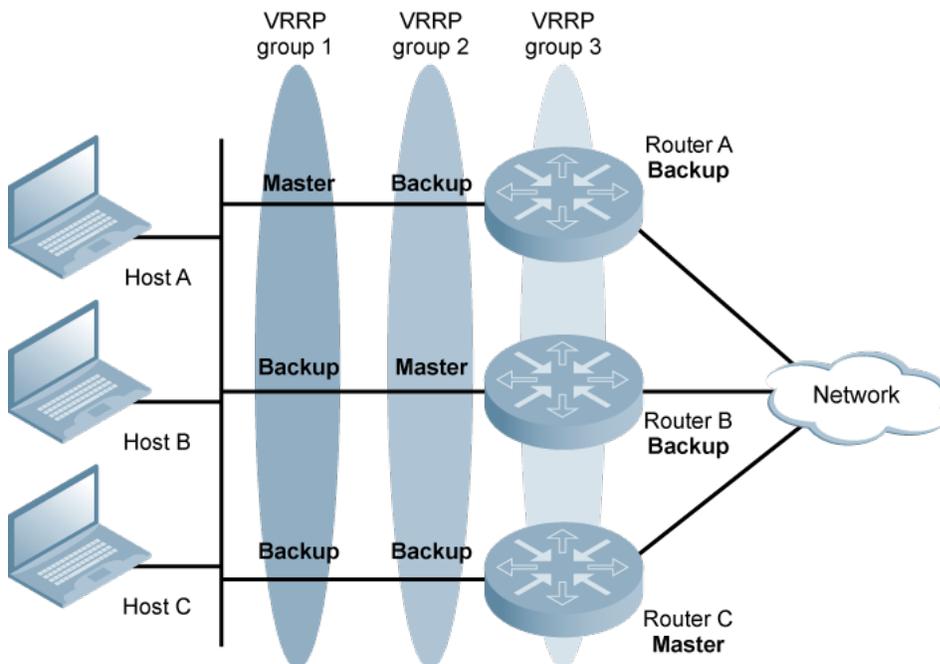


In [Figure 16](#), the active (master) Mobility Access Switch and standby (backup) Mobility Access Switch are participating in VRRP. The VRRP protocol creates a virtual router with 10.100.10.1 as the Virtual IP address. This IP address serves as the default gateway for IP clients connected to the master and backup Mobility Access Switches. Host 1, 2, and 3 now have the default gateway address as 10.100.10.1. If the master Mobility Access Switch fails or should become unavailable at any point of time, the backup Mobility Access Switch takes over from the master Mobility Access Switch. Due to the loss of availability of a route in the master Mobility Access Switch, traffic continues to flow from the host to the network.

Active-Active Deployment

In the active-standby deployment, the backup Mobility Access Switch remains under-utilized as no traffic is routed through this Mobility Access Switch. Active-active deployment does load-balancing and is the most common and preferred deployment model. [Figure 17](#) shows a typical active-active deployment.

Figure 17 Active-Active Deployment



A Mobility Access Switch can be a part of multiple VRRP groups and can hold a different priority in a different group. In [Figure 17](#), there are three VRRP groups.

- VRRP group 1: Router A is the master; Router B and Router C are the backups.
- VRRP group 2: Router B is the master; Router A and Router C are the backups.
- VRRP group 3: Router C is the master; Router A and Router B are the backups.

For load-balancing between Router, A, B, and C, hosts on the LAN is configured to use VRRP group 1, 2, and 3 as the default gateway respectively. The VRRP priorities are configured in such a way, that each router takes the expected role in the group. The Mobility Access Switch with the highest priority wins the election for the role of master in a pre-emptive mode of operation. For more information on VRRP priorities, see [Enabling and Configuring VRRP on page 213](#).

Enabling and Configuring VRRP

This section describes the VRRP configuration on Mobility Access Switch.

VRRP Profile Configuration

The following CLI commands enable and configure VRRP on the Mobility Access Switch.

```
(host) (config) #vrrp <id>
  advertise <interval>
  clone <source>
  ip <address>
  no
  preempt
  preemption delay <seconds>
  priority <level>
  shutdown
  tracking vlan <vlanId>
```

Table 24: VRRP Parameter Definition

Parameter	Description
vrrp <id>	Unique virtual router ID of the VRRP profile.
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.
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. This is the default setting. 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.
preemption delay <seconds>	Delay in seconds, the backup should wait for before transitioning to master.
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.
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.

You can view the VRRP interface profile state and statistics by using the following CLI command:

```
(host) #show vrrp [<id> statistics]
```

You can verify the VRRP interface profile configuration by using the following CLI command:

```
(host) #show vrrp-config [<id>]
```

Once you configure the VRRP profile, apply this profile to the layer-3 VLAN interface. The CLI commands are as follows:

```
(host) (config) #interface vlan <id>
    vrrp-profile <id>
```

Load-Balancing using VRRP

To achieve load-balancing in a Mobility Access Switch, you can apply a maximum of 2 VRRP profiles with different Virtual Router ID to a layer-3 VLAN interface of the Mobility Access Switch. Sample example follows:

```
(host) (config) #interface vlan 1
(host) (vlan "1") #vrrp-profile 1
(host) (vlan "1") #vrrp-profile 2
```

You can verify the configuration by using the following CLI command:

```
(host) #show interface-config vlan <id>
```

Clear VRRP statistics

You can clear the VRRP operational statistics from the running configuration of the Mobility Access Switch by using the following CLI command:

```
(host) #clear vrrp <id> statistics
```

Sample Configuration

This section describes a sample example of configuring VRRP on the Mobility Access Switch.

The following example configures a VRRP profile on the Mobility Access Switch.

```
(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
```

Apply the newly configured VRRP profile to the VLAN interface. The CLI commands are as follows:

```
(host) (config) #interface vlan 1
(host) (vlan "1") #vrrp-profile 1
```

You can view the VRRP interface profile state and statistics by using the following CLI command:

```
(host) #show vrrp 1
```

```
VRRP Instance Information
```

Virtual 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

You can verify the VRRP interface profile configuration by using the following CLI command:

```
(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
```

You can verify the VLAN configuration by using the following CLI commands:

```
(host) #show interface-config vlan 1
```

```
vlan "1"
-----
Parameter                               Value
-----
Interface OSPF profile                   N/A
Interface PIM profile                    N/A
Interface IGMP profile                   N/A
Interface VRRP profile                 1
Directed Broadcast Enabled               Disabled
Interface shutdown                       Disabled
Session-processing                       Disabled
mtu                                       1500
IP Address                               192.0.2.1
IP NAT Inside                            Disabled
IPv6 Address                             N/A
IPv6 link local Address                  N/A
DHCP client                              Disabled
DHCP relay profile                       N/A
Ingress ACL                              N/A
Interface description                    N/A
```

This chapter describes the following topics:

- [Policy Based Routing Overview on page 217](#)
- [Configuring Policy-Based Routing on page 217](#)
- [Sample Configurations on page 219](#)

Policy Based Routing Overview

Policy-based routing (PBR) provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator. By default, PBR is disabled. When enabled, you can implement policies that selectively cause packets to take different paths. PBR is used to route IP unicast packets based on a policy. Unlike the traditional destination IP based route lookups, the switch uses ACLs to determine how to forward a packet. This could be beneficial in the branch deployments where traffic could be sent on different uplinks based on packet characteristics. For example, if a branch has two ISPs, traffic matching a certain criteria as determined by an ACL could be send to ISP1 and traffic matching different criteria could be send to ISP2.

Important Points to Remember

- Only IPv4 unicast packets can be policy routed.
- Next hop IP address must be same as that of the L3 router that is adjacent/directly connected.
- PBR can be applied only to VLAN interfaces.
- PBR would take precedence over IPsec routing.
- ACLs that have next hop/L3 GRE tunnel/IPsec map cannot be applied to port or user and ACLs applied to ports/users cannot be modified to have new ACE entries with next hop/L3 GRE tunnel/IPsec.
- MAS supports 32 unique nexthops for PBR.
- Stateless ACLs have an implicit deny at the end of the ACL. So a permit statement without nexthop/redirect option must be configured to allow traffic that needs to be permitted, but not subjected to policy routing.
- Traffic destined to the switch will also get policy routed if it matches any of the entries configured for policy routing. Permit statement without nexthop/redirect option must be configured before policy routing statements for traffic destined to the switch.

Configuring Policy-Based Routing

PBR is configured as extensions to stateless ACLs, with next hop as part of the ACE entry in permit or redirect for redirection over a tunnel/IPsec interface. Once a stateless ACL has been configured, it can be applied to a VLAN interface, that need to be policy routed.

Configuring Nexthop IP as part of ACE Entry

Use the following command to enter stateless ACL configuration mode:

```
(host) (config) #ip access-list stateless st
(host) (config-stateless-st) #?
alias                Match a IPv4 network resource
any                  Match any IPv4 source traffic
host                 Match a single IPv4 host address
network              Match IPv4 subnet
no                   Delete Command
```

The following example configures the Nexthop IP:

```
(host) (config) #ip access-list stateless abc
(host) (config-stateless-abc) # any any tcp <port-number><port-number> permit nexthop <ip-addr>
```

Configuring Redirect to Tunnel as part of ACE Entry

```
(host) (config-stateless-st)#any any udp 10 100 ?
deny                Specify packets to reject
permit             Specify packets to forward
redirect           Redirect packets
(host) (config-stateless-st)#any any udp 10 100 redirect ?
ipsec              Redirect based on IPsec map
tunnel            Redirect packets to tunnel
(host) (config-stateless-st)#any any udp 10 100 redirect tunnel ?
<1-50>            Tunnel ID
(host) (config-stateless-st)#any any udp 10 100 redirect tunnel 10
```

The following example configures redirect to tunnel:

```
(host) (config-stateless-abc) #any any udp <port-number><port-number> redirect tunnel <id>
```



Ensure that the tunnel ID that is used in the redirect keyword for PBR is a Layer 3 GRE tunnel.

Configuring IPsec Map as part of ACE Entry

```
(host) (config-stateless-st)#any any udp 200 500 redirect ?
ipsec              Redirect based on IPsec map
tunnel            Redirect packets to tunnel
(host) (config-stateless-st)#any any udp 200 500 redirect ipsec ?
<mapname>         ipsec map name [1..30]
(host) (config-stateless-st)#any any udp 200 500 redirect ipsec ipsec1
(host) (config-stateless-st)#end
```

The following example configures an IPsec map:

```
(host) (config-stateless-st) # any any udp <port-number><port-number> redirect ipsec <mapname>
```

Configuring a Deny Entry

```
(host) (config-stateless-st)#any any ?
<0-255>           IP protocol number
STRING            Name of network service
any              Match any traffic
arp              Match ARP traffic
tcp              Match TCP traffic
udp              Match UDP traffic
(host) (config-stateless-st)#any any tcp 400 50 ?
deny             Specify packets to reject
permit          Specify packets to forward
redirect        Redirect packets
(host) (config-stateless-st)#any any tcp 400 500 ?
deny             Specify packets to reject
permit          Specify packets to forward
redirect        Redirect packets
(host) (config-stateless-st)#any any tcp 400 500 deny
```

You can use the following command to configure a deny entry:

```
(host) (config-stateless-abc) # any any tcp <port-number> <port-number> deny
```

Applying Stateless ACL on VLAN Interface

```
(host) (config) #interface vlan <number>
(host) (vlan "number") #ip access-group in abc
```

Sample Configurations

To configure the policy based routing:

```
(host) (config) #ip access-list stateless st
(host) (config-stateless-st) # any any tcp 10 100 permit nexthop 200.0.0.5
(host) (config-stateless-st) # any any udp 10 100 redirect tunnel 10
(host) (config-stateless-st)# any any udp 10 101 redirect ipsec ipsec1
(host) (config) #interface vlan 100
(host) (vlan 100) #ip access-group in st
```

To apply stateless ACL on VLAN interface:

```
(host) (config) #interface vlan 100
(host) (vlan 100) #ip access-group in st
```

Verifying Configuration

```
(host) #show interface-config vlan 100
vlan "100"
```

```
-----
Parameter                               Value
-----
Interface OSPF profile                   N/A
Interface PIM profile                    N/A
Interface IGMP profile                   N/A
Directed Broadcast Enabled               Disabled
Interface shutdown                       Disabled
mtu                                       1500
IP Address                               100.0.0.1/255.255.255.0
IP NAT Inside                            Disabled
IPv6 Address                             N/A
IPv6 link local Address                  N/A
DHCP client                              Disabled
DHCP relay profile                       N/A
Ingress ACL                              st
Interface description                    N/A
```


This chapter describes the DHCP server and relay support on the Mobility Access Switch. It contains the following sections:

- [Understanding DHCP Server and DHCP Relay on page 221](#)
- [Configuring DHCP Server and DHCP Relay on page 221](#)
- [Verifying DHCP Server and DHCP Relay on page 224](#)
- [Local DHCP Server Device Reservation on page 226](#)

Understanding DHCP Server and DHCP Relay

Dynamic Host Configuration Protocol automates network-parameter assignment to network devices from one or more DHCP servers. Even in small networks, DHCP is useful because it makes it easy to add new machines to the network.

When a DHCP-configured client connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, other servers such as time servers, and so forth.

On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting, and must complete before the client can initiate IP-based communication with other hosts.

During initialization, network clients try to dynamically obtain their IP addresses. In small networks, where all the systems are in the same IP subnet, the client and the server can communicate directly.

Clients on subnets that are not directly connected to a DHCP server must go through a "relay agent."

If DHCP relay is not enabled on the VLAN on which the request is received, but a pool is configured for that subnet, the IP is assigned from the internal DHCP server.

DHCP relay is enabled when a DHCP relay profile is attached to a VLAN interface. At this point, the relay agent receives the DHCP broadcast packets from the client and unicast them to one or more of the DHCP servers that are configured on the VLAN interface.



Mobility Access Switch does not support DHCP server identifier override sub-option.

Configuring DHCP Server and DHCP Relay

This section contains the following sections:

- [Configuring DHCP Server on page 221](#)
- [Configuring DHCP Relay on page 222](#)
- [Applying DHCP Relay Profile to VLAN on page 223](#)

Configuring DHCP Server

DHCP server configuration is profile based. To configure the DHCP server, follow these steps:

1. Enable DHCP server configuration.

- ```
(host)(config) #service dhcp
```
2. Configure a DHCP server profile.
 

```
(host)(config) #ip dhcp pool pool-1
(host)(dhcp server profile "pool-1") #
```
  3. Configure the domain name in the pool profile.
 

```
(host)(dhcp server profile "pool-1") #domain-name doc-domain
```
  4. Configure the DNS servers. You can configure up to 8 DNS servers in a DHCP pool one by one.
 

```
(host)(dhcp server profile "pool-1") #dns-server 192.168.1.2
```
  5. Configure the default router. Up to 8 routers can be configured.
 

```
(host)(dhcp server profile "pool-1") #default-router 192.168.1.1
```
  6. Configure the Netbios name server. Up to 8 Netbios name servers can be configured.
 

```
(host)(dhcp server profile "pool-1") #netbios-name-server 192.168.1.3
```
  7. Configure the lease time in days, hours, minutes, and seconds.
 

```
(host)(dhcp server profile "pool-1") #lease 30 24 60 60
```
  8. Configure the network.
 

```
(host)(dhcp server profile "pool-1") #network 192.168.1.0 255.255.255.0
```
  9. Configure the range between two IP addresses to be excluded.
 

```
(host)(dhcp server profile "pool-1") #exclude-address 192.168.1.1 192.168.1.3
```
  10. Configure a vendor-class-identifier.
 

```
(host)(dhcp server profile "pool-1") #vendor-class-identifier testVendor
```
  11. Configure server options.
 

```
(host)(dhcp server profile "pool-1") #option 50 ip 192.168.1.1
(host)(dhcp server profile "pool-1") #option 54 text server1
```

## Configuring DHCP Relay

DHCP-Relay is supported with DHCP Option 82. DHCP Option 82 allows a DHCP relay agent to insert circuit specific information into a request that is being forwarded to a DHCP server.

DHCP Option 82 works by setting two sub-options:

- Circuit ID  
The circuit ID includes information specific to the circuit on which the request arrives. Circuit identifier parameters can be interface-name, VLAN ID, or both.
- Remote ID  
The remote ID carries information relating to the remote host end of the circuit. Remote identifier parameters can be the MAC address, the hostname of the relay agent, or a user defined string.

DHCP Relay Option 82 can be configured using DHCP Relay profile. To configure a DHCP Relay profile, follow these steps:

1. Configure a DHCP Relay profile under an interface profile.
 

```
(host)(config) #interface-profile dhcp-relay-profile relay1
```
2. Configure a helper address.
 

```
(host)(dhcp relay profile "relay1") #helper-address 172.16.30.1
```
3. Configure Option 82 circuit-identifier a VLAN only, an interface-name only or both VLAN and interface-name:
 

```
(host)(dhcp relay profile "relay1") #option82 circuit-identifier vlan
(host)(dhcp relay profile "relay1") #option82 circuit-identifier interface-name
(host)(dhcp relay profile "relay1") #option82 circuit-identifier interface-name vlan
```
4. Configure Option 82 remote-identifier with the host-name option.

```
(host) (dhcp relay profile "relay1") #option82 remote-identifier host-name
```

5. Configure Option 82 remote-identifier as MAC.

```
(host) (dhcp relay profile "relay1") #option82 remote-identifier mac
```

6. Configure Option 82 with the user defined option "myOwnString."

```
(host) (dhcp relay profile "relay1") #option82 remote-identifier myOwnString
```

## Applying DHCP Relay Profile to VLAN

The DHCP relay profile must be applied to the VLAN where DHCP clients connect. To configure a DHCP Relay profile to a VLAN, follow these steps:

1. Configure a VLAN interface.

```
(host) (config) #interface vlan 11
```

2. Configure an IP address on the VLAN interface.

```
(host) (vlan "11") #ip address 172.16.4.1 netmask 255.255.255.0
```

3. Configure DHCP Relay profile on the VLAN interface.

```
(host) (vlan "11") #dhcp-relay-profile relay1
```

## Configuring a VLAN with a Relay Profile as DHCP Client

Keep the following points in mind before you configure a VLAN with a relay profile as DHCP client.

### Points to Remember

- You can configure both static default gateway and default gateway import from DHCP.
- Static and OSPF routes have preference over DHCP and DHCP has preference over OSPF AS External routes.
- The DHCP routes will be installed only if **default gateway import dhcp** is specified in the ip-profile.
- If multiple VLANs act as DHCP clients with the **default-gw import dhcp** option, then the first valid DHCP gateway received in the response will be installed in the routing table.

### Configuration Steps

1. Configure a VLAN.

```
(host) (config) #interface vlan 4
```

2. Configure a DHCP relay profile.

```
(host) (vlan "4") #dhcp-relay-profile relay1
```

3. Set the IP address of an interface and use DHCP to obtain an IP address.

```
(host) (vlan "4") #ip address dhcp-client
(host) (vlan "4") #end
```

4. Display the VLAN Interface

```
(host) #show interface-config vlan 4
```

```
vlan "4"

Parameter Value

Interface OSPF profile N/A
Interface PIM profile N/A
Interface IGMP profile N/A
Interface shutdown Disabled
mtu 1500
IP Address N/A
IPv6 Address 2012::12/64
IPv6 link local Address fe80::b:8600:a6a:3300
```

|                       |         |
|-----------------------|---------|
| DHCP client           | Enabled |
| DHCP relay profile    | relay1  |
| Interface description | N/A     |

## Verifying DHCP Server and DHCP Relay

This section contains the following sections:

- [Verifying DHCP Relay Option 82 Logs on page 224](#)
- [Show Commands for IP DHCP on page 224](#)

### Verifying DHCP Relay Option 82 Logs

The debug level can be configured to log the DHCP relay messages. It can be configured in network or system logs.

#### Network Log

```
(host)(config) #logging level debugging network process dhcpd subcat dhcp
```

#### System Log

```
(host)(config) #logging level debugging system process dhcpd subcat all
```

The DHCP relay functionality can be verified by checking network or system logs as has been configured:

```
Sep 27 07:30:43 dhcpdwrap[1497]: <202523> <DEBUG> |dhcpdwrap| |dhcp| dhcprelay: dev=eth1, length=341, from_port=67, op=2, giaddr=172.16.4.1
Sep 27 07:30:43 dhcpdwrap[1497]: <202527> <DEBUG> |dhcpdwrap| |dhcp| RelayToClient: OFFER dest=172.16.4.2 client yiaddr=172.16.4.1 MAC=1c:75:08:9e:60:c8
Sep 27 07:30:43 dhcpdwrap[1497]: <202541> <DEBUG> |dhcpdwrap| |dhcp| Received DHCP packet from Datpath, sos msg hdr flags 0x42 opcode 0x5a ingress 0x0 vlan 11 egress 0xb src mac 00:0b:86:6a:41:40
Sep 27 07:30:43 dhcpdwrap[1497]: <202544> <DEBUG> |dhcpdwrap| |dhcp| Datapath vlan11: ACK 1c:75:08:9e:60:c8 clientIP=172.16.4.2
```

### Show Commands for IP DHCP

This section describes the following commands:

- [show interface-profile dhcp-relay-profile on page 224](#)
- [show ip dhcp database on page 224](#)
- [show ip dhcp binding on page 225](#)
- [show ip dhcp statistics on page 225](#)

#### show interface-profile dhcp-relay-profile

To display an IP DHCP Relay profile, use the following command:

```
(host)#show interface-profile dhcp-relay-profile relay1
```

```
dhcp relay profile "relay1"

Parameter Value
----- -
DHCP helper address 172.16.30.1
Option82 Circuit-Id option vlan interface-name
Option82 Remote-Id option myOwnString
Giaddr as Source IP Disabled
```

#### show ip dhcp database

To display the complete IP DHCP database, use the following command:

```
(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;
```

## show ip dhcp binding

To display the DHCP binding table, use the following command:

```
(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";
}
```



---

The DHCP server assigns the abandoned leases only after all the free entries are exhausted.

---

## show ip dhcp statistics

Displays the statistics in the pools stating the number of active leases, free leases etc

```
(host)#show ip dhcp statistics

Network Name 172.16.1.0/24
 Free leases 249
 Active leases 3
 Expired leases 0
 Abandoned leases 0
```

## show ip dhcp pool

Displays the list of the dhcp pools configured and information about their references:

```
(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
```

## show ip dhcp pool

```
(host)#show ip dhcp pool <pool_name>
```

This command displays the details of the pool

```
(host)#show ip dhcp pool pool-1
```

```
dhcp server profile "pool-1"
```

```

Parameter Value

Domain name for the pool www.test.com
DHCP server pool 192.168.1.0/255.255.255.0
DHCP pool lease time 0 12 0 0
Vendor Class Identifier testStr
DHCP default router address 192.168.1.253
Configure DNS servers N/A
Configure netbios name servers N/A
DHCP Option 43 ip 192.168.1.254
Exclude address 192.168.1.254
Exclude address 192.168.1.253
```

## Local DHCP Server Device Reservation

The Mobility Access Switch provides support for assigning a fixed IP address for a specific device using DHCP based on the MAC address of the device. You can configure the IP address for a device from a locally configured DHCP pool using the CLI.

### Configuring DHCP Device Reservation

Use the following CLI command to configure a specific IP to a device:

```
(host) (config) #service dhcp
(host) (service dhcp) #exit
(host) (config) #ip dhcp pool <pool>
(host) (dhcp server profile "<pool>") #network <address> <mask>
(host) (dhcp server profile "<pool>") #hardware-address <mac-address> ip-address <address>
(host) (dhcp server profile "<pool>") #exit
(host) (config) #interface vlan <id>
(host) (vlan "<id>") #ip address <addr> <mask>
(host) (vlan "<id>") #no shut
```

### Sample Configuration

```
(host) #configure terminal
(host) (config) #service dhcp
(host) (service dhcp) #exit
(host) (config) #ip dhcp pool pool_4
```

```
(host) (dhcp server profile "pool_4") #network 4.4.4.0 255.255.255.0
(host) (dhcp server profile "pool_4") #hardware-address 00:00:ac:07:01:13 ip-address 4.4.4.2
(host) (dhcp server profile "pool_4") #hardware-address 00:00:ac:07:01:14 ip-address 4.4.4.3
(host) (dhcp server profile "pool_4") #hardware-address 00:00:ac:07:01:15 ip-address 4.4.4.4
(host) (dhcp server profile "pool_4") #exit
(host) (config) #interface vlan 4
(host) (vlan "4") #ip address 4.4.4.1 255.255.255.0
(host) (vlan "4") #no shut
```

## Verifying DHCP Reservation Configuration




---

In ArubaOS 7.3.2 ,the **show ip dhcp binding** command output does not display the DHCP reservation details.

---

Use the following command to view a configured DHCP pool with device reservations:

```
(host) #show ip dhcp pool pool_4
dhcp server profile "pool_4"

Parameter Value

Domain name for the pool N/A
DHCP server pool 4.4.4.0/255.255.255.0
DHCP pool lease time 0 days 12 hr 0 min 0 sec
Vendor Class Identifier ArubaAP
DHCP default router address N/A
Configure DNS servers N/A
Configure netbios name servers N/A
DHCP Option N/A
Exclude address N/A
Device reservation 00:00:ac:07:01:13 4.4.4.2
Device reservation 00:00:ac:07:01:14 4.4.4.3
Device reservation 00:00:ac:07:01:15 4.4.4.4
```

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
```

## Limitations

- If there are more than 498 DHCP reservations, the output of the **show ip dhcp pool <poolname>** command does not display anything.
- When the number of DHCP reservations exceeds 695 the leased IPs are not displayed in the output of the **show ip dhcp reserved** command .
- After a system switchover, the list of DHCP reservations do not appear in the output of the **show ip dhcp reserved** command.



This chapter contains the following sections:

- [OSPF Feature Overview on page 229](#)
- [Configuring OSPF on page 229](#)
- [OSPF MD5 Authentication on page 234](#)

## OSPF Feature Overview

Open shortest path first (OSPFv2) is a dynamic interior gateway routing protocol (IGP) based on IETF RFC 2328. Aruba's implementation of OSPFv2 allows the Mobility Access Switch to be effectively deployed in a Layer 3 topology.

### Key Features Supported by Mobility Access Switch

- All stub area types
- Area border router (ABR)
- OSPF on VLAN and loopback interfaces
- OSPF MD5 authentication
- One OSPF instance
- Redistribute VLANs
- OSPF interface can belong to only one area
- Route Summarization

### LSAs Originated by Mobility Access Switch

With current implementation, the following Link State Advertisement (LSA) types are generated by Mobility Access Switch:

- Type 1 Router LSA
- Type 2 Network LSA
- Type 3 Summary LSA
- Type 4 ASBR Summary LSA

Notes:

- Routes learned from VLAN-based access interfaces are distributed to OSPF as Router LSAs (Type 1).
- Mobility Access Switch can process Type 5 AS External LSA.
- Mobility Access Switch can process Type 7 NSSA External LSA.

## Configuring OSPF

This section contains the following sections:

- [Configuring OSPF on page 230](#)
- [Configuring OSPF Area Types on page 230](#)
- [Configuring prefix-list with OSPF on page 231](#)
- [Verifying the Configuration on page 231](#)

- [Enabling OSPF on a Loopback Interface on page 233](#)
- [Enabling OSPF with L3 GRE Tunnel Interface on page 234](#)

## Configuring OSPF




---

The **router ospf** command must be configured to start the OSPF process.

---

To configure OSPF, follow these steps:

1. Enter the global OSPF configuration mode.

```
(host) (config) #router ospf
(host) (Global OSPF profile)
```

2. Assign the router identification.

```
(host) (Global OSPF profile) router-id 5.5.5.5
```

3. Assign areas.

```
(host) (Global OSPF profile) area 0.0.2.0
(host) (Global OSPF profile) area 0.0.0.1 stub
```

4. Create the interface OSPF profile "techpubs."

```
(host) (config) #interface-profile ospf-profile techpubs
(host) (Interface OSPF profile "techpubs") #
```

5. Assign an area and cost to the profile "techpubs."

```
(host) (Interface OSPF profile "techpubs") #area 0.0.2.0
(host) (Interface OSPF profile "techpubs") #cost 10
```

6. Attach the OSPF profile "techpubs" to a VLAN.

```
(host) (config) #interface vlan 2
(host) (vlan "2") #ospf-profile techpubs
(host) (vlan "2") #ip address 172.0.10.254 255.255.255.0
```

## Configuring OSPF Area Types

ArubaOS Mobility Access Switch supports all Open Shortest Path First (OSPF) area types including Totally Stubby Area (TSA) and Not-So-Stubby-Area (NSSA). The following new commands are added to the Command Line Interface (CLI).

In the configuration mode, type **router ospf** to enter global OSPF profile mode.

To set an area as NSSA:

```
(host) (Global OSPF profile) #area <areaid> nssa
```

To set an area as Totally NSSA:

```
(host) (Global OSPF profile) #area <areaid> nssa no-summary
```

To set an area as TSA:

```
(host) (Global OSPF profile) #area <areaid> stub no-summary
```

To enable sending default route in NSSA:

```
(host) (Global OSPF profile) #area <areaid> nssa default-info-originate metric <cost> metric-type <mtype>
```

To generate default Link State Advertisement (LSA) in normal area:

```
(host) (Global OSPF profile) #default-info-originate [always] | [metric <cost> metric-type <mtype>]
```

For additional parameters, see *ArubaOS 7.4.x Command Line Interface* guide.

## Sample Configuration

```
(host) (config) #router ospf
(host) (Global OSPF profile) #area 0.0.0.1 nssa
(host) (Global OSPF profile) #area 0.0.0.2 nssa no-summary
(host) (Global OSPF profile) #area 0.0.1.0 stub no-summary
(host) (Global OSPF profile) #area 0.0.2.0 nssa default-info-originate metric 1 metric-type 1
(host) (Global OSPF profile) #default-info-originate always
```

## Configuring prefix-list with OSPF

You can filter networks received from LSA updates. The **prefix-list** command is used to configure IP prefix filtering. Prefix lists are used to either permit or deny the configured prefix based on a matching condition.



---

For a detailed description of the IP Prefix-list feature, see [IP Prefix List on page 202](#).

---

The **distribute-list** command filter networks received in updates. This command references to the user-defined prefix-list.

```
(host) (config) #router ospf
(host) (Global OSPF profile) #distribute-list <prefix-list name>
```

The **show router ospf** command verifies the distribute-list configuration.

```
(host) (config) #show router ospf
```

For **show router ospf** sample configuration, see [Verifying the Configuration on page 231](#).

## Sample Configuration



---

This example assumes that a prefix-list called **aruba** has already been created.

---

```
(host) (config) #router ospf
(host) (Global OSPF profile) #distribute-list aruba
```

## Verifying the Configuration

View the global OSPF profile values.

```
(host) (config) #show router ospf
```

```
Global OSPF profile "default"

Parameter Value

State Enabled
Area 0.0.0.0
Area 0.0.1.0 (stub)
Area 0.0.0.1 (nssa)
Area 0.0.0.2 (nssa)
Area 0.0.2.0 (nssa)
Area 0.0.0.4 (totally-stubby)
Router-id 10.10.10.10
Redistribute vlan 2
Distribute-list aruba
```

View the parameters and values for the interface OSPF profile "techpubs".

```
(host) (vlan "2") #show interface-profile ospf-profile techpubs
```

```
Interface OSPF profile "techpubs"

```

```

Parameter Value

Area 0.0.2.0
Cost 10
Dead-interval Auto
Hello-interval 10
Retransmit-interval 5
Transmit-delay 1
Priority 1
State Enabled

```

### View the interface configuration for VLAN 2.

```
(host) (vlan "2") #show interface-config vlan 2
```

```

vlan "2"

Parameter Value

Interface OSPF profile techpubs
Interface PIM profile N/A
Interface IGMP profile N/A
Interface shutdown Disabled
mtu 1500
IP Address 172.0.10.254/255.255.255.0
IPv6 Address N/A
IPv6 link local Address N/A
DHCP client Disabled
DHCP relay profile N/A
Interface description N/A

```

### Verify that the OSPF interface is running on VLAN 2.

```
(host) #show ip ospf interface vlan 2
```

```

Interface is vlan2, line protocol is up
Internet Address 172.0.10.254, Mask 255.255.255.0, Area 0.0.2.0
Router ID 5.5.5.5, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router id 0.0.0.0, Interface Address 0.0.0.0
Backup designated Router id 0.0.0.0, Interface Address 0.0.0.0
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

```

### Verify the IP Routes

```
(host) #show ip route
```

```

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 10.232.10.1 to network 0.0.0.0 at cost 17
O(IA) * 0.0.0.0 /0 [17] via 10.232.10.1
O(IA) 1.0.0.99 /32 [2] via 10.232.10.1
O(IA) 1.0.0.103/32 [2] via 10.232.20.1

```

```

O(IA) 1.0.0.104/32 [3] via 10.232.10.1
O(IA) 1.0.0.105/32 [3] via 10.232.10.1
O(IA) 1.0.0.106/32 [3] via 10.232.10.1
O(IA) 1.0.0.108/32 [3] via 10.232.10.1
S 10.0.0.0 /8 [0] via 10.4.135.254
M 10.4.135.0/24 is directly connected: mgmt
M 10.4.135.91/32 is directly connected: mgmt
C 10.64.8.0/24 is directly connected: vlan66
C 10.64.8.1/32 is directly connected: vlan66
C 10.65.8.0/24 is directly connected: vlan21
C 10.65.8.1/32 is directly connected: vlan21
C 10.69.8.0/24 is directly connected: vlan61
C 10.69.8.1/32 is directly connected: vlan61
C 10.70.8.0/24 is directly connected: vlan81
C 10.70.8.1/32 is directly connected: vlan81
C 10.128.63.1/32 is directly connected: loopback0
C 10.128.64.0/24 is directly connected: vlan64
<omitted>

```

```
(host) #show ip route summary
```

```

Route Source Total

connected 419
static 1
ospf-intra 400
ospf-inter 820
ospf-ext1 0
ospf-ext2 0
ospf-nssa 0

```

## Enabling OSPF on 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
```

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

```

5. 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
Interface description N/A
```

#### 6. 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
```

## Enabling OSPF with L3 GRE Tunnel Interface

1. Create L3 GRE tunnel interface. See [Configuring an L3 GRE Tunnel on page 187](#).

2. Create OSPF profile.

a. Create the interface OSPF profile “techpubs.”

```
(host) (config) #interface-profile ospf-profile techpubs
(host) (Interface OSPF profile "techpubs") #
```

b. Assign an area and cost to the profile “techpubs.”

```
(host) (Interface OSPF profile "techpubs") #area 0.0.2.0
(host) (Interface OSPF profile "techpubs") #cost 10
```

3. Attach the ospf-profile “techpubs” to the L3 GRE interface.

```
host) (config) #interface tunnel ip 1
host) (config) (Tunnel "1") # ospf-profile techpubs
```

4. Verify OSPF-profile interface.

```
(host) #show ip ospf interface
(host) #show ip ospf interface brief
```

The following sample displays the output of the **show ip ospf interface brief** command in a tabular format:

```
(host) # show ip ospf interface brief
Brief OSPF Interface Information

Interface Instance Area IP Address/Mask Cost State Neighbors F/C

vlan201 0 0.0.0.0 69.1.1.1/255.255.255.0 1 DOWN 0/0
vlan202 0 0.0.0.1 79.11.1.1/255.255.255.0 1 DOWN 0/0
```



---

The **show ip ospf interface brief** command is applicable from ArubaOS 7.4.1.0 release version.

---

## OSPF MD5 Authentication

This section contains the following sections:

- [Important Points to Remember on page 235](#)
- [Understanding OSPF MD5 Authentication on page 235](#)
- [Configuring OSPF MD5 Authentication on page 235](#)
- [Verifying OSPF MD5 Authentication on page 235](#)

## Important Points to Remember

- Mobility Access Switch supports only OSPF MD5 authentication on a per-interface basis.
- Mobility Access Switch supports only OSPF MD5 authentication key and does not support simple OSPF authentication.

## Understanding OSPF MD5 Authentication

To protect Open Shortest Path First (OSPF) connections from spoofing attacks, the Mobility Access Switch supports MD5 authentication. MD5 is a message-digest algorithm that is specified in RFC 1321 and considered to be the most secure OSPF authentication mode.

Without MD5 authentication, a remote attacker can spoof an OSPF packet so that it appears to come from a trusted source, but can then change the routing tables of the unprotected device or exploit other vulnerabilities in the AOS OSPF network.

Note that you must configure the same MD5 key and password on both OSPF neighbors. The neighbor-ship only forms when both devices have the matching key and password.

Mobility Access Switch supports only MD5 OSPF authentication and not simple OSPF authentication. With simple authentication, the password traverses the network in clear-text. With MD5 OSPF authentication, the password does not traverse the network.

## Configuring OSPF MD5 Authentication

To configure OSPF MD5 authentication, follow these steps:

1. Configure an OSPF profile in an interface profile:  

```
(host) (config) #interface-profile ospf-profile ospf1
```
2. Configure an MD5 key and password.  

```
(host) (Interface OSPF profile "ospf1") #message-digest-key 1 md5-passwd Aruba
```
3. Attach the interface OSPF profile to the vlan interface:  

```
(host) (config) #interface vlan 1
(host) (vlan "1") #ospf-profile ospf1
```

## Verifying OSPF MD5 Authentication

This section contains the following sections:

- [Verifying OSPF MD5 Authentication Configuration from the Interface Profile on page 235](#)
- [Verifying the OSPF MD5 Authentication Configuration on page 236](#)
- [Verifying OSPF MD5 Authentication on page 236](#)

## Verifying OSPF MD5 Authentication Configuration from the Interface Profile

To verify the OSPF MD5 Authentication configuration from the Interface Profile, use the following show command:

```
(host) (config) #show interface-profile ospf-profile ospf1
```

```
Interface OSPF profile "ospf1"

Parameter Value

Area 0.0.0.0
Cost 1
Dead-interval Auto
Hello-interval 10
Retransmit-interval 5
Transmit-delay 1
```

```
Priority 1
md5-key 1
md5-passwd *****
State Enabled
```

## Verifying the OSPF MD5 Authentication Configuration

To verify the OSPF MD5 Authentication configuration, use the following show command:

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

```
Building Configuration...
router ospf
 area 0.0.0.0
interface-profile ospf-profile "ospf1"
 message-digest-key 1 md5-passwd 2aa9fdf39271f7779771543efd658fd0
 area 0.0.0.0
```

## Verifying OSPF MD5 Authentication

To verify the OSPF MD5 Authentication, use the following show command:

```
(host) (config) #show ip ospf interface vlan 1
```

```
Interface is vlan1, line protocol is up
Internet Address 10.10.10.2, Mask 255.255.255.0, Area 0.0.0.0
Router ID 10.10.10.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router id 10.10.10.2, Interface Address 10.10.10.2
Backup designated Router id 0.0.0.0, Interface Address 0.0.0.0
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Message digest authentication enabled key id:1
Neighbor Count is 0
Tx Stat: Hellos 19 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 19
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
```

## OSPF Route Summarization

Route summarization, also called route aggregation, is a method of minimizing the number of routing entries in a routing table. Starting from ArubaOS 7.3.1, Mobility Access Switch supports OSPF Route summarization functionality. This feature provides benefits such as minimizing number of routing tables, reducing the routing traffic, and minimizing the Shortest Path First (SPF) computation time in an OSPF network.

There are two types of summarization:

- **External route summarization:** External route summarization is specific to external routes that are injected into OSPF using route re-distribution. Ensure that external ranges that are being summarized are contiguous. The external route summarization can be done on Autonomous System Border Routers (ASBRs).
- **Inter-area route summarization:** You can configure inter-area route summarization on Area Border Routers (ABRs) and summarize routes between areas in the autonomous system.

## Configuring OSPF Route Summarization

Use the following command to configure external route summarization:

```
(host) (config)# router ospf
(host) (Global OSPF profile)# summary-address <ip> <netmask>
```

Use the following command to configure inter-area route summarization to consolidate and summarize the routes at the boundary:

```
(host) (config)# router ospf
(host) (Global OSPF profile)# area-range <ip> <netmask> <area-id>
```

## Sample Configuration

To configure external routes:

In the following example, the summary address 10.7.0.0/20 includes the addresses 10.7.0.1, 10.7.8.1, 10.7.12.1, and so on. However, only the address 10.7.0.0/20 is advertised in an external Link-State Advertisement (LSA).

```
(host) (config) #router ospf
(host) (Global OSPF profile) # router-id 2.3.4.5
(host) (Global OSPF profile) # summary-address 10.7.0.0 255.255.240.0
(host) (Global OSPF profile) # exit
(host) (config) #interface vlan 3333
(host) (vlan "3333") # ip address 10.7.0.1 255.255.248.0
(host) (vlan "3333") # exit
(host) (config) #interface vlan 400
(host) (vlan "400") # ip address 10.7.8.1 255.255.252.0
(host) (vlan "400") # exit
(host) (config) #interface vlan 4000
(host) (vlan "4000") # ip address 10.7.12.1 255.255.254.0
```

To configure inter-area route summarization:

The following example specifies one summary route to be advertised by the ABR to other areas for VLANs 10, 20, 30 and 40.

```
(host) (config)# router ospf
(host) (Global OSPF profile)# interface-profile ospf-profile "area254"
(host) (Interface OSPF profile "area254") #cost 1000
(host) (Interface OSPF profile "area254") #area 10.0.0.254
(host) (Interface OSPF profile "area254") # exit
(host) (config)# interface vlan 10
(host) (vlan 10)# ip address 192.168.1.0 255.255.255.0
(host) (vlan 10)# ospf-profile area254
(host) (vlan 10)# exit
(host) (config)# interface vlan 20
(host) (vlan 20)# ip address 192.168.2.0 255.255.255.0
(host) (vlan 20)# ospf-profile area254
(host) (vlan 20)# exit
(host) (config)# interface vlan 30
(host) (vlan 30)# ip address 192.168.3.0 255.255.255.0
(host) (vlan 30)# ospf-profile area254
(host) (vlan 30)# exit
(host) (config)# interface vlan 40
(host) (vlan 40)# ip address 192.168.4.0 255.255.255.0
(host) (vlan 40)# ospf-profile area254
(host) (vlan 40)# exit
(host) (config)# router ospf
(host) (Global OSPF profile)# area-range 192.168.0.0 255.255.0.0 10.0.0.254
```



The IPv6 protocol enables the next generation of large-scale IP networks by supporting addresses that are 128 bits long. This allows  $2^{128}$  possible addresses (versus  $2^{32}$  possible IPv4 addresses).

IPv6 addresses are represented as eight colon-separated fields of up to four hexadecimal digits each. The following are examples of IPv6 addresses:

```
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:0:800:200C:417A
```

The use of the “::” symbol is a special syntax that you can use to compress one or more 16-bit groups of zeros or to compress leading or trailing zeros in an address. The “::” can appear only once in an address. For example, the address, 1080:0:0:0:0:800:200C:417A can also be represented as 1080::800:200C:417A.

IPv6 uses subnet identifiers to identify subnetworks to which nodes are attached. The subnet mask is a bitmask that specifies the prefix length. For example, 1080::800:200C:417A ffff:ffff:ffff:ffff:: represents all IPv6 addresses with the subnet identifier 1080:0:0:0.

## IPv6 Support for Mobility Access Switch

ArubaOS provides IPv6 support on the Mobility Access Switch.




---

IPv6 support is currently limited to management functionality.

---

Following are the IPv6 functionalities supported on the Mobility Access Switch:

- Default IPv6 support on all RVI interfaces and Management interface.
- Auto-configured link local address on all IPv6 interfaces based on the MAC address and VLAN Id combination.
- Ability to override the auto configured link local address with another link local address.
- Ability to configure multiple global unicast addresses.
- Ability to ping other IPv6 hosts.
- Telnet support.
- Default gateway configuration support.

You can perform the following IPv6 operations on the Mobility Access Switch:

- [Configure an IPv6 Interface Address](#)
- [Configure IPv6 Default Gateway](#)
- [Debug IPv6 Mobility Access Switch](#)

You can also view the IPv6 related information on the Mobility Access Switch using the following commands:

- **show interface <intf name>**: View the IPv6 auto configured link local address and global unicast address of a VLAN interface
- **show ipv6 neighbors**: View the IPv6 neighbors
- **show ipv6 route**: View the IPv6 routes
- **show ipv6 interface brief**: View the list of IPv6 interfaces on the Mobility Access Switch
- **show ipv6 interface**: View detailed information about IPv6 interfaces

## Configure an IPv6 Interface Address

You can configure an IPv6 address for the management interface and VLAN interface of the Mobility Access Switch. The Mobility Access Switch can have multiple IPv6 addresses for each VLAN interface. You can configure IPv6 interface addresses using the following CLI commands.

To modify the auto-configured link local address of the VLAN interface, execute the following commands:

```
(host) (config) #interface vlan <vlan#>
(host) (vlan "#") #ipv6 address link-local <link_local>
```

To configure the global unicast address, execute the following commands:

```
(host) (config) #interface vlan <vlan#>
(host) (vlan "#") #ipv6 address <prefix> prefix_len <prefix_length>
```

To configure global unicast address on the management interface, execute the following commands:

```
(host) (config) #interface mgmt
(host) (mgmt) #ipv6 address <prefix> prefix_len <prefix_length>
```

To modify the auto-configured link local address of the management interface, execute the following commands:

```
(host) (config) #interface mgmt
(host) (mgmt) #ipv6 address link-local <link_local>
```

## Configure IPv6 Default Gateway

You can configure IPv6 default gateway using the following CLI command:

```
(host) (config) #ipv6-profile
(host) (ipv6-profile) #default-gateway <nextHop>
```

## Debug IPv6 Mobility Access Switch

You can now use the Ping command to debug IPv6 hosts.

To ping the global unicast address execute the following command:

```
(host) #ping ipv6 <global-address>
```

To ping the link-local address of the host connected to the VLAN interface execute the following command:

```
(host) #ping ipv6 interface vlan <vlan-id> <linklocal-address>
```

To ping the link-local address of the host connected to the management interface execute the following command:

```
(host) #ping ipv6 interface mgmt <linklocal-address>
```

This chapter contains the following major sections:

- [Important Points to Remember on page 241](#)
- [Understanding IGMP, PIM-SM and PIM-SSM on page 241](#)
- [Configuring IGMP on page 242](#)
- [Configuring PIM Sparse Mode on page 244](#)
- [Configuring PIM Source Specific Multicast on page 246](#)

### Important Points to Remember

- PIM-SM and PIM-SSM run on top of IGMP and needs an IGMP profile for the VLAN interface.
- IGMP must be enabled to run PIM-SM or PIM-SSM.
- IGMP version 2 is enabled by default.

### Understanding IGMP, PIM-SM and PIM-SSM

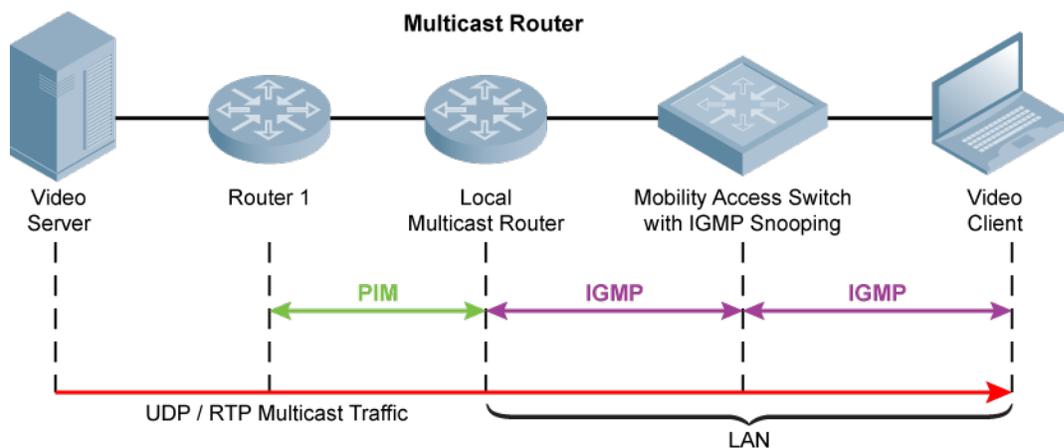
This section contains the following sections:

- [IGMP on page 241](#)
- [Basic IGMP Network Architecture on page 241](#)
- [PIM on page 242](#)
- [PIM Sparse Mode on page 242](#)
- [PIM-Source Specific Multicast on page 242](#)

### IGMP

The Mobility Access Switch supports Internet Group Management Protocol (IGMP) as defined in IETF RFC 1112 (IGMPv1) and RFC 2236 (IGMPv2). IGMP allows hosts and adjacent routers on IP networks to establish multicast group memberships.

### Basic IGMP Network Architecture



## PIM

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols such as the Border Gateway Protocol (BGP).

There are four variants of PIM, of which the Mobility Access Switch supports PIM Sparse Mode (PIM-SM).

### PIM Sparse Mode

PIM-SM explicitly builds unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source. PIM-SM generally scales fairly well for wide-area usage. PIM-SM is useful for routing multicast streams between VLANs, subnets, or local area networks (LANs) in applications such as IPTV

### PIM-Source Specific Multicast

Mobility Access Switch provides support for source specific multicast (SSM) protocol. Clients can request for traffic only from a specific source list in a given group of addresses using SSM. You can enable SSM on a Mobility Access Switch using the CLI.

## Configuring IGMP

This section contains the following sub-sections:

- [Configuring and Applying an IGMP Profile to a VLAN Interface on page 242](#)
- [Viewing IGMP Interface Profile on page 243](#)
- [Viewing IGMP Groups on page 243](#)
- [Viewing IGMP Interface VLAN on page 243](#)
- [Viewing IGMP Interface VLAN Statistics on page 243](#)

### Configuring and Applying an IGMP Profile to a VLAN Interface

To configure an IGMP profile, follow these steps:

1. Create an IGMP profile under the interface profile.

```
(host) (config) #interface-profile igmp-profile igmp1
(host) (Interface IGMP profile "igmp1") #
```
2. Enable IGMP profile (by default, IGMP version 2 is enabled).

```
(host) (Interface IGMP profile "igmp1") #no disable
```
3. Enable IGMP version 3 (optional):

```
(host) (Interface IGMP profile "igmp1") #version v3
```



---

Disabling IGMP version 3 using the **no version v3** command enables the IGMP version 2.

---

4. Assign IGMP profile to a VLAN interface.

```
(host) (Interface IGMP profile "igmp1") #interface vlan 2
(host) (vlan "2") #igmp-profile igmp1
```
5. Verify the IGMP configuration on a VLAN interface.

```
(host) (vlan "2") #show interface-config vlan 2
vlan "2"

```

```

Parameter Value

Interface OSPF profile ospf-a0
Interface PIM profile default
Interface IGMP profile igmp1
Interface shutdown Disabled
mtu 1500
IP Address 20.1.1.4/255.255.255.0
IPv6 Address N/A
IPv6 link local Address N/A
DHCP client Disabled
DHCP relay profile N/A
Interface description N/A

```

## Viewing IGMP Interface Profile

To view the default interface IGMP profile, use the following command:

```

(host) #show interface-profile igmp-profile default
Interface IGMP profile "default" (N/A)

```

```

Parameter Value

IGMP query interval(secs) 125
Enable IGMP protocol Enabled
IGMP version v2

```

## Viewing IGMP Groups

To view IGMP groups, use the following command:

```

(host)#show ip igmp groups
IGMP Group Information

```

```

Interface Group UpTime Expiry Last Reporter Compatibility Mode

vlan11 225.0.0.3 00h:02m:21s Never 11.1.1.3 v3

```

## Viewing IGMP Interface VLAN

To view IGMP interface VLAN information, use the following command:

```

(host)#show ip igmp interfaces vlan 12

```

```

vlan12 is up, line protocol is up
 Internet address is 20.12.1.1
 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: 1 joins, 0 leaves
 IGMP querying routers 20.12.1.1

```

## Viewing IGMP Interface VLAN Statistics

Use the following command to view the IGMP interface VLAN statistics:

```

(host) # show ip igmp stats interface vlan 3333

```

```

Flags: IN - INCLUDE, EX - EXCLUDE, SRC - SOURCE, lmqt - Last Member Query Timer

```

```

IGMP Statistics

Interface Counter Value

vlan3333 Rx v1v2 Queries 0000
Rx v1v2 Reports 0000
Rx Leaves 0000
Tx v2 Queries 0000
Rx v3 Queries 0000
Rx v3 Reports 66182
Rx v3 IS_IN record 33091
Rx v3 IS_EX record 0000
Rx v3 TO_IN record 0000
Rx v3 TO_EX record 0000
Rx v3 BLOCK_SRC record 0000
Rx v3 ALLOW_SRC record 33091
Tx v3 General Queries 0312
Tx v3 Group Queries 0000
Tx v3 (S,G) Queries 0000
Tx v3 (S,G) lmqt Queries 0000

```

## Configuring PIM Sparse Mode

This section contains the following sections:

- [Configuring PIM-SM End to End on page 244](#)
- [Verifying PIM Sparse Mode on page 245](#)

### Configuring PIM-SM End to End

To configure PIM-SM end to end, follow these steps:

1. Create a VLAN.

```
(host) (config) #vlan 7
(host) (VLAN "7") #exit
```

2. Create an interface-profile switching-profile profile to associate with a physical interface.

```
(host) (config) #interface-profile switching-profile ip-sp-profile
```

3. Add an access-vlan to set the VLAN when interface is in access mode.

```
(host) (switching profile "ip-sp-profile") #access-vlan 7
(host) (switching profile "ip-sp-profile") #exit
```

4. Associate the interface-profile switching-profile with a physical interface profile.

```
(host) (config) #interface gigabitethernet 0/0/0
(host) (gigabitethernet "0/0/0") #switching-profile ip-sp-profile
(host) (gigabitethernet "0/0/0") #exit
```

5. Create the routed VLAN interface (RVI).

```
(host) (config) #interface vlan 7
(host) (vlan "7") #
```

6. Assign an IP address to the routed VLAN interface (RVI).

```
(host) (vlan "7") #ip address 20.2.1.1 netmask 255.255.255.0
```

7. Associate the "default" PIM profile with the routed VLAN interface (RVI).

```
(host) (vlan "7") #pim-profile default
(host) (vlan "7") #exit
```

8. Use the router pim command to enter Global PIM profile mode and define the RP address and group range.

```
(host) (config) #router pim
(host) (Global PIM profile) #rp-address 224.0.0.1 group-range 225.0.0.0 255.0.0.0
```



---

When configuring static RP, please ensure the RP is active and reachable. If the RP is not reachable, multicast traffic fails.

---

## Verifying PIM Sparse Mode

This section contains the following sections:

- [Displaying PIM RPF Information on page 245](#)
- [Displaying PIM Neighbor Information on page 245](#)
- [Displaying PIM RP Information on page 245](#)
- [Displaying PIM Mroute Information on page 245](#)
- [Displaying PIM Statistical Information on page 246](#)

Starting from ArubaOS 7.4.0.2, the counters for multicast route entries are included in the output of the following **show** commands:

- show ip pim mroute
- show ip pim mroute detail

### Displaying PIM RPF Information

```
(host) #show ip pim rpf 10.10.10.10
PIM RPF Information

Address Nexthop RPF Interface

10.10.10.10 20.20.1.9 vlan20
```

### Displaying PIM Neighbor Information

To display PIM neighbor information, use the following command:

```
(host)# show ip pim neighbor
PIM Neighbor Information

Interface Neighbor IP UpTime Expiry

vlan11 11.11.22.22 07:58:51 08:00:20
```

### Displaying PIM RP Information

To display PIM RP information, use the following command:

```
(host)# show ip pim rp
PIM RP-Group Mapping

Group/Prefix RP

224.0.0.0/4 11.11.22.22
```

### Displaying PIM Mroute Information

To display PIM Mroute information, use the following command:

```
(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.

## Displaying PIM Statistical Information

To display PIM statistical information, use the following command:

```
(host)# show ip pim stats
PIM Statistics

Interface Counter Value
----- -
vlan11 Rx Hellos 0056
 Rx Join/Prune 0000
 Rx Join 0000
 Rx Prune 0000
 Rx Register-Stop 0000
 Tx Hellos 0057
 Tx Join/Prune 0016
 Tx Join 0000
 Tx Prunes 0000
 Tx Register 0000
 Invalid Hellos 0000
 Invalid Join/Prune 0000
 Invalid Join 0000
 Invalid Prune 0000
 Invalid Register 0000
 Invalid Register-Stop 0000
```

## Configuring PIM Source Specific Multicast

This section contains the following sections:

- [Enabling PIM-SSM on page 246](#)
- [Viewing List of SSM Addresses on page 246](#)
- [Viewing SSM Range of Mroutes on page 247](#)

### Enabling PIM-SSM

Use the following CLI command to enable PIM-SSM on the Mobility Access Switch:

```
(host) (config) #router pim
(host) (Global PIM profile) # ssm
```

### Viewing List of SSM Addresses

Starting from ArubaOS 7.4.0.2, the counters for multicast route entries are included in the output of the following **show** commands:

- `show ip pim-ssm mroute`
- `show ip pim-ssm mroute detail`

Execute the following command to view the list of source addresses for the specified group of addresses:

```
(host) #show ip igmp groups <group_ip> detail
```

The following command displays the source list details for the IP group, 225.1.2.3:

```
(host) #show ip igmp groups 225.1.2.3 detail
Interface: vlan4001
Group: 225.1.2.3
Uptime: 00h:04m:56s
```

```

Group Mode: INCLUDE
Group Compatibility Mode: IGMPV3
Group Expiry: Never
Last Reporter: 144.40.40.41
Group source list

```

| Source       | UpTime      | Expiry      | Last Member Query |
|--------------|-------------|-------------|-------------------|
| 99.99.99.100 | 00h:04m:56s | 00h:04m:12s | NOT RUNNING       |

## Viewing SSM Range of Mroutes

Use the following command to view 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
Total (S,G) Entries : 0

```

**Total (S,G) Entries** is the number of multicast routes from a specific source to a specific group.

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

```



You can enable multicast support on the Mobility Access Switch with IGMP snooping. You can enable the Mobility Access Switch to listen in on the IGMP conversation between hosts and network devices, and create a mapping table of which links need which IP multicast streams and which multicasts can be filtered from the links which do not need them.

This chapter includes the following topics:

- [Important Points to Remember on page 249](#)
- [Multicast Support with IGMP Snooping on page 249](#)
- [Mrouter on page 254](#)
- [Creating and Applying an IGMP Snooping Profile to a VLAN on page 251](#)
- [Sample Configuration on page 251](#)
- [IGMP Snooping Factory Initial and the Default Profiles on page 250](#)
- [Verifying IGMP Snooping Configuration on page 252](#)
- [Monitoring IGMP Snooping on page 253](#)

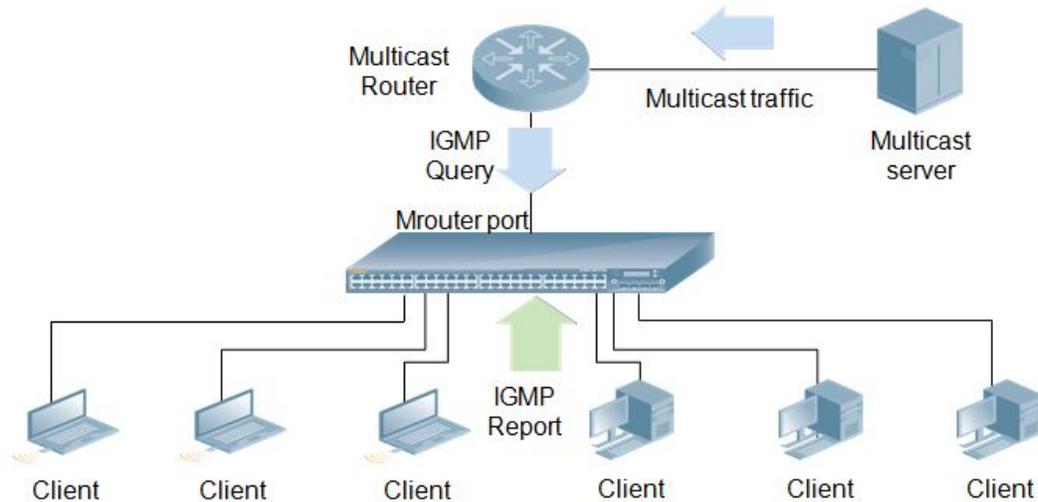
## Important Points to Remember

- IGMP Snooping version 2 is enabled by default.
- IGMP Snooping is enabled on per-VLAN basis.
- IGMP Snooping profile must be referenced in the VLAN and not on the interface.
- IGMP versions 1, 2, and 3 are supported for Snooping.

## Multicast Support with IGMP Snooping

The Mobility Access Switch supports IGMP snooping, which prevents multicast flooding on Layer 2 network treating multicast traffic as broadcast traffic. All streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would be receiving all the streams only to be discarded without snooping.

When you enable IGMP snooping, the switch becomes IGMP-aware and processes the IGMP control messages as received. You must do this to correctly process all IGMP membership reports and IGMP leave messages. IGMP snooping is handled by the hardware for performance. Multicast routers and multicast receivers associated with each IP multicast group are learnt dynamically.



## Snooping Report and Query Support

The Mobility Access Switch relays IGMP report from all receiver per group to the multicast router. In IGMP snooping proxy mode, reports to multicast router ports are suppressed. Query from multicast router is relayed to all ports in the VLAN. When snooping proxy is enabled, the switch queries hosts for interested receivers and it floods the query message received from a multicast router. When IGMP query message is seen, it becomes a mrouter port in IGMP snooping table. This port is used for forwarding multicast frames that are sourced from a VLAN to a multicast router for further processing.

## Support for IGMPv3 Snooping

IGMPv3 Snooping is used to snoop the membership reports that have group records of different types. These group records specify the source specific Multicast (SSM) traffic for a particular group.

The group record types used by v3 in the membership reports are as follows:

- IS\_INCLUDE
- IS\_EXCLUDE
- TO\_INCLUDE
- TO\_EXCLUDE
- ALLOW\_SRCS
- BLOCK\_SRCS

IGMP Snooping is configured as a profile under `vlan-profile` and is attached to a VLAN. By default, v3 snooping is disabled and v2 snooping is enabled in an `igmp-snooping` profile. A new configuration command is introduced to enable v3 snooping explicitly.



IGMPv3 Snooping is effective only when all the clients under the VLAN are v3 capable. If a V2 client joins the IGMPv3 Snooping enabled VLAN, the VLAN downgrades the snooping to IGMPv2 causing the v3 capable clients on the VLAN to receive traffic from all sources in that group.

## IGMP Snooping Factory Initial and the Default Profiles

Execute the following commands to view the IGMP snooping factory initial and the default profiles, respectively:

```
(host)# show vlan-profile igmp-snooping-profile igmp-snooping-factory-initial
```

```
igmp-snooping-profile "igmp-snooping-factory-initial" (N/A)
```

```

Parameter Value

IGMP snooping Enabled
IGMPv3 snooping Disabled
IGMP snooping proxy Disabled
IGMPv3 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
```

```
(host) (config) #show vlan-profile igmp-snooping-profile default
igmp-snooping-profile "default" (N/A)
```

```

Parameter Value

IGMP snooping Enabled
IGMPv3 snooping Disabled
IGMP snooping proxy Disabled
IGMPv3 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
```

## Creating and Applying an IGMP Snooping Profile to a VLAN

Use the following command to create an IGMP Snooping profile:

```
(host) (config) # vlan-profile igmp-snooping-profile <profile-name>
clone <source>
```

You can use the following CLI command to enable IGMPv3 snooping in an igmp-snooping profile:

```
(host) (config) #vlan-profile igmp-snooping-profile <profile-name>
(host) (igmp-snooping-profile "<profile-name>") #snooping v3
```

To enable v2 snooping proxy, use the following command:

```
(host) (igmp-snooping-profile "<profile-name>") #snooping-proxy
```

To enable v3 snooping proxy, use the following command:

```
(host) (igmp-snooping-profile "<profile-name>") #snooping-proxy v3
```

To apply the IGMP snooping profile to a VLAN interface, use the following command:

```
(host) (config) # vlan <vlan-id>
vlan-profile igmp-snooping-profile <profile-name>
```

### Sample Configuration

Use the following sample to configure an IGMP v2 Snooping:

```
(host) (config) # vlan-profile igmp-snooping-profile IGMP_SNOOP
```

```
(host) (igmp-snooping-profile "IGMP_SNOOP") fast-leave
(host) (igmp-snooping-profile "IGMP_SNOOP") last-member-query-count 2
(host) (igmp-snooping-profile "IGMP_SNOOP") last-member-query-interval 15
(host) (igmp-snooping-profile "IGMP_SNOOP") query-interval 6000
(host) (igmp-snooping-profile "IGMP_SNOOP") query-response-interval 5
(host) (igmp-snooping-profile "IGMP_SNOOP") robustness-variable 2
(host) (igmp-snooping-profile "IGMP_SNOOP") snooping
(host) (igmp-snooping-profile "IGMP_SNOOP") snooping-proxy
(host) (igmp-snooping-profile "IGMP_SNOOP") startup-query-count 5
(host) (igmp-snooping-profile "IGMP_SNOOP") startup-query-interval 6000
(host) (config)# vlan 200
(host) (VLAN "200") #vlan-profile igmp-snooping-profile IGMP_SNOOP
```

Use the following sample to configure an IGMP v3 Snooping:

```
(host) (config) #vlan-profile igmp-snooping-profile igmp-snoop-11
(host) (igmp-snooping-profile "igmp-snoop-11") #snooping v3
(host) (igmp-snooping-profile "igmp-snoop-11") #snooping-proxy v3
(host) (config) #vlan 11
(host) (VLAN "11") #igmp-snooping-profile igmp-snoop-11
```

## Verifying IGMP Snooping Configuration

Use the following show command to verify the IGMP Snooping configuration:

```
(host) # show vlan-profile igmp-snooping-profile igmp-snoop-11
```

```
igmp-snooping-profile "igmp-snoop-11" (N/A)
```

```

Parameter Value

IGMP snooping Enabled
IGMPv3 snooping Enabled
IGMP snooping proxy Enabled
IGMPv3 snooping proxy Enabled
Enable fast leave Enabled
startup-query-count 2
startup-query-interval (secs) 31
query-interval (secs) 15000
query-response-interval (secs) 10
last-member-query-count 2
last-member-query-interval (secs) 10
robustness-variable 2
```

You can use the following command on a VLAN interface to know the IGMP Snooping version in use:

```
(host) #show vlan 11 extensive
```

```
Dot1q tag: 11, Description: VLAN0011
IGMP-snooping profile name: igmp-snoop-11
IGMP-snooping: Enabled, Version: 3
IGMP-snooping proxy: Enabled, Version: 3
MAC aging time: 5 minutes
Number of interfaces: 28, Active: 22
VLAN membership:
GE0/0/2* Access Trusted Untagged
GE0/0/3* Access Trusted Untagged
GE0/0/4* Access Trusted Untagged
GE0/0/5* Access Trusted Untagged
GE0/0/6* Access Trusted Untagged
GE0/0/7* Access Trusted Untagged
```

## Monitoring IGMP Snooping

```
(host)# show igmp-snooping counters vlan 2
```

```
IGMP Snooping Multicast Counters
```

```

Name Value
---- -
received-total 0000
received-queries 0000
received-v1-reports 0000
received-v2-reports 0000
received-v3-reports 0000
received-pimv1-hello 0000
received-pimv2-hello 0000
received-leaves 0000
received-unknown-types 0000
len-errors 0000
checksum-errors 0000
transmitted-queries 0000
transmitted-joins 0000
transmitted-leaves 0000
transmitted-errors 0000
forwarded-queries 0000
forwarded-joins 0000
forwarded-leaves 0000
```

```
(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
```

You can also use the following commands:

```
(host)# show igmp-snooping counters vlan <vlan-id>
(host)# show igmp-snooping groups vlan <vlan-id>
(host)# show igmp-snooping membership vlan <vlan-id> | detail
(host)# show igmp-snooping mrouter vlan <vlan-id> | detail
```

## Clearing IGMP Counters and Membership

```
(host)(config)# clear igmp-snooping counters
(host)(config)# clear igmp-snooping counters vlan <vlan-id>
(host)(config)# clear igmp-snooping membership
(host)(config)# clear igmp-snooping membership vlan <vlan-id>
(host)(config)# clear igmp-snooping mrouter
(host)(config)# clear igmp-snooping mrouter vlan <vlan-id>
```

## Enabling IGMP Snooping Trace Options

```
(host)(config)# traceoptions
 igmp-snooping flags {all|config|errors|receive|transmit}
```

## Mrouter

VLANs in a Layer 2 switch need to know the path to the PIM router that connects Layer 2 domain to the Layer 3 Network. When the multicast source is present on the Layer 2 switch, the traffic that originates from the Layer 2 switches need to know a port through which multicast traffic can reach the Layer 3 PIM router. For this reason, the VLAN in the Layer 2 switch on which IGMP snooping is enabled will designate a port as Mrouter port. The mrouter port can be detected dynamically or statically. The dynamic detection is based on IGMP query message or PIM hello messages. You can also configure static mrouter ports.

When multicast receivers are present on the VLAN in a Layer 2 switch, the IGMP report message from the host is forwarded out of the mrouter port towards the PIM router to let the PIM router know that there are receivers interested in receiving multicast traffic, so that, PIM routers can add the VLAN interface to the outgoing list in the multicast route on a multicast router.

## Configuring a Static Mrouter Port

To configure a static mrouter port, follow these steps:

```
(host)(config)# interface gigabitethernet <slot/module/port>
 igmp-snooping mrouter-vlan <vlan-id|vlan-list>
 igmp-snooping mrouter-vlan {add | delete} <vlan-id>
```

## Example Configuration

```
(host)(config)# interface gigabitethernet 0/0/9
 igmp-snooping mrouter-vlan 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
```



This chapter contains the following major sections:

- [Important Points to Remember on page 257](#)
- [Understanding MLD Snooping on page 257](#)
- [Configuring MLD Snooping on page 257](#)
- [Verifying MLD Snooping on page 258](#)

## Important Points to Remember

- Mobility Access Switch supports only MLDv1 (RFC 2710) and hence does not process the MLDv2 specific packets.
- MLD snooping prevents multicast flooding on an Ethernet link, but it requires complex processing for each of the interfaces on switches that were not initially designed for this kind of task.
- MLD is embedded in ICMPv6, unlike IGMP, which uses a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.

## Understanding MLD Snooping

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link. When multicast is supported at the IPv6 level, it often broadcasts at lower levels. So, for example, an Ethernet switch broadcasts multicast traffic on all ports, even if only one host wants to receive it.

To prevent entire Ethernet segments from being flooded, MLD snooping can be implemented on Ethernet switches. The MLD snooping solution is similar to the IGMP snooping solution for IPv4. When MLD snooping is implemented on a switch, it detects all MLD version 1 messages that are exchanged on the link. It also maintains a table that indicates which IPv6 multicast groups should be forwarded for each of the interfaces.

## Configuring MLD Snooping

This section contains the following sections:

- [Configuring MLD Snooping on page 257](#)
- [Deleting an Mrouter Port on a VLAN on page 258](#)

### Configuring MLD Snooping

To configure MLD snooping, follow these steps:

1. Configure an MLD snooping profile in a VLAN profile.

```
(host) (config) #vlan-profile mld-snooping-profile MLD_Doc
(host) (mld-snooping-profile "MLD_Doc") #snooping
(host) (mld-snooping-profile "MLD_Doc") #
```

2. Apply the MLD snooping profile to the VLAN.

```
(host) (config) #vlan 10
(host) (VLAN "10") #mld-snooping-profile MLD_Doc
(host) (VLAN "10") #
```

3. Configure a static mrouter port.

```
(host) (config) #interface gigabitethernet 0/0/46
```

```
(host) (gigabitethernet "0/0/46") #mld-snooping mrouter-vlan 10
```

## Deleting an Mrouter Port on a VLAN

To delete an mrouter port on a VLAN, use the following command:

```
(host) (gigabitethernet "0/0/4") #mld-snooping mrouter-vlan delete 2
```

## Verifying MLD Snooping

This section contains the following sections:

- [Verifying the MLD Snooping Profile on page 258](#)
- [Verifying the Static and Dynamic Mrouter Port for MLD Snooping on page 258](#)
- [Verifying the MLD Snooping Mrouter Detail on page 258](#)
- [Verifying MLD Snooping Member Ports on page 260](#)
- [Verifying the MLD Group on page 260](#)
- [Verifying the MLD Snooping Group Count on page 261](#)
- [Verifying the MLD Snooping Statistics on page 261](#)

### Verifying the MLD Snooping Profile

To verify an MLD snooping profile, use the following command:

```
(host) #show vlan-profile mld-snooping-profile MLD_Doc
```

```
mld-snooping-profile "MLD_Doc"

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
```

### Verifying the Static and Dynamic Mrouter Port for MLD Snooping

To verify the static and dynamic mrouter port for MLD snooping, use the following command:

```
(host) #show mld-snooping mrouter vlan 1
Flags: D - Dnyamic, S - Static, P - PIM, M - IGMP/MLD
```

```
MLD Snooping Multicast Router Ports

VLAN Elected-Querier Ports (Flags) Expiry UpTime
---- -
0001 3555:5555:6666:6666:7777:7777:8888:8888 GE0/0/0 (S) 00:00:00 00:10:35
 GE0/0/3 (DM) 00:04:20 00:10:33
 GE0/0/3 (DP) 00:04:19 00:10:33
```

### Verifying the MLD Snooping Mrouter Detail

To verify the mld-snooping mrouter detail and show identifiers for each field, use the following command:

```
(host) (VLAN "1") #show mld-snooping mrouter detail
```

```
Flags: D - Dnyamic, S - Static, P - PIM, M - IGMP/MLD
```

```
Vlan:0001 Elected-Querier:3555:5555:6666:6666:7777:7777:8888:8888
```

```

GEO/0/0 (S) Expiry Time: 00:00:00 Uptime: 00:03:54
 Router IP: N/A
 Router MAC: 00:00:00:00:00:00
GEO/0/3 (DM) Expiry Time: 00:01:32 Uptime: 00:03:52
 Router IP: 3555:5555:6666:6666:7777:7777:8888:8888
 Router MAC: 00:00:00:00:02:00
GEO/0/3 (DP) Expiry Time: 00:01:31 Uptime: 00:03:52
 Router IP: fe80::200:24ff:fef9:7ccd
 Router MAC: 00:00:24:f9:7c:cd
(host) (VLAN "1") #show igmp-snooping mrouter detail

```

Flags: D - Dynamic, S - Static, P - PIM, M - IGMP/MLD

```

Vlan:0001 Elected-Querier:111.1.0.12
 GEO/0/0 (DM) Expiry Time: 00:04:12 Uptime: 00:00:08
 Router IP: 111.1.0.12
 Router MAC: 00:00:33:00:05:00
Vlan:0004 Elected-Querier:11.11.11.3
 GEO/0/4 (S) Expiry Time: 00:00:00 Uptime: 00:19:54
 Router IP: N/A
 Router MAC: 00:00:00:00:00:00
 GEO/0/4 (DM) Expiry Time: 00:04:09 Uptime: 00:00:11
 Router IP: 11.11.11.3
 Router MAC: 00:00:09:0b:91:6d

```

## Verifying the Two Mrouter Entries with the Same IP Address

Two mrouter entries with the same router IP address can be created if the PIM router is also the IGMP querier based on both protocol packets. To distinguish between the two IP addresses, flags are displayed in the commands **show igmp-snooping mrouter** and **show mld-snooping mrouter**.

```
(host) (VLAN "1") #show igmp-snooping mrouter
```

Flags: D - Dnyamic, S - Static, P - PIM, M - IGMP/MLD

IGMP Snooping Multicast Router Ports

```

VLAN Elected-Querier Ports (Flags) Expiry UpTime Src-Ip
---- -
0004 11.11.11.3 GE0/0/4 (S) 00:00:00 00:26:26 -
 GE0/0/4 (DM) 00:03:52 00:06:43 11.11.11.3
 GE0/0/4 (DP) 00:04:19 00:00:02 11.11.11.3
 GE0/0/3 (DM) 00:03:52 00:06:43 11.11.11.11

```

If the 80 column limit is exceeded when displaying the **src-ip** and the elected querier in the same row of the **show mld-snooping mrouter** output, the **src-ip** is not shown. To find the **src-ip**, use the **show mld-snooping mrouter detail** command.

```
(host) (VLAN "1") #show mld-snooping mrouter
```

Flags: D - Dnyamic, S - Static, P - PIM, M - IGMP/MLD

MLD Snooping Multicast Router Ports

```

VLAN Elected-Querier Ports (Flags) Expiry UpTime
---- -
0001 3555:5555:6666:6666:7777:7777:8888:8888
 GE0/0/0 (S) 00:00:00 00:10:35
 GE0/0/3 (DM) 00:04:20 00:10:33
 GE0/0/3 (DP) 00:04:19 00:10:33

```

Similar to the output of **show mld-snooping mrouter detail**, the output the **show mld-snooping membership detail** now includes labels for each field to enhance readability.

```
(host) (VLAN "1") #show igmp-snooping membership detail

Flags: H - IGMP/MLD listener, M - Multicast Router

Group:225.0.0.9 Vlan:0001
 Port: GE0/0/2 Expiry: 00:00:00 Uptime: 00:01:21
 (M) IP: 0.0.0.0 MAC: 00:0b:86:6a:20:80
 Port: GE0/0/4 Expiry: 00:02:59 Uptime: 00:01:21
 (H) IP: 11.11.11.1 MAC: 00:00:09:0b:91:6c
Group:225.0.0.10 Vlan:0001
 Port: GE0/0/2 Expiry: 00:00:00 Uptime: 00:01:21
 (M) IP: 0.0.0.0 MAC: 00:0b:86:6a:20:80
 Port: GE0/0/4 Expiry: 00:02:59 Uptime: 00:01:21
 (H) IP: 11.11.11.1 MAC: 00:00:09:0b:91:6c
```

```
(host) #show mld-snooping membership detail
Flags: H - IGMP/MLD listener, M - Multicast Router

Group:ff03::3 Vlan:0001
 Port: GE0/0/0 Expiry: 00:04:08 Uptime: 00:00:12
 (H) IP: fe80::5001 MAC: 00:00:02:00:05:00
 Port: GE0/0/4 Expiry: 00:00:00 Uptime: 00:00:12
 (M) IP: fe80::5002 MAC: 00:00:00:00:03:00
```

## Verifying MLD Snooping Member Ports

To verify the MLD snooping member ports, use the following command:

```
(host) #show mld-snooping membership vlan 10
```

```
MLD Snooping Multicast Membership

VLAN Group Port Expiry UpTime
---- -
0010 ff03::1 GE0/0/22 00:04:11 00:00:15
 GE0/0/47 00:00:00 00:00:15
0010 ff03::2 GE0/0/22 00:04:11 00:00:15
 GE0/0/47 00:00:00 00:00:15
0010 ff03::3 GE0/0/22 00:04:11 00:00:15
 GE0/0/47 00:00:00 00:00:15
0010 ff03::4 GE0/0/22 00:04:11 00:00:15
 GE0/0/47 00:00:00 00:00:15
0010 ff03::5 GE0/0/22 00:04:11 00:00:15
 GE0/0/47 00:00:00 00:00:15
0010 ff03::6 GE0/0/22 00:04:11 00:00:15
 GE0/0/47 00:00:00 00:00:15
0010 ff03::7 GE0/0/22 00:04:11 00:00:15
 GE0/0/47 00:00:00 00:00:15
0010 ff03::8 GE0/0/22 00:04:11 00:00:15
 GE0/0/47 00:00:00 00:00:15
0010 ff03::9 GE0/0/22 00:04:11 00:00:15
 GE0/0/47 00:00:00 00:00:15
0010 ff03::a GE0/0/22 00:04:11 00:00:15
```

```
MLD Snooping Multicast Membership

VLAN Group Port Expiry UpTime
---- -
 GE0/0/47 00:00:00 00:00:15
```

## Verifying the MLD Group

To verify the MLD group, use the following command:

```
(host) # show mld-snooping groups vlan 10
```

#### MLD Snooping Multicast Route Table

```

VLAN Group Port List
---- -
0010 ff03::1 GE0/0/47 GE0/0/22
0010 ff03::2 GE0/0/47 GE0/0/22
0010 ff03::3 GE0/0/47 GE0/0/22
0010 ff03::4 GE0/0/47 GE0/0/22
0010 ff03::5 GE0/0/47 GE0/0/22
0010 ff03::6 GE0/0/47 GE0/0/22
0010 ff03::7 GE0/0/47 GE0/0/22
0010 ff03::8 GE0/0/47 GE0/0/22
0010 ff03::9 GE0/0/47 GE0/0/22
0010 ff03::a GE0/0/47 GE0/0/22
```

## Verifying the MLD Snooping Group Count

To verify the MLD snooping group count, use the following command:

```
(host) # show mld-snooping groups vlan 10 count
MLD Snooping Multicast Route Count
```

```

VLAN Count
---- -
0010 0010
```

## Verifying the MLD Snooping Statistics

To verify the MLD snooping statistics, use the following command:

```
(host) #show mld-snooping counters vlan 10
MLD Snooping Counters
```

```

Name Value
---- -
received-total 1110
received-queries 0036
received-v1-reports 1074
received-leaves 0000
received-unknown-types 0000
len-errors 0000
checksum-errors 0000
forwarded 0930
```

## List of MLD Snooping Commands and Sample Outputs

This section contains the following commands:

- [Show MLD Snooping Counters on page 262](#)
- [Show MLD Snooping Counters per VLAN on page 262](#)
- [Show MLD Mrouter Ports on page 262](#)
- [Show MLD Mrouter Ports Detail on page 262](#)
- [Show MLD Router Ports Per VLAN on page 262](#)
- [Show Detected MLD Multicast Addresses on page 263](#)
- [Show Detected MLD Multicast Addresses Per VLAN on page 263](#)
- [Show Detected MLD Multicast Membership Information on page 263](#)
- [Show Detected MLD Multicast Membership Information \(Detailed Version\) on page 263](#)
- [Show Detected MLD Multicast Membership Information Per VLAN on page 264](#)

- [Show MLD-Snooping Profile on page 264](#)
- [Show List of MLD-Snooping Profiles on page 264](#)
- [Show List of References for MLD-Snooping Profile on page 264](#)

## Show MLD Snooping Counters

```
(host) #show mld-snooping counters
```

```
MLD Snooping Counters
```

```

Name Value
---- -
received-total 0005
received-queries 0001
received-vl-reports 0004
received-leaves 0000
received-pim-v6 0000
received-unknown-types 0000
len-errors 0000
checksum-errors 0000
forwarded 0000
```

## Show MLD Snooping Counters per VLAN

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

```
MLD Snooping Counters
```

```

Name Value
---- -
received-total 0005
received-queries 0001
received-vl-reports 0004
received-leaves 0000
received-pim-v6 0000
received-unknown-types 0000
len-errors 0000
checksum-errors 0000
forwarded 0000
```

## Show MLD Mrouter Ports

```
(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 fe11::d0d0 GE0/0/4 (DM) 00:04:12 00:00:08
```

## Show MLD Mrouter Ports Detail

```
(host) #show mld-snooping mrouter detail
```

```
Flags: D - Dynamic, S - Static, P - PIM, M - IGMP/MLD query
```

```
Vlan:0001 Elected-Querier:fe11::d0d0
 GE0/0/4 (DM) Expiry Time: 00:04:06 Uptime: 00:00:14
 Router IP: fe11::d0d0
 Router MAC: 00:00:00:00:03:00
```

## Show MLD Router Ports Per VLAN

```
(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
```

### Show Detected MLD Multicast Addresses

```
(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
```

### Show Detected MLD Multicast Addresses Per VLAN

```
(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
```

### Show Detected MLD Multicast Membership Information

```
(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
```

### Show Detected MLD Multicast Membership Information (Detailed Version)

```
(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

## Show Detected MLD Multicast Membership Information Per VLAN

```
(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
```

## Show MLD-Snooping Profile

```
(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
```

## Show List of MLD-Snooping Profiles

```
(host) #show VLAN-profile mld-snooping-profile
mld-snooping-profile List
```

```

Name References Profile Status
---- -
default 2
Total:1
```

## Show List of References for MLD-Snooping Profile

```
(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
```

This chapter contains the following major sections:

- [DHCP Snooping Overview on page 265](#)
- [Configuring DHCP Snooping on page 265](#)

## DHCP Snooping Overview

When DHCP snooping is enabled, the system snoops the DHCP messages to view DHCP lease information and build and maintain a database of valid IP address to MAC address bindings called the DHCP snooping database.

DHCP snooping helps to build the binding database to support the security features like IP Source Guard (IPSG) and Dynamic ARP Inspection (DAI).

### Important Points to Remember

- By default, DHCP Snooping is disabled on the VLAN.
- When DHCP Snooping is enabled on the VLAN, the IP to MAC binding is created in the system.

## Configuring DHCP Snooping

The following command adds a static binding on a VLAN:

```
(host) ("vlan id") #dhcp-snooping-database <mac> gigabitethernet <slot/module/port> <ip_
address>
```

The following command deletes a static binding on a VLAN:

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

The following command enables and configures DHCP snooping and static binding on a VLAN:

```
(host) ("vlan id")# vlan-profile dhcp-snooping-profile <profile-name>
(host) (dhcp-snooping-profile "profile-name")# enable
```

The following command attaches DHCP Snooping profile on the VLAN:

```
(host) ("vlan id")# dhcp-snooping-profile <profile name>
```

### Sample Configuration

The following example enables and configures DHCP Snooping on a VLAN:

```
(host) ("vlan 6")# vlan-profile 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
```

### Verifying Configuration

The following command displays the DHCP Snooping configuration details:

```
(host) (config) #show vlan-profile dhcp-snooping-profile DHCP
dhcp-snooping-profile "DHCP"
```

-----

Parameter Value

-----  
DHCP Snooping Enabled

The following command displays the DHCP Snooping database details:

```
(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 following command displays static entries of DHCP Snooping database:

```
(host) (config) #show dhcp-snooping-database
Total DHCP Snoop Entries : 4
Learnt Entries : 0, Static Entries : 4
DHCP Snoop Table
```

-----

| MAC               | IP      | BINDING-STATE | LEASE-TIME    | VLAN-ID | INTERFACE             |
|-------------------|---------|---------------|---------------|---------|-----------------------|
| ---               | --      | -----         | -----         | -----   | -----                 |
| 00:00:11:33:66:77 | 7.7.7.7 | Static entry  | No lease time | 6       | gigabitethernet1/0/11 |
| 00:00:11:51:77:11 | 7.7.7.7 | Static entry  | No lease time | 3       | gigabitethernet0/0/4  |
| 00:00:77:11:66:33 | 6.6.6.6 | Static entry  | No lease time | 3       | gigabitethernet0/0/4  |
| 00:11:77:22:88:22 | 9.9.9.9 | Static entry  | No lease time | 6       | gigabitethernet1/0/4  |

This chapter describes the following topics:

- [Port Security Overview on page 267](#)
- [Configuring Port Security Functionality on page 269](#)
- [Sample Configurations on page 275](#)

## Port Security Overview

ArubaOS Mobility Access Switch supports for Port Security functionality to provide network security at Layer 2. You can now filter the unauthorized devices to send the control packets, restrict the number of MACs allowed on the interface, and detect unwanted loops in the network when not running spanning-tree protocol.

You can enable or disable this functionality at an interface level.

### Router Advertisement Guard

The Router Advertisement (RA) Guard functionality analyzes the RAs and filters out RA packets sent by unauthorized devices. The RA guard feature is disabled by default. By enabling, the RA packets received on the interface are dropped and the port can be shutdown based on the interface configuration. The port can be re-activated after the configured time by configuring the **auto-recovery** option.

#### Points to Remember

- The following RA messages are filtered by enabling the RA guard:
  - RA message with no extension header
  - RA message with multiple extension headers
  - RA message fragmented
- The following Unicast RA messages are not filtered by enabling the RA guard:
  - Unicast RA messages with multiple extension headers.
  - Unicast RA messages fragmented

### DHCP Trust

The DHCP trust functionality provides support to filter the IPv4 DHCP packets from the unauthorized devices. The following IPv4 DHCP messages are filtered on an interface configured not to trust DHCP.

- DHCP offer messages
- DHCP Ack messages

You can enable DHCP trust on any interface. By default, the DHCP Trust setting in a port-security-profile is to filter (block) these OFFER and ACK messages. You must explicitly enable DHCP Trust (`trust dhcp`) in the port-security-profile (if applied to a port) to allow these DHCP messages from valid devices.

### Loop Protect

The Loop Protect functionality detects the unwanted physical loops in your network. You can enable or disable this functionality at an interface level. A proprietary protocol data unit (PDU) is used to detect the physical loops in the network. When the system detects a loop, it disables the port that sends the PDU. You can re-enable the port automatically or manually.

## Points to Remember

- It is recommended that you enable Loop Protect on all the Layer 2 interfaces when the spanning tree is disabled on the Mobility Access Switch.
- The Loop Protect functionality will not detect any loops when MSTP or PVST (on any VLAN) is enabled on the Mobility Access Switch.
- The Loop Protect functionality will work only on non-HSL interfaces. An error will be displayed when you try to enable this functionality on HSL interfaces.

## MAC Limit

The MAC limit feature restricts the maximum number of MACs that can be learnt on the interface. When the MAC limit is enabled, it provides support to log the excess MACs or drop the new MAC learning requests or shuts down the port.

## Sticky MAC

Sticky MAC is a port security feature that dynamically learns MAC addresses on an interface and retains the MAC information in case the Mobility Access Switch reboots.

Sticky MAC is an alternative to the tedious and manual configuration of static MAC addresses on a port or to allow the port to continuously learn new MAC addresses after interface-down events. Allowing the port to continuously learn MAC addresses is a security risk. Sticky MAC prevents traffic losses for trusted workstations and servers because the interface does not have to relearn the addresses from ingress traffic after a restart.

Enable Sticky MAC in conjunction with MAC limit to restrict the number of MAC addresses learning.

Sticky MAC with MAC limit prevents Layer 2 denial of service (DoS) attacks, overflow attacks on the Ethernet switching table, and DHCP starvation attacks by limiting the MAC addresses allowed while still allowing the interface to dynamically learn a specified number of MAC addresses. The interface is secured because after the limit has been reached, additional devices cannot connect to the port.

By enabling Sticky MAC learning along with MAC limiting, interfaces can be allowed to learn MAC addresses of trusted workstations and servers during the period from when the interface are connected to the network until the limit for MAC addresses is reached. This ensures that after this initial period with the limit reached, new devices will not be allowed even if the Mobility Access Switch restarts.

Sticky MAC is disabled by default.

## Points to Remember

- Sticky MAC is not supported on untrusted interfaces.
- Sticky MAC is not supported on HSL interfaces.
- No global configuration to enable or disable Sticky MAC address learning. The Sticky MAC feature will be enabled at interface level as part of port-security profile.
- Though the feature is enabled at the interface level, the MAC addresses are learned at the VLAN level.
- Configure on access or edge ports. However, there is no restriction for configuring Sticky MAC on trunk ports.
- Once a MAC address is learned on one interface, it will not be learned on any other interface in the same VLAN (no MAC move).
- Clear command with Sticky keyword can be used to remove Sticky MAC Addresses. All sticky MAC addresses will be removed when the VLAN is removed or the port-security profile is removed from the interface.
- Sticky MAC address can be learned on interfaces in other VLANs.
- Sticky MAC addresses, Phone MAC addresses and Dynamic addresses are considered as a part of MAC limit. Static addresses are not included in MAC limit.

- Sticky MAC feature does not influence the packet forwarding. Packet forwarding is only driven by the MAC limit. Packets from a Sticky MAC address received on other interfaces will be forwarded but will not be learnt on the new interface. Ensure to clear the sticky MAC address before it is learnt again on other interfaces.
- Shutting down a Sticky MAC enabled interface, linkdown, and STP TCN of an interface will not remove Sticky MAC entries learned on that interface.
- Sticky MAC entries are retained in case of a Mobility Access Switch reboot.

## IP Source Guard

IP Source Guard (IPSG) functionality permits IP traffic from certain IP addresses, while denying the rest of IP traffic or manually configured IP source bindings and prevents IP spoofing attacks. When IPSG is enabled on an interface, the Mobility Access Switch blocks all IP traffic received on the interface, except for DHCP packets allowed by DHCP snooping. The port allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

### Important Points to Remember

- IPSG is disabled by default
- IPSG can be enabled for source IP and MAC address filtering
- If IPSG is enabled on the trusted interfaces, the number of users supported on untrusted interfaces will be reduced
- IPSG drops only IP traffic, Layer 2 traffic is not validated by IPSG

## Dynamic ARP Inspection (DAI)

DAI is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings.

DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database. This database is built by DHCP snooping, if DHCP snooping is enabled on the VLANs. The Mobility Access Switch forwards the ARP packets received on trusted and untrusted ports only if the validations on the ARP packets are successful. If the validation is not successful, the ARP packet is dropped and a log is generated.

### Important Points to Remember

- DAI is disabled by default on all the interfaces.

## Configuring Port Security Functionality

The port security functionality will be configured as part of the port level security configuration. This profile can be attached to the interface.

## Configuring RA Guard Functionality

RA Guard functionality can be enabled at the port level. Configure the RA guard as part of the port level security configuration and attach to the interface.

```
(host)(config)# interface-profile port-security-profile <profile-name>
 ipv6-ra-guard action {drop|shutdown}auto-recovery-time <recovery-time>
```

The following example shows how to enable the RA Guard functionality:

```
(host)(config)# interface-profile port-security-profile RA-Guard1
 ipv6-ra-guard action shutdown auto-recovery-time 60
```

## Configuring DHCP Trust Functionality

The DHCP trust functionality will be configured as part of the port level security configuration. This profile can be attached to the interface.

DHCP Trust can be enabled on any interface. By default, the DHCP Trust setting in a port-security-profile is to filter (block) these OFFER and ACK messages. You must explicitly enable DHCP Trust (trust dhcp) in the port-security-profile (if applied to a port) to allow these DHCP messages from valid devices.

```
(host) (config) # interface-profile port-security-profile <profile-name>
 trust dhcp
```

When **no trust dhcp** is configured the DHCP packets are dropped and a message is logged.

The following example shows how to enable the DHCP Trust functionality:

```
(host) (config) # interface-profile port-security-profile ps1
 trust dhcp
```

## Configuring Loop Protect Functionality

Port Loop Protect functionality is configured as part of the port level security configuration. You can attach the port-security profile to any Layer 2 interface. Enabling Loop Protect will disable a port when it detects a loop. You can automatically re-enable the port by setting the auto-recovery option. Otherwise, you can recover the port manually using the **clear** command.

Use the following CLI commands to enable Loop Protect and the auto-recovery option:

```
(host) (config) #interface-profile port-security-profile <profile-name>
(host) (Port security profile "<profile-name>") #loop-protect auto-recovery-time <time in
seconds>
```

Set a value for **auto-recovery-time** to enable the auto-recovery option. The port automatically re-enables and recovers from the error after the specified time. By default, auto-recovery is disabled. Auto-recovery remains disabled, if you enable **loop-protect** without setting the **auto-recovery-time** option or by setting the value to 0.

Use the following command to disable the auto-recovery option:

```
(host) (Port security profile "<profile-name>") #no loop-protect auto-recovery-time
```

Use the following command to disable the Loop Protect functionality:

```
(host) (Port security profile "<profile-name>") #no loop-protect
```

---

It is recommended that you disable Spanning Tree using the following command before enabling Loop Protect on an interface:

```
(host) (config) #spanning-tree no mode
```

Otherwise, you will see the following warning message:

```
Warning: Port Loop Protect configured in the port-security-profile, will be inactive. It
becomes active when MSTP/PVST is disabled.
```

---



## Configuring MAC Limit Functionality

The MAC Limit functionality will be configured as part of the port level security configuration. You can attach this profile to an interface.

Use the following command to configure the MAC Limit:

```
(host) (config) # interface-profile port-security-profile <profile-name>
 mac-limit <limit> action {drop|log|shutdown}
 auto-recovery-time <time in seconds>
```

The following example shows how to enable the MAC Limit functionality:

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



---

The maximum value for **auto-recovery-time** for all the port security functionalities is 65,535 seconds. You can apply `auto-recovery-time` option only if the action is shutdown.

---

## Configuring Sticky MAC

The Sticky MAC learning is configured as part of the port-level security configuration. You can attach this profile to an interface.

Starting from ArubaOS 7.4.0.2, the Mobility Access Switch allows you to configure the Sticky MAC feature with an action to take when a Sticky MAC violation occurs. The allowed actions are:

- Drop—Drops any new MAC addresses trying to connect to the interface. This is the default option.
- Shutdown—Shuts down the port on which the sticky MAC violation occurs. You can also optionally set an auto-recovery time between 0-65,535 seconds for the interface to recover.

### Enabling Sticky MAC

Use the following command to enable Sticky MAC:

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

Use the following command to configure a Sticky MAC action:

```
(host) (Port security profile "<profile-name>") #sticky-mac action [drop | shutdown
autorecovery-time <1-65535>]
```

The following example shows how to enable Sticky MAC:

```
(host) (config) # interface-profile port-security-profile PSP sticky-mac
```

Use the following command to disable Sticky MAC:

```
(host) (config) # interface-profile port-security-profile <profile-name> no sticky-mac
```

The following example shows how to enable Sticky MAC:

```
(host) (config) # interface-profile port-security-profile PSP no sticky-mac
```

The following example shows how to configure a Sticky MAC action in case of a Sticky MAC violation:

```
(host) (Port security profile "<profile-name>") #sticky-mac action shutdown auto-recovery-time
10
```

### Viewing Sticky MAC

Execute the following command to view the Sticky MAC addresses on a Mobility Access Switch:

```
(host) show mac-address-table sticky
```

Execute the following command to view the Sticky MAC addresses on a VLAN:

```
(host) show mac-address-table vlan <id> sticky
```

Execute the following command to view the Sticky MAC addresses on an interface:

```
(host) show mac-address-table interface <interface-name> sticky
```

### Verifying Sticky MAC Configuration

Execute the following command to verify the Sticky MAC configuration:

```
(host) #show interface-profile port-security-profile <profile-name>
```

The following command verifies the sample configuration:

```
(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

```

## Clearing Sticky MAC Addresses

Execute the following command to remove the Sticky MAC addresses on a Mobility Access Switch:

```
(host) clear mac-address-table sticky
```

Execute the following command to remove the Sticky MAC addresses on a VLAN:

```
(host) clear mac-address-table vlan <id> sticky
```

Execute the following command to remove the Sticky MAC addresses on an interface:

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

Execute the following command to remove a specific Sticky MAC address on a VLAN:

```
(host) clear mac-address-table vlan <id> mac <mac-address> sticky
```

Execute the following command to remove a specific Sticky MAC address on an interface:

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

Execute the following command to remove a specific Sticky MAC address on a VLAN port:

```
(host) clear mac-address-table vlan <id> interface <interface name> sticky
```

## Configuring IP Source Guard

The IPSG functionality can be configured as part of the port level security configuration. This profile can be attached to the interface.

Use the following command to configure the IPSG:

```
(host)(config)# interface-profile port-security-profile <profile-name>
ip-src-guard
```

## Verifying IP Source Guard

You can use the following command to display all the interface on which IPSG is enabled, and the type of IPSG filter:

```
(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

```

You can use the following command to display if IPSG is enabled on a specific interface, along with type of filter:

```

(host) #show ip source-guard interface gigabitethernet 0/0/12 ← Shows if ipsgr is enabled on
specific interface, along with type of filter
IPSG interface Info

Interface IPSG MAC Binding

GE0/0/12 Enabled Disabled

```

You can use the following command to display details about the IP and MAC combination:

```

(host) #show ip source-guard interface gigabitethernet 0/0/12 detail
IPSG allowed users on the interface

IP Address Mac Address VLAN

172.2.1.255 NA 2

```

You can use the following command to verify the IPSG configuration:

```

(host) #show interface-profile port-security-profile techpubs
Port security profile "techpubs"

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
Trust DHCP No
Port Loop Protect N/A
Port Loop Protect Auto Recovery Time N/A
Sticky MAC N/A
IP Source Guard Enabled
IP Source Guard with MAC binding N/A
Dynamic Arp Inspection N/A

```

## Configuring DAI

The DAI functionality can be configured as part of the port level security configuration. This profile can be attached to the interface.

You can use the following command to configure the DIA:

```

(host) (config)# interface-profile port-security-profile <profile-name>
dynamic-arp-inspection

```

## Verifying DAI

You can use the following command to verify the DAI configuration:

```

(host) #show interface-profile port-security-profile abc
Port security profile "abc"

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
Trust DHCP No
Port Loop Protect N/A
Port Loop Protect Auto Recovery Time N/A
Sticky MAC N/A
Dynamic Arp Inspection Enabled

```

## Attaching Port Security Profile to Interface

To enable the Port Security functionality on an interface, you must attach a port-security profile to it. Use the following commands to associate a port-security profile with an interface:

For Gigabitethernet:

```

(host) (config) #interface gigabitethernet <slot/mod/port>
(host) (gigabitethernet "<slot/mod/port>") #port-security-profile <profile-name>

```

For Port-channel:

```

(host) (config) #interface port-channel <id>
(host) (port-channel "<id>") #port-security-profile <profile-name>

```

## Viewing Port Errors

Use the following command to view 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:

```
(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)
GE0/0/5 Log (MAC Limit exceed) No Auto recovery
 Drop (RA guard) No Auto recovery
GE1/0/24 Shutdown (BPDU received) 2012-10-18 11:25:17 (PST)
 No Auto Recovery

```

## Recovering Ports Manually

Use the CLI to manually recover the port errors. To recover the ports on a specific interface execute the following command:

```
(host) #clear port-error-recovery interface <interface-name>
```

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

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

To clear the port errors on all interfaces execute the following command:

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

## Sample Configurations

To configure the port security profile:

```
(host) (config) # interface-profile port-security-profile port-security-1
(host (port security profile port-security-1)#
 ipv6-ra-guard action drop auto-recovery-time 60
 no trust dhcp
 loop-protect auto-recovery-time 10
 mac-limit 30 action drop auto-recovery-time 50
 ip-src-guard include-mac-binding
 dynamic-arp-inspection
```

To attach the port security profile to the interface:

```
(host)(config)# interface gigabitethernet 0/0/6
 port-security-profile port-security-1
(host) (config) #interface port-channel 3
 port-security-profile port-security-1
```



Some protocols or features prevents bridge loops in a Layer 2 network, rogue switches, or end hosts can degrade the network by creating and propagating traffic storms.

Storm control prevents interfaces from disruptions by providing protection against excessive ingress rates of unknown-unicast, multicast, and broadcast traffic.

### Important Points to Remember

- The configured storm control bandwidth percentage applies to all types of traffic.
- If the rate is 100%, no traffic is rate limited. If the rate is 50% then 50% of configured traffic is rate limited.
- Individual levels of storm control per traffic type is not supported. All types are set to single percentage.
- The **storm-control-bandwidth** is the maximum combined limit of broadcast, unknown-unicast and multicast traffic (not enabled by default) on an interface. For example, if the bandwidth rate is set to 10%, any mix of broadcast, unknown-unicast and multicast traffic up to 10% of the interface speed is allowed.
- By default, storm control is enabled for unknown-unicast and broadcast traffic.
- Storm Control is configured from the command line only. You can configure it under the switching-profile.

### Configuration Steps

Use the following steps, from the command line, to configure and verify Storm Control.

1. Define the level of storm-control based on percentage of interface speed. Range is 1 to 100%.

```
(host) (config) #interface-profile switching-profile STORM_CONTROL
(host) (switching profile "STORM_CONTROL") #storm-control-bandwidth 80
```

2. Enable the type(s) of traffic you want controlled.

```
(host) (switching profile "STORM_CONTROL") #storm-control-unknown-unicast
(host) (switching profile "STORM_CONTROL") #storm-control-multicast
(host) (switching profile "STORM_CONTROL") #storm-control-broadcast
```

3. Apply the configured switching-profile to the interface.

```
(host) (config) #interface gigabitethernet 0/0/20
(host) (gigabitethernet "0/0/20") #switching-profile STORM_CONTROL
```

4. Verify the configuration.

```
(host) #show interface-profile switching-profile STORM_CONTROL
```

```
switching profile "STORM_CONTROL"

Parameter Value

Switchport mode access
Access mode VLAN 1
Trunk mode native VLAN 1
Enable broadcast traffic rate limiting Enabled
Enable multicast traffic rate limiting Enabled
Enable unknown unicast traffic rate limiting Enabled
Max allowed rate limit traffic on port in percentage 80
Trunk mode allowed VLANs 1-4094
```



Access control lists (ACLs) are a common way of restricting certain types of traffic on a physical port. The Mobility Access Switch supports multiple types of access control lists to provide flexibility to control the traffic. This chapter describes the different types of ACLs supported and how to configure them on the Mobility Access Switch.

This chapter includes the following topics:

- [Types of ACLs on page 279](#)
- [Configuring the ACLs on page 280](#)
- [Verifying the ACL configuration on page 282](#)

## Types of ACLs

- Ethertype ACLs are used to filter based on the Ethertype field in the frame header. Ethertype ACLs can be either named or numbered, with valid numbers in the range of 200-299. These ACLs can be used to permit IP while blocking other non-IP protocols, such as IPX or AppleTalk.
- MAC ACLs are used to filter traffic on a specific source MAC address or range of MAC addresses. MAC ACLs can be either named or numbered, with valid numbers in the range of 700-799 and 1200-1299.
- Standard ACLs permit or deny traffic based on the source IP address of the packet. Standard ACLs can be either named or numbered, with valid numbers in the range of 1-99 and 1300-1399. Standard ACLs use a bitwise mask to specify the portion of the source IP address to be matched.
- Extended ACLs permit or deny traffic based on source or destination IP address, or IP protocol. Extended ACLs can be named or numbered, with valid numbers in the range 100-199 and 2000-2699.
- Stateless ACLs are used to define stateless packet filtering and quality of service (QoS). A stateless ACL statically evaluates packet contents. The traffic in the reverse direction will be allowed unconditionally. Stateless ACLs are named ACLs.

Mobility Access Switch provides both standard and extended ACLs for compatibility with router software from popular vendors, however firewall policies provide equivalent and greater function than standard and extended ACLs and should be used instead.

You can apply MAC and Ethertype ACLs to a user role, however these ACLs apply only to non-IP traffic from the user.

## Router ACLs (RACLs)

Router ACLs perform access control on all traffic entering the specified Routed VLAN Interface. Router ACLs provide access control based on the Layer 3 addresses or Layer 4 port information and ranges. RACLs can only be applied to ingress traffic.

## Port ACLs (PACLs)

ACLs provide the ability to filter ingress traffic based on conditions specified in the ACL. Port ACLs perform access control on all traffic entering or leaving the specified Layer 2 port. PACLs provide access control based on the Layer 3 addresses (for IP protocols), Layer 2 MAC addresses (for non-IP protocols), or Layer 4 port information and ranges. A Layer 2 port is a physical LAN or trunk port that belongs to a VLAN. The PACLs are applied on both the ingress and egress traffic with the following exceptions for egress traffic:

- Egress ACLs are applied only on interfaces and not on user roles.

- When QoS-profile is applied on egress ACL, only the dot1p and dscp values are applicable. The trafficclass, drop-precedence are not applicable.



---

You can apply all the types of ACLs to a port and only the MAC, Ethertype and Stateless ACLs can be applied to a user role. The MAC and Ethertype ACLs only apply to non-IP traffic and the Stateless ACL to IP traffic from the user.

---

## User ACLs (UACLs)

User ACLs perform access control on all traffic received from a specified user. User ACLs provide access control based on the Layer 3 addresses (for IP protocols), Layer 2 MAC addresses (for non-IP protocols), or Layer 4 port information and ranges. UACLs are only applied to ingress traffic.

## Configuring the ACLs

ACL is order dependent. ACLs are executed in the sequential order in which access control entries (ACE) are defined. The Mobility Access Switch process the ACEs in the order in which it is configured. Usually the deny ACEs are configured before permit ACEs. There is an implicit deny at the end of every ACL. Therefore, if there are no matching ACEs for a given packet, then that packet will be dropped.

This section describes the CLIs to configure the different ACLs:

### Ethertype ACL

The below command configures an Ethertype access control list (ACL).

```
(host)(config) #ip access-list eth ETHER_TYPE
(host)(config-eth-ETHER_TYPE) #deny 0x880
(host)(config-eth-ETHER_TYPE) #permit any
(host)(config-stateless-ETHER_TYPE) #exit
```

To configure the ACL when a particular access control entry(ACE) is changed in a particular ACL:

```
(host)(config) #ip access-list eth ETHER_TYPE
(host)(config-eth-ETHER_TYPE) #deny 0x0806
(host)(config-eth-ETHER_TYPE) #permit any
(host)(config-eth-ETHER_TYPE) #exit
```

### MAC ACL

A range of MAC address can be matched by using a wildcard mask or a particular host using the `host` keyword:

```
(host)(config) #ip access-list mac MAC_LIST
(host)(config-mac-MAC_LIST) #deny 00:11:22:00:00:00 00:00:00:FF:FF:FF
(host)(config-mac-MAC_LIST) #deny host 00:66:77:88:99:AA
(host)(config-mac-MAC_LIST) #permit any
(host)(config-mac-MAC_LIST) #exit
```

### Standard ACL

The Standard ACL match the source IP address of the packet. The IP address to be matched can be either a range of IP Addresses using wildcard mask or a particular host:

```
(host)(config) #ip access-list standard STANDARD
(host)(config-standard-STANDARD) #deny 1.1.1.0 0.0.0.255
(host)(config-standard-STANDARD) #deny host 192.168.10.100
(host)(config-standard-STANDARD) #permit any
(host)(config-standard-STANDARD) #exit
```

## Extended ACL

The Extended ACL extends the standard ACL by matching IP address of the source and destination, port number of the source and destination, and the protocol:

```
(host)(config) #ip access-list extended EXTENDED
(host)(config-extended-EXTENDED) #deny icmp 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255 echo-reply
(host)(config-extended-EXTENDED) #deny tcp host 192.168.1.1 eq 53 host 20.1.1.1 range 20 30
established
(host)(config-extended-EXTENDED) #permit any any any
(host)(config-extended-EXTENDED) #exit
```

## Stateless ACL

Stateless ACL provides userlevel access control on statically configured ACL.

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

Stateless ACL provides additional options that can be specified on matching the traffic. [Table 25](#) describes the parameters you configure for a stateless ACL.

**Table 25:** Stateless ACL Configuration Parameters

| Parameter       | Description                                                                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| blacklist       | Configure the ACL blacklist user when the ACL rule is matched. If the ACE entry is matched, the traffic from that particular user is denied and the user is blacklisted for 3600 seconds |
| log             | Configure to display the log information when the ACL is applied.                                                                                                                        |
| policer-profile | To attach the policer-profile to the ACL                                                                                                                                                 |
| position        | Defines or redefines the position of an ACE in an 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      | Associate a time-range to an ACL. This configures the ACL to filter traffic during the specified time-range                                                                              |

The following ACL actions are not supported for Egress ACLs (For Stateless ACL applied in egress direction):

- Blacklist
- Log

For the policer profile attached to the egress ACL, only the following are permitted:

- Action: drop/permit
- counters

To apply ACL to a port in ingress direction, use the following CLI:

```
(host)(config) #interface gigabitethernet 0/0/0
(host)(gigabitethernet "0/0/0") #ip access-group in <acl_name>
(host)(gigabitethernet "0/0/0") #exit
```

To apply ACL to a port in egress direction, use the following CLI:

```
(host)(config) #interface gigabitethernet 0/0/0
```

```
(host) (gigabitethernet "0/0/0") #ip access-group out <acl_name>
(host) (gigabitethernet "0/0/0") #exit
```

## Verifying the ACL configuration

Use the following commands to verify the ACL configuration:

```
(host) #show ip access-list ETHER_TYPE
ETHER_TYPE

Priority Action EtherType Mirror

1 deny 0x8800
2 permit any
```

You can use the same command to verify the ACL configuration after changing the ACE:

```
(host) #show ip access-list ETHER_TYPE
ip access-list eth ETHER_TYPE
ETHER_TYPE

Priority Action EtherType Mirror

1 deny 0x880
2 permit any
3 deny 0x806
(host) #show ip access-list MAC_LIST
ip access-list mac MAC_LIST
deny 00:11:22:00:00:00 00:00:00:ff:ff:ff
deny host 00:66:77:88:99:aa
permit any
```

```
(host) #show ip access-list STANDARD
ip access-list standard STANDARD
deny 1.1.1.0 0.0.0.255
deny host 192.168.10.100
permit any
```

```
(host) #show ip access-list EXTENDED
ip access-list extended EXTENDED
deny icmp 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255 echo-reply
deny tcp host 192.168.1.1 eq 53 host 20.1.1.1 range 20 30
permit any any any
```

```
(host) #show ip access-list STATELESS
ip access-list stateless STATELESS
STATELESS

```

| Priority | Source       | Destination    | Service | Action | TimeRange | Log |
|----------|--------------|----------------|---------|--------|-----------|-----|
| 1        | 10.100.100.0 | 255.255.255.0  | any     | deny   |           | Yes |
| 2        | any          | 10.100.100.200 | any     | deny   |           | Yes |
| 3        | any          | any            | any     | permit |           |     |

```
Expired QoS Policer Blacklist Mirror IPv4 Nexthop

4
4
4
```

This chapter describes how to configure quality of service (QoS) on the Mobility Access Switch. This chapter contains the following major sections:

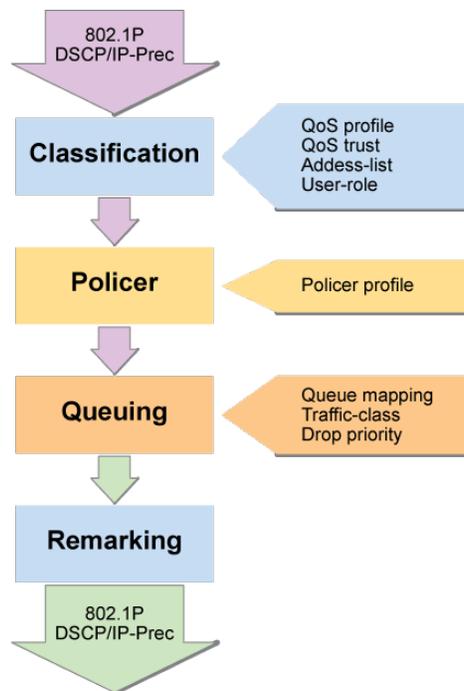
- [QoS Concepts on page 283](#)
- [Configuring QoS on page 285](#)

## QoS Concepts

This section contains the following sections:

- [Overview on page 283](#)
- [Profiles and Queues on page 283](#)
- [Classification on page 284](#)
- [Policing on page 285](#)

### Overview



### Profiles and Queues

The Mobility Access Switch supports:

- A QoS profile that can be applied to an interface, user role, and traffic flow.
- Eight queues per interface in hardware.
- Eight traffic classes (TC), which map to the corresponding queue (0 - 7).
- Drop-precedence for controlling tail-drop.

## Classification

This section contains the following sections:

- [Trust Mode on page 284](#)
- [Untrusted Mode on page 284](#)

### Trust Mode

When the QoS mode on a port is set to be trusted, the received 802.1P/DSCP is considered trustworthy and the frame is allowed to exit with those values intact. The received DSCP or 802.1P value is used to index predefined QoS profiles to determine traffic class and drop precedence. These QoS profiles cannot be edited at this time.

Starting from ArubaOS 7.4.0.3, if **qos-trust** is enabled on a Tunneled Node port, the QoS markings (DSCP/dot1p) of the incoming packet are copied to the outer GRE header packet as well. This enables appropriate QoS treatment along the tunnel path.

The Mobility Access Switch supports several modes:

- Layer 2 QoS Trust Mode - Port is configured to trust the IEEE 802.1P user priority. This is relevant for 802.1Q packets
- Layer 3 QoS Trust Mode - Port is configured to trust the received DSCP value of the frame.
- Auto (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.

The following table shows DSCP-Queue mapping:

**Table 26:** DSCP-Queue Mapping

| DSCP  | 802.1p | Queue |
|-------|--------|-------|
| 0-7   | 0      | 0     |
| 8-15  | 1      | 1     |
| 16-23 | 2      | 2     |
| 24-31 | 3      | 3     |
| 32-39 | 4      | 4     |
| 40-47 | 5      | 5     |
| 48-55 | 6      | 6     |
| 56-63 | 7      | 7     |

- DP is defined as low for first 4 values (0-3) and high for last 4 values (4-7) for each DSCP range.
- For 802.1p, DP is defined low for all values.

### Untrusted Mode

- The default is “untrust” for all interfaces where all incoming traffic are mapped to TC “0” and are then subsequently mapped to egress queue 0.

### Profile

- QoS profile can be configured to assign specific TC/DP, DSCP, and 802.1p values.

- The QoS profile can be then applied to:
  - Interface (interface-profile)
  - Stateless access-list
  - User-role
  - Policer profile

## Policing

- Limits inbound transmission rate of a class of traffic on the basis of user-defined criteria.
- Policer can be applied to stateless ACL, interface, and user-role.
- 1-rate 3-color policer is supported.
  - Traffic rate below CIR or burst below CBS limit is considered “conforming” and is allowed to pass through the policer.
  - Traffic rate exceeding CIR, and bursting below EBS limit is considered “exceeding” and is allowed to pass through the policer by default.
  - Traffic rate exceeding CIR, and bursting above EBS limit is considered “violating” and is dropped at the policer by default.

## Configuring QoS

This section contains the following sections:

- [Configuring QoS Trust Mode on page 285](#)
- [Configuring QoS-Profile under an Interface on page 286](#)
- [Configuring QoS-Profile under a Stateless ACL on page 286](#)
- [Configuring QoS-Profile under a User-Role on page 286](#)
- [Configuring Policer under Policer-Profile on page 286](#)
- [Configuring Policer-Profile under an Interface on page 286](#)
- [Configuring Policer-Profile under a Stateless ACL on page 287](#)
- [Configuring QoS-Profile under a User-Role on page 286](#)

### Configuring QoS Trust Mode

To configure QoS trust mode, follow these steps:

1. In the configuration mode, configure the appropriate interface:
 

```
(host) (config) #interface gigabitethernet 0/0/6
```
2. In the interface mode, you can configure the following options:
  - To configure QoS trust aruba-device, use the following command:
 

```
(host) (gigabitethernet "0/0/6") #qos trust aruba-device
```
  - To configure QoS trust auto, use the following command:
 

```
(host) (gigabitethernet "0/0/6") #qos trust auto
```
  - To disable QoS trust, use the following command:
 

```
(host) (gigabitethernet "0/0/6") #qos trust disable
```
  - To configure QoS trust dot1p, use the following command:
 

```
(host) (gigabitethernet "0/0/6") #qos trust dot1p
```
  - To configure QoS trust dscp, use the following command:
 

```
(host) (gigabitethernet "0/0/6") #qos trust dscp
```
  - To configure QoS trust pass-through, use the following command:

```
(host) (gigabitethernet "0/0/6") #qos trust pass-through
To display the predefined QoS profiles, use the following command.
(host) (config)#show qos-profile trusted
```

When configuring QoS trust, note the following guidelines:

- 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-vevice option. But will take effect only if no aruba-device is detected.

## Configuring QoS-Profile

To configure a QoS under a QoS profile, use the following commands:

```
(host) (config) #qos-profile QOS1
(host) (QoS Profile "QOS1") #dot1p <value>
(host) (QoS Profile "QOS1") #drop-precedence <low/high>
(host) (QoS Profile "QOS1") #dscp <value>
(host) (QoS Profile "QOS1") #traffic-class <value>
```

## Configuring QoS-Profile under an Interface

To configure a QoS profile on an Interface, use the following commands:

```
(host) (config) #interface gigabitethernet 0/0/19
(host) (gigabitethernet "0/0/19") #qos-profile QOS1
```

## Configuring QoS-Profile under a Stateless ACL

To configure QoS Profile under a Stateless ACL, use the following commands:

```
(host) (config) #ip access-list stateless STATELESS
(host) (config-stateless-STATELESS)#any any any permit qos-profile QOS1
```

## Configuring QoS-Profile under a User-Role

To configure QoS Profile under a user-role, use the following commands:

```
(host) (config) #user-role EMPLOYEE_1
(host) (config-role) #qos-profile QOS1
```

## Configuring Policer under Policer-Profile

To configure Policer under a Policer profile, use the following commands:

```
(host) (config) #policer-profile 100MBPS
(host) (Policer Profile "100MBPS") #cir 100000 (100m)
(host) (Policer Profile "100MBPS") #cbs 100000 (100m)
(host) (Policer Profile "100MBPS") #ebs 110000 (110m)
(host) (Policer Profile "100MBPS") #exceed-action <permit | remark | drop>
(host) (Policer Profile "100MBPS") #exceed-profile <QoS profile for remark>
(host) (Policer Profile "100MBPS") #violate-action <permit | remark | drop>
```



---

When remark action is configured, a corresponding QoS profile must be configured also.

---

## Configuring Policer-Profile under an Interface

To configure a policer profile on an interface, use the following commands:

```
(host) (config) #interface gigabitethernet 0/0/19
(host) (gigabitethernet "0/0/19") #policer-profile 100MBPS
```

## Configuring Policer-Profile under a Stateless ACL

To configure a policer profile on an interface, use the following commands:

```
(host) (config) #ip access-list stateless STATELESS
(host) (config-stateless-STATELESS)#any any any permit policer-profile 100MBPS
```

## Configuring Policer-Profile under a User-role

```
(host) (config) #user-role EMPLOYEE_1
(host) (config-role) #policer-profile 100MBPS
```

You can also optionally configure the policer-profile for granular rate limiting using the per-user parameter. The sample command for using per-user parameter to configure the policer-profile for granular rate limiting is given in the following example:

```
(host) (config-role) #policer-profile 100MBPS per-user
```



This chapter describes how to configure authentication servers. It contains the following sections:

- [Important Points to Remember on page 289](#)
- [Server and Server Group Concepts on page 289](#)
- [Configuring Authentication Servers on page 290](#)
- [Internal Database Concepts on page 296](#)
- [Configuring the Internal Database on page 297](#)
- [Server Group Concepts on page 298](#)
- [Assigning Server Groups on page 302](#)
- [Authentication Timers on page 305](#)

### Important Points to Remember

The Mobility Access Switch allows you to use an external authentication server or the internal user database to authenticate clients who need to access the wired network.

For an external authentication server to process requests from the Mobility Access Switch, you must configure the server to recognize the switch. Refer to the vendor documentation for information on configuring the authentication server.

### Server and Server Group Concepts

The Mobility Access Switch supports the following external authentication servers:

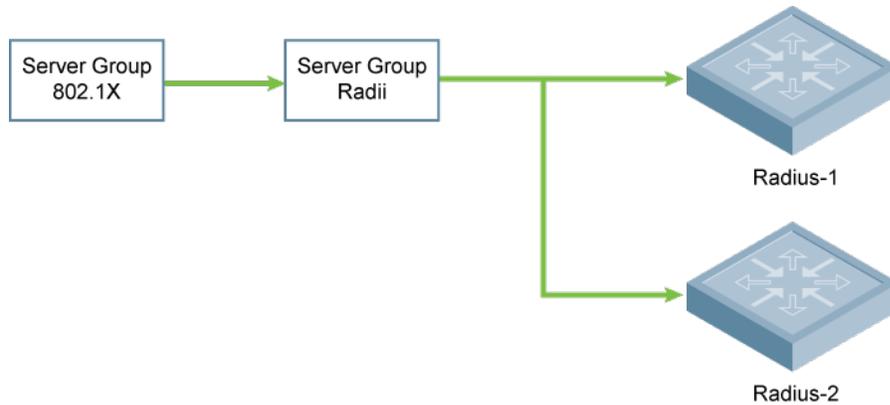
- RADIUS (Remote Authentication Dial-In User Service)
- LDAP (Lightweight Directory Access Protocol)
- TACACS+ (Terminal Access Mobility Access Switch Access Control System)

Additionally, you can use the Mobility Access Switch's internal database to authenticate users. You create entries in the database for users and their passwords and default role.

You can create groups of servers for specific types of authentication. For example, you can specify one or more RADIUS servers to be used for 802.1X authentication. The list of servers in a server group is an ordered list. This means that the first server in the list 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 one group — for example, you can include the internal database as a backup to a RADIUS server.

[Figure 18](#) shows a server group named Radii that contains two RADIUS servers, Radius-1 and Radius-2. The Radii server group is assigned to the server group for 802.1X authentication.

**Figure 18** Server Group



Server names must be unique. You can configure the same server in multiple server groups, and you must configure the server before you can add it to a server group.



If you are using the Mobility Access Switch's internal database for user authentication, use the predefined "Internal" server group.

You can also include conditions for server-derived user roles or VLANs in the server group configuration. The server derivation rules apply to all servers in the group.

## Configuring Authentication Servers

This section describes how to configure authentication servers on the Mobility Access Switch. It contains the following sections:

- [RADIUS Server Username/Password Authentication](#)
- [RADIUS Server Authentication with VSA](#)
- [RADIUS Server Authentication with Server-Derivation Rule](#)
- [Configuring Authentication Servers](#)
- [Verifying the configuration](#)
- [Configuring a RADIUS Server on page 292](#)
- [Configuring an LDAP Server on page 293](#)
- [Configuring a TACACS+ Server on page 295](#)

### RADIUS Server Username/Password Authentication

In this example, an external RADIUS server is used to authenticate management users. Upon authentication, users are assigned the default role root.

#### In the CLI

```
aaa authentication-server radius rad1
 host <ipaddr>
 key <string>
aaa server-group corp_rad
 auth-server rad1
aaa authentication mgmt
 default-role root
 enable
 server-group corp_rad
```

## RADIUS Server Authentication with VSA

In this scenario, an external RADIUS server authenticates management users and returns to the Mobility Access Switch the Aruba vendor-specific attribute (VSA) called Aruba-Admin-Role that contains the name of the management role for the user. The authenticated user is placed into the management role specified by the VSA.

The Mobility Access Switch configuration is identical to the [RADIUS Server Username/Password Authentication on page 290](#). The only difference is the configuration of the VSA on the RADIUS server. Ensure that the value of the VSA returned by the RADIUS server is one of the predefined management roles. Otherwise, the user will have *no* access to the Mobility Access Switch.

## RADIUS Server Authentication with Server-Derivation Rule

A RADIUS server can return to the Mobility Access Switch a standard RADIUS attribute that contains one of the following values:

- The name of the management role for the user
- A value from which a management role can be derived

For either situation, configure a server-derivation rule for the server group.

In the following example, the RADIUS server returns the attribute Class to the Mobility Access Switch. The value of the attribute can be either “root” or “network-operations” depending upon the user; the returned value is the role granted to the user.



---

Ensure that the value of the attribute returned by the RADIUS server is one of the predefined management roles. Otherwise, the management user will not be granted access to the Mobility Access Switch.

---

### In the CLI

```
aaa authentication-server radius rad1
 host <ipaddr>
 key <string>
aaa server-group corp_rad
 auth-server rad1
 set role condition Class value-of
aaa authentication mgmt
 default-role read-only
 enable
 server-group corp_rad
```

## Disabling Authentication of Local Management User Accounts

You can disable authentication of management user accounts in local switches if the configured authentication server(s) (RADIUS or TACACS+) are not available.

You can disable authentication of management users based on the results returned by the authentication server. When configured, locally-defined management accounts (for example, admin) are not allowed to log in if the server(s) are reachable and the user entry is not found in the authentication server. In this situation, if the RADIUS or TACACS+ server is unreachable, meaning it does not receive a response during authentication, or fails to authenticate a user because of a timeout, local authentication is used and you can log in with a locally-defined management account.

### In the CLI

```
mgmt-user localauth-disable
```

## Verifying the configuration

To verify if authentication of local management user accounts is enabled or disabled, use the following command:

```
show mgmt-user local-authentication-mode
```

## Configuring a RADIUS Server

[Table 27](#) describes the parameters you configure for a RADIUS server.

**Table 27:** RADIUS Server Configuration Parameters

| Parameter           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                | IP address of the authentication server.<br>Default: N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Key                 | Shared secret between the Mobility Access Switch and the authentication server. The maximum length is 128 characters.<br>Default: N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Authentication Port | Authentication port on the server.<br>Default: 1812                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Accounting Port     | Accounting port on the server<br>Default: 1813                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Retransmits         | Maximum number of retries sent to the server by the Mobility Access Switch before the server is marked as down.<br>Default: 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Timeout             | Maximum time, in seconds, that the Mobility Access Switch waits before timing out the request and resending it.<br>Default: 5 seconds                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| NAS ID              | Network Access Server (NAS) identifier to use in RADIUS packets.<br>Default: N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| NAS IP              | NAS IP address to send in RADIUS packets.<br>You can configure a “global” NAS IP address that the Mobility Access Switch 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 in the CLI, enter the <b>ip radius nas-ip &lt;ipaddr&gt;</b> command.<br>Default: N/A                                                                                                                                                                                                                                                                           |
| Source Interface    | Enter a VLAN number ID.<br>Allows you to use source IP addresses to differentiate RADIUS requests.<br>Associates a VLAN interface with the RADIUS server to allow the group-specific source interface to override the global configuration. <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul> |
| Use MD5             | Use MD5 hash of cleartext password.<br>Default: disabled                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Mode                | Enables or disables the server.<br>Default: enabled                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Using the CLI

```
aaa authentication-server radius <name>
 host <ipaddr>
 key <key>
 enable
```

## RADIUS Server Authentication Codes

A configured RADIUS server will return the following standard response codes.

**Table 28:** RADIUS Authentication Response Codes

| Code | Description                                                                     |
|------|---------------------------------------------------------------------------------|
| 0    | Authentication OK.                                                              |
| 1    | Authentication failed—user/password combination not correct.                    |
| 2    | Authentication request timed out—No response from server.                       |
| 3    | Internal authentication error.                                                  |
| 4    | Bad Response from RADIUS server. Verify shared secret is correct.               |
| 5    | No RADIUS authentication server is configured.                                  |
| 6    | Challenge from server. (This does not necessarily indicate an error condition.) |

## RADIUS Change of Authorization

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

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

The following command configures an RFC 3576 server:

```
(host) #aaa rfc-3576-server 10.1.1.245
(host) #key asdfjkl;
```

## Configuring an LDAP Server

[Table 29](#) describes the parameters you configure for an LDAP server.

**Table 29: LDAP Server Configuration Parameters**

| Parameter                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                      | IP address of the LDAP server.<br>Default: N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Admin-DN                  | Distinguished name for the admin user who has read/search privileges across all the entries in the LDAP database (the user need not have write privileges but the user should be able to search the database, and read attributes of other users in the database).                                                                                                                                                                                                                                                                                                                               |
| Admin Password            | Password for the admin user.<br>Default: N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Allow Clear-Text          | Allows clear-text (unencrypted) communication with the LDAP server.<br>Default: disabled                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Authentication Port       | Port number used for authentication.<br>Default: 389                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Base-DN                   | Distinguished Name of the node which contains the entire user database to use.<br>Default: N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Filter                    | Filter that should be applied to search of the user in the LDAP database:<br>Default: (objectclass=*)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Key Attribute             | Attribute that should be used as a key in search for the LDAP server. For Active Directory, the value is sAMAccountName.<br>Default: sAMAccountName                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Timeout                   | Timeout period of a LDAP request, in seconds.<br>Default: 20 seconds                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Mode                      | Enables or disables the server.<br>Default: enabled                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Preferred Connection Type | Preferred type of connection between the Mobility Access Switch and the LDAP server. The default order of connection type is: <ol style="list-style-type: none"> <li>1. ldap-s</li> <li>2. start-tls</li> <li>3. clear-text</li> </ol> The Mobility Access Switch 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.<br><b>NOTE:</b> If you select <b>clear-text</b> as the preferred connection type, you must also enable the <b>allow-cleartext</b> option. |

## Using the CLI

```

aaa authentication-server ldap <name>
admin-dn The Distinguished Name for the Admin user who can
 search for the LDAP user. E.g.
 (cn=Admin-Name,cn=Users,dc=department-name,dc=domain-
 name,dc=com)
admin-password The password for the Admin user who can search for
 the LDAP user
allow-cleartext Allow unencrypted communication with LDAP server
authport Specify port number used for authentication. Range:
 1-65535. Default : 389. Port 636 will be attempted
 for LDAP over SSL - LDAPS, 389 will be attempted for
 SSL over LDAP - Start TLS and for clear text.

```

|                     |                                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| base-dn             | The Base Distinguished Name of search for the LDAP server. E.g. (cn=Users,dc=qa,dc=domain,dc=com)                                                                       |
| clone               | Copy data from another LDAP Server                                                                                                                                      |
| enable              | Enable LDAP server                                                                                                                                                      |
| filter              | The filter that should be used as a key in a search for the LDAP server                                                                                                 |
| host                | IP address of LDAP server                                                                                                                                               |
| key-attribute       | The attribute that should be used as a key in search for the LDAP server. For PAP, the value is sAMAccountName. For EAP-TLS termination the value is userPrincipalName. |
| no                  | Delete Command                                                                                                                                                          |
| preferred-conn-type | Preferred connection type                                                                                                                                               |
| timeout             | Timeout period for LDAP request. Range: 1-30. Default: 20.                                                                                                              |

## Configuring a TACACS+ Server

[Table 30](#) defines the TACACS+ server parameters.

**Table 30:** TACACS+ Server Configuration Parameters

| Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                  | IP address of the server.<br>Default: N/A                                                                                                                                                                                                                                                                                                                                                                                                       |
| Key                   | Shared secret to authenticate communication between the TACACS+ client and server.<br>Default: N/A                                                                                                                                                                                                                                                                                                                                              |
| TCP Port              | TCP port used by server.<br>Default: 49                                                                                                                                                                                                                                                                                                                                                                                                         |
| Retransmits           | Maximum number of times a request is retried.<br>Default: 3                                                                                                                                                                                                                                                                                                                                                                                     |
| Timeout               | Timeout period for TACACS+ requests, in seconds.<br>Default: 20 seconds                                                                                                                                                                                                                                                                                                                                                                         |
| Mode                  | Enables or disables the server.<br>Default: enabled                                                                                                                                                                                                                                                                                                                                                                                             |
| Session Authorization | Enables or disables session authorization. Session authorization turns on the optional authorization session for admin users.<br>Default: disabled                                                                                                                                                                                                                                                                                              |
| Source Interface      | VLAN number ID to select a specific source interface IP address for the outgoing TACACS packets. The parameters are: <ul style="list-style-type: none"> <li>loopback: Assigns the switch IP as the source IP.</li> <li>vlan &lt;id&gt;: Assigns the IP address of the specified VLAN interface as the source IP.</li> <li>secondary &lt;ip&gt;: Assigns a secondary source IP address in A.B.C.D format. This parameter is optional.</li> </ul> |

## Using the CLI

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

```

aaa authentication-server tacacs <name>
 clone default
 host <ipaddr>

```

```
key <key>
enable
session-authorization
```

Starting from ArubaOS 7.4.1, the Mobility Access Switch introduces the source-interface command at the global and profile levels for the TACACS+ server. This command allows you to select a specific source interface IP address for the outgoing TACACS+ packets.

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.

The syntax for the global source-interface command is as follows:

```
(host) (config) #ip tacacs source-interface {loopback | vlan <id> [secondary <ip>]}
```

The following is a sample global source-interface command:

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

The syntax for the profile-level source-interface command is as follows:

```
(host) (config) # aaa authentication-server tacacs <tacacs_server_name>
(host) (TACACS Server "<tacacs_server_name>") #source-interface {loopback | vlan <id>
[secondary <ip>]}
```

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
```

The following sample command configures the secondary IP address of VLAN 10 as the source interface IP address for all TACACS+ server request packets, provided there is no profile-level configuration:

```
(host) (config) #ip tacacs source-interface vlan 10 secondary 10.1.1.1
```

The following sample command configures the secondary IP address of VLAN 20 as the source interface IP address for a specific TACACS+ server:

```
(host) (config) #aaa authentication-server tacacs tac1
(host) (TACACS Server "tac1") #source-interface vlan 20 secondary 10.1.1.2
```

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
```

## Internal Database Concepts

You can create entries, in the Mobility Access Switch's internal database, to use to authenticate clients. The internal database contains a list of clients along with the password and default role for each client. When you configure the internal database as an authentication server, client information in incoming authentication requests is checked against the internal database.



## Managing Internal Database Files

ArubaOS allows you to import and export tables of user information to and from the internal database. These files should not be edited once they are exported. ArubaOS only supports the importing of database files that were created during the export process. Note that importing a file into the internal database overwrite and removes all existing entries.

### Using the CLI

Enter the following command in enable mode:

```
local-userdb export <filename>
local-userdb import <filename>
```

## Internal Database Utilities

The local internal database also includes utilities to clear all users from the database and to restart the internal database to repair internal errors. Under normal circumstances, neither of these utilities are necessary.

## Server Group Concepts

You can create groups of servers for specific types of authentication — for example, you can specify one or more RADIUS servers to be used for 802.1x authentication. You can configure servers of different types in one group — for example, you can include the internal database as a backup to a RADIUS server.

## Configuring Server Groups

Server names are unique. You can configure the same server in more than one server group. The server must be configured before you can include it in a server group.

### Using the CLI

```
aaa server-group <name>
auth-server <name>
```

## Configuring Server List Order and Fail-Through

The list of servers in a server group is an ordered list. By default, the first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure the order of servers in the server group. In the CLI, use the **position** parameter to specify the relative order of servers in the list (the lowest value denotes the first server in the list).

As mentioned previously, the first available server in the list is used for authentication. If the server responds with an authentication failure, there is no further processing for the user or client for which the authentication request failed. You can optionally enable *fail-through* authentication for the server group so that if the first server in the list returns an authentication deny, the Mobility Access Switch attempts authentication with the next server in the ordered list. The Mobility Access Switch attempts authentication with each server in the list until either there is a successful authentication or the list of servers in the group is exhausted. This feature is useful in environments where there are multiple, independent authentication servers; users may fail authentication on one server but can be authenticated on another server.

Before enabling fail-through authentication, note the following:

- This feature is not supported for 802.1x authentication with a server group that consists of external EAP-compliant RADIUS servers. You can, however, use fail-through authentication when the 802.1x authentication is terminated on the Mobility Access Switch (AAA FastConnect).

- Enabling this feature for a large server group list may cause excess processing load on the Mobility Access Switch. Aruba recommends that you use server selection based on domain matching whenever possible (see [Configuring Dynamic Server Selection on page 299](#)).
- Certain servers, such as the RSA RADIUS server, lock out the Mobility Access Switch if there are multiple authentication failures. Therefore you should not enable fail-through authentication with these servers.

In the following example, you create a server group 'corp-serv' with two LDAP servers (ldap-1 and ldap-2), each of which contains a subset of the usernames and passwords used in the network. When fail-through authentication is enabled, users that fail authentication on the first server in the server list should be authenticated with the second server.

### Using the CLI

```
aaa authentication-server ldap ldap-1
 host 10.1.1.234
aaa authentication-server ldap ldap-2
 host 10.2.2.234
aaa server-group corp-serv
 auth-server ldap-1 position 1
 auth-server ldap-2 position 2
 allow-fail-through
```

### Configuring Dynamic Server Selection

The Mobility Access Switch can dynamically select an authentication server from a server group based on the user information sent by the client in an authentication request. For example, an authentication request can include client or user information in one of the following formats:

- <domain>\<user> — for example, corpnet.com\darwin
- <user>@<domain> — for example, darwin@corpnet.com
- host/<pc-name>.<domain> — for example, host/darwin-g.finance.corpnet.com (this format is used with 802.1x machine authentication in Windows environments)

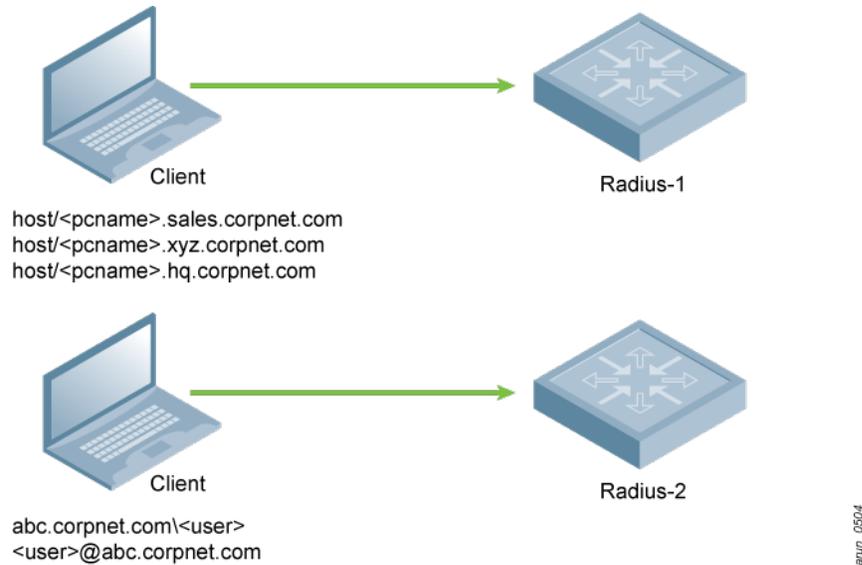
When you configure a server in a server group, you can optionally associate the server with one or more match rules. A match rule for a server can be one of the following:

- The server is selected if the client/user information contains a specified string.
- The server is selected if the client/user information begins with a specified string.
- The server is selected if the client/user information exactly matches a specified string.

You can configure multiple match rules for the same server. The Mobility Access Switch compares the client/user information with the match rules configured for each server, starting with the first server in the server group. If a match is found, the Mobility Access Switch sends the authentication request to the server with the matching rule. If no match is found before the end of the server list is reached, an error is returned and no authentication request for the client/user is sent.

For example, [Figure 19](#) depicts a network consisting of several subdomains in corpnet.com. The server radius-1 provides 802.1x machine authentication to PC clients in xyz.corpnet.com, sales.corpnet.com, and hq.corpnet.com. The server radius-2 provides authentication for users in abc.corpnet.com.

**Figure 19** Domain-Based Server Selection Example



You configure the following rules for servers in the corp-serv server group:

- radius-1 will be selected if the client information starts with "host/".
- radius-2 will be selected if the client information contains "abc.corpnet.com".

### Using the CLI

```
aaa server-group corp-serv
 auth-server radius-1 match-authstring starts-with host/ position 1
 auth-server radius-2 match-authstring contains abc.corpnet.com position 2
```

### Trimming Domain Information from Requests

Before the Mobility Access Switch forwards an authentication request to a specified server, it can truncate the domain-specific portion of the user information. This is useful when user entries on the authenticating server do not include domain information. You can specify this option with any server match rule. This option is only applicable when the user information is sent to the Mobility Access Switch in the following formats:

- <domain>\<user> — the <domain>\ portion is truncated
- <user>@<domain> — the @<domain> portion is truncated



---

This option does not support client information sent in the format host/<pc-name>.<domain>

---

### Using the CLI

```
aaa server-group corp-serv
 auth-server radius-2 match-authstring contains abc.corpnet.com trim-fqdn
```

### Configuring Server-Derivation Rules

When you configure a server group, you can set the VLAN or role for clients based on attributes returned for the client by the server during authentication. The server derivation rules apply to all servers in the group. The user role or VLAN assigned through server derivation rules takes precedence over the default role and VLAN configured for the authentication method.



The authentication servers must be configured to return the attributes for the clients during authentication. For instructions on configuring the authentication attributes in a Windows environment using IAS, refer to the documentation at <http://technet2.microsoft.com/windowsserver/en/technologies/ias.mspix>

The server rules are applied based on the first match principle. The first rule that is applicable for the server and the attribute returned is applied to the client and would be the only rule applied from the server rules. These rules are applied uniformly across all servers in the server group.

[Table 32](#) describes the server rule parameters you can configure.

**Table 32:** Server Rule Configuration Parameters

| Parameter    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Role or VLAN | The server derivation rules can be for either user role or VLAN assignment. With Role assignment, a client can be assigned a specific role based on the attributes returned. In case of VLAN assignment, the client can be placed in a specific VLAN based on the attributes returned.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Attribute    | This is the attribute returned by the authentication server that is examined for <i>Operation</i> and <i>Operand</i> match.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Operation    | This is the match method by which the string in <i>Operand</i> is matched with the attribute value returned by the authentication server. <ul style="list-style-type: none"><li>contains – The rule is applied if and only if the attribute value contains the string in parameter <i>Operand</i>.</li><li>starts-with – The rule is applied if and only if the attribute value returned starts with the string in parameter <i>Operand</i>.</li><li>ends-with – The rule is applied if and only if the attribute value returned ends with the string in parameter <i>Operand</i>.</li><li>equals – The rule is applied if and only if the attribute value returned equals the string in parameter <i>Operand</i>.</li><li>not-equals – The rule is applied if and only if the attribute value returned is not equal to the string in parameter <i>Operand</i>.</li><li>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 Mobility Access Switch when the rule is applied.</li></ul> |
| Operand      | This is the string to which the value of the returned attribute is matched.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Value        | The user role or the VLAN applied to the client when the rule is matched.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| position     | Position of the condition rule. Rules are applied based on the first match principle. 1 is the top.<br>Default: bottom                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Using the CLI

```
aaa server-group <name>
 auth-server <name>
 set {role|vlan} condition <condition> set-value {<role>|<vlan>}
 [position number]
```

## Configuring a Role Derivation Rule for the Internal Database

When you add a user entry in the Mobility Access Switch's internal database, you can optionally specify a user role (see [Internal Database Concepts on page 296](#)). In order for the role specified in the internal database entry

to be assigned to the authenticated client, you must configure a server derivation rule as shown in the following sections:

## Using the CLI

```
aaa server-group internal
 set role condition Role value-of
```

## Assigning Server Groups

You can create server groups for the following purposes:

- user authentication
- management authentication
- accounting

You can configure all types of servers for user and management authentication. However, TACACS+ is not supported for 802.1x authentication. For Accounting only RADIUS and TACACS+ servers are supported (see [Table 33](#)).

**Table 33:** *Server Types and Purposes*

|                           | RADIUS | TACACS+                           | LDAP | Internal Database |
|---------------------------|--------|-----------------------------------|------|-------------------|
| User authentication       | Yes    | Yes (for MAC Authentication only) | Yes  | Yes               |
| Management authentication | Yes    | Yes                               | Yes  | Yes               |
| Accounting                | Yes    | Yes                               | No   | No                |

## User Authentication

For information about assigning a server group for user authentication, see the configuration chapter for the authentication method.

## Management Authentication

Users who need to access the Mobility Access Switch to monitor, manage, or configure the Aruba user-centric network can be authenticated with RADIUS, TACACS+, or LDAP servers or the internal database.



---

Only user record attributes are returned upon a successful authentication. Therefore, to derive a different management role other than the default mgmt auth role, set the server derivation rule based on the user attributes.

---

## Using the CLI

```
aaa authentication mgmt
 server-group <group>
```

## Radius Accounting

This section describes how user statistics are maintained and made available for RADIUS accounting. It contains the following sections:

- [Understanding Radius Accounting on page 303](#)
- [Configuring RADIUS Accounting on page 305](#)

## Understanding Radius Accounting

RADIUS accounting supports sending user statistics in radius accounting stop and interim records. This document describes how user statistics are maintained and made available for RADIUS accounting.

When RADIUS accounting is enabled in the AAA profile, RADIUS accounting start and stop records are sent to the server. RADIUS accounting stop records contain received bytes and packet counters. The accounting start record is sent when a user authenticates. The stop record is sent when a user logs out or is deleted from the system. If interim accounting is enabled, updates are sent out at a fixed interval. Each interim record includes cumulative user statistics.

Currently, only received packets and bytes in accounting records are transmitted to the radius server.

### User Activity and Statistics

RADIUS accounting allows user activity and statistics to be reported from the Mobility Access Switch to RADIUS servers. RADIUS accounting works as follows:

- The Mobility Access Switch generates an Accounting Start packet when a user logs in. The code field of transmitted RADIUS packet is set to 4 (Accounting-Request). Note that sensitive information, such as user passwords, are not sent to the accounting server. The RADIUS server sends an acknowledgement of the packet.
- The Mobility Access Switch sends an Accounting Stop packet when a user logs off; the packet information includes various statistics such as elapsed time, input and output bytes and packets. The RADIUS server sends an acknowledgement of the packet. The following is the list of attributes that the Mobility Access Switch can send to a RADIUS accounting server:
  - Acct-Status-Type:  
This attribute marks the beginning or end of accounting record for a user. Currently, possible values include Start and Stop.
  - User-Name:  
Name of user.
  - Acct-Session-Id:  
A unique identifier to facilitate matching of accounting records for a user. It is derived from the user name, IP address and MAC address. This is set in all accounting packets.
  - Acct-Authentic:  
This indicates how the user was authenticated. Current values are 1 (RADIUS), 2 (Local) and 3 (LDAP).
  - Acct-Session-Time:  
The elapsed time, in seconds, that the client was logged in to the Mobility Access Switch. This is only sent in Accounting-Request records where the Acct-Status-Type is Stop.
  - Acct-Terminate-Cause:  
Indicates how the session was terminated and is sent in Accounting-Request records where the Acct-Status-Type is Stop. Possible values are:
    - 1: User logged off
    - 4: Idle Timeout
    - 5: Session Timeout. Maximum session length timer expired.
    - 7: Admin Reboot: Administrator is ending service, for example prior to rebooting the Mobility Access Switch.
  - NAS-Identifier:  
This is set in the RADIUS server configuration.

NAS-IP-Address: IP address of the master Mobility Access Switch. You can configure a “global” NAS IP address: in the WebUI, navigate to the Configuration > Security > Authentication > Advanced page; in the CLI, use the `ip radius nas-ip` command.

- NAS-Port:  
Physical or virtual port (tunnel) number through which the user traffic is entering the Mobility Access Switch.
- NAS-Port-Type:  
Type of port used in the connection. This is set to one of the following:  
5: admin login  
15: wired user type  
19: wireless user
- Framed-IP-Address: IP address of the user.
- Calling-Station-ID: MAC address of the user.
- Called-station-ID: MAC address of the Mobility Access Switch.

The following attributes are sent in Accounting-Request packets when Acct-Status-Type value is Start:

- Acct-Status-Type
- User-Name
- NAS-IP-Address
- NAS-Port
- NAS-Port-Type
- NAS-Identifier
- Framed-IP-Address
- Calling-Station-ID
- Called-station-ID
- Acct-Session-Id
- Acct-Authentic

The following attributes are sent in Accounting-Request packets when Acct-Status-Type value is Stop:

- Acct-Status-Type
- User-Name
- NAS-IP-Address
- NAS-Port
- NAS-Port-Type
- NAS-Identifier
- Framed-IP-Address
- Calling-Station-ID
- Called-station-ID
- Acct-Session-Id
- Acct-Authentic
- Terminate-Cause
- Acct-Session-Time

The following attributes are sent only in Accounting Stop packets (they are not sent in Accounting Start packets):

- Acct-Input-Octets
- Acct-Output-Octets
- Acct-Input-Packets
- Acct-Output-Packets

## Configuring RADIUS Accounting

Radius accounting support is enabled and disabled in the AAA profile. By default, it is disabled.

To enable radius-accounting, use the command radius-accounting:

```
(host) #configure terminal
(host) (config)#aaa profile default
(host) (AAA Profile "default") #radius-accounting foobar
(host) (AAA Profile "default") #show aaa profile test
```

AAA Profile "TEST"

-----

| 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        | foobar   |
| RADIUS Interim Accounting             | Disabled |
| XML API server                        | 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 |

To disable the feature, use the command no radius-accounting:

```
(host) (AAA Profile "default") #no radius-accounting
```

## TACACS+ Accounting

TACACS+ accounting allows commands issued on the Mobility Access Switch to be reported to TACACS+ servers. You can specify the types of commands that are reported (action, configuration, or show commands) or have all commands reported.

### Using the CLI

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

## Authentication Timers

[Table 34](#) describes the timers you can configure that apply to all clients and servers. These timers can be left at their default values for most implementations.

**Table 34: Authentication Timers**

| Timer                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Idle Timeout               | <p>Maximum period after which a client is considered idle if there is no user traffic from the client.</p> <p>The timeout period is reset if there is a user traffic. If Mobility Access Switch does not see traffic from the user for more than the timeout period, then that user entry will be deleted from the system. If the keyword <b>seconds</b> is not specified, the value defaults to minutes at the command line.</p> <p>Range: 1 to 255 minutes (30 to 15300 seconds)<br/>Default: 5 minutes (300 seconds)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Authentication Server Dead Time | <p>Maximum period, in minutes, that the Mobility Access Switch considers an unresponsive authentication server to be "out of service".</p> <p>This timer is only applicable if there are two or more authentication servers configured on the Mobility Access Switch. If there is only one authentication server configured, the server is never considered out of service and all requests are sent to the server.</p> <p>If one or more backup servers are configured and a server is unresponsive, it is marked as out of service for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as down for the dead time.</p> <p>Range: 0-50<br/>Default: 10 minutes</p> <p><b>NOTE:</b> Setting the server dead time to 0, will not mark any server as out of service.</p> |
| Logon User Lifetime             | <p>Maximum time, in minutes, unauthenticated clients are allowed to remain logged on.</p> <p>Range: 0-255<br/>Default: 5 minutes</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Using the CLI

To set an authentication timer, use the following command:

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

This chapter describes AAA authentication. It contains the following major sections:

- [AAA Authentication Profile on page 307](#)
- [Configuring Authentication End to End on page 312](#)
- [RADIUS Fail-Open on page 314](#)
- [Preauth Role Assignment on page 319](#)
- [Deny DHCP Role for 802.1x Authentication on page 321](#)
- [Delay EAP Success for dot1x Authentication on page 321](#)
- [Port Bounce on page 322](#)

## AAA Authentication Profile

- [Authentication Profile Concepts on page 307](#)
- [Authentication Schemes on page 308](#)
- [Role/VLAN Derivation on page 309](#)
- [User Roles on page 311](#)
- [Authentication Roles on page 311](#)
- [User Derivation Rules on page 311](#)

### Authentication Profile Concepts

The AAA profile can be applied on a global or per port or per VLAN basis, but only if the port is marked as un-trusted. If no AAA profile is configured on a port or a VLAN that the port is part of, the AAA profile configured under the wired authentication profile (aaa authentication wired) is applied globally by default.

AAA profile cannot be attached to an interface that is configured with a Tunneled Node profile.

If the port is marked as trusted, no authentication can be applied to traffic to the port.

The global AAA profile has limited ability to perform granular access control. The ability to apply an AAA profile on a per port/VLAN basis provides the administrator with greater flexibility and more granular access control. With per-port AAA profile, users can specify a unique AAA profile for each un-trusted port.

The AAA profile can be configured with the following parameters:

#### Initial Role

- The Initial Role is applied to all packets before a Layer 3 user entry is created.

#### MAC Auth Profile

- The MAC Auth Profile contains the MAC authentication profile parameters.

#### MAC Default Role

- The MAC Default Role is the default role a user receives upon successful MAC authentication.

#### 802.1x Auth Profile

- The 802.1x Auth Profile contains the 802.1x authentication profile parameters.

## 802.1x Default Role

- The 802.1x Default Role is the default role a user receives upon successful 802.1x authentication.

## User Derivation Rules

- The User Derivation Rules provide the means to derive a new VLAN or role, based on user attributes.

## Authentication Schemes

The Mobility Access Switch supports the following authentication schemes:

- MAC Based Authentication
- 802.1X Authentication
- Layer2 Authentication Fail-through

## MAC-Based Authentication

MAC-Based Authentication is a simple authentication method that is used more often as a filtering mechanism than as an actual authentication method. MAC-Based Authentication is frequently used when devices such as phones, printers, and scanners do not support 802.1x. It is also used in conjunction with 802.1x, so that the 802.1x authenticator and the back-end authentication server do not have to handle the load of authenticating users or devices that are not part of the back end database.

## 802.1x Authentication

802.1x authentication is a sophisticated method of network authentication that is widely supported across client OS and networking devices. This scheme provides a number of authentication methods, including PEAP and TLS. Both of these methods rely on TLS protocol to establish a secure tunnel to exchange user credentials, and authenticate the user. User validation can be done using a password or a certificate. The Mobility Access Switch supports using 802.1x authentications in the following modes:

- Authenticator Mode
- Authentication (EAP-Termination) Mode

### Authenticator Mode

The authenticator mode is a generic method where the EAP frames from the user are packaged and sent to a RADIUS server. In the authentication server mode, also known as eap-termination mode, the controller can terminate the EAP frames to provide crypto hardware acceleration support to terminate the TLS tunnel. The controller dataplane terminates the phase 1 of the 802.1x authentication and provides with the TLS keys to the control plane to terminate the TLS tunnel. The phase 2 continues in the control plane with the user validation done using MSChapV2, PAP or Certification verification depending on the EAP mode the user was configured.

### Authentication Server (EAP-Termination) Mode

In the authentication server mode, or eap-termination mode, the controller can terminate the EAP frames to provide crypto hardware acceleration support to terminate the TLS tunnel.

802.1x also supports key exchange in data encryption for wireless users. For wired users that are deployed today there is no key exchange and the security is limited to authenticating the user.

## Layer2 Authentication Fail-through

Layer2 Authentication Fail-through is used to perform mixed authentication which includes both MAC and 802.1x authentication. This feature automatically switches to 802.1x authentication when MAC authentication fails.



---

By default, the Layer2 Authentication Fail-through option is enabled.

---

## Role/VLAN Derivation

A user can be assigned a role/VLAN at different stages in its life cycle and the derivation can be done on various parameters. The precedence of the assignment is from 1 to 5 with 1 being the lowest and 5 being the highest. A user can be assigned a different role/VLAN in the following stages:

### 1. Initial Role/VLAN

This role is applied to the ingress on which the user traffic arrives. For wireless and tunneled-mode users, the ingress is a GRE tunnel and for wired users it is a port or VLAN. This role provides the means to control what kind of initial traffic is allowed, which is predominantly determined based on the allowed modes of authentication. There are cases where initial role is configured to deny all DHCP traffic so that the creation of the user happens after MAC based or 802.1x authentication is completed.

### 2. User Derived Role/VLAN

This role is only assigned based on the user MAC address. For this role derivation, user-derivation-rules must be defined and applied under the AAA profile.

### 3. Default Authentication Role/VLAN

This role is assigned when a user successfully completes a specific authentication type. Each authentication type can have a different role and this provision is defined in the AAA profile for Layer 2 authentication types. A VLAN can be configured under the default authentication role. This VLAN is assigned to the user after successful authentication. If a VLAN is not present under the user role, the client gets a default port based VLAN or VLAN derived via user derivation rule, server derivation rule or Vendor Specific Attribute.

### 4. Server Derived Role/VLAN

This role is derived from the attributes sent by the back-end authentication server. For this role to be applied, a set of “server derivation rules” must be defined under the server-group. The server group contains both the server definitions and the rules that are applied to the attributes returned from the list of servers.

### 5. Aruba VSA

Aruba Vendor Specific Attributes (VSA) override any of the above rules and derivations. If the back-end authentication server sends an VSA like Aruba-User-Role or Aruba-User-VLAN, the value of these attributes are sent to the user.

There are no rules that must be configured for this derivation to happen.



---

Roles and VLANs can be derived using VSA, but neither user role nor VLAN derivation is possible using two separate entries of VSA attributes under an IAS profile of the Windows authentication server.

---

## Role Assignment Precedence

The precedence of role assignment in reducing order is as follows:

1. Vendor specific attribute (VSA) derived via Captive Portal authentication
2. Server derived via Captive Portal authentication
3. Default Captive Portal authentication
4. VSA derived via 802.1x authentication
5. Server derived via 802.1x authentication
6. Default 802.1x authentication
  - 802.1X authentication Default Role—Users get this role after successful machine (if it is enabled) and user authentication (username/password or certificates).

- Machine authentication-Default User Role—Users get this role after a successful user authentication (username/password or certificates) and a failed machine authentication.
  - Machine Authentication-Default Machine Role—Users get this role after a successful machine authentication and a failed user authentication.
7. MAC authentication default role
  8. Role derived via UDR matching the MAC address
  9. AAA Profile Initial Role




---

If the “dhcp-option” based UDR or a device-type based UDR is configured to derive a role and if the rule matches, it overrides all the above precedence. The client will get a VLAN configured under the respective UDR. If a VLAN is not configured, then the client will either stay in current VLAN or follow the VLAN assignment precedence. For more details, see [VLAN Assignment Precedence: on page 310](#).

---

### VLAN Assignment Precedence:

The precedence of VLAN assignment in reducing order is given below:




---

No VLAN will be derived if Captive Portal authentication is successful. Any VLAN derived will be ignored after a successful Captive Portal authentication.

---

1. Explicit VSA derived via 802.1x authentication
2. VLAN configured under VSA derived 802.1x authentication role
3. Explicit server derived via 802.1x authentication
4. VLAN configured under server derived 802.1x authentication role
5. VLAN defined under the respective default authentication role
  - 802.1X authentication default role
  - Machine authentication—default user role
  - Machine authentication—default machine role
  - MAC authentication default role
6. Explicit UDR based on MAC address match to derive a VLAN
7. VLAN defined under UDR based on matching MAC address
8. VLAN defined under AAA profile initial role
9. Default VLAN assigned to the port




---

If the dhcp-option based UDR or a device-type based UDR is configured to derive a VLAN and if the rule matches, it overrides all the above precedence.

---

### Current Limitations

- If the MAC authenticated client has received a VLAN via SDR or VSA and going further for successful 802.1x authentication, its VLAN is overwritten and client is assigned a new VLAN (precedence is based on points 1 to 9 above).
- SDR and VSA are not available for machine authentication.

### Layer 2 Entry

Layer 2 user entry is created when the wired station connects to the network or when a Layer 2 “miss trigger” is sent to the control plane for a wired user. The Layer 2 user entry with 0.0.0.0 and MAC address is created both in the control plane and dataplane. The user entry inherits the initial role or the user derived role from the AAA

profile. This user entry controls the Layer 2 traffic the user can send prior to getting an IP address. It also maintains the statistics for a given MAC address, assuming a user can potentially get multiple IP addresses. Location based ACLs are applied using the Layer 2 user entry.

## Layer 3 Entry

After getting an IP address, the user entry shows up in the user table as “Layer 3 Entry.”

## User Roles

User roles are a key component for role based policy enforcement.

Fully authenticated Layer 2 roles are assigned when a user has successfully completed all configured Layer 2 authentication methods.

The following authentication command is available in all roles:

```
reauthentication-interval <minutes>
 policer-profile <policer profile name>
 qos-profile <qos profile name>
 voip-profile <voip profile name>
```



---

For more detail, see [Roles and Policies on page 325](#).

---

## Authentication Roles

After authentication, the station or user is given a role that defines the behavior of the user. The role can be defined with the following:

- Access List
- VLAN
- Reauthentication Interval

## Access List

This ACL is applied to the user. Three types of ACLs can be applied:

- Ether ACL  
These access rules can be applied to specific Ether types.
- MAC ACL  
These access rules are applied based on MAC address
- Layer 2 - 4  
These access rules are applied based on Layer 3 and Layer 4 information such as IP-Address, protocol, and port.

## VLAN

The VLAN attribute is set on initial roles or Layer 2 authenticated roles, so that the user ends on a new VLAN.

- Reauthentication Interval

This is defined in terms of minutes and is sometimes used to re-trigger authentication after a specified interval.

## User Derivation Rules

This section contains the following sections:

- [Configuring User Derivation Rules on page 312](#)
- [Displaying User Derivation Rules on page 312](#)




---

DHCP Signature (DHCP-Option) is supported in addition to MAC Address-based UDRs.

---

## Configuring User Derivation Rules

To configure user derivation rules, use the following command:

```
aaa derivation-rules user student
 set role condition macaddr equals "00:25:90:0a:95:d2" set-value student-role
 set vlan condition macaddr equals "00:25:90:0a:95:d2" set-value 202
```

## Displaying User Derivation Rules

To display user derivation rules, use the following command:

```
(host)(config) #show aaa derivation-rules user udr_rule1
User Rule Table

Pr Attribute Operation Operand Action Value Total New Desc
-- -
1 macaddr equals 00:aa:bb:cc:dd:e1 set role authentic 0 0
2 macaddr equals 00:aa:bb:cc:dd:e2 set vlan 3912 0 0
Rule Entries: 2
```

## Configuring Authentication End to End

This section describes how to configure authentication end-to-end using the command-line interface. This section contains the following sections:

- [Configuring Authentication Server on page 312](#)
- [Configuring Management Authentication on page 314](#)
- [Configuring AAA Timers on page 314](#)

## Configuring Authentication Server

Prior to configuring authentication, an authentication server must be defined. The Mobility Access Switch supports the following authentication server types: RADIUS, TACACS+, LDAP, and the Internal Database.




---

TACACS+ is not supported for 802.1X authentication.

---

## Configuring a RADIUS Authentication Server

To configure a RADIUS authentication server, use the following commands:

```
(host)(config) #aaa authentication-server radius RADIUS1
(host)(RADIUS Server "RADIUS1") #host 10.20.20.200
(host)(RADIUS Server "RADIUS1") #key <shared-secret>
(host)(RADIUS Server "RADIUS1") #exit
```

## Displaying the Authentication Server Configuration

To display the authentication server configuration for verification, use the following command:

```
(host) #show aaa authentication-server all
Auth Server Table

Name Type IP addr AuthPort AcctPort Status Requests

Internal Local 172.16.0.254 n/a n/a Enabled 0
RADIUS1 Radius 10.20.20.200 1812 1813 Enabled 0
```

## Configuring an Authentication Server Group



---

Authentication servers are referenced in server groups.

---

To configure the server in a server group, use the following commands:

```
(host) (config) #aaa server-group AUTH_SERVER
(host) (Server Group "AUTH_SERVER") #auth-server RADIUS1
(host) (Server Group "AUTH_SERVER") #exit
```

### Configuring a Server for Fail-Over with the Internal Database

You can define multiple authentication servers for fail-over purposes. When you define multiple authentication servers, reference the servers in a single server-group.

```
(host) (config) #aaa server-group AUTH_SERVER
(host) (Server Group "AUTH_SERVER") #auth-server Internal
(host) (Server Group "AUTH_SERVER") #auth-server RADIUS2
```

### Configuring Internal Server Under a Server-Group

To configure the internal database server, use the Internal keyword for the authentication-server, and the following commands:

```
(host) (config) #aaa server-group INTERNAL_SERVER
(host) (Server Group "INTERNAL_SERVER") #auth-server Internal
(host) (Server Group "INTERNAL_SERVER") #exit
```

### Configuring a User Account with the Internal Database

To use the Internal Server, create a user account with the following command:

```
(host) #local-userdb add username <username> password <password> role dot1x-authenticated
```

### Displaying the Internal Database

To display the user database, use the following commands:

```
(host) # show local-userdb
```

```
User Summary
```

```

```

| Name  | Password | Role  | E-Mail | Enabled | Expiry | Status | Sponsor-Name | Remote-IP | Grantor-Name |
|-------|----------|-------|--------|---------|--------|--------|--------------|-----------|--------------|
| USER1 | *****    | guest |        | Yes     |        | Active |              | 0.0.0.0   | admin        |

```
User Entries: 1
```

### Maintaining Existing Accounts with the Internal Database

To add an existing user account, use the following command:

```
(host) #local-userdb add username labuser1 password abcdef
```

To modify an existing user account, use the following command:

```
(host) #local-userdb modify username USER1 role <ROLE>
```

To delete an existing user account, use the following command:

```
(host) #local-userdb del username USER1
```

To delete all existing user accounts, use the following command:

```
(host) #local-userdb del-all
```

## Configuring Management Authentication

Similar to user/port authentication, management user can also be authenticated by using the AAA profile, such as using central authentication server for authenticating access to the network devices.

Authentication server can be the same server used for user authentication, or a separate server can be created for management authentication purpose. Similar to AAA authentication server configuration, the server needs to be defined first, then referenced on the server-group:

```
(host) (config) #aaa authentication-server tacacs TACACS1
(host) (TACACS Server "TACACS1") #host 10.20.20.202
(host) (TACACS Server "TACACS1") #key <shared-secret>
(host) (TACACS Server "TACACS1") #exit

(host) (config) #aaa server-group MGMT_AUTH_SERVER
(host) (Server Group "MGMT_AUTH_SERVER") #auth-server TACACS1
(host) (Server Group "MGMT_AUTH_SERVER") #exit
```

Once the server-group is defined (or used existing server-group), the AAA profile for management can be configured:

```
(host) (config) #aaa authentication mgmt
(host) (Management Authentication Profile) #enable
(host) (Management Authentication Profile) #server-group MGMT_AUTH_SERVER
(host) (Management Authentication Profile) #exit
```

## Configuring AAA Timers

AAA timers such as dead-time, timeout for idle, as well as logon-lifetime can be defined at global level:



---

Logon-lifetime is not applicable for 802.1x and MAC authentication as the user entry is deleted and the session is terminated when the idle-timeout hits.

---

```
(host) (config) #aaa timers dead-time 10
(host) (config) #aaa timers idle-timeout 300
(host) (config) #aaa timers logon-lifetime 5
(host) (config) #aaa timers stats-timeout 300 seconds
```



---

If server dead time is set to 0, the servers will not be marked as **out-of-service**.

---

Timers can be viewed using the following CLI command:

```
(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
```

The idle-timeout is set to 5 minutes, which is the default.

## RADIUS Fail-Open

When wired users try to access a network where AAA servers are unreachable, they will be unable to authenticate and will continue to stay in the configured initial role. As a result, a user may effectively be blocked off the network due to a restrictive initial-role. To overcome this problem, ArubaOS provides support for RADIUS Fail-open. This feature enables the IT administrators to provide an alternate user-role (unreachable-role) to the users for network connectivity during a AAA server outage. When AAA servers are unreachable, the RADIUS Fail-open feature assigns the unreachable-role to the users trying to authenticate. The users will stay in the unreachable-role until at least one of the AAA servers is back in service.

## Enabling RADIUS Fail-Open

RADIUS Fail-open is an optional configuration. It is enabled only if:

- the unreachable-role is configured under the AAA profile, and
- the AAA server dead time expiry feature is enabled (i.e. the dead time value is set above 0)

## Configuring Unreachable Role

Use the following command to configure the unreachable-role:

```
(host) (config) #aaa profile profile1
(host) (AAA Profile "profile1") # unreachable-role <user-role>
```

The following is a sample configuration:

```
(host) (config) #aaa profile profile1
(host) (AAA Profile "profile1") # unreachable-role new-role
```

## Verifying Unreachable Role Configuration

You can use the following commands to verify the unreachable-role configuration:

```
(host) #show aaa profile profile1
AAA Profile "profile1"

Parameter Value

Initial role logon
MAC Authentication Profile N/A
MAC Authentication Default Role guest
MAC Authentication Server Group N/A
802.1X Authentication Profile dot1x-auth-profile
802.1X Authentication Default Role default-role
802.1X Authentication Server Group server-group
Download Role from ClearPass Enabled
L2 Authentication Fail Through Disabled
RADIUS Accounting Server Group N/A
RADIUS Interim Accounting Disabled
XML API server N/A
AAA unreachable role new-role
RFC 3576 server N/A
User derivation rules N/A
SIP authentication role N/A
Enforce DHCP Disabled
Authentication Failure Blacklist Time 3600 sec
(host) # show running-config
...
...
...
aaa profile "profile1"
authentication-dot1x "dot1x-auth-profile"
dot1x-default-role "default-role"
dot1x-server-group "server-group"
unreachable-role "new-role"
...
...
...
```

## Key Points to Remember

- A client remains in the initial role until all the AAA servers in the server group are processed. The unreachable-role is assigned to a user only when:

- no intermediate role (such as UDR, MAC auth, and 802.1x machine-auth-machine-role) has been derived i.e. the user is still in initial role, and
- the last AAA server in the AAA server group has been processed, and
- if one or more AAA servers have timed out and the rest have failed the authentication, or if all the servers have timed out.




---

A role derived after authenticating UDR or MAC auth will have more privileges than the initial or unreachable-role.

---

- A client will transition from the switch profile VLAN to AAA unreachable-role-based-VLAN only if:
  - AAA unreachable-role is assigned to that MAC, and
  - no intermediate VLAN has been derived.




---

AAA unreachable-role-based-VLAN (high priority) takes precedence over the switching profile's VLAN (low priority).

---

- Clients that attempted AAA authentication and got timed out are added to the mac-in-unreachable-list table. This list also includes the clients that have derived an intermediate role (such as UDR and MAC auth) but failed AAA authentication due to time-out.

You can use the following command to view the list of clients in the unreachable-role:

```
(host) #show aaa mac-in-unreachable-list
Station Entry

MAC AAA profile Name AAA server Group Port

00:60:6e:00:f1:7d dot1x mac gigabitethernet0/0/7
Entries: 1
```

- When the dead timer has expired (default 10 minutes), the Mobility Access Switch sends a dummy authentication request to the AAA server (username: DummyArubaUser). When the AAA server comes back in service, all the clients corresponding to that server group are cleared from the mac-in-unreachable-list table. The clients then re-attempt authentication.
- When a client is removed from the mac-in-unreachable-list table, the port to which it is connected is administratively disabled (shutdown) and then re-enabled (in 5 seconds). This is to ensure that the client initiates the DHCP process again when it re-attempts authentication. The port is administratively disabled and then re-enabled in the following scenarios:
  - When all the clients on the same port are removed from the mac-in-unreachable-list table, if there are more than one client on the same port.
  - When aaa user delete command is executed to delete a client entry that is in the mac-in-unreachable-list table.




---

The port does not get shut when the client entry that is in the unreachable-role ages out due to AAA timer expiry..

---

- If the AAA server dead time expiry is set to 0, the clients that are in the unreachable-role are rolled back to initial role and are removed from the mac-in-unreachable-list table. No clients will be assigned the unreachable-role as RADIUS Fail-open gets disabled.
- If a system switch over happens (the secondary switch becomes the new primary and the primary switch becomes the new secondary) in the network while RADIUS Fail-Open is active, the following process takes place:

- The servers that were marked out of service in the old primary are marked as in-service in the new primary.
- The user table entries for the clients that were in mac-in-unreachable-list table are deleted and their respective interfaces are administratively disabled and then re-enabled. These clients re-attempt authentication and derive a role based on the authentication outcome.
- If the servers are still out of service during the authentication re-attempt, they will be marked as out of service.
- When more than one server is configured under a server group and when server-group fail-through option is disabled, then the unreachable-role is assigned to the user only if:
  - all the servers are out of service, or
  - when all the servers except the last one in the server group are out of service and the last one fails authentication.

## Limitations

- RADIUS Fail-Open is not supported when re-authentication timer is enabled.
- RADIUS Fail-Open is not supported when EAP-Termination is enabled under 802.1x authentication profile.
- When the unreachable-role is assigned to a captive portal user, the user may be misled to the welcome screen indicating that the authentication has succeeded. It is recommended to configure the Captive Portal Authentication Profile under the unreachable-role to avoid such misleading scenarios.

## Authentication Survivability

The authentication survivability (or the auth survivability) feature supports 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.

Starting from ArubaOS 7.4.1, Mobility Access Switch supports the following authentication methods with Authentication Survivability:

- 802.1X clients with Termination disabled/enabled: EAP-TLS with CPPM as RADIUS server.
- MAC-Based Authentication clients: PAP method. CPPM server is not mandatory in this case.




---

ArubaOS 7.4.1 supports only EAP-TLS standard for Authentication Survivability.

---

When the authentication survivability feature is enabled, the following authentication process is used:

1. The wired client connects to a Mobility Access Switch and authenticates to the external authentication server. The external authentication server can be CPPM.
2. Upon successful authentication, the Mobility Access Switch caches the authentication credentials of the connected users for the configured duration. The cache expiry duration for authentication survivability can be set within the range of 1–72 hours, with 24 hours being the default cache timeout duration.
3. If the client roams or tries to reconnect to the Mobility Access Switch and the remote link fails due to the unavailability of the authentication server, the Mobility Access Switch uses the cached credentials in the internal authentication server to authenticate the user. However, if the user tries to reconnect after the cache expiry, the authentication fails.
4. When the authentication server is available and if the client tries to reconnect, the Mobility Access Switch detects the availability of server and allows the client to authenticate to the server. Upon successful authentication, the Mobility Access Switch cache details are refreshed.

The following attributes are supported from CPPM server along with the caching credentials:

- ARUBA\_ROLE
- ARUBA\_VLAN
- ARUBA\_CPPM\_ROLE (Downloadable Role)
- ARUBA\_ADMIN\_ROLE

## Important Points to Remember

- Any client connected through CPPM and authenticated through Mobility Access Switch remains authenticated with the Mobility Access Switch even if the client is removed from the CPPM server during the CPPM downtime.
- For EAP-TLS authentication, ensure that CPPM 6.5.1/CPPM 6.5.2 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.
- When the role download fails for a user after successful authentication from CPPM, the user will remain in initial or a previously known role even though the cache table cached the name of the role that failed to download, The role is not applied to the user when the CPPM server is down. The clients must do a fresh authentication with the cached credentials.
- When the CPPM server is unreachable, the user gets authenticated with the cached credentials only if all the following entries match the cached entries:
  - mac address
  - username
  - auth-type (EAP-TLS or PAP)
- When a user is authenticated through the CPPM server, the user credentials are cached. When the server goes down, the user gets authenticated through cached entry. Even after the server is available and reachable, depending on the configured dead time value (aaa timers dead-time), the user gets authenticated only through the cached entry (until the dead timer) and then gets authenticated through the server. If it has to take over instantly, then configure **aaa timers dead-time** to 0. The default value for this parameter is 10 minutes.

## Configuring Authentication Survivability

You can enable authentication survivability on the Mobility Access Switch using the following CLI command:

```
(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>
```

Specify a value in hours for Cache timeout. The allowed range is 1–72 hours and the default value is 24 hours.

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> Name of the Server Certificate
```

## Sample Configuration

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

```
(host) (config) #aaa auth-survivability cache-lifetime 25
```

## Verifying Authentication Survivability Configuration

Execute the following command to verify the Authentication Survivability configuration on the Mobility Access Switch:

```
(host) #show aaa auth-survivability
Auth-Survivability: Enabled (Running)
Survival-Server Server-Cert: server-crt
Survival-Server Cache lifetime: 72 hours
```

## Viewing Survived Authentication Entries

To view the cached entries on Mobility Access Switch, use the following command:

```
(host) #show aaa auth-survivability-cache
Auth-Survivability Cached Data

MAC User Name Authenticated By Authenticated On

04:7d:7b:1e:d1:bf user1 cppm 2014-07-21 17:13
aa:bb:cc:00:00:01 guest1 cppm 2014-07-21 18:15
aa:7b:cc:00:1f:09 cp_guest cppm 2014-07-21 19:20

Attributes AuthType

CPPM Role(new_profile-3120-12) EAP-TLS
CPPM Role(guest_profile-25) PAP
CPPM Role(cp_guest_profile-15) PAP
```

## Clearing Cache Entries

To clear the cache entries manually, use the following commands:

```
(host) (config) #clear aaa auth-survivability-cache mac <mac address of client>
(host) (config) #clear aaa auth-survivability-cache all
```

## Limitations

- 802.1X reauthentication timer value should be less than the dead interval time.

## Preauth Role Assignment

Starting from ArubaOS 7.3.1 Mobility Access Switch introduces a new role, **preauth** in the system. 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.

By default, this feature is disabled. You can use the CLI to configure **preauth** role on the Mobility Access Switch. By default, no ACL is configured as part of the **preauth** role and hence, it will deny all L2/L3 traffic from the device except the control packets. You cannot delete this role from the system. However, you may configure ACLs in it to allow specific traffic.



---

It is recommended not to configure *allow dhcp* ACE in the **preauth** role to avoid obtaining an intermediate IP address before passing through all the configured authentication methods.

---

## Configuring Pre-authentication Role

You can enable the **preauth** role on the Mobility Access Switch in the **aaa profile** command using CLI:

```
(host) (config) # aaa profile <profile-name>
```

```
(host) (AAA Profile "<profile-name>") # preauth
```

## Sample Configuration

```
(host) (config) # aaa profile Profile1
(host) (AAA Profile "Profile1") # preauth
```

## Verifying Pre-authentication Role Configuration

You can verify the **preauth** role configuration using the following show command:

```
(host) (AAA Profile "Profile1") #show aaa profile Profile1
```

```
(host) #show aaa profile Profile1
AAA Profile "Profile1"

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
Preauth Enabled
Enforce DHCP Disabled
Authentication Failure Blacklist Time 3600 sec
```

## Viewing Pre-authentication Role Assignment

You can use the **show station table** command to view the role assignment for the clients. The **Role** column in the output displays **preauth** until the clients derive the final role after all the configured authentication methods are complete. After the clients pass through all the configured authentication methods, the **Role** column in the output displays the final role derived by the clients.

```
(host) #show station-table
```

```
Station Entry

MAC Name Role Age (d:h:m) Auth Interface Profile

00:60:6e:00:f1:7d 00606e00f17d preauth 00:00:00 No 0/0/8 Profile1
```

```
Station Entries: 1
```

## Limitations

The DHCP discovery time interval for a device connected to a network may increase if the authentication time increases. The authentication time may increase due to one of the following reasons:

- Large number of servers in a server group.
- User delay in providing 802.1x credentials.

- Increased value of retransmit and time out intervals configured for the servers.

## Recommendations

To improve the DHCP discovery time for devices that do not support 802.1x authentication, it is recommended to adjust the following values in the **aaa authentication dot1x profile**:

- Set the **reauth-max** value to 1.
- Set the **timer idrequest\_period** value to 10 for preboot execution environment (PXE) clients and 20 or lower for non-PXE clients.




---

However, it is recommended to set these values in the dot1x profile based on your network settings.

---

## Deny DHCP Role for 802.1x Authentication

Deny DHCP is an enhancement added to the 802.1x profile to ensure that the 802.1x clients obtain the correct IP addresses in the correct VLANs/subnets by denying DHCP requests from the clients till the dot1x authentication is complete. If this feature is enabled, the Mobility Access Switch enforces the **denydhcp** role to the 802.1x clients till the authentication is complete. In the meantime if there are any DHCP requests from the client, the Mobility Access Switch drops the requests until the client derives the final role. After the 802.1x authentication is complete, the client derives the final role and overwrites the **denydhcp** role. After the final VLAN is assigned, if the final role of the client allows DHCP, the client will get an IP address in the correct subnet. By default, this option is disabled.

### Configuring Deny DHCP Role

You can configure the **denydhcp** role in the **aaa authentication dot1x** profile using the following commands:

```
(host) (config) #aaa authentication dot1x <profile-name>
(host) (802.1X Authentication Profile "<profile-name>") #deny-dhcp
```

### Sample Configuration

```
(host) (config) #aaa authentication dot1x Profile1
(host) (802.1X Authentication Profile "Profile1") #deny-dhcp
```

### Verifying Deny DHCP Configuration

Use the following command to verify if dhcpdeny role is enabled on a dot1x profile:

```
(host) #show aaa authentication dot1x Profile1
802.1X Authentication Profile "Profile1"

Parameter Value

...
Deny DHCP Enabled
...
```

## Delay EAP Success for dot1x Authentication

The new command **delay-eap-success** under the 802.1X profile helps the clients to obtain an IP address in the correct VLAN by introducing a delay of one second in sending the EAP Success message to the client after it completes the 802.1X authentication. This option is disabled by default.

## Configuring Delay EAP Success

Execute the following command under the **aaa authentication dot1x** profile to delay the EAP Success message to the clients by one second:

```
(host) (config) #aaa authentication dot1x Profile1
(host) (802.1X Authentication Profile "Profile1") #delay-eap-success
```

## Verifying Delay EAP Success Configuration

Use the following command to verify if **delay-eap-success** is enabled on the dot1x profile:

```
(host) #show aaa authentication dot1x Profile1
802.1X Authentication Profile "Profile1"

Parameter Value

...
Delay EAP Success Enabled
...

```

## Port Bounce

The Port Bounce feature is used to force a client to reinitiate a DHCP request when there is a VLAN change. It is also used to assign appropriate VLAN after health check and profiling.

Starting from ArubaOS 7.4.0.3, Mobility Access Switch provides support for the port bounce feature which enables a client to re-initiate a DHCP request when there is a VLAN change. When a RADIUS server such as CPPM sends Disconnect-Request with a Vendor-Specific Attribute (VSA 40) to the Mobility Access Switch to trigger an interface shutdown for a specified period, this feature allows the device to reinitiate a DHCP request for obtaining an IP address in the changed subnet.

The Disconnect-Request must include the following information:

- Calling Station-Id—MAC address of the user
- VSA—40
- Integer—0-60

VSA 40 represents Aruba-Port-Bounce-Host. The integer value indicates the time in seconds for which the Mobility Access Switch must shut the interface down. If the integer value received is 0 or a number greater than 60, the Mobility Access Switch does not shut the interface down.



---

During a port bounce, the client connected to the interface is removed from the user table and is added back after the port is up.

---

## Prerequisites

The following are the prerequisites for the Port Bounce feature to work:

- RADIUS server must have Aruba Port Bounce available in the Dictionary
- AAA profile with any type of authentication configured on non-trusted port

## Configuration

The following set of configurations is required for the Port Bounce feature to work:

### Creating RADIUS Authentication Server Profile

```
(host) (config) #aaa authentication-server radius <servername>
(host) (RADIUS Server "<servername>") #host <host name>
```

```
(host) (RADIUS Server "<servername>") #c ppm username <username> password <password>
(host) (RADIUS Server "<servername>") #key <passkey>
```

Key should be the same as that on the RADIUS server where this device is added)

```
(host) (RADIUS Server "<servername>") #enable
(host) (RADIUS Server "<servername>") #exit
```

## Creating RADIUS Authentication Server Profile (Global Config)

```
(host) (config) #aaa rfc-3576-server <server-ip-addr>
(host) (RFC 3576 Server "<server-ip-addr>") #key <passkey>
(host) (RFC 3576 Server "<server-ip-addr>") #exit
```

## Configuring RFC Server with AAA Profile

```
(host) (config) #aaa profile <mac-profile-name>
(host) (AAA Profile "<mac-profile-name>") #mac-server-group <group>
(host) (AAA Profile "<mac-profile-name>") #authentication-mac <auth-profile-name>
(host) (AAA Profile "<mac-profile-name>") #rfc-3576-server "<server-ip-addr>"
```

## Configuring Interface with AAA Profile

```
(host) (config) #interface gigabitethernet <slot/module/port>
(host) (gigabitethernet "<slot/module/port>") #no trusted port
(host) (gigabitethernet "<slot/module/port>") #switching-profile <switching-profile-name>
(host) (gigabitethernet "<slot/module/port>") #aaa-profile <aaa-profile-name>
(host) (gigabitethernet "<slot/module/port>") #no shutdown
```



---

Enable logging level debugging for network, security, and DHCP process.

---

## Verification

Execute the following command to view the security logs during and after a port bounce:

```
(host) #show log security all | include Port
```

The following sample shows the output after a port bounce:

```
Press 'q' to abort.
Apr 29 06:06:19 :124004: <DEBUG> |authmgr| Port Bounce Link Down flag set. Port =
gigabitethernet0/0/6.
Apr 29 06:06:19 :124004: <DEBUG> |authmgr| LIF_OPER_STATE_UP. Port = gigabitethernet0/0/6.
Apr 29 06:06:20 :124004: <DEBUG> |authmgr| Port will come up within 60 secs. link = 0x106ea2ac.
Apr 29 06:07:20 :124004: <DEBUG> |authmgr| Port Bounce Link DOWN flag reset. Port =
gigabitethernet0/0/6.
```

## Sample Configuration

To configure an interface with AAA profile so that the Port Bounce feature can take effect, execute the following commands:

```
(host) (config) #interface gigabitethernet 1/0/9
(host) (gigabitethernet "1/0/9") #no trusted port
(host) (gigabitethernet "1/0/9") #switching-profile vlan100
(host) (gigabitethernet "1/0/9") #aaa-profile mac_profile
(host) (gigabitethernet "1/0/9") #no shutdown
```



Every client is associated with a user role, which determines the client's network privileges and how often it must re-authenticate. A *policy* is a set of rules that applies to traffic that passes through the ArubaOS Mobility Access Switch. You specify one or more policies for a user role. Finally, you can assign a user role to clients before or after they authenticate to the system.

This chapter describes assigning and creating roles and policies using the ArubaOS command line. This chapter describes the following topics:

- [Firewall Policies on page 325](#)
- [User Roles on page 331](#)
- [User Role Assignments on page 332](#)
- [Deny Inter-User Traffic on page 334](#)

## Firewall Policies

A firewall policy identifies specific characteristics about a data packet passing through the Mobility Access Switch and takes some action based on that identification. In a Mobility Access Switch, that action can be a firewall-type action such as permitting or denying the packet, an administrative action such as logging the packet, or a quality of service (QoS) action such as setting 802.1p bits or placing the packet into a priority queue. You can apply firewall policies to user roles to give differential treatment to different users on the same network to apply the same policy to all traffic through the port.

Firewall policies are categorized as follows on the Mobility Access Switch:

- Stateful
- Stateless




---

Stateful and stateless firewall policies are mutually exclusive and cannot co-exist on the same user-role.

---

The following table compares the stateful and stateless firewall policies.

**Table 35:** *Comparison of Stateful and Stateless Firewall Policies*

| Stateful Firewall Policies                                                                                                                                                                                                                             | Stateless Firewall Policies                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Stateful—Recognize flows in a network and keep track of the state of sessions. For example, if a firewall policy permits telnet traffic from a client, the policy also recognizes that inbound traffic associated with that session should be allowed. | Stateless—Statically evaluate the packet contents. The traffic in the reverse direction will be allowed unconditionally.  |
| Bidirectional— Keep track of data connections traveling into or out of the network. ACLs are applied to either an inbound traffic or an outbound traffic.                                                                                              | Uni-directional—Keep track of data connections traveling into or out of the network. ACLs are applied to inbound traffic. |
| Dynamic— The address information in the policy rules can change as the policies are applied to the users. For example, the alias user in a policy automatically applies to the IP address assigned to a particular user.                               | Static— The address information in the policy rules is static                                                             |

## Stateful Firewall Policy (Session ACL)

A session ACL is a stateful firewall which keeps track of the state of network connections such as TCP streams and UDP communication that hit the firewall. The firewall distinguishes the legitimate packets for different types of connections and allows only those packets that match a known active connection.

Mobility Access Switch provides supports for stateful firewall using the session ACLs which can be applied on user-roles. Mobility Access Switch enforces the stateful firewall policy exclusively on the traffic routed through a firewall-enabled VLAN interface (up-link VLAN) and forwards the internal traffic in a stateless manner.

### Configuring a Stateful Firewall Policy

This section describes how to configure a stateful firewall policy using session ACLs. To configure a stateful firewall policy, you must

1. Create a session ACL and apply it to a user-role.
2. Enable firewall on the up-link VLAN interface.



---

If you Modify a session ACL in the middle of an ongoing session, the policy is not enforced on the session until it is terminated.

---

### Creating a Session ACL

Execute the following command to create a session ACL:

```
(host) (config) #ip access-list session <acl-name>
(host) (config-sess-<acl-name>) # <source> <dest> <service> <action> [<extended action>]
```



---

To choose source NAT as an extended action under the redirect option, ensure that it is the last option configured in the access control entry (ACE) .

---

Execute the following command to apply the session ACL to a user-role:

```
(host) (config) #user-role <user>
(host) (config-role) #access-list session <acl-name>
```

### Enabling Firewall on an Up-link VLAN Interface

Execute the following command to enable firewall on a specific VLAN.

```
(host) (config) #interface vlan <id>
(host) (vlan "id") #session-processing
```



---

You can enable **session-processing** on multiple VLAN interfaces.

---

### Sample Configuration

The following example creates a policy, web-only that allows web (HTTP and HTTPS) access.

```
(host) (config) #ip access-list session web-only
 any any svc-http permit
 any any svc-https permit
```

The following command applies the session ACL, web-only to the user-role user2

```
(host) (config) #user-role user2
(host) (config-role) #access-list session web-only
```

The following example enables firewall on VLAN 5:

```
(host) (config) #interface vlan 5
(host) (vlan "5") #session-processing
```

## Verifying the Configuration

Execute the following command to verify the session ACL configuration:

```
(host) #show ip access-list web-only
ip access-list session web-only
web-only

Priority Source Destination Service Action TimeRange Log Expired
----- -
1 any any svc-http permit
2 any any svc-https permit
Queue TOS 8021P Blacklist Mirror DisScan ClassifyMedia IPv4/6
----- -
Low
Low
```



You can use the command **show ip access-list hardware** to view the ACL equivalent .of the session ACL used to forward the internal traffic.

Execute the following command to verify if the session ACL is applied to the user-role, user2:

```
(host) #show rights user2

Derived Role = 'user2'
Periodic reauthentication: Disabled
ACL Number = 54/0
Max Sessions = 65535

access-list List

Position Name Type Location
----- -
1 web-only session
web-only

Priority Source Destination Service Action TimeRange Log Expired
----- -
1 any any svc-http permit
2 any any svc-https permit
Queue TOS 8021P Blacklist Mirror DisScan ClassifyMedia IPv4/6
----- -
Low
Low
Expired Policies (due to time constraints) = 0
```

Execute the following command to verify if the specified VLAN interface is firewall-enabled:

```
(host) (config) #show interface-config vlan 5
vlan "5"

Parameter Value
----- -
Interface OSPF profile N/A
Interface PIM profile N/A
Interface IGMP profile N/A
Directed Broadcast Enabled Disabled
Interface shutdown Disabled
session-processing Enabled

mtu 1500
```

|                         |                       |
|-------------------------|-----------------------|
| IP Address              | 5.5.5.2/255.255.255.0 |
| IP NAT Inside           | Disabled              |
| IPv6 Address            | N/A                   |
| IPv6 link local Address | N/A                   |
| DHCP client             | Disabled              |
| DHCP relay profile      | N/A                   |
| Ingress ACL             | pbr_acl               |
| Interface description   | N/A                   |

## Understanding Application-Level Gateways (ALG) Support on Mobility Access Switch

An application-level gateway (ALG) is a firewall proxy that provides security to networks by filtering the incoming application data such as File Transfer Protocol (FTP) and Real Time Streaming Protocol (RTSP) based on respective protocol specifications.

ArubaOS provides support for the following types of ALGs on the Mobility Access Switch:

- **Data ALGs:** FTP, RTSP, DNS, and DHCP.
- **Voice ALGs:** SIP and SCCP (Skinny)

The following are the limitations on the ALG support for Mobility Access Switch:

- No support for SIP initiated voice calls that use an IP other than the one used for the call initiation
- No support for VoIP over NAT
- No Support for RTSP over NAT
- No support for Multicast
- Maximum pause time limit of 300 seconds for streaming in RTSP ALG

You can configure data ALGs on the Mobility Access Switch for services running on both standard and non-standard ports.




---

Aruba recommends that the VoIP ALGs are configured only for services running on standard ports.

---

By default, all the ALGs are enabled on the Mobility Access Switch. You can enable or disable the VoIP ALGs using the **firewall** command.




---

You cannot disable the Data ALGs on the Mobility Access Switch.

---

### Configuring Application-Level Gateways (ALG)

You can configure ALG for a service by creating an alias for the network service using the **netservice** command and applying it to a session ACL.




---

ALGs are functional only if Stateful firewall is enabled.

---

### Sample ALG Configuration for FTP Running on a Non-Standard Port

For configuring ALGs on non-standard ports, create an alias and specify the port(s) on which the service is running and apply it for ip access-list.

```
(host) (config) #netservice ftp1 tcp 10000 ALG ftp
(host) (config) #ip access-list session ftp_session
(host) (config-sess-ftp_session) #host 20.20.20.20 any ftp1 permit
```




---

ftp1 is the alias defined for FTP service running on a non-standard port (10000).

---

## Sample ALG Configuration for FTP Running on Standard Port

```
(host) (config) #netsservice ftp2 tcp 21 ALG ftp
(host) (config) #ip access-list session ftp_session
(host) (config-sess-ftp_session) #host 20.20.20.20 any ftp2 permit
```

Enable **session-processing** on the up-link port to enable ALG processing. The following sample enables **session-processing** on VLAN 100:

```
(host) (config) #interface vlan 100
(host) (vlan "5") #session-processing
```

## Enabling/Disabling VoIP ALG

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

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

You can verify the firewall configuration using the following command:

```
(host) #show firewall
Global firewall policies

Policy Action Rate Port

...
Stateful SIP Processing Disabled
Stateful SCCP Processing Enabled
...
```

## Stateless Firewall Policy (Stateless ACL)

Stateless ACL does not store information on the connection state. It filters the packets based only on the information contained in the packet such as the source and destination address of the packet, its protocol, and the port number for TCP and UDP traffic.

Stateless ACLs are applicable to the network and physical layers, and sometimes the transport layer to find out the source and destination port numbers. When a packet originates from the sender and filters through a firewall, the device checks for matches to any of the ACL rules that are configured in the firewall and drops or rejects the packet accordingly. When the packet passes through the firewall, it filters the packet on a protocol/port number basis. For example, if a rule in the firewall exists to block telnet access, then the firewall will block the TCP protocol for port number 23.

## Creating a Stateless Firewall Policy

This section describes how to configure the rules that constitute a stateless firewall policy (stateless ACL). A stateless ACL can then be applied to a user role (until the policy is applied to a user role, it does not have any effect).

The following command is used to create a stateless ACL:

```
(host) (config) #ip access-list stateless <acl-name>
(host) (config-sess-<acl-name>) # <source> <dest> <service> <action> [<extended action>]
```

The following command is used to apply the stateless ACL to a user-role:

```
(host) (config) #user-role <user>
(host) (config-role) #access-list stateless <acl-name>
```

## Sample Configuration

The following example creates a policy, STATELESS:

```
(host) (config) #ip access-list stateless STATELESS
(host) (config-stateless-STATELESS) #network 10.100.100.0 255.255.255.0 any tcp 8888 deny log
(host) (config-stateless-STATELESS) #any host 1.100.100.200 any deny log
(host) (config-stateless-STATELESS) #any any any permit
```

The following command applies the stateless ACL, STATELESS to the user-role user1:

```
(host) (config) #user-role user1
(host) (config-role) #access-list session STATELESS
```

## Verifying the Configuration

Execute the following command to verify the stateless ACL configuration:

```
(host) #show ip access-list STATELESS
ip access-list stateless STATELESS
STATELESS

Priority Source Destination Service Action
----- -
1 10.100.100.0 255.255.255.0 any tcp 8888 deny
2 any 1.100.100.200 any deny
3 any any any permit

TimeRange Log Expired QoS Policer Blacklist Mirror IPv4 Nexthop
----- -
 Yes Yes Yes Yes Yes Yes Yes Yes
 Yes Yes Yes Yes Yes Yes Yes Yes
 Yes Yes Yes Yes Yes Yes Yes Yes
```

Execute the following command to verify if the stateless ACL is applied to the user-role, user1:

```
(host) #show rights user1
Derived Role = 'user1'
Periodic reauthentication: Disabled
ACL Number = 55/0/56
access-list List

Position Name Type Location
----- -
1 STATELESS stateless
STATELESS

Priority Source Destination Service Action
----- -
1 10.100.100.0 255.255.255.0 any tcp 8888 deny
2 any 1.100.100.200 any deny
3 any any any permit

TimeRange Log Expired QoS Policer Blacklist Mirror IPv4 Nexthop
----- -
 Yes Yes Yes Yes Yes Yes Yes Yes
 Yes Yes Yes Yes Yes Yes Yes Yes
 Yes Yes Yes Yes Yes Yes Yes Yes

Expired Policies (due to time constraints) = 0
```

## Global Firewall Policies

You can set the following optional firewall parameters on the Mobility Access Switch using the **firewall** command in the CLI:

- **disable-stateful-sccp-processing**—Disables stateful SCCP processing. Default option is enabled.
- **disable-stateful-sip-processing**—Disables stateful SIP processing. Default option is enabled.
- **drop-ip-fragments**—Drops all IP fragments.
- **enable-per-packet-logging**—Enables per-packet logging. Default is per-session logging.
- **enforce-tcp-handshake**—Enforces TCP handshake before allowing data.
- **enforce-tcp-sequence**—Enforces TCP sequence numbers for all packets.

- **log-icmp-error**—Logs all received ICMP errors.
- **prohibit-arp-spoofing**—Prohibits ARP spoofing.
- **prohibit-ip-spoofing**—Prohibits IP spoofing.
- **prohibit-rst-replay**—Prohibits TCP RST replay attack.
- **session-idle-timeout**—Sets idle or closed session timeout in seconds.
- **session-mirror-destination**—Configures destination for a mirrored session.
- **session-mirror-ipsec**—Configures session mirror of all frames that are processed by IPSec.
- **session-voip-timeout**—Sets VoIP session idle timeout in seconds.

## Creating a Network Service Alias

A network service alias defines a TCP, UDP or IP protocol and a list or range of ports supported by that service. When you create a network service alias, you can use that alias when specifying the network service for multiple session ACLs.

To define a service alias via the command-line interface, access the CLI in config mode and issue the following command:

```
(host) (config) #netSERVICE <name> <protocol>|tcp|udp {list <port>,<port>}|{<port> [<port>]}[ALG <service>]
```

## User Roles

This section describes how to create a new user role. When you create a user role, you specify one or more policies for the role. [Table 36](#) lists the parameters you can configure for the user role.

**Table 36:** *User Role Parameters*

| Field                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Policies (required)            | One or more policies that define the privileges of a wired client in this role. There are three ways to add a access policy to a user role: <ul style="list-style-type: none"> <li>• Use an existing policy via CLI</li> <li>• Edit and use the existing policy via CLI</li> <li>• Create a new policy CLI</li> </ul> <b>NOTE:</b> For more information, see <a href="#">Configuring the ACLs on page 280</a> . |
| Re-authentication Interval (optional) | Time, in minutes, after which the client is required to reauthenticate. Enter a value between 0-4096. 0 disables reauthentication.<br>Default: 0 (disabled)                                                                                                                                                                                                                                                     |
| Role VLAN ID (optional)               | By default, a client is assigned a VLAN on the basis of the ingress VLAN for the client to the Mobility Access Switch. You can override this assignment and configure the VLAN ID that is to be assigned to the user role. You configure a VLAN by navigating to the <b>Configuration &gt; VLANs</b> page.                                                                                                      |
| policer-profile (optional)            | Specifies the policer activities configuration parameters for the user under this role.                                                                                                                                                                                                                                                                                                                         |
| qos-profile (optional)                | Specifies the QoS configuration parameters for the user under this role.                                                                                                                                                                                                                                                                                                                                        |
| voip-profile (optional)               | Specifies the VOIP configuration parameters for an user connected to the interface (VOIP devices and/or PCs and Laptops).                                                                                                                                                                                                                                                                                       |

## Creating a User Role

The following example creates the user role 'web-guest' and assigns the previously-configured 'web-only' policy to this user role.



---

You cannot delete a user-role that is referenced in a **aaa-profile**. Remove all references to the role and then perform the delete operation. Deleting user-roles used by external authentication servers is also inadvisable without first modifying the external authentication server not to reference that role.

---

### In the CLI

```
user-role web-guest
 access-list stateless web-only position 1
```

After assigning the user role, you can use the **show reference user-role <role>** command to see the profiles that reference this user role.

## User Role Assignments

A client is assigned a user role by one of several methods. A role assigned by one method may take precedence over one assigned by a different method. The methods of assigning user roles are, from lowest to highest precedence:

1. The user role can be derived from user attributes upon the client's association with an interface (this is known as a user-derived role). You can configure rules that assign a user role to clients that match the mac address. For example, you can configure a rule to assign the role "VoIP-Phone" to any client that has a MAC address that starts with bytes xx:yy:zz. User-derivation rules are executed before client authentication.
2. The user role can be the default user role configured for an authentication method, such as 802.1x or MAC authentication. For each authentication method, you can configure a default role for clients who are successfully authenticated using that method.
3. The user role can be derived from attributes returned by the authentication server (this is known as a server-derived role). If the client is authenticated via an authentication server, the user role for the client can be based on the attribute returned by the server during authentication. In case the attribute is not returned by the server, the client gets the default authentication role defined under aaa profile. Server-derivation rules are executed after client authentication.
4. The user role can be derived from Aruba Vendor-Specific Attributes (VSA) for RADIUS server authentication. A role derived from an Aruba VSA takes precedence over any other user roles.

The following sections describe the methods of assigning user roles.

### User Role in AAA Profile

An AAA profile defines the user role for unauthenticated clients (initial role) as well as the default user role for MAC and 802.1x authentication. To configure user roles in the AAA profile:

#### In the CLI

```
aaa profile <profile>
 initial-role <role>
 dot1x-default-role <role>
 mac-default-role <role>
```

### User-Derived Roles or VLANs

Attributes derived from the client's can be used to assign the client to a specific role or VLAN, as user-derivation rules are executed before the client is authenticated.

You configure the user role or VLAN to be assigned to the client by specifying condition rules; when a condition is met, the specified user role or VLAN 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 optionally add a description of the user role.

[Table 37](#) describes the conditions for which you can specify a user role or VLAN.

**Table 37:** Conditions for a User-Derived Role or VLAN

| Rule Type                 | Condition                                                                                                                                                                  | Value                                                                 |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| DHCP-Option               | One of the following: <ul style="list-style-type: none"> <li>• equals</li> <li>• starts with</li> </ul>                                                                    | DHCP signature ID.<br><b>NOTE:</b> This string is not case sensitive. |
| MAC address of the client | One of the following: <ul style="list-style-type: none"> <li>• contains</li> <li>• ends with</li> <li>• equals</li> <li>• does not equal</li> <li>• starts with</li> </ul> | MAC address (xx:xx:xx:xx:xx:xx)                                       |

## Configure a User-derived Role or VLAN in the CLI

```
aaa derivation-rules user <name>
 set role|vlan
 condition macaddr
 contains|ends-with|equals|not-equals|starts-with <string>
 set-value <role>
 position <number>
```




---

There are many online tools available for converting ASCII text to a hexadecimal string.

---

## Default Role for Authentication Method

For each authentication method, you can configure a default role for clients who are successfully authenticated using that method. To configure a default role for an authentication method:

### In the CLI

To configure the default user role for MAC or 802.1x authentication:

```
aaa profile <profile>
 mac-default-role <role>
 dot1x-default-role <role>
```

## Server-Derived Role

If the client is authenticated via an authentication server, the user role for the client can be based on one or more attributes returned by the server during authentication. 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 define server rules based on client MAC address, even though the MAC address is not returned by the server as an attribute.




---

The roles and VLANs in the sample below are defined under the **aaa server-group <server-group-name>** configuration.

---

## Sample configuration

```
set role|vlan
 condition <attribute name>
 contains|ends-with|equals|not-equals|starts-with <attribute value>
 set-value <role> | <vlan>
 position <number>
```

## VSA-Derived Role

Many Network Address Server (NAS) vendors, including Aruba, use VSAs to provide features not supported in standard RADIUS attributes. For Aruba systems, VSAs can be employed to provide the user role and VLAN for RADIUS-authenticated clients, however the VSAs must be present on your RADIUS server. This involves defining the vendor (Aruba) and/or the vendor-specific code (14823), vendor-assigned attribute number, attribute format (such as string or integer), and attribute value in the RADIUS dictionary file. VSAs supported on Mobility Access Switches conform to the format recommended in RFC 2865, "Remote Authentication Dial In User Service (RADIUS)".

## Deny Inter-User Traffic

Deny Inter-user Traffic feature enables Mobility Access Switches to block the communication between users with the same role. For example, an organization can block communication between any two guest users. If the role has voip-profile configured, then the traffic across the VoIP users is also denied.



---

The inter-user traffic denial happens only within an ArubaStack and does not span across multiple Mobility Access Switches or ArubaStack.

---

By default this feature is disabled. You can configure Deny Inter-user Traffic for a maximum of seven user-roles (including CPPM downloaded roles) on a per user-role basis.

## Limitations

- The traffic originated from a user with a role that has Deny Inter-user Traffic enabled, is denied even to the users with different roles, if they are connected to the same port and VLAN of the user to which the traffic must be denied.
- L3 multicast traffic originated from users cannot be denied across users when the users are in different VLANs and same role.
- Where there are two users in same role and different VLAN and if session processing or NAT is enabled on the RVI, then the inter-user-traffic is not dropped.

## Configuring Deny Inter-User Traffic

You can configure this feature using the following CLI command:

```
(host) (config) #user-role <role-name>
(host) (config-role) #deny-inter-user-traffic
```

## Sample Configuration

```
(host) (config) #user-role Guest
(host) (config-role) #deny-inter-user-traffic
```

## Verifying Deny Inter-User Traffic Configuration

Use the following command to view 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

Use the following command to view the details of the interfaces on which the role is applied and traffic is denied:

```
(host) #show user-table role guest
```

Users

-----

| IP         | MAC               | Name       | Role  | Age (d:h:m) | Auth         |
|------------|-------------------|------------|-------|-------------|--------------|
| 192.0.2.11 | 04:7d:7b:1e:d1:bf | test-user1 | Guest | 00:02:18    | 802.1x-Wired |
| 192.0.2.10 | 00:25:45:93:bf:d8 | test-user2 | Guest | 00:02:18    | 802.1x-Wired |

| Connection | Interface | Profile | Vlan     |
|------------|-----------|---------|----------|
| Wired      | 3/0/44    | dot1x   | 1 (3911) |
| Wired      | 3/0/44    | dot1x   | 1 (3913) |

User Entries: 2/2



This chapter describes the following topics:

- [MAC-Based Authentication Concepts on page 337](#)
- [Configuring MAC-Based Authentication on page 337](#)
- [Configuring Clients on page 338](#)

## MAC-Based Authentication Concepts

MAC-based authentication is used to authenticate devices based on their physical media access control (MAC) address. While not the most secure and scalable method, MAC-based authentication implicitly provides an additional layer of security authentication devices. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to the rest. For example, if clients are allowed access to the network via station A, then one method of authenticating station A is MAC-based. Clients may be required to authenticate themselves using other methods depending on the network privileges required.

## Configuring MAC-Based Authentication

This section describes how to configure MAC-based authentication on the Mobility Access Switch. Before configuring MAC-based authentication, you must configure:

- The user role that will be assigned as the default role for the MAC-based authenticated clients.
- You configure the default user role for MAC-based authentication in the AAA profile. If derivation rules exist or if the client configuration in the internal database has a role assignment, these values take precedence over the default user role.
- The authentication server group that the Mobility Access Switch uses to validate the clients. The internal database can be used to define clients for MAC-based authentication.

## Configuring the MAC Authentication Profile

[Table 38](#) describes the MAC-based authentication parameters.

**Table 38: MAC Authentication Profile Configuration Parameters**

| Parameter                   | Description                                                                                                                                                                                                                                                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delimiter                   | Delimiter used in the MAC string: <ul style="list-style-type: none"> <li>● colon specifies the format xx:xx:xx:xx:xx:xx</li> <li>● dash specifies the format xx-xx-xx-xx-xx-xx</li> <li>● none specifies the format xxxxxxxxxxxx</li> <li>● oui-nic specifies the format xxxxxx-xxxxxx</li> </ul> Default: none |
| Case                        | The case (upper or lower) used in the MAC string.<br>Default: lower                                                                                                                                                                                                                                             |
| Max Authentication failures | Number of times a station can fail to authenticate before it is blacklisted. A value of 0 disables blacklisting.<br>Default: 0                                                                                                                                                                                  |

## Using the CLI

```
aaa authentication mac <profile>
 case {lower|upper}
 delimiter {colon|dash|none|oui-nic}
 max-authentication-failures <number>
```

## Configuring Clients

You can create entries in the Mobility Access Switch's internal database that can be used to authenticate client MAC addresses. The internal database contains a list of clients along with the password and default role for each client. To configure entries in the internal database for MAC authentication, you enter the MAC address for both the user name and password for each client.



---

You must enter the MAC address using the delimiter format configured in the MAC authentication profile. The default delimiter is none, which means that MAC addresses should be in the format xxxxxxxxxxxx. If you specify colons for the delimiter, you can enter MAC addresses in the format xx:xx:xx:xx:xx:xx.

---

## Using the CLI to configure clients in the internal database

Enter the following command in enable mode:

```
local-userdb add username <macaddr> password <macaddr>
```

This chapter describes the following topics:

- [802.1x Authentication Concepts on page 339](#)
- [Configuring 802.1x Authentication on page 341](#)
- [Configuring 802.1x Authentication with Machine Authentication on page 343](#)

## 802.1x Authentication Concepts

IEEE 802.1x is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1x group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1x authentication involves three parties:

- The *supplicant*, or client, is the device attempting to gain access to the network. You can configure the Aruba user-centric network to support 802.1x authentication for wired users.
- The *authenticator* is the gatekeeper to the network and permits or denies access to the supplicants. The Aruba Mobility Access Switch acts as the authenticator, relaying information between the authentication server and supplicant. The EAP type must be consistent between the authentication server and supplicant and is transparent to the Mobility Access Switch.
- The *authentication server* provides a database of information required for authentication and informs the authenticator to deny or permit access to the supplicant.

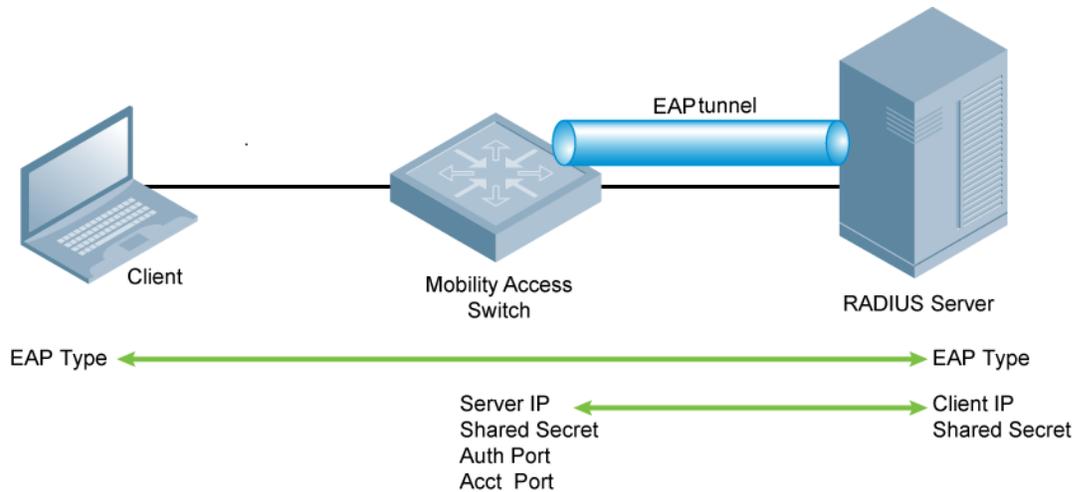
The 802.1x authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS) server which can authenticate either users (through passwords or certificates) or the client computer.

In Aruba user-centric networks, you can terminate the 802.1x authentication on the Mobility Access Switch. The Mobility Access Switch passes user authentication to its internal database or to a “backend” non-802.1x server. This feature is useful for deployments where an 802.1x EAP-compliant RADIUS server is not available or required for authentication.

### Authentication with a RADIUS Server

See [Table 39](#) below for an overview of the parameters that you need to configure on authentication components when the authentication server is an 802.1x EAP-compliant RADIUS server.

**Figure 20** 802.1x Authentication with RADIUS Server



The supplicant and authentication server must be configured to use the same EAP type. The Mobility Access Switch does not need to know the EAP type used between the supplicant and authentication server.

For the Mobility Access Switch to communicate with the authentication server, you must configure the IP address, authentication port, and accounting port of the server on the Mobility Access Switch. The authentication server must be configured with the IP address of the RADIUS client, which is the Mobility Access Switch in this case. Both the Mobility Access Switch and the authentication server must be configured to use the same shared secret.



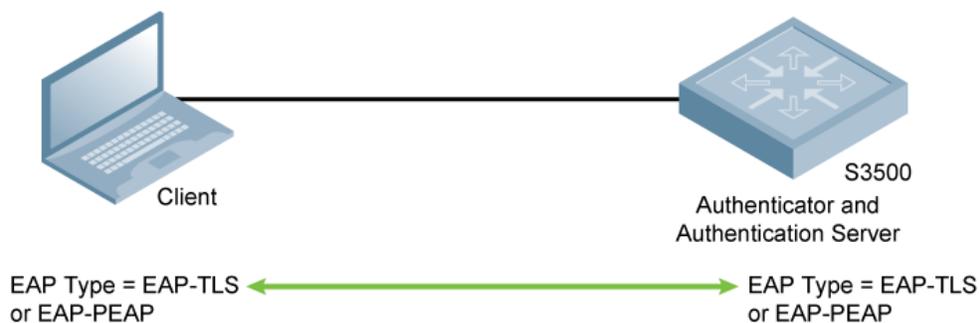
Additional information on EAP types supported in a Windows environment, Microsoft supplicants, and authentication server, is available at [http://technet.microsoft.com/en-us/library/cc782851\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc782851(WS.10).aspx).

The client communicates with the Mobility Access Switch through an EAP tunnel in order to authenticate to the network. Therefore, the network authentication and encryption configured must be the same on both the client and the Mobility Access Switch.

### Authentication Terminated on the Mobility Access Switch

User authentication is performed either via the Mobility Access Switch's internal database or a non-802.1x server.

**Figure 21** 802.1x Authentication with Termination on Mobility Access Switch



In this scenario, the supplicant is configured for EAP-Transport Layer Security (TLS) or EAP-Protected EAP (PEAP).

- EAP-TLS is used with smart card user authentication. A smart card holds a digital certificate which, with the user-entered personal identification number (PIN), allows the user to be authenticated on the network. EAP-TLS relies on digital certificates to verify the identities of both the client and server.  
EAP-TLS requires that you import server and certification authority (CA) certificates onto the Mobility Access Switch. The client certificate is verified on the Mobility Access Switch (the client certificate must be signed by a known CA) before the user name is checked on the authentication server.
- EAP-PEAP uses TLS to create an encrypted tunnel. Within the tunnel, one of the following “inner EAP” methods 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 an LDAP or RADIUS server as the user authentication server. You can also enable caching of user credentials on the Mobility Access Switch as a backup to an external authentication server.
  - EAP-Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2): Described in RFC 2759, this EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the backend authentication server.

If you are using the Mobility Access Switch’s internal database for user authentication, you need to add the names and passwords of the users to be authenticated. If you are using an LDAP server for user authentication, you need to configure the LDAP server on the Mobility Access Switch, and configure user IDs and passwords. If you are using a RADIUS server for user authentication, you need to configure the RADIUS server on the Mobility Access Switch.

## Configuring 802.1x Authentication

The Mobility Access Switch supports 802.1x (dot1x) authentication including **termination**. For example, the list of termination options for the profile name *techpubsAuth* is shown below.

```
(host) (802.1X Authentication Profile "techpubsAuth") # termination ?
eap-type Configure the EAP method.Default method is EAP-PEAP
enable Enable Dot1x Termination.Default is disabled
enable-token-caching Enable Token Caching.Default is disabled
inner-eap-type Configure the inner EAP method.Default method is
 EAP-MSCHAPV2
token-caching-period Configure the Token Caching Period
```

The following example configures various options for the 802.1x Authentication profile *techpubsAuth*.

```
(host) (802.1X Authentication Profile "techpubsAuth") #termination enable
(host) (802.1X Authentication Profile "techpubsAuth") #termination eap-type eap-peap
(host) (802.1X Authentication Profile "techpubsAuth") #max-authentication-failures 2
(host) (802.1X Authentication Profile "techpubsAuth") #timer reauth-period 3600
(host) (802.1X Authentication Profile "techpubsAuth") #framed-mtu 1500
(host) (802.1X Authentication Profile "techpubsAuth") #reauth-max 2
(host) (802.1X Authentication Profile "techpubsAuth") #reauthentication
```

To verify the above configurations, execute the show command below:

```
(host) (config) #show aaa authentication dot1x techpubsAuth
```

```
802.1X Authentication Profile "techpubsAuth"
```

```

Parameter Value

Max authentication failures 2 <--
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                                     | 3600 sec   | <-- |
| Use Server provided Reauthentication Interval                 | Disabled   |     |
| Authentication Server Retry Interval                          | 30 sec     |     |
| Authentication Server Retry Count                             | 2          |     |
| Framed MTU                                                    | 1500 bytes | <-- |
| Number of times ID-Requests are retried                       | 3          |     |
| Maximum Number of Reauthentication Attempts                   | 2          | <-- |
| Maximum number of times Held State can be bypassed            | 0          |     |
| Reauthentication Termination                                  | Enabled    | <-- |
| Termination                                                   | Enabled    | <-- |
| Termination EAP-Type                                          | eap-peap   | <-- |
| 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   |     |
| Check certificate common name against AAA server              | Enabled    |     |




---

Use the privileged mode in the CLI to configure users in the Mobility Access Switch's internal database.

---

To add users to the local database, use the following command:

```
local-userdb add username <user> password <password> role <user_role>
```

## Configuring a Server Rule Using the CLI

```
aaa server-group dot1x_internal
set role condition Role value-of
```

## LDAP Servers

If you are using a LDAP server for authentication, the following variables should be set.

- termination enabled
- EAP type of TLS or PEAP (with inner-EAP-type set to GTC)

Below is an example configuration for the profile *techpubsAuth* for an LDAP server:

```
(host) (802.1X Authentication Profile "techpubsAuth") #termination enable
(host) (802.1X Authentication Profile "techpubsAuth") #termination eap-type eap-peap
(host) (802.1X Authentication Profile "techpubsAuth") # termination inner-eap-type eap-gtc
```

To verify the configuration, execute the **show aaa authentication dot1x <profile\_name>** command.

## Configuring Certificates with Auth Termination

The Mobility Access Switch supports 802.1x authentication using digital certificates for auth termination.

- **Server Certificate**—A server certificate installed in the Mobility Access Switch verifies the authenticity of the Mobility Access Switch for 802.1x authentication. Aruba Mobility Access Switches ship with a demonstration digital certificate. Until you install a customer-specific server certificate in the Mobility Access Switch, this demonstration certificate is used by default for all secure HTTP connections and auth termination. This certificate is included primarily for the purposes of feature demonstration and convenience and is not intended for long-term use in production networks. Users in a production environment are urged to obtain and install a certificate issued for their site or domain by a well-known certificate authority (CA). You can generate a Certificate Signing Request (CSR) on the Mobility Access Switch to submit to a CA. For information on how to generate a CSR and how to import the CA-signed certificate into the Mobility Access Switch, see [Managing Certificates on page 56](#).
- **Client Certificates**—Client certificates are verified on the Mobility Access Switch (the client certificate must be signed by a known CA) before the user name is checked on the authentication server. To use client certificate authentication for auth termination you need to import the following certificates into the Mobility Access Switch (see [Importing Certificates on page 57](#)):
  - Mobility Access Switch's server certificate
  - CA certificate for the CA that signed the client certificates

## Using the CLI

```
aaa authentication dot1x <profile>
 termination enable
 server-cert <certificate>
 ca-cert <certificate>
```

## Configuring 802.1x Authentication with Machine Authentication

When a Windows device boots, it logs onto the network domain using a machine account. Within the domain, the device is authenticated before computer group policies and software settings can be executed; this process is known as *machine authentication*. Machine authentication ensures that only authorized devices are allowed on the network.

You can configure 802.1x for both user and machine authentication (select the **Enforce Machine Authentication** option described in [Table 39](#)). This tightens the authentication process further since both the device and user need to be authenticated.

### Role Assignment with Machine Authentication Enabled

When you enable machine authentication, there are two additional roles you can define in the 802.1x authentication profile:

- Machine authentication default machine role
- Machine authentication default user role

While you can select the same role for both options, you should define the roles as per the policies that need to be enforced. Also, these roles can be different from the 802.1x authentication default role configured in the AAA profile.

With machine authentication enabled, the assigned role depends upon the success or failure of the machine and user authentications. In certain cases, the role that is ultimately assigned to a client can also depend upon attributes returned by the authentication server or server derivation rules configured on the Mobility Access Switch.

[Table 39](#) describes role assignment based on the results of the machine and user authentications.

**Table 39: Role Assignment for User and Machine Authentication**

| Machine Auth Status | User Auth Status | Description                                                                                                                                                                                                         | Role Assigned                                                                                                                                                |
|---------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Failed              | Failed           | Both machine authentication and user authentication failed. L2 authentication failed.                                                                                                                               | Initial role defined in the AAA profile will be assigned. If no initial role is explicitly defined, the default initial role (logon role) is assigned.       |
| Failed              | Passed           | Machine authentication fails (for example, the machine information is not present on the server) and user authentication succeeds. Server-derived roles do not apply.                                               | Machine authentication default user role configured in the 802.1x authentication profile.                                                                    |
| Passed              | Failed           | Machine authentication succeeds and user authentication has not been initiated. Server-derived roles do not apply.                                                                                                  | Machine authentication default machine role configured in the 802.1x authentication profile.                                                                 |
| Passed              | Passed           | Both machine and user are successfully authenticated. If there are server-derived roles, the role assigned via the derivation take precedence. This is the <i>only</i> case where server-derived roles are applied. | A role derived from the authentication server takes precedence. Otherwise, the 802.1x authentication default role configured in the AAA profile is assigned. |

For example, if the following roles are configured:

- 802.1x authentication default role (in AAA profile): dot1x\_user
- Machine authentication default machine role (in 802.1x authentication profile): dot1x\_mc
- Machine authentication default user role (in 802.1x authentication profile): guest

Role assignments would be as follows:

- If both machine and user authentication succeed, the role is dot1x\_user. If there is a server-derived role, the server-derived role takes precedence.
- If only machine authentication succeeds, the role is dot1x\_mc.
- If only user authentication succeeds, the role is guest.
- On failure of both machine and user authentication, the initial role defined in the AAA profile is assigned.

With machine authentication enabled, the VLAN to which a client is assigned (and from which the client obtains its IP address) depends upon the success or failure of the machine and user authentications. The VLAN that is ultimately assigned to a client can also depend upon attributes returned by the authentication server or server derivation rules configured on the Mobility Access Switch. If machine authentication is successful, the client is associated to the VLAN configured on the interface. However, the client can be assigned a derived VLAN upon successful user authentication.



You can optionally assign a VLAN as part of a user role configuration. It is recommended not to use VLAN derivation if user roles are configured with VLAN assignments.

[Table 40](#) describes VLAN assignment based on the results of the machine and user authentications when VLAN derivation is used.

**Table 40: VLAN Assignment for User and Machine Authentication**

| Machine Auth Status | User Auth Status | Description                                                                                                                        | VLAN Assigned                                                                                                |
|---------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Failed              | Failed           | Both machine authentication and user authentication failed. L2 authentication failed.                                              | VLAN configured on the interface<br>or,<br>VLAN configured under initial role                                |
| Failed              | Passed           | Machine authentication fails (for example, the machine information is not present on the server) and user authentication succeeds. | VLAN configured on the interface<br>or,<br>VLAN configured under Machine authentication default user role    |
| Passed              | Failed           | Machine authentication succeeds and user authentication has not been initiated.                                                    | VLAN configured on the interface<br>or,<br>VLAN configured under Machine authentication default machine role |
| Passed              | Passed           | Both machine and user are successfully authenticated.                                                                              | Derived VLAN<br>or,<br>VLAN configured on the interface                                                      |

## Authentication with an 802.1x RADIUS Server

- An EAP-compliant RADIUS server provides the 802.1x authentication. The RADIUS server administrator must configure the server to support this authentication. The administrator must also configure the server to all communications with the Aruba Mobility Access Switch.
- 802.1x authentication based on PEAP with MS-CHAPv2 provides both computer and user authentication. If a user attempts to log in without the computer being authenticated first, the user is placed into a more limited “guest” user role.

Windows domain credentials are used for computer authentication, and the user’s Windows login and password are used for user authentication. A single user sign-on facilitates both authentication to the network and access to the Windows server resources.

You can create the following policies and user roles for:

- Student
- Faculty
- Guest
- Sysadmin
- Computer

## Creating an Alias for the Internal Network

### Using the CLI

```
netdestination "Internal Network"
network 10.0.0.0 255.0.0.0
```

```
network 172.16.0.0 255.255.0.0
```

## Creating the Student Role and Policy

The **student** policy prevents students from using telnet, POP3, FTP, SMTP, SNMP, or SSH to the wired portion of the network. The **student** policy is mapped to the **student** user role.

### Using the CLI

```
ip access-list stateless student
 any alias "Internal Network" svc-telnet deny
 any alias "Internal Network" svc-pop3 deny
 any alias "Internal Network" svc-ftp deny
 any alias "Internal Network" svc-smtp deny
 any alias "Internal Network" svc-snmp deny
 any alias "Internal Network" svc-ssh deny
user-role student
access-list stateless student
access-list stateless allowall
```

## Creating the Faculty Role and Policy

The **faculty** policy is similar to the **student** policy. However, the faculty members are allowed to use POP3 and SMTP. The **faculty** policy is mapped to the **faculty** user role.

### Using the CLI

```
ip access-list stateless faculty
 any alias "Internal Network" svc-telnet deny
 any alias "Internal Network" svc-ftp deny
 any alias "Internal Network" svc-snmp deny
 any alias "Internal Network" svc-ssh deny
user-role faculty
access-list stateless faculty
access-list stateless allowall
```

## Creating the Guest Role and Policy

The **guest** policy permits only access to the Internet (via HTTP or HTTPS) and only during daytime working hours. The **guest** policy is mapped to the **guest** user role.

### Using the CLI

```
time-range working-hours periodic
 weekday 07:30 to 17:00
ip access-list stateless guest
 any host 10.1.1.25 svc-dhcp permit time-range working-hours
 any host 10.1.1.25 svc-dns permit time-range working-hours
 any alias "Internal Network" any deny
 any any svc-http permit time-range working-hours
 any any svc-https permit time-range working-hours
 any any any deny
user-role guest
access-list stateless guest
```

## Configuring the RADIUS Authentication Server

You can set the role condition to identify the user's group. The Mobility Access Switch uses the literal value of this attribute to determine the role name. The following example uses the RADIUS server name *radiusTechPubs* to configure the Radius server.

```
(host) (config) #aaa authentication-server radius radiusTechPubs
```

```
(host) (RADIUS Server "radiusTechPubs") #host 10.41.255.30
(host) (RADIUS Server "radiusTechPubs") #key hometown
(host) (RADIUS Server "radiusTechPubs") #exit

(host) (config) #aaa server-group radiusTechpubs
(host) (Server Group "radiusTechpubs") #auth-server radiusTechpubs
(host) (Server Group "radiusTechpubs") #set role condition Class Value-of
```

## Configuring 802.1x Authentication Profile

In the 802.1x authentication profile, configure enforcement of machine authentication before user authentication. If a user attempts to log in without machine authentication taking place first, the user is placed in the limited guest role.

### Using the CLI

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

## Configuring AAA Profile

A AAA profile specifies the 802.1x authentication profile and 802.1x server group to be used for authenticating clients. The AAA profile also specifies the default user roles for 802.1x authentication.

### Using the CLI

```
aaa profile aaa_dot1x
 dot1x-default-role faculty
 authentication-dot1x dot1x
 dot1x-server-group radiusTechpubs
```



Captive portal is an L3 authentication method supported by Mobility Access Switch. A captive portal presents a Web page which requires user action before network access is granted. The required action can be simply viewing and agreeing to an acceptable use policy, entering Email ID, or entering a user ID and password which must be validated against a database of authorized users. The Mobility Access Switch supports both internal and external captive portals.

This chapter describes the following topics:

- [Captive Portal Overview on page 349](#)
- [Configuring Captive Portal Authentication on page 349](#)
- [Captive Portal Configuration Example on page 351](#)
- [Personalizing the Captive Portal Page on page 353](#)
- [Creating Walled Garden Access on page 355](#)
- [Mobility Access Switch Server Certificate on page 355](#)

## Captive Portal Overview

You can configure captive portal for guest users where no authentication is required, or for registered users who must be authenticated against an external authentication server or the Mobility Access Switch's internal user database.



---

Captive portal is most often used for guest access, access to open systems (such as public hot spots), or as a way to connect to a VPN.

---

You can use captive portal for guest and registered users at the same time. The default captive portal Web page provided with ArubaOS Mobility Access Switch displays login prompts only for registered users. The Mobility Access Switch supports the creation of 16 different customer login pages. The login page displayed is based on the AAA Profile applied to the port that the user is connected.

## Configuring Captive Portal Authentication

This section describes how to configure Captive Portal authentication on the Mobility Access Switch. Before configuring Captive Portal authentication, you must configure the following:

- The user role that will be assigned as the initial role. This initial role does not require any Captive Portal specific ACLs because once Captive Portal is added to the user-role, the necessary ACLs will automatically be added.
- The authentication server group that the Mobility Access Switch uses to validate the guest or registered users. The internal user database or an external authentication server may be used.



---

A read-only ACL using the same name defined in **captive-portal <name>** is automatically generated upon adding **captive-portal <name>** to a user-role. This ACL is configured to redirect http/https traffic and permit DNS and DHCP traffic. You can use the **show rights <user-role>** command to verify this ACL.

---

## Captive Portal Configuration Parameters

[Table 41](#) describes configuration parameters for Captive Portal Authentication profile page in the WebUI. In the CLI, you configure these options with the **aaa authentication captive-portal** commands.

**Table 41:** *Captive Portal Authentication Profile Parameters*

| Parameter                            | Description                                                                                                                                                                                                                            |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default-guest-role                   | Role assigned to guest.<br>Default: guest                                                                                                                                                                                              |
| default-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.<br>Default: guest |
| enable-welcome-page                  | Displays the configured welcome page before the user is redirected to their original URL. If this option is disabled, redirection to the Web URL happens immediately after the user logs in.<br>Default: Enabled                       |
| guest-logon                          | Enables Captive Portal logon without authentication.<br>Default: 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.<br>Default: Disabled                                                                                                    |
| login-page                           | URL of the page that appears for the user logon. This can be set to any URL.<br>Default: /auth/index.html                                                                                                                              |
| logon-wait                           | Configure parameters for the logon wait interval<br>Default: 10 seconds                                                                                                                                                                |
| Logon wait CPU utilization threshold | CPU utilization percentage above which the Logon wait interval is applied when presenting the user with the logon page.<br>Default: 60%                                                                                                |
| 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. This works in conjunction with the Logon wait CPU utilization threshold parameter.<br>Default: 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.<br>Default: Enabled                 |
| max-authentication-failures          | The number of authentication failures before the user is blacklisted.<br>Default : 0, Range: 0-10                                                                                                                                      |
| 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.<br>Default: disabled (HTTPS is used)                                                      |
| 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.<br>Default: 10 seconds     |

| Parameter                  | Description                                                                                                                                                                                                                                                                                        |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server-group               | Name of the group of servers used to authenticate Captive Portal users.                                                                                                                                                                                                                            |
| 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.<br>Default: Disabled                                                   |
| show-acceptable-use-policy | Show the acceptable use policy page before the logon page.<br>Default: Disabled                                                                                                                                                                                                                    |
| single-session             | Allows only one active user session at a time.<br>Default: Disabled                                                                                                                                                                                                                                |
| switchip-in-redirect-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.<br>Default: Disabled |
| use-chap                   | Use CHAP protocol. You should not use this option unless instructed to do so by an Aruba representative.<br>Default: Disabled                                                                                                                                                                      |
| user-logon                 | Enables Captive Portal with authentication of user credentials.<br>Default: Enabled                                                                                                                                                                                                                |
| user-vlan-in-redirect-url  | Sends VLAN ID of the user in the redirection URL when external captive portal servers are used.                                                                                                                                                                                                    |
| welcome-page               | URL of the page that appears after logon and before redirection to the Web URL. This can be set to any URL.<br>Default: /auth/welcome.html                                                                                                                                                         |
| white-list                 | Name of an existing white list on an IPv4 or IPv6 network destination. The white list contains authenticated Web sites that a guest can access.                                                                                                                                                    |

## Captive Portal Configuration Example

You can configure Captive Portal either using the WebUI or using the CLI.

### Configuring Captive Portal via the CLI

To configure Captive Portal via the command-line interface, access the CLI configuration mode and issue the following commands:

#### 1. 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
```



It is assumed that a AAA server-group named "cp-srv" was previously created. To create a AAA server-group, refer the procedure mentioned in [Configuring Server Groups on page 298](#).

You can use the following URL to configure an external captive portal authentication on an external server:

```
(host) (config) #aaa authentication captive-portal cp-profile
```

```
(host) (Captive Portal Authentication Profile "cp-profile") #login-page https://<external_server_IP>/<login_page_path>
```

You can use the following URLs to configure an external captive portal authentication on ClearPass Policy Manager (CPPM):

For pre-6.0 ClearPass Policy Manager (Onboard, Legacy Captive Portal Capability):

```
(host) (Captive Portal Authentication Profile "cp-profile") #login-page https://<clearpass-server>/agent/portal/
```

For pre-6.0 ClearPass Guest:

```
(host) (Captive Portal Authentication Profile "cp-profile") #login-page https://<clearpass-guest-server>/<admin-defined-name>.php
```

For 6.0 ClearPass Policy Manager and ClearPass Guest (Integrated Platform):

```
(host) (Captive Portal Authentication Profile "cp-profile") #login-page https://<clearpass-server>/agent/portal/ (Onboard, Legacy Captive Portal Capability)
```

```
(host) (Captive Portal Authentication Profile "cp-profile") #login-page https://<clearpass-server>/guest/ (ClearPass Guest)
```

Please refer to ClearPass Policy Manager and ClearPass Guest documentation for more details.

## 2. Attach a Captive Portal profile to a user role

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

## 3. Designate the **cp-first** user-role as the initial role of the AAA profile **cp\_aaa**

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

## 4. Apply the configured AAA profile to the interface

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



---

By default, the authenticated Captive Portal users will be assigned the **guest** user-role.

---

## Configuring Captive Portal via the WebUI



---

You can create the user role using the CLI. For more information, see [Creating a User Role on page 332](#).

---

1. Navigate to the **Configuration>Authentication** page.
2. Select initial role as **cp-first** from the **Initial-Role** drop-down list.
3. Click the **New** button to create a new AAA profile, enter the name of the profile (for example, **profile1**) in the **Name** textbox.
4. Select the authentication method as **captive-portal** from the **Authentication Method** drop-down list.
5. Select the **specify new profile** radio button and enter the captive portal profile name (for example, **c-portal**) in the **Profile Name** textbox.
6. Select the server-group as **cp-srv** from the **Auth Server** drop-down list.



---

It is assumed that a AAA server-group named "cp-srv" was previously created. To create a AAA server-group, refer the procedure mentioned in [Configuring Server Groups on page 298](#).

---

7. Click **Ok** and **Apply**.
8. To assign AAA profile to the port, select the port from the **Ports Assign** list.
9. Click **Ok** and **Apply**.

10. To make the port untrusted, navigate to **Configuration>Ports** page and select the port from the **Ports** list.
11. Select the **Disabled** radio button from the **Trusted** list.
12. Click **Ok** and **Apply**.



---

By default, authenticated Captive Portal users will be assigned the **guest** user-role.

---

## Personalizing the Captive Portal Page

Starting from ArubaOS 7.4.0.2, the **Authentication Required** page appearing before the actual captive portal login page is removed from the Mobility Access Switch.

The following can be personalized on the default captive portal page:

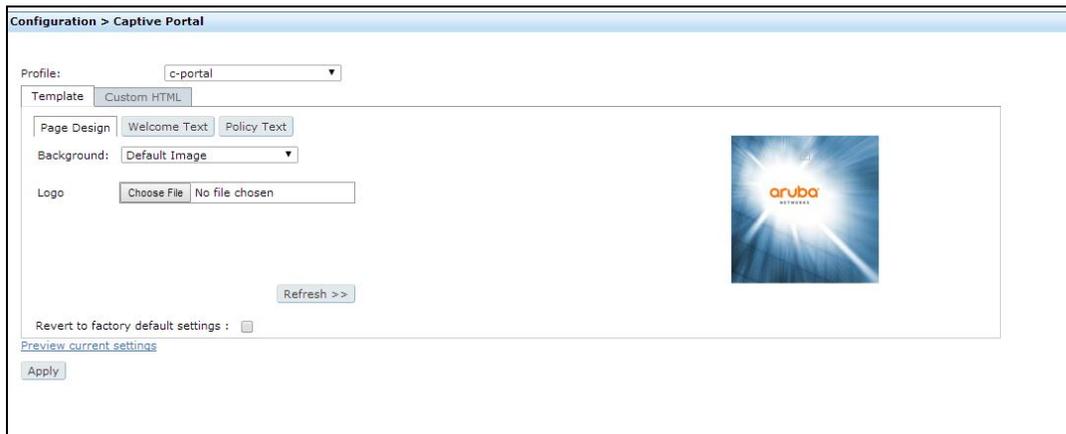
- Captive portal background
- Page text

The background image and text should be visible to users with a browser window on a 1024 by 768 pixel screen. The background should not clash if viewed on a much larger monitor. A good option is to have the background image at 800 by 600 pixels, and set the background color to be compatible. The maximum image size for the background can be around 960 by 720 pixels, as long as the image can be cropped at the bottom and right edges. Leave space on the left side for the login box.

1. Navigate to the **Configuration > Captive Portal** page.
2. Select the captive portal profile that you want to customize from the **Profile** drop-down list.
3. Select the image that you want to customize from the **Background** drop-down list.

The default page design is as shown below:

**Figure 22** *Personalizing the Captive Portal - Default Image*



4. To add the policy text:
  - a. Click on the **policy text** tab and enter the acceptable use policy for guests in HTML format.
  - b. Click **Apply**.
  - c. To view the changes, click on the **Preview current settings** link which displays the Captive Portal page as it will be seen by users.



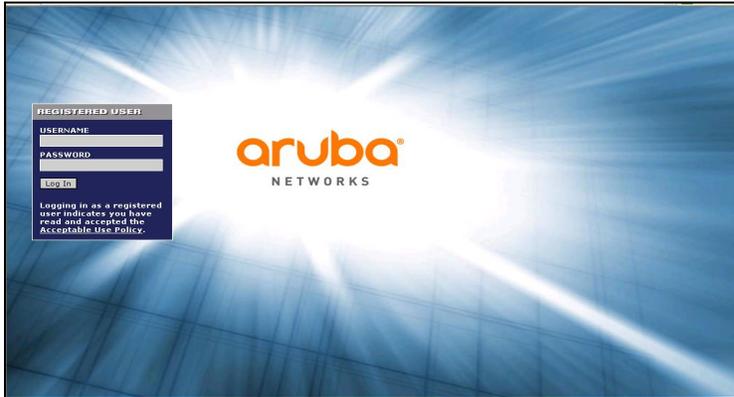
---

You can configure policy text from the WebUI. To enable it from the CLI, use `show-acceptable-use-policy` command.

---

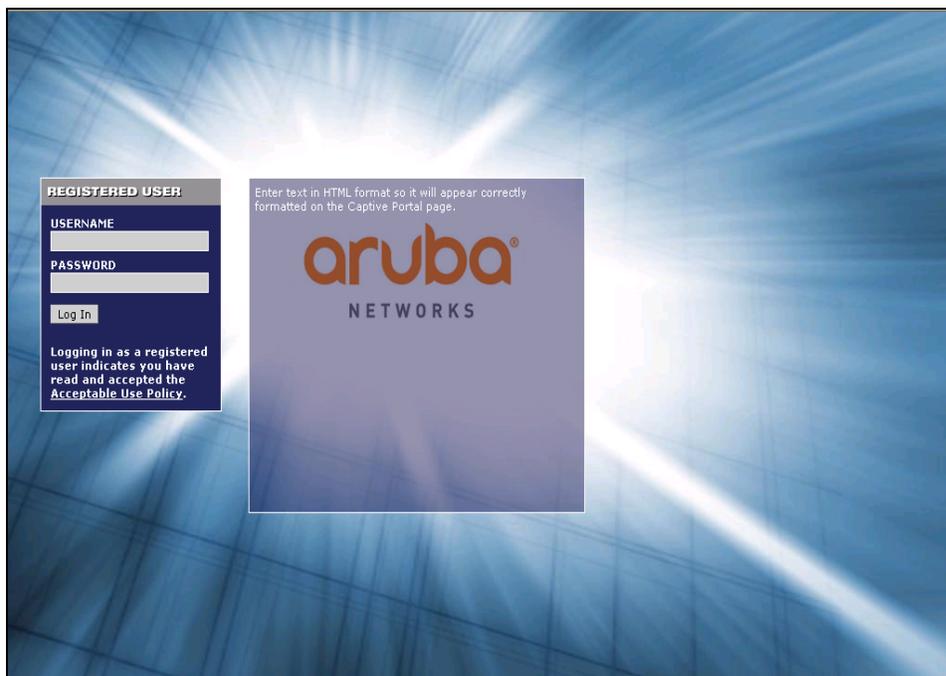
5. To customize the page background:
  - a. Select the **CUSTOM Image** from the **Background** drop-down list.
  - b. Set the background color in the custom page background color field. The color code must a hexadecimal value in the format #hhhhh.
  - c. To view the page background changes, click on the **Preview current settings** link. This displays the Captive Portal page as seen by the users.

**Figure 23** Customizing the Captive Portal Background Page



6. To customize the captive portal background text:
  - a. Enter the text that needs to be displayed in the **Welcome Text (in HTML format)** message box.
  - b. To view the background text changes, click **Preview current settings link** at the bottom on the page. This displays the Captive Portal page as it will be seen by users.

**Figure 24** Customizing the Captive Portal Background Text



## Creating Walled Garden Access

On the Internet, a walled garden typically controls a user's access to web content and services. The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites.

### Creating Walled Garden Access

Walled garden access is needed when an external or internal captive portal is used. A common example could be a hotel environment where unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

Users who do not sign up for Internet service can view "allowed" websites (typically hotel property websites). The website names must be DNS-based (not IP address based) and support the option to define wildcards. This works for client devices with or without HTTP proxy settings.

When a user attempts to navigate to other websites not configured in the white list walled garden profile, the user is redirected back to the login page. In addition, the black listed walled garden profile is configured to explicitly block navigation to websites from unauthenticated users.

### Using the CLI to create walled garden access

This example configures a destination named Mywhite-list and adds the domain names, google.com and cnn.com to that destination. It then adds the destination name Mywhite-list (which contains the allowed domain names google.com and cnn.com) to the white list.

```
(host) (config) #netdestination "Mywhite-list"
(host) (config) #name www.google.com
(host) (config) #name www.cnn.com

(host) (config) #aaa authentication captive-portal default
(host) (Captive Portal Authentication Profile "default") #white-list Mywhite-list
```



---

Ensure not to prefix named netdestination with "http://" or "https://".

---

## Mobility Access Switch Server Certificate

The Mobility Access Switch is designed to provide secure services through the use of digital certificates. A server certificate installed in the Mobility Access Switch verifies the authenticity of the Mobility Access Switch for captive portal.

ArubaOS Mobility Access Switch ships with a demonstration digital certificate. Until you install a customer-specific server certificate in the Mobility Access Switch, this demonstration certificate is used by default for all secure HTTP connections such as captive portal. This certificate is included primarily for the purposes of feature demonstration and convenience and is not intended for long-term use in production networks. Users in a production environment are urged to obtain and install a certificate issued for their site or domain by a well-known certificate authority (CA). You can generate a Certificate Signing Request (CSR) on the Mobility Access Switch to submit to a CA.

You can use the following command to assign a customized captive portal certificate:

```
(host) (config) #web-server
(host) (Web Server Configuration) #captive-portal-cert
(host) (Web Server Configuration) #captive-portal-cert <captive-portal-cert-name>
```



---

For information on how to generate a CSR and to import a certificate into the Mobility Access Switch, see [Obtaining a Server Certificate on page 56](#).

---



Tunneled Node (previously known as Mux) provides the ability to tunnel the ingress packets (via GRE) from an interface on the Mobility Access Switch (Tunneled Node port) to a Mobility Controller (Tunneled Node server). You can use the Tunneled Nodes to allow the Mobility Controller to provide centralized security policy, authentication, and access-control.

This chapter includes the following topics:

- [Important Points to Remember on page 357](#)
- [Tunneled Nodes Overview on page 358](#)
- [Support for Tunneled Node Back-up Server on page 359](#)
- [Creating and Configuring Tunneled Node Profile on page 359](#)
- [Verifying and Monitoring Tunneled Nodes on page 360](#)
- [Verifying and Monitoring the Tunneled Nodes on the Controller on page 360](#)

### Important Points to Remember

- The minimum required version of Mobility Controller ArubaOS is 6.1.2.4.
- Multiple VLAN interfaces are supported in ArubaOS and the GRE tunnel is sourced with the “Switch IP” of the switch.
- Only the following Aruba Mobility Controllers support Tunneled Nodes:
  - 7200 Series Controllers
  - 6000 Series Chassis (M3 module).
  - 3000 Series Controllers
  - 600 Series Controllers
- Ensure that there is an IP reachability between the Mobility Access Switch and the Mobility Controller.
- The Tunneled Node is configured on per-port basis.
- The Tunneled Node is not supported on port-channels. However, Tunneled Node traffic can traverse port-channels.
- The GRE tunnel is created when the interface state transitions to *up* state and the controller is reachable.
- If the interface is up but the Mobility Controller is not reachable, the Mobility Access Switch will retry at every 60 seconds to form a GRE tunnel.
- The Mobility Access Switch allocates an internal VLAN for every Tunneled Node interface. This VLAN is used only for Tunneled Node internal processing. An available internal VLAN ID with the highest number (starting with 4094) is used by default. If you create a new VLAN with the ID that is already assigned to a Tunneled Node, then that VLAN ID is released and then the system allocates the next available VLAN ID. There can be traffic disruption in the mean time.
- Ensure that the VLANs specified in the switching profile and assigned to the Tunneled Node interface is present on the Mobility Controller.
- Only one Tunneled Node profile is supported on the Mobility Access Switch and hence only one Mobility Controller can be used as the Tunneled Node server.
- Spanning tree processing does not take place on the Tunneled Node interface.
- A policer-profile and qos-profile may be applied to a Tunneled Node interface.

- To support Tunneled Node, the Mobility Controller must have an AP and Security bundle license per Mobility Access Switch or ArubaStack.

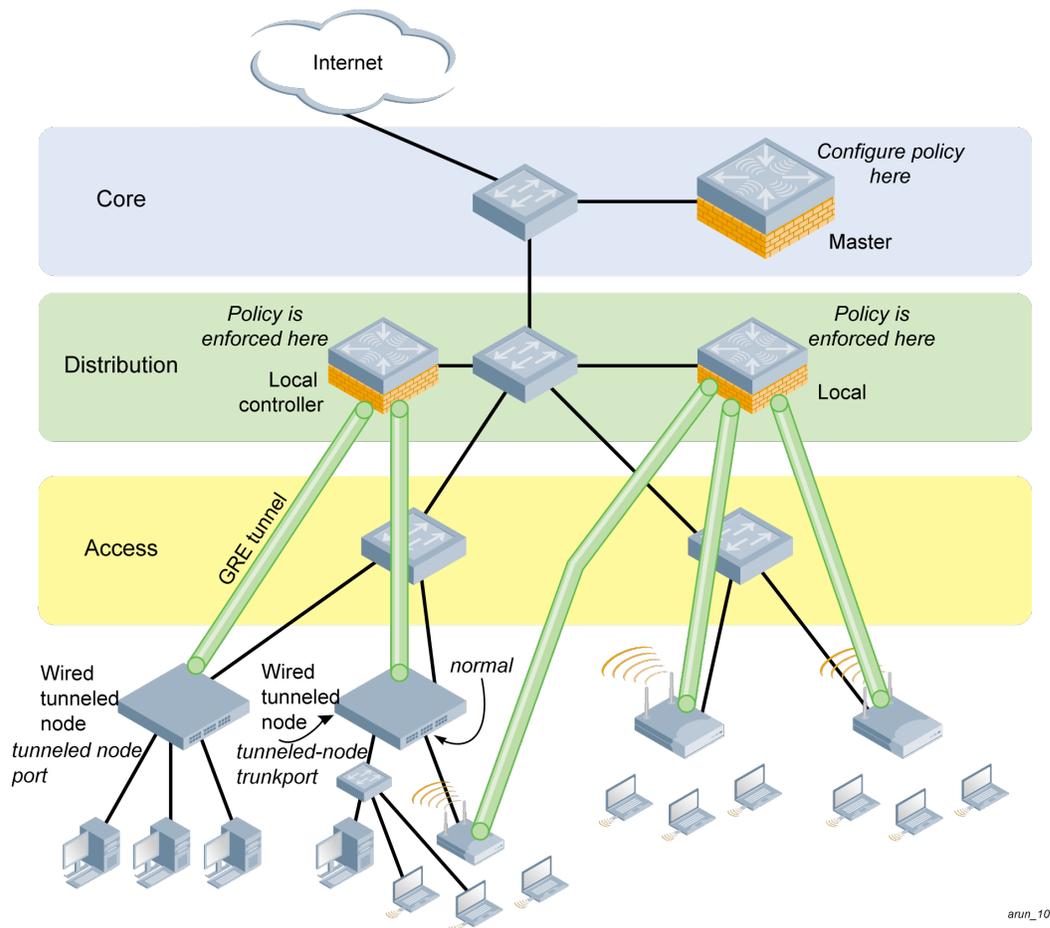
## Tunneled Nodes Overview

This section provides detailed information on the Tunneled Node, also known as a wired Tunneled Node. The Tunneled Node provides access and security using an overlay architecture.

The Tunneled Node connects to one or more client devices at the edge of the network and then establishes a GRE tunnel to the controller. This approach allows the controller to support all the centralized security features, such as IEEE 802.1x authentication, captive-portal authentication, and stateful firewall.

To configure the Tunneled Node, you must specify the IP address of the controller and identify the ports that are to be used as Tunneled Node ports. A tunnel is established between the controller and the Mobility Access Switch for each active Tunneled Node port. [Figure 25](#) shows how the Tunneled Node fits into network operations. Traffic moves through GRE tunnels between the active Tunneled Node ports and the controller. Policies are configured and enforced on the controller. On the controller, you can assign the same policy to Tunneled Node user traffic as you would to any untrusted wired traffic.

**Figure 25** Tunneled Node configuration operation



The Tunneled Node port can also be configured as a trunk port. This allows you to have multiple clients on different VLANs on the trunk port.

## Support for Tunneled Node Back-up Server

ArubaOS provides support for Tunneled Node back-up server by allowing you to configure primary and back-up controllers in the Tunneled Node profile. The Mobility Access Switch keeps checking for the reachability of both primary and the back-up servers configured on the Tunneled Node profile. When the primary controller goes down and if the back-up controller is reachable, the Mobility Access Switch automatically establishes a Tunneled Node between the back-up controller. This ensures that the ports on the Mobility Access Switch do not lose connectivity at any point. The Mobility Access Switch switches back to the primary controller as soon as it finds the primary controller reachable.

## Creating and Configuring Tunneled Node Profile

You can create, configure, view, and apply a Tunneled Node profile to an interface using the following commands:

To create a Tunneled Node Profile:

```
(host) (config) # interface-profile tunneled-node-profile <profile-name>
```

To configure the primary and the back-up server for a Tunneled Node:

```
(host) (config) (Tunneled Node Server profile "<profile-name>") #
 backup-controller-ip <IP-address>
 clone <source>
 controller-ip <IP-address>
 keepalive <1-40>
 mtu <1024-1500>
 no {...}
```

To view a Tunneled Node profile configuration, execute the following command:

```
(host) # show interface-profile tunneled-node-profile tunnell1
Tunneled Node Server profile "tunnell1"
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
```

To apply the Tunneled Node profile to an interface:

```
(host) (config) # interface gigabitethernet <slot/module/port>
 tunneled-node-profile <profile-name>
```



---

Tunneled Node profile must be applied to the interface along with the switching profile.

---



---

For information about how to configure the Tunneled Node server (controller) to use the appropriate Tunneled Node clients, see the appropriate version of the controller User Guide.

---

## Path MTU Discovery

The MTU specified in the Tunneled Node profile must match the path MTU on your network. To determine the correct path MTU between the Tunneled Node client and the controller, use the **ping <ip-address> mtu discovery do size <size>** command. For example, see the following output:

```
(host) # ping 10.13.6.44 mtu_discovery do size 16508
Press 'q' to abort.
```

```

PING 10.13.6.44 (10.13.6.44)
From 10.16.48.21 icmp_seq=1 Frag needed and DF set (mtu = 1500)
From 10.16.48.21 icmp_seq=1 Frag needed and DF set (mtu = 1500)
From 10.16.48.21 icmp_seq=1 Frag needed and DF set (mtu = 1500)
From 10.16.48.21 icmp_seq=1 Frag needed and DF set (mtu = 1500)
From 10.16.48.21 icmp_seq=1 Frag needed and DF set (mtu = 1500)

```

## Verifying and Monitoring Tunneled Nodes

```

(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

```

```

(host)# show tunneled-node config
Tunneled Node Client: Enabled
Tunneled Node Server: 172.16.30.2
Tunneled Node Loop Prevention: Disabled

```



The **show tunneled-node config** command displays the Tunneled Node server IP address of the controller to which Mobility Access Switch is connected at that moment.

```

(host)# show vlan
VLAN CONFIGURATION

VLAN Description Ports
---- -
4088 MUX Internal VLAN GE 0/0/11 TUNNEL-0
<output truncated>

```

## Verifying and Monitoring the Tunneled Nodes on the Controller

```

(host)# show tunneled-node state
Tunneled Node State

```

```

IP MAC s/p state vlan tunnel inactive-time
-- --- --- -
172.16.50.2 00:0b:86:6a:23:80 gigabitethernet0/0/34 complete 400 9 1
172.16.50.2 00:0b:86:6a:23:80 gigabitethernet0/0/11 complete 400 10 1

```

```

(host)# show user-table
Users

```

```

IP MAC Name Role Age (d:h:m) Auth VPN link

172.16.100.25 00:25:90:0c:5b:6e authenticated 00:00:02
172.16.100.252 00:25:90:0c:59:bc authenticated 00:00:02

```

```

AP name Roaming Essid/Bssid/Phy Profile Forward mode Type

tunnel 10 Wired 172.16.50.2:2/24 wired-aaa-profile tunnel Win XP
tunnel 10 Wired 172.16.50.2:2/24 wired-aaa-profile tunnel Win XP
<output truncated>

```

This chapter describes the following topics:

- [Aruba Instant Overview on page 361](#)
- [Aruba AP Integration with Mobility Access Switch on page 361](#)
- [Viewing the Blacklisted MAC Address of the Rogue APs on page 363](#)

## Aruba Instant Overview

Aruba Instant virtualizes Aruba Mobility Controller capabilities on 802.11n access points (APs), creating a feature-rich enterprise-grade wireless LAN (WLAN) that combines affordability and configuration simplicity.

Aruba Instant is a simple, easy to deploy turn-key WLAN solution consisting of one or more access points. An Ethernet port with routable connectivity to the Internet or a self-enclosed network, is used to deploy an Instant Wireless Network. An Instant Access Point (IAP) can be installed at a single site or deployed across multiple geographically-dispersed locations. Designed specifically for easy deployment, and proactive management of networks, Instant is ideal for small customers or remote locations without any on-site IT administrator.

Aruba Instant consists of an Instant Access Point (IAP) and a Virtual Controller (VC). The Virtual Controller resides within one of the access points. In an Aruba Instant deployment only the first IAP needs to be configured. After the first IAP is deployed, the subsequent IAPs will inherit all the required information from the Virtual Controller.

## Supported Devices

The following is a list of Instant devices supported by Aruba:

- IAP-92
- IAP-93
- IAP-104
- IAP-105
- IAP-134
- IAP-135
- IAP-175P/175AC
- RAP-3WN/3WN-US/3WNP/3WNP-US



---

IAP-104, IAP-105, IAP-134, IAP-135, and IAP-175 support an unlimited number of IAPs on Layer 2 networks. IAP -92/93 supports 16 IAPs.

---

For more information on IAP, see the *Instant Access Point 6.2.0.0-3.2 User Guide*.

## Aruba AP Integration with Mobility Access Switch

ArubaOS Mobility Access Switch includes new integration features with Aruba Instant AP (IAP) 3.1 software.

## Aruba AP Integration Features

The Aruba AP integration features save the wastage of power and bandwidth consumed by the rogue APs on the wired network.

Following features are supported only on IAP:

- Rogue AP containment
- GVRP Integration

Following features are supported on both IAP and Campus AP:

- PoE prioritization
- Auto QoS Trust



---

Ensure that LLDP is enabled on ports where IAPs are connected.

---

### Rogue AP Containment

When an IAP detects an AP as rogue, it sends out the MAC Address of the AP to the Mobility Access Switch using the Aruba's proprietary LLDP TLV protocol (MAC information TLV with action as Blacklist). The Mobility Access Switch allows you to enable or disable rogue AP containment and configure the action to be taken on the list of MAC addresses received from IAP.

You can enforce one of the following actions on the MAC addresses received from the IAP using the CLI:

- 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. 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.

This feature is enabled by default.

### Important Points to Remember

Remember the following points about rogue AP containment:

- To enable the rogue AP containment, connect the IAPs to the LLDP enabled MAS ports.
- The rogue AP containment functionality is supported only on trusted ports.

### Configuring Rogue AP Enforcement

Execute the following CLI commands to enable the AP rogue containment:

```
(host) (config) #rogue-ap-containment
(host) (rogue-ap-containment) # enable
```

Use the following command to disable AP rogue enforcement

```
(host) (rogue-ap-containment) #no enable
```

Use the following command to set enforcement action on the MAC addresses received from the IAP

```
(host) (rogue-ap-containment) #action default <auto-recovery- time> | log
```

### Sample Configuration

```
(host) (rogue-ap-containment) #enable
(host) (rogue-ap-containment) #action default auto-recovery-time 50
```

### Verifying Rogue AP Enforcement

Use the following command to verify the rogue AP enforcement:

```
(host) (rogue-ap-containment) #show ap-rogue-enforcement
rogue-ap-containment "default"
```

```

Parameter Value

Enforce Rouge AP Enabled
Action default
Auto Recovery Time 50
```

## GVRP Integration

Configuring GVRP in Mobility Access Switch enables the switch to register/de-register the dynamic VLAN information received from a GVRP applicant such as an IAP in the network. GVRP support also enables the switch to propagate the registered VLAN information to the neighboring bridges in the network.



---

When VLANs are added on WLAN or wired profiles, the VLANs are advertised to the upstream switch using GVRP messages.

---

For information on enabling and configuring GVRP on Mobility Access Switch, see [Enabling and Configuring GVRP Functionality on page 143](#).

## PoE Prioritization

When an IAP is plugged into a PoE enabled port on the Mobility Access Switch, the Mobility Access Switch automatically increases the PoE priority from low (default) to high. This only occurs if the **poe-profile** associated with the given port is using the **poe-factory-initial** profile and the default **poe-priority** has not been manually changed.

For information on PoE and configuring the PoE on MAS, see [Power Over Ethernet on page 107](#).

## Auto QoS Trust

A new option, `aruba-device` is introduced in ArubaOS under the `qos trust` command to automatically trust Aruba IAPs.

```
(host) (gigabitethernet "0/0/0") #qos trust ?
aruba-device Trust DSCP/802.1p for Aruba-Device otherwise
pass-through
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
pass-through Pass-through DSCP/802.1p
```

If an Aruba device is detected using Aruba LLDP TLV, then DSCP is preserved for IP packets and 802.1p for non-IP packets. To use **qos-profile trusted** command for queuing mapping. If `aruba-device` is not detected, then the detected Aruba device falls back to pass-through and preserve sDSCP/802.1p markings.

## Viewing the Blacklisted MAC Address of the Rogue APs

You can use the following command to view details on the blacklisted MAC addresses received from the IAPs:

```
(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: d8:c7:c8:ce:0d:63
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

```

## Viewing Port Errors

The following command displays the state of the interface due to the detection of the blacklisted rogue AP by the MAS:

```
(host) # show port-error-recovery
```

```
Layer-2 Interface Error Information
```

```

Interface Error Error seen time Recovery time
----- -
GE0/0/47 Blacklisted device detected 2012-05-09 20:37:10 (PST) 2012-05-09 20:42:10 (PST)

```

## Recovering Ports Manually

You can use the following command to manually recover the state of the interface:

```
(host) (config) #clear port-error-recovery interface <interface-name>
```

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

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

To clear the port errors on all interfaces execute the following command:

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




---

The interface recovers from the port error state automatically after five minutes and can be re-activated.

---

This chapter describes the Dynamic Port Reconfiguration support on the Mobility Access Switch.

### Device-Group Configuration

Mobility Access Switch 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.



---

In this release, the Mobility Access Switch provides support only for the device-type and Aruba APs that support Aruba's proprietary LLDP TLV.

---

For example, when an Aruba IAP is connected to a port, the device is automatically detected as an AP and the corresponding AP device-group configuration is applied on it. The AP/IAP device configuration can enable quality of service (QoS), security features, POE prioritization, and provide a dedicated VLAN using appropriate profiles on the Mobility Access Switch.

You can enable device-group configuration using the CLI. It is disabled by default.

#### Important Points to Remember

- 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.

#### Managing Device-Group Configuration

To enable Auto device configuration for a device-type, use the following CLI command:

```
(host) (config) #device-group <device-type>
(host) (device-group <device-type>) #enable
```

To administratively bring an interface down on which device-group configuration is applied, use the following CLI command:

```
(host) (device-group <device-type>) #shutdown <interface-list>
```

#### Sample Configuration

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

#### Viewing Device-Group Configuration

Use the following command to view the profiles and parameters configured in a device-group:

```
(host) #show device-group-config <device-type>
(host) #show device-group-config ap
```

```

device-group access-point (N/A)

Parameter Value

Enable Device Config true
Enable Auto LACP false
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 N/A
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

```

Use the following command to view the list of interfaces on which device-group configuration is applied:

```

(host) #show device-group interfaces
Device-Group Config Attached Interfaces

Device Type Interface List

access-point 1/0/22

```

Use the following command to view the details of an interface on which device-group configuration is applied:

```

(host) #show interface-config gigabitethernet 1/0/22
gigabitethernet "1/0/22"

Parameter Value Config Derivation

Interface MSTP Profile default ap_device_prof
Interface Rapid PVST Profile default ap_device_prof
Interface GVRP Profile N/A ap_device_prof
Interface Tunneled Node Profile N/A ap_device_prof
Interface VOIP Profile N/A ap_device_prof
Interface LLDP Profile device_group_default ap_device_prof
Interface PoE Profile device_group_default ap_device_prof
Interface Ethernet Link Profile default ap_device_prof
Interface OAM Profile N/A ap_device_prof
Interface LACP Profile N/A ap_device_prof
Interface QoS Profile N/A ap_device_prof
Interface Policer Profile N/A ap_device_prof
Interface AAA Profile N/A ap_device_prof
Interface Shutdown Disabled ap_device_prof
Interface MTU 1514 ap_device_prof
Interface Ingress ACL N/A ap_device_prof
Interface Egress ACL N/A ap_device_prof
Interface QoS Trust Mode auto ap_device_prof
Interface Description N/A ap_device_prof
Interface Switching Profile default ap_device_prof
Interface Security Profile N/A ap_device_prof
Ingress Port Mirroring Profile N/A ap_device_prof
Egress Port Mirroring Profile N/A ap_device_prof

```

|                                                 |         |                |
|-------------------------------------------------|---------|----------------|
| Static IGMP Multicast Router port for the VLANs | 0       | ap_device_prof |
| Static MLD Multicast Router port for the VLANs  | 0       | ap_device_prof |
| Interface Trusted Mode                          | Enabled | ap_device_prof |
| HSL backup interface                            | N/A     | ap_device_prof |
| HSL preemption mode                             | Off     | ap_device_prof |
| HSL preemption delay                            | 100     | ap_device_prof |



This chapter describes the following topics:

- [Overview on page 369](#)
- [Configuring mDNS packet forwarding on page 369](#)
- [Sample Configuration on page 370](#)

## Overview

Aruba AirGroup is a unique enterprise-class capability that leverages zero configuration networking to allow mobile devices to use services like the Apple AirPrint wireless printer service and the Apple AirPlay streaming service. These services use multicast DNS (mDNS) packets to locate devices and the services that those devices offer.

To ensure Wired and Wireless AirPrint/AirPlay devices can communicate with one another previously required all devices to be on the same Layer-2 network which may not be desirable. Airgroup, which was introduced in ArubaOS 7.2 for the Mobility Access Switch and ArubaOS 6.1.3.4-AirGroup for the Mobility Controller, avoids that need by enabling the ability to just redirect mDNS traffic to a Mobility Controller regardless of VLAN. A simple rule on the MAS is used to redirect all incoming mDNS packets on a port to an L2-GRE tunnel which is then terminated on a Mobility Controller. This allows the Mobility Controller to handle the rest of the AirGroup functionality.

Aruba AirGroup is available in two deployment models; Integrated and Overlay. The location of the mDNS proxy function primarily differentiates the two deployment models. The Mobility Access Switch can interoperate in either deployment model but uses the same underlying features like L2-GRE tunnels used in the Overlay Deployment Model between Mobility Controller.

For more information about Aruba AirGroup, Overlay Deployment Model, and configuration, see the *Aruba AirGroup Deployment Guide*.

## Configuring mDNS packet forwarding

To configure mDNS packet forwarding to an AirGroup Mobility Controller, see the following procedures.

1. Create a switching profile and add VLAN for mDNS traffic.

```
(host) (config) #interface-profile switching-profile <profile-name>
(host) (switching profile) #switchport-mode trunk
(host) (switching profile) #trunk allowed vlan <vlan-list>
```



---

Both ends of an L2-GRE tunnel must carry the same user VLANs.

---

2. Configure an L2-GRE tunnel and apply the switching profile.

ArubaOS Mobility Access Switch supports L2 connectivity through GRE tunnel. L2-GRE tunnel extends VLANs across switches and Aruba controllers.



---

If the MAS and AirGroup controller are on the same L2 network, L2-GRE tunnel is not required.

---

```
(host) (config) #interface tunnel ethernet <tunnel-id>
(host) (Tunnel "tunnel-id") #description <interface-description>
```

```
(host) (Tunnel "tunnel-id") #source-ip <source-tunnel-ip>
(host) (Tunnel "tunnel-id") #destination-ip <destination-tunnel-ip>
(host) (Tunnel "tunnel-id") #switching-profile <profile-name>
(host) (Tunnel "tunnel-id") #keepalive <Tunnel heartbeat interval in seconds (1-86400)>
<Tunnel Heartbeat Retries (1-1024)>
```

### 3. Configure a stateless ACL with mDNS UDP port 5353 redirect rule.

```
(host) (config) #ip access-list stateless <name of the access-list>
(host) (config-stateless)#any any udp 5353 redirect tunnel <L2-GRE-tunnel-ID>
```




---

The Extended-action options appearing in a stateless ACL after `redirect tunnel <ID>` are unsupported.

---

### 4. Apply redirect ACL to either a port or user role.

#### a. Apply redirect ACL to a port.




---

Before you apply redirect ACL to a port, you must create explicit allow rules while configuring mDNS redirect ACL to permit non-mDNS traffic.

---

```
(host) (config) #interface gigabitethernet <slot/module/port>
(host) (gigabitethernet) #ip access-group in <ingress-access-control-list>
```

#### b. Apply redirect ACL to a user role.




---

Add the mDNS redirect ACL to position one of the user-role.

---

```
(host) (config) #user-role <role-name>
(host) (config-role) #access-list stateless <name-of-access-list> position 1
```

## Inter-tunnel flooding

There can be multiple switches from the same L2 network having L2-GRE tunnel terminating at a single controller. This may generate inter-tunnel flooding resulting in loops within the switch network. To avoid this scenario, disable inter-tunnel flooding in the switch and the controller.

```
(host) (config) #interface tunnel ethernet <tunnel-id>
(host) (Tunnel "tunnel-id") #no inter-tunnel-flooding
```

## Sample Configuration

To create a switching profile and add VLAN for mDNS traffic:

```
(host) (config) #interface-profile switching-profile mDNS_vlan_200
(host) (switching profile "mDNS_vlan_200") #switchport-mode trunk
(host) (switching profile "mDNS_vlan_200") #trunk allowed vlan 200
```

To configure an L2-GRE tunnel and apply the switching profile:

```
(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
```

To configure stateless ACL with mDNS redirect rule:

```
(host) (config) #ip access-list stateless mDNS_redirect
(host) (config-stateless-mDNS_redirect)#any any udp 5353 redirect tunnel 1
```

To apply redirect ACL to a port:

```
(host) (config) #interface gigabitethernet 0/0/1
(host) (gigabitethernet "0/0/1") #ip access-group in mDNS_redirect
```

To apply redirect ACL to a user role:

```
(host) (config) #user-role employee
(host) (config-role) #access-list stateless mDNS_redirect position 1
```



ArubaOS for the Mobility Access Switch and ClearPass Policy Manager (CPPM) include support for centralized policy definition and distribution. ArubaOS Mobility Access Switch introduces downloadable roles. By using this feature, when CPPM successfully authenticates a user, the user is assigned a role by CPPM and if the role is not defined on the Mobility Access Switch, the role attributes can also be automatically downloaded.

This chapter contains the following sections:

- [Introduction on page 373](#)
- [Important Points to Remember on page 373](#)
- [Enabling Role-Download on Mobility Access Switch on page 374](#)
- [Deleting Downloadable Roles on page 375](#)
- [Sample Configuration on page 375](#)

## Introduction

In order to provide highly granular per-user level access, user roles can be created when a user has been successfully authenticated. During the configuration of a policy enforcement profile at CPPM, the administrator can define a role that should be assigned to the user after successful authentication. In RADIUS authentication, when CPPM successfully authenticates a user, the user is assigned a role by CPPM and if the role is not defined on the Mobility Access Switch, the role attributes can also be automatically downloaded. Mobility Access Switch also provides support for deleting the downloadable roles.

## Important Points to Remember

- Under [Advanced](#) mode, CPPM does not perform any error checking to confirm accuracy of the role definition. Therefore, it is recommended that you review the role defined in CPPM prior to enabling this feature.
- Attributes that are listed below, herein referred to as whitelist role attributes, can be defined in CPPM. The VLAN attribute under user-role may be referenced, but cannot be defined in CPPM.
  - **netdestination**
  - **netservice**
  - **ip access-list stateless**
  - **ip access-list eth**
  - **ip access-list mac**
  - **ip access-list session**
  - **user-role**
    - **re-authentication interval**
  - **time-range**
    - **periodic**
    - **absolute**
  - **aaa authentication captive-portal**

**NOTE:** Under **aaa authentication captive-portal** profile, **server-group** parameter can be referenced, but cannot be defined in CPPM.

- **qos-profile**

- **policer-profile**
- **interface-profile voip-profile**
- The above attributes that are referred to by a role definition must either be defined within the role definition itself or configured on the Mobility Access Switch before the policy is downloaded.
- In CPPM, two or more attributes (as listed above) should not have the same name. Example below is considered invalid as both the attributes have **test** as the profile/net destination name.

```
qos-profile test
netdestination test
```

- An instance name (name of a whitelist role attribute as stated above) is case-sensitive. Attributes must adhere to the following rules:
  - Should not match any CLI option nested under a command from the whitelist.
  - Should not contain a number or a combination of numbers.
  - Should not contain any periods '.'.
  - Should not contain any spaces.

Example below are considered as invalid configurations and will fail CPPM role download on Mobility Access Switch:

```
netservice 'tcp' tcp 443
```

The first instance of **tcp** is a user-defined field while the second is an operator of the **netservice** command. This violates the first rule.

```
netdestination 'alias'
```

The user-defined name **alias** is also a valid operator of the **netdestination** command. This violates the first rule.

```
netdestination '10.1.5'
```

This user-defined name uses both numbers and periods. This violates the second and third rule.

```
ip access-list stateless '100'
```

This user-defined name uses numbers. This violates the second rule.

```
qos-profile emp role
```

This profile name **emp role** contains spaces. This violates the fourth rule.

It is recommended that some naming convention similar to the CamelCase (mixture of upper and lower case letters in a single word) be used to avoid collisions with the CLI options in the role description.

## Enabling Role-Download on Mobility Access Switch

You can enable role download using the CLI or WebUI.

### Using the WebUI

1. Navigate to the **Configuration > Authentication > Profiles** tab.
2. Select an AAA profile.
3. Select **Enabled** from the **Role Download** drop-down list.

### Using the CLI

```
(host) (config) #aaa profile <profile-name>
(host) (AAA profile) #download-role
```

## Deleting Downloadable Roles

Starting from ArubaOS 7.4.1, Mobility Access Switch provides support for deleting downloadable roles from the CPPM server if the following conditions are met:

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

Execute the following CLI command for deleting a role downloaded from the CPPM server:

```
(host) #downloadable-role-delete <role>
```



---

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>**

---

You can delete downloadable roles using the CLI.

### Using the CLI

The following sample CLI command deletes the abc\_profile-3023-8 user role:

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

## Sample Configuration

The following example shows the configuration details to integrate CPPM server with Mobility Access Switch to automatically download roles.

### CPPM Server Configuration

#### Adding a Device

1. From the **Configuration > Network > Devices** page, click the **Add Device** link.
2. On the **Device** tab, enter the **Name, IP or Subnet Address**, and **RADIUS Shared Secret** fields.  
Keep the rest of the fields as default.
3. Click **Add**.

The fields are described in [Figure 26](#) and [Table 42](#).

**Figure 26** *Device Tab*

**Table 42:** *Device Tab*

| Container            | Description                                                                        |
|----------------------|------------------------------------------------------------------------------------|
| Name                 | Specify the name or identity of the device.                                        |
| IP or Subnet Address | Specify the IP address or subnet (example 10.1.1.1/24) of the device.              |
| RADIUS Shared Secret | Enter and confirm a Shared Secret for each of the two supported request protocols. |

### Adding Enforcement Profile

1. From **Configuration > Enforcement > Profiles** page, click **Add Enforcement Profile**.
2. On the **Profile** tab, select **Aruba Downloadable Role Enforcement** from the **Template** drop-down list.
3. Enter the **Name** of the enforcement profile.
4. From the **Role Configuration Mode**, select **Standard** or **Advanced**.  
Keep the rest of the fields as default.
5. Click **Next**.  
For the rest of the configuration, see [Standard Role Configuration Mode](#) or [Advanced Role Configuration Mode](#).

The fields are described in [Figure 27](#) and [Table 43](#).

**Figure 27** Enforcement Profiles Page

Configuration » Enforcement » Profiles » Add Enforcement Profile

### Enforcement Profiles

**Profile** | Role Configuration | Summary

Template: Aruba Downloadable Role Enforcement

Name: Enforcement\_Profile\_1

Description:

Type: RADIUS

Action:  Accept  Reject  Drop

Device Group List:

--Select--

Remove  
View Details  
Modify

Role Configuration Mode:  Standard  Advanced

**Table 43:** Enforcement Profiles Page

| Container               | Description                                                                                                                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Template                | Policy Manager comes pre-packaged with several enforcement profile templates. In this example, select <b>Aruba Downloadable Role Enforcement</b> - RADIUS template that can be filled with user role definition to create roles that can be assigned to users after successful authentication. |
| Name                    | Specify the name of the enforcement profile.                                                                                                                                                                                                                                                   |
| Role Configuration Mode | Standard—Configure enforcement profile role using standard mode.<br>Advanced—Configure enforcement profile role using advanced mode.                                                                                                                                                           |

### Standard Role Configuration Mode

- Under **Role Configuration** tab, enter the parameters based on [Table 44](#).
- Click **Save**.

The fields are described in [Figure 28](#) and [Table 44](#).

**Figure 28** Enforcement Profiles Role Configuration Tab

Configuration » Enforcement » Profiles » Add Enforcement Profile

### Enforcement Profiles

**Profile** | Role Configuration | Summary

Captive Portal Profile: cap-prof-1 [Add Captive Portal Profile](#)

Policer Profile: cpol [Add Policer Profile](#)

QoS Profile: qos-prof [Add QoS Profile](#)

VoIP Profile: voip-prof [Add VoIP Profile](#)

Reauthentication Interval Time (0-4096): 15 minutes

VLAN To Be Assigned (1-4094): 101

NetService Configuration: [Manage NetServices](#)

NetDestination Configuration: [Manage NetDestinations](#)

Time Range Configuration: [Manage Time Ranges](#)

ACL:

ether-acl [Ethertype]  
macacl-1 [MAC]  
MANAGEMENT-SSH-ACL-SESSION-B [Session]  
allow\_all [Stateless]

Move Up  
Move Down  
Remove

[Add Stateless Access Control List](#)  
[Add Session Access Control List](#)  
[Add EtherType/MAC Access Control List](#)

ACL Type: ACL Name:  
EtherType

Add

User Role Configuration: Check Summary tab for generated Role Configuration

**Table 44: Enforcement Profiles Role Configuration Tab**

| Container                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Captive Portal Profile                  | This parameter defines a Captive Portal authentication profile.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Policer Profile                         | This parameter defines a policer profile to manage the transmission rate of a class of traffic based on user-defined criteria.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| QoS Profile                             | This parameter defines a QoS profile to assign Traffic-Class/Drop-Precedence, Differentiated Services Code Point (DSCP), and 802.1p values to an interface or policer profile of a Mobility Access Switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| VoIP Profile                            | This parameter defines a VoIP profile that can be applied to any interface, interface group, or a port-channel of a Mobility Access Switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Reauthentication Interval Time (0—4096) | Time interval in minutes after which the client is required to reauthenticate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| VLAN To Be Assigned (0—4094)            | Identifies the VLAN ID to which the user role is mapped.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| NetService Configuration                | Defines an alias for network protocols. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| NetDestination Configuration            | Defines an alias for an IPv4 network host, subnet mask, or a range of addresses. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Time Range Configuration                | The following time-range can be defined:<br><b>Periodic</b> —Specifies a recurring time range. Specify the start and end time and Daily, Weekday, Weekend, or the day of the week.<br><b>Absolute</b> —Specifies an absolute time range, with a specific start and/or end time and date.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ACL                                     | Adds the following Access Control List (ACL):<br><b>Ethertype</b> —Defines an Ethertype ACL.<br>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.<br><b>MAC</b> —Defines a MAC ACL.<br>MAC ACLs allow filtering of non-IP traffic. This ACL filters on a specific source MAC address or range of MAC addresses.<br><b>Session</b> —Defines a session ACL.<br>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.<br><b>Stateless</b> —Defines a stateless ACL.<br>A stateless ACL statically evaluates packet contents. The traffic in the reverse direction is allowed unconditionally.<br><b>NOTE:</b> In CPPM, do not configure the <b>Next Hop</b> parameter under Stateless ACL configuration. |
| User Role Configuration                 | See the <b>Summary</b> tab for auto-generated Role Configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Advanced Role Configuration Mode

1. On the **Attributes** tab, select **Radius:Aruba** from the **Type** drop-down list.
2. From the **Name** drop-down list, select **Aruba-CPPM-Role**.
3. In the **Value** field, enter the attribute for the downloadable-role.
4. Click the save icon to save the attribute.
5. Click **Save** to save the enforcement profile.

The fields are described in [Figure 29](#) and [Table 45](#).

**Figure 29** Enforcement Profiles Attributes Tab

**Table 45:** Enforcement Profiles Attributes Tab

| Container | Description                                                                                                                                                                     |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type      | Type is any RADIUS vendor dictionary that is pre-packaged with Policy Manager, or imported by the Administrator. This field is pre-populated with the dictionary names.         |
| Name      | Name is the name of the attribute from the dictionary selected in the Type field. The attribute names are pre-populated from the dictionary.                                    |
| Value     | Value is attribute for the downloadable role. You can enter free-form text to define the role and policy.<br><b>NOTE:</b> The maximum limit for free form text is 16,000 bytes. |

## Adding Enforcement Policy

1. From **Configuration > Enforcement > Policies** page, click **Add Enforcement Policy**.
2. On the **Enforcement** tab, enter the name of the enforcement policy.
3. From the **Default Profile** drop-down list, select **[Deny Access Profile]**.  
Keep the rest of the fields as default.
4. Click **Next**.

The fields are described in [Figure 30](#) and [Table 46](#).

**Figure 30** Enforcement Policies Enforcement Tab

**Table 46:** Enforcement Policies Enforcement Tab

| Container       | Description                                                                                                                                                                                                                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name            | Specify the name of the enforcement policy.                                                                                                                                                                                                                                                                                                |
| Default Profile | An Enforcement Policy applies Conditions (roles, health, and time attributes) against specific values associated with those attributes to determine the Enforcement Profile. If none of the rules matches, Policy Manager applies the Default Profile.<br>See <a href="#">Adding Enforcement Profile on page 376</a> to add a new profile. |

- On the **Rules** tab, click **Add Rule**.
- On the **Rules Editor** pop-up, select the appropriate values in the **Conditions** section and click the save icon.
- In the **Enforcement Profiles** section, select the RADIUS enforcement profile that you created in step [Adding Enforcement Profile on page 376](#) from the **Profile Names** drop-down list.
- Click **Save**.

The fields are described in [Figure 31](#) and [Table 47](#).

**Figure 31** Enforcement Policies Rules Editor

**Table 47: Enforcement Policies Rules Editor**

| Container     | Description                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type          | The rules editor appears throughout the Policy Manager interface. It exposes different namespace dictionaries depending on Service type. When working with service rules, you can select <b>Authentication</b> namespace dictionary |
| Name          | Drop-down list of attributes present in the selected namespace. In this example, select <b>Source</b> .                                                                                                                             |
| Operator      | Drop-down list of context-appropriate (with respect to the attribute) operators. In this example, select <b>EQUALS</b> .                                                                                                            |
| Value         | Drop-down list of the Authentication source database. In this example, select <b>[Local User Repository]</b> .                                                                                                                      |
| Profile Names | Name of the RADIUS enforcement profile.                                                                                                                                                                                             |

### Adding Services

1. From the **Configuration > Services** page, click the **Add Service** link.
2. On the **Service** tab, select **802.1X Wired** from the **Type** drop-down-list.
3. In the **Name** field, enter the name of the service.  
Keep the rest of the fields as default.
4. Click **Next**.

The fields are described in [Figure 32](#) and [Table 48](#).

**Figure 32 Service Tab**

Configuration » Services » Add

### Services

Service | Authentication | Roles | Enforcement | Summary

Type: 802.1X Wired

Name: Service\_1

Description: 802.1X Wired Access Service

Monitor Mode:  Enable to monitor network access without enforcement

More Options:  Authorization  Posture Compliance  Audit End-hosts  Profile Endpoints

Service Rule

Matches  ANY or  ALL of the following conditions:

| Type               | Name          | Operator   | Value                                                  |
|--------------------|---------------|------------|--------------------------------------------------------|
| 1. Radius:IETF     | NAS-Port-Type | EQUALS     | Ethernet (15)                                          |
| 2. Radius:IETF     | Service-Type  | BELONGS_TO | Login-User (1), Framed-User (2), Authenticate-Only (8) |
| 3. Click to add... |               |            |                                                        |

**Table 48: Service Tab**

| Container | Description                                                                                            |
|-----------|--------------------------------------------------------------------------------------------------------|
| Type      | Select the desired service type from the drop down menu. In this example, select <b>802.1X Wired</b> . |
| Name      | Specify the name of the service.                                                                       |

- On the **Authentication** tab, select **[Local User Repository] [Local SQL DB]** from the **Authentication Sources** drop-down list.

Keep the rest of the fields as default.

- Click **Next** twice.

The fields are displayed in [Figure 33](#).

**Figure 33 Authentication Tab**

Configuration » Services » Add

### Services

Service Authentication Roles Enforcement Summary

Authentication Methods:

- [EAP PEAP]
- [EAP FAST]
- [EAP TLS]
- [EAP TTLS]
- [EAP MSCHAPv2]

--Select to Add--

Authentication Sources:

- [Local User Repository] [Local SQL DB]

--Select to Add--

Strip Username Rules:  Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

- On the **Enforcement** tab, select the enforcement policy that you created in step [Adding Enforcement Policy on page 379](#) from the **Enforcement Policy** drop-down list.

Keep the rest of the fields as default.

- Click **Save**.

The fields are displayed in [Figure 34](#).

**Figure 34** Enforcement Tab

For more configuration details on CPPM, refer to the *ClearPass Policy Manager 6.2 User Guide*.

## Mobility Access Switch Configuration

### Configuring CPPM Server on Mobility Access Switch

```
(host) (config) #aaa authentication-server radius cppm_server
(host) (RADIUS Server "cppm_server") #host <ip_address_of_cppm_server>
(host) (RADIUS Server "cppm_server") #key <shared_secret>
```

### Configuring Server Group to include CPPM Server

```
(host) (config) #aaa server-group cppm_grp
(host) (Server Group "cppm_grp") #auth-server cppm_server
```

### Configuring 802.1X Profile

```
(host) (config) #aaa authentication dot1x cppm_dot1x_prof
```

### Configuring AAA Profile

```
(host) (config) #aaa profile cppm_aaa_prof
(host) (AAA Profile "cppm_aaa_prof") #authentication-dot1x cppm_dot1x_prof
(host) (AAA Profile "cppm_aaa_prof") #dot1x-server-group cppm_grp
(host) (AAA Profile "cppm_aaa_prof") #download-role
```

### Show AAA Profile

```
(host) #show aaa profile cppm_aaa_prof
```

```
AAA Profile "cppm_aaa_prof"
```

```

Parameter Value

Initial role logon
MAC Authentication Profile N/A
MAC Authentication Default Role guest
MAC Authentication Server Group default
802.1X Authentication Profile cppm_dot1x_prof
802.1X Authentication Default Role guest
802.1X Authentication Server Group cppm_grp
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 |

## CPPM Server Authentication

Starting from CPPM 6.4.3, the Mobility Access Switch requires to provide the CPPM server admin credentials to download roles from the CPPM server. To facilitate this, a new CLI command is introduced in ArubaOS 7.4.0.2. Using this command, you can configure the CPPM admin username/password under **authentication-server** definition on the Mobility Access Switch.

### Configuring CPPM Server Credentials

Use the following command to configure CPPM username/password:

```
(host) (config) #aaa authentication-server radius <server-name>
(host) (RADIUS Server "<server-name>") #cppm username <username> password <password>
```

### Sample Configuration

```
(host) (config) #aaa authentication-server radius cppm1
(host) (RADIUS Server "cppm1") #host 1.1.1.1
(host) (RADIUS Server "cppm1") #key key123
(host) (RADIUS Server "cppm1") #cppm username admin password password123
(host) (RADIUS Server "cppm1") #exit
```

### Verifying Configuration

The following **show** command displays the CPPM server credentials configured on the Mobility Access Switch:

```
(host) (config) #show aaa authentication-server radius cppm1
RADIUS Server "cppm1" (N/A)

Parameter Value

Host 1.1.1.1
Key *****
CPPM credentials admin/*****
Auth Port 1812
Acct Port 1813
Retransmits 3
Timeout 5 sec
NAS ID N/A
NAS IP N/A
Source intf N/A
Use MD5 Disabled
Use IP address for calling station ID Disabled
Mode Enabled
```

Wireless networks can use virtual private network (VPN) connections to further secure wireless data from attackers.



---

The Mobility Access Switch supports only Site-to-Site VPN configurations in tunnel mode and does not support IPsec transport mode.

---



---

There is no Equal Cost Multiple Path (ECMP) support over VPN.

---

## Site-to-Site VPN

Site-to-site VPNs allow networks (for example, a branch office network) to connect to other networks (for example, a corporate network). Unlike a remote access VPN, hosts in a site-to-site VPN do not run VPN client software. All traffic for the other network is sent and received through a VPN gateway which encapsulates and encrypts the traffic.

The following IKE authentication methods are supported for site-to-site VPNs:

- Preshared Key authentication
- Certificate authentication. You can configure a RSA server certificate and a CA certificate for each site-to-site VPN IPsec map configuration. If you are using certificate-based authentication, the peer must be identified by its certificate subject-name distinguished name (for deployments using IKEv2) or by the peer's IP address (for IKEv1).



---

Certificate-based authentication is supported for site-to-site VPN between two Aruba devices with static IP addresses. Additionally, Certificate-based authentication is also supported with dynamic IP addresses when IKEv2 is used.

---

## Selecting an IKE protocol

Mobility Access Switches running ArubaOS 7.2 and later support both IKEv1 and the newer IKEv2 protocol to establish IPsec tunnels. IKEv2 is simpler, faster, and a more reliable protocol than IKEv1.

If your IKE policy uses IKEv2, you should be aware of the following caveats when you configure your VPN:

- ArubaOS does not support separate pre-shared keys for both directions of an exchange; the same pre-shared key must be used by both peers. ArubaOS does not support mixed authentication with both pre-shared keys and certificates; each authentication exchange requires a single authentication type. (For example, if a Site-to-Site peer authenticates with a pre-shared key, the other peer must also authenticate with a pre-shared key.)
- ArubaOS does not support IKEv2 mobility (MOBIKE), Authentication Headers (AH) or IP Payload Compression Protocol (IPComp).



---

In this release of Mobility Access Switch, site-to-site tunnels are not coming up using Internet Key Exchange (IKEv1) protocol when SHA1-96 is used as the hash algorithm. As a workaround, use (SHA1-160) as the hash algorithm.

---

## Supported IKE Modes

ArubaOS supports site-to-site VPNs using IKEv2 or IKEv1 Main-mode/Aggressive-mode. By default, site-to-site VPN uses IKEv1 Main-mode with Pre-Shared-Keys to authenticate the IKE security association (SA). This method requires static IP addresses between the peers and therefore will not work for dynamically addressed peers.

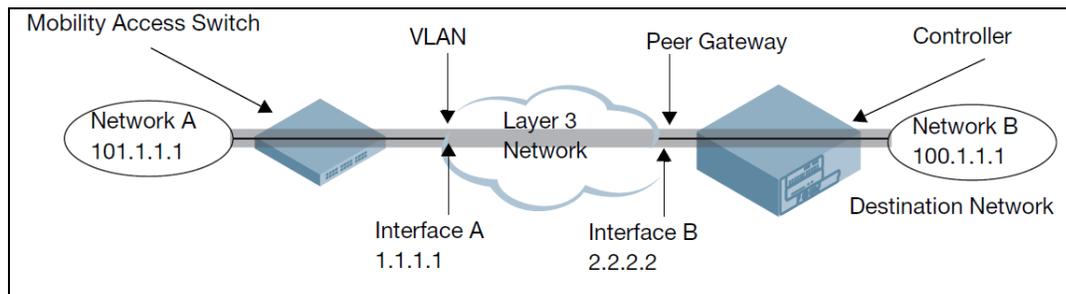
To support site-site VPN with dynamically addressed devices, you must use IKEv1 Aggressive-mode or IKEv2 with certificates. The VPN endpoint with a dynamic IP address must be configured to be the initiator and the endpoint with the static IP address must be configured as the responder.

Aruba Mobility Access Switch and Mobility Controllers can use IKEv1 or IKEv2 to establish a site-to-site VPN between another Mobility Access Switch or Mobility Controller or between that Mobility Access Switch and third party device. Note, however, that only Aruba devices (Mobility Access Switches or Mobility Controllers) and devices running Windows 2008 Server or Strongswan 4.3 support IKEv2 authentication.

## VPN Topologies

You must configure VPN settings on the devices at both the local and remote sites. In the following figure, a VPN tunnel connects Network A to Network B across the Internet.

**Figure 35** Site-to-Site VPN Configuration Components



To configure the VPN tunnel on Mobility Access Switch, you need to configure the following:

- The source network (Network A).
- The destination network (Network B).
- The VLAN or loopback interface on the Mobility Access Switch connected to the Layer-3 network (Interface A in the [Figure 35](#)).
- The peer gateway address, which is the IP address of the Mobility Controller's interface connected to the Layer-3 network (Interface B in the [Figure 35](#)).

## Configuring Site to Site VPN

To configure a site-to-site VPN with a static IP Mobility Access Switch device and static IP Mobility Controller using IKEv1, execute the following commands:

```
(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) #interface [loopback <loopback-number>|vlan <vlan-id>]
(host) (config-ipsec-map) #version v1
(host) (config-ipsec-map) #pre-connect enable|disable
```

For multiple subnets in the destination, you can add routes to the subnets and map them to the existing IPsec tunnel in the IP profile. To add routes to the subnets, execute the following commands:

```
(host) (config) #ip-profile
(host) (ip-profile) #route <dest-network> <netmask> ipsec <ipsec-map>
```

For certificate authentication:

```
(host) (config) #set ca-certificate <cacert-name>
(host) (config) #set server-certificate <cert-name>
(host) (config) #crypto isakmp policy <priority>
 (host) (config-isakmp) #encryption {3des|aes128|aes192|aes256|des}
 (host) (config-isakmp) #version v1
 (host) (config-isakmp) #authentication rsa-sig
 (host) (config-isakmp) #group 1|2
 (host) (config-isakmp) #hash {md5|sha|sha1-96}
 (host) (config-isakmp) #lifetime <seconds>
```

For pre-shared key authentication:

```
(host) (config) #crypto-local isakmp key <key> address <ipaddr> netmask <mask>
(host) (config) #crypto isakmp policy <priority>
 (host) (config-isakmp) #encryption {3des|aes128|aes192|aes256|des}
 (host) (config-isakmp) #version v1
 (host) (config-isakmp) #authentication pre-share
 (host) (config-isakmp) #group {1|2}
 (host) (config-isakmp) #hash {md5|sha|sha1-96}
 (host) (config-isakmp) #lifetime <seconds>
```

To configure site-to-site VPN with a static Mobility Access Switch and a dynamically addressed Mobility Controller 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 [loopback <loopback-number>|vlan <vlan-id>]
 (host) (config-ipsec-map) #pre-connect [enable|disable]
```

For the Pre-shared-key:

```
crypto-local isakmp key <key> address <ipaddr> netmask 255.255.255.255
```

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

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

For the Pre-shared-key:

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

For a static IP Mobility Access Switch 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) #vlan <id>
```

For the Pre-shared-key for All FQDNs:

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

## Configuration Examples

### Main-Mode

The following example shows a Mobility Access Switch with static IP address and Mobility Controller with a static IP address.

Mobility Access Switch:

```
(host) (config) #crypto-local ipsec-map Test1 1
(host) (config-ipsec-map) #src-net 1.1.1.1 255.255.255.0
(host) (config-ipsec-map) #dst-net 2.2.2.2 255.255.255.0
(host) (config-ipsec-map) #peer-ip 159.116.110.10
(host) (config-ipsec-map) #local-fqdn sample@arubanetworks.com
(host) (config-ipsec-map) #interface vlan 62
(host) (config-ipsec-map) #version v2
(host) (config-ipsec-map) #pre-connect enable
(host) (config-ipsec-map) #exit
(host) (config) #crypto-local isakmp key 12345678 159.116.110.10 netmask 255.255.255.255
```

For other subnets in the destination, add routes to the subnets and map them to the existing IPsec tunnel in the IP profile as given in the following example:

```
(host) (config) #ip-profile
(host) (ip-profile) #route 3.1.1.0 255.255.255.0 ipsec tn-vpn 2
```

Controller:

```
(host) (config) #crypto-local ipsec-map Test2 1
(host) (config-ipsec-map) #src-net 2.2.2.0 255.255.255.0
(host) (config-ipsec-map) #dst-net 1.1.1.0 255.255.255.0
(host) (config-ipsec-map) #peer-ip 0.0.0.0
(host) (config-ipsec-map) #peer-fqdn fqdn-id sample@arubanetworks.com
(host) (config-ipsec-map) #vlan 1
(host) (config-ipsec-map) #version v2
(host) (config-ipsec-map) #trusted enabled
(host) (config-ipsec-map) #exit
(host) (config) #crypto-local isakmp key 12345678 fqdn sample@arubanetworks.com
```

### Verifying VPN Tunnel Configuration

You can use the following CLI commands to verify the VPN configuration.

- show datapath session
- show datapath tunnel
- show crypto ipsec sa
- show crypto isakmp sa

Use the following command to verify if the VPN is established :

```
(host) # show datapath session
```

```
Datapath Session Table Entries
```

```

```

```
Flags: F - fast age, S - src NAT, N - dest NAT
```

```
D - deny, R - redirect, Y - no syn
```

```
H - high prio, P - set prio, T - set ToS
```

```
C - client, M - mirror, V - VOIP
```

```
Q - Real-Time Quality analysis
```

```
I - Deep inspect, U - Locally destined
```

```
E - Media Deep Inspect, G - media signal
```

```
u - User Index
```

```
Source IP/ Destination IP Prot SPort DPort Cntr Prio ToS Age Destination TAge
Destination MAC
```

```

```

```

62.62.62.10 159.116.110.10 17 500 500 0/0 0 0 1 local 16d
159.116.110.10 62.62.62.10 17 500 500 0/0 0 0 2 local 16d
UsrIdx UsrVer Flags

2 2 FC
0 0 F

```

Use the following command to verify the incoming and outgoing packets over the VPN tunnel:

**(host) # show datapath tunnel**

Datapath Tunnel Table Statistics

```

Current Entries 6
Pending Deletes 0
High Water Mark 6
Maximum Entries 8191
Total Entries 6
Allocation Failures 0
Max link length 1
Datapath Tunnel Table Entries

```

Flags: E - Ether encap, I - Wi-Fi encap, R - Wired tunnel, F - IP fragment OK  
W - WEP, K - TKIP, A - AESCCM, G - AESGCM, M - no mcast src filtering  
S - Single encrypt, U - Untagged, X - Tunneled node, 1(cert-id) - 802.1X Term-PEAP  
2(cert-id) - 802.1X Term-TLS, T - Trusted, L - No looping, d - Drop Bcast/Mcast,  
D - Decrypt tunnel, a - Reduce ARP packets in the air, e - EAPOL only  
C - Prohibit new calls, P - Permanent, m - Convert multicast  
n - Don't convert IPv6 Mcast RA to Ucast, s - Split tunnel

| #  | Source         | Destination    | Prt | Type | MTU  | VLAN | Acls      | BSSID |
|----|----------------|----------------|-----|------|------|------|-----------|-------|
| 67 | SPIFAED5E00out | 159.116.110.10 | 50  | IPSE | 1500 | 0    | routeDest | 0000  |
| 68 | SPIE8812300 in | 62.62.62.10    | 50  | IPSE | 1500 | 0    | routeDest | 0000  |

```

Decaps Encaps Heartbeats Cpu QSz Flags

0 0
0 0

```

To view the ISAKMP information, use the following command:

**(host) #show crypto isakmp sa**

ISAKMP SA Active Session Information

```

Initiator IP Responder IP Flags Start Time Private IP

62.62.62.10 159.116.110.10 i-v2-p Aug 1 05:04:55 -

```

Flags: i = Initiator; r = Responder  
m = Main Mode; a = Agressive Mode v2 = IKEv2  
p = Pre-shared key; c = Certificate/RSA Signature; e = ECDSA Signature  
x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled  
3 = 3rd party AP; C = Campus AP; R = RAP, A = Aruba VPN  
V = VIA; S = VIA over TCP  
Total ISAKMP SAs: 1

To view the IPsec information, use the following command:

**(host) #show crypto ipsec sa**

IPSEC SA (V2) Active Session Information

```

Initiator IP Responder IP SPI(IN/OUT) Flags Start Time Inner IP

62.62.62.10 159.116.110.10 e8812300/faed5e00 T2 Aug 1 05:04:55 -

```

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap  
L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2  
Total IPSEC SAs: 1

## Aggressive-Mode with Tunneled Node over VPN

ArubaOS Mobility Access Switch also adds support for Tunneled Node over VPN. This allows you to provide all the centralized security policy, authentication, and access-control from a tunneled node over a VPN connection.

The following example shows site-to-site VPN configured between Mobility Access Switch with a dynamic IP address and Mobility Controller with a static IP address. In this example, the Mobility Access Switch is configured to be the initiator of IKE Aggressive-mode and the Mobility Controller is the responder of IKE Aggressive-mode.

1. Establish a VPN connection between the Mobility Access Switch and the Mobility Controller.

Mobility Access Switch:

```
(host) (config) #crypto-local ipsec-map here-there-vpn 100
(host) (config-ipsec-map) #src-net 101.1.1.1 255.255.255.0
(host) (config-ipsec-map) #dst-net 100.1.1.1 255.255.255.0
(host) (config-ipsec-map) #peer-ip 2.2.2.2
(host) (config-ipsec-map) #local-fqdn test@abc.com
(host) (config-ipsec-map) #interface vlan 2
(host) (config) #crypto-local isakmp key secret address 2.2.2.2 netmask 255.255.255.255
```

Mobility Controller:

```
(host) (config) #crypto-local ipsec-map there-here-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 0.0.0.0
(host) (config-ipsec-map) #peer-fqdn fqdn-id test@abc.com
(host) (config-ipsec-map) #vlan 2
(host) (config) #crypto-local isakmp key secret fqdn test@abc.com
```

2. Establish a Tunneled Node connection between the Mobility Access Switch and Mobility Controller. Ensure that the Mobility Access Switch's switch IP is in the IPSec source network and the Mobility Controller's IP address is in the IPSec destination network.

```
(host) (config) (Tunneled Node Server profile "tunnell")#
(host) (config) #controller-ip 100.1.1.1
(host)# show interface-profile tunneled-node-profile tunnell
Tunneled Node Server profile "tunnell"
Parameter Value

Controller IP Address 100.1.1.1
Keepalive timeout in seconds 10
MTU on path to controller 1400
```

3. Apply the tunneled node profile to an interface.

## Site-to-Site VPN Interface Survivability

The Mobility Access Switch provides support for a standby VPN uplink when the primary VPN uplink interface goes down. Whenever the primary uplink is detected to be down, the standby uplink is used to establish VPN.



---

Ensure that you enable Route monitoring on both the primary and standby uplinks of the Mobility Access Switch to determine the status of the uplinks. For more information on Route Monitoring, see [Route Monitoring on page 204](#).

---

Mobility Access Switch also provides support for preemption so that when the primary VPN uplink is found to be up while on the standby uplink, it automatically re-establishes VPN connection using the primary uplink. Preemption is enabled by default. It is applicable only for the standby configuration. You can choose to disable or enable it back.



---

VPN survivability is supported with IKE version 2 only.

---

## Configuring Standby Uplink for VPN

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

```
(host) (config) #crypto-local ipsec-map <map-name> <map-number>
(host) (config-ipsec-map) #standby-interface vlan <ipsec-map-standby-vlan-id>
```

### Sample Configuration

```
(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
```

### Verifying Standby Configuration

You can use the following command to verify the standby VPN configuration on the Mobility Access Switch:

```
(host) #show running-config| begin ipsec-map
crypto-local ipsec-map mapA 10
 peer-ip 20.1.1.2
 local-fqdn test.arubanetworks.com
 interface vlan 2
 standby-interface vlan 4
 src-net 4.1.1.0 255.255.255.255
 dst-net 3.1.1.0 255.255.255.255
 set transform-set "default-transform"
 pre-connect disable
 force-natt disable
 !
```

Use the following command to view the uplink VLAN interface in use:

```
(host) #show crypto-local ipsec-map
Crypto Map Template "mapA" 10
 IKE Version: 2
 IKEv2 Policy: 10
 Lifetime: 7200] seconds, no volume limit
 PFS (Y/N): N
 Transform sets={ default-transform}
 Peer gateway: 20.1.1.2
 Local FQDN: test.arubanetworks.com
 Interface: vlan 2
 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
```

The following examples display the status of the primary and the standby VPN uplink interface before and after a switch-over. The **Probe** column in the following examples indicates the status of the uplink:

```
(host) #show ip interface brief
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 2    | 10.1.1.1 / 255.255.255.0 | Up    | Up       | U     |       |
| vlan 4    | 10.1.2.1 / 255.255.255.0 | Up    | Up       | U     |       |

```
(host) #show ip interface brief
```

```
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 2    | 10.1.1.1 / 255.255.255.0 | Up    | Up       | D     |       |
| vlan 4    | 10.1.2.1 / 255.255.255.0 | Up    | Up       | U     |       |

The following command displays that the VPN is on the standby uplink after the switchover:

```
(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
```

## Default Route to VPN

A branch office Mobility Access Switch has VPN tunnel which terminates on a Firewall. Any client non-corporate traffic from Mobility Access Switch is forwarded to the firewall through the VPN tunnel. This requires a default gateway route on Mobility Access Switch pointing to a VPN tunnel.

## Configuring Default Route to VPN

You can use the following command to configure the default route to a VPN tunnel:

```
(host) (config) #crypto-local ipsec-map <map-name> <map-number>
```

```
(host) (config-ipsec-map) #dst-net 0.0.0.0 0.0.0.0
```

## Sample Configuration

```
(host) (config) #crypto-local ipsec-map map-firewall 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 0.0.0.0 0.0.0.0
```

## Verifying Default Route Configuration

Use the following command to verify the default route to VPN configuration:

```
(host) #show ip route
```

```
Codes: C - connected
```

```
O - OSPF, O(IA) - OSPF inter area
```

```
O(E1) - OSPF external type 1, O(E2) - OSPF external type 2
```

```
O(N1) - OSPF NSSA type 1, O(N2) - OSPF NSSA type 2
```

```
M - mgmt, S - static, * - candidate default
```

```
D - DHCP
```

```
C 0.0.0.0 /0 [1] is an ipsec map: map-firewall
```

## Aruba VPN

The Aruba-VPN architecture includes the following two components:

- Mobility Access Switches at branch sites
- Controller at the datacenter

The Mobility Access Switch at the branch acts as the VPN endpoint and the controller at the datacenter acts as the VPN concentrator. When a Mobility Access Switch is set up for VPN, it forms an IPsec tunnel to the controller to secure sensitive corporate data. IPsec authentication and authorization between the controller and the Mobility Access Switches is based on the RAP whitelist configured on the controller.

You can configure an Aruba VPN tunnel either manually or through Zero Touch Provisioning (ZTP).

### Prerequisites

The following minimum configuration is required on the controller with which the Aruba VPN tunnel is established for a Mobility Access Switch:

- Add the mac address of the Mobility Access Switch in the whitelist database using the following command on the controller. To establish an Aruba VPN tunnel for an ArubaStack, the MAC addresses of all the members must be added in the whitelist database:

```
(controller) #whitelist-db rap add mac-address <mac_addr> ap-group default
```



---

The MAC address of the Mobility Access Switch can be obtained by executing the command **show tpm cert-info** on the Mobility Access Switch. For an ArubaStack, use the command **show tpm cert-info member all**.

---

- Create an IP pool for the Mobility Access Switch on the controller:  
(controller) (config) #ip local pool <name> <pool\_start\_address>
- Ensure that the switch IP of the controller is not the same as the crypto peer under the Aruba VPN configuration on the Mobility Access Switch.

### Sample Configuration

```
(controller) #whitelist-db rap add mac-address 00:0b:86:91:3d:37 ap-group default
(controller) (config) #ip local pool map_pool 3.3.3.1 3.3.3.255
```

### VPN Tunnel Establishment Using Zero Touch Provisioning

A factory default Mobility Access Switch can automatically be provisioned using the ZTP method. During the ZTP process, the Mobility Access Switch can automatically establish a tunnel with the Aruba VPN controller. This is achieved by provisioning the controller IP in the Activate server along with the AMP details.

Once the Mobility Access Switch comes up in the network, you can verify if the VPN tunnel is established using the CLI. For more information see, [Verifying Aruba VPN Tunnel Establishment on page 394](#).

### Configuring Aruba VPN Tunnel Manually

You can use the following CLI commands to configure the Aruba VPN tunnel on the Mobility Access Switch:

To configure the corporate network route, execute the following commands:

```
(host) (config) #ip-profile
(host) (ip-profile) #route <dest-ip> <net-mask> ipsec aruba-vpn
To configure the Aruba VPN tunnel, execute the following commands:
(host) (config) #crypto aruba-vpn
(host) (config-aruba-vpn)# peer-ip <aruba-vpn-peer-ip>
(host) (config-aruba-vpn)# interface vlan <aruba-vpn-vlan-id>
```

## Sample Configuration

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

## Verifying Aruba VPN Tunnel Establishment

You can verify the Aruba VPN tunnel establishment on the Mobility Access Switch as well as on the controller.

### In the Mobility Access Switch

Use the following CLI commands to verify the Aruba VPN tunnel establishment on the Mobility Access Switch:

To view the established Aruba VPN tunnel use the following command:

```
(host) #show crypto-local ipsec-map
Crypto Map Template "aruba-vpn" 9999
IKE Version: 2
IKEv2 Policy: 10006
lifetime: [300 - 86400] seconds, no volume limit
PFS (Y/N): N
Transform sets={ default-rap-transform }
Peer gateway: 192.168.165.2
Interface: vlan 1
Source network: 0.0.0.0/0.0.0.0
Destination network: 172.16.1.10/255.255.255.255
Pre-Connect (Y/N): Y
Tunnel Trusted (Y/N): Y
Forced NAT-T (Y/N): Y
Factory Certificate
```

To view the IP address obtained from the controller use the following commands:

```
(host) #show crypto isakmp sa
ISAKMP SA Active Session Information

Initiator IP Responder IP Flags Start Time Private IP

192.168.135.248 192.168.165.2 i-v2-c-A Jul 24 06:45:23 3.3.3.1
Flags: i = Initiator; r = Responder
m = Main Mode; a = Agressive Mode v2 = IKEv2
p = Pre-shared key; c = Certificate/RSA Signature; e = ECDSA Signature
x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled
3 = 3rd party AP; C = Campus AP; R = RAP, A = Aruba VPN
V = VIA; S = VIA over TCP
Total ISAKMP SAs: 1
(host) #show crypto ipsec sa
IPSEC SA (V2) Active Session Information

Initiator IP Responder IP SPI(IN/OUT) Flags Start Time Inner IP

192.168.135.248 192.168.165.2 318d3600/435ed500 UT2 Jul 24 10:23:46 3.3.3.1
Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
Total IPSEC SAs: 1

(host) #show ip-profile
ip-profile "default"

Parameter Value

Default Gateway N/A
Import DHCP Gateway Disabled
```

```

controller-ip N/A
route 172.16.1.10 255.255.255.255 ipsec aruba-vpn 0

```

## In the Controller

Once the Mobility Access Switch comes up on the network, execute the following commands on the controller to verify if the IP of the Mobility Access Switch is listed in the pool created:

```

(controller) #show vpdn l2tp local pool mas_pool
IP addresses used in pool rap_pool
3.3.3.1
3.3.3.2
Total:-
2 IPs used - 253 IPs free - 255 IPs configured
IP pool allocations / de-allocations - L2TP: 0/0 IKE: 389/387
(host) #show whitelist-db rap
AP-entry Details

Name AP-Group AP-Name Full-Name Authen-Username
---- -
00:0b:86:91:3d:37 default 00:0b:86:91:3d:37
Revoke-Text AP_Authenticated Description Date-Added Enabled Remote-IP

 Provisioned Wed Jun 25 Yes 0.0.0.0
 02:31:39
 2014

```

## Distributed DHCP Scopes

Mobility Access Switch allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

Mobility Access Switch provides support for Distributed, L3 DHCP scope. In Distributed L3 mode, DHCP server resides in the local branch on the Mobility Access Switch and each branch location is assigned a dedicated subnet. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server is configured with a unique subnet.




---

It is recommended to have same subnet range and client count on all branches for contiguous subnet allocation.

---

### Prerequisites

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.

### Configuring Distributed, L3 DHCP Scope

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

```

(host) (config) # service dhcp
(host) (config) # ip dhcp aruba-vpn-pool <profile-name>

```

Use the following command to configure the range of IP addresses which can be divided in to multiple IP subnets for the specified client count in Distributed,L3 scope:

```

(host) (Aruba VPN DHCP Pool <pool-name>) # ip-range <start-IP> <end-IP>

```

Use the following command to configure the number of clients per branch in Distributed,L3 scope:

```
(host) (Aruba VPN DHCP Pool <pool-name>)# client-count <number>
```

Use the following command to configure the server type for distributed DHCP scope. This release supports only Distributed, L3 mode which is the default server type.

```
(host) (Aruba VPN DHCP Pool <pool-name>)# ip dhcp server-type <Distributed,L3>
```

Use the following commands to optionally configure the IP address of the DNS server and domain name:

```
(host) (Aruba VPN DHCP Pool <pool-name>)# dns-server <address>
(host) (Aruba VPN DHCP Pool <pool-name>)# domain-name <domain-name>
```

Use the following command to optionally configure the lease time for the client IP address.

```
(host) (Aruba VPN DHCP Pool <pool-name>)# lease <days> <hours> <minutes> <seconds>
```

The default value is 12 hours.

Use the following command to optionally reserve the specified number of IP addresses in the beginning or end of the subnet :

```
(host) (Aruba VPN DHCP Pool <pool-name>)# reserve {first | last} <count>
```

Use the following command to optionally configure the DHCP Option for the distributed DHCP Scope:

```
(host) (Aruba VPN DHCP Pool <pool-name>)#option <code> [ip <address> | text <string>]
```

## Applying DHCP Scope Profile to VLAN Interface

Use the following command to apply the configured DHCP scope profile to a VLAN interface:

```
(host) (config) #interface vlan <id>
(host) (vlan "id") #aruba-vpn-pool-profile <profile-name>
```



---

You can configure up to six DHCP Scope profiles 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.

---

## Sample Configuration

```
(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") #aruba-vpn-pool-profile Distributed,L3
```

## Verifying Configuration

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
L3
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

```

## Static Route Support for VPN

You can also configure a static route to be used with VPN to and from your Mobility Access Switch. Use the following command to configure a static route using an IPsec map.

```

(host) (config) #ip-profile
(host) (ip-profile) #route <destip> <netmask> ipsec <mapname> metric <metric>

```

The value **metric** is used to enable IPsec route redundancy. **Metric** is cost assigned to the IPsec map that determines which map should be used first and which map should be used if the first map is unavailable.

```

(host) (ip-profile) #route 5.5.5.0 255.255.255.0 ipsec map1 metric 10
(host) (ip-profile) #route 5.5.5.0 255.255.255.0 ipsec map2 metric 20

```

In the above example, map1 would be used over map2. However, if map1 was unavailable, map2 would be used.




---

**Pre-connect** must be enabled on the IPsec maps for IPsec route redundancy.

---

The static route to IPsec map can be configured before or after the crypto map. If the static route is configured before the IPsec map, the static route is kept in the configuration; however, the route is not pushed to the routing table.

## Troubleshooting

You can use the following commands to troubleshoot VPN related issues:

- `show log security all | include ike`—View the logs.
- `show datapath tunnel`—Verify the encapsulation/decapsulation information.

You can also use the following commands to clear the crypto information:

- `clear crypto dp`—Clears crypto latest DP packets.
- `clear crypto ipsec`—Clears crypto IPsec state.
- `clear crypto isakmp`—Clears crypto ISAKMP state.



You can use port mirroring to send copies of all or sampled packets seen on specific port(s) or port-channel to a destination. You can use this method for appliances such as sniffers that monitor network traffic for further analysis.

This chapter includes the following topics:

- [Important Points to Remember on page 399](#)
- [The Source Port on page 399](#)
- [The Destination Port on page 399](#)
- [Mirroring Sampled Ratio on page 399](#)
- [Creating and Applying a Mirroring Profile to an Interface on page 400](#)
- [Sample Configuration on page 400](#)
- [Verifying Port Mirroring Configuration on page 400](#)

## Important Points to Remember

- The destination port must be a local interface.
- A VLAN cannot be configured as the destination.
- The Mobility Access Switch mirroring session limit is one.

## The Source Port

You can use port mirroring to take a copy of the ingress and egress packets on one or more ports. Packets are sent to the destination without modification at Layer 2. Any number of network ports can be configured for monitoring. Port-channel can also be the source for mirroring. If the bandwidth for source is greater than the destination, packets loss can occur. The Mobility Access Switch does not distinguish whether the source port is a Layer 2 access or trunk interface.

## The Destination Port

One port can be the destination interface; Port-channels and VLANs cannot be a destination. Normal traffic forwarding will not be performed on the destination port. Only the mirrored packets can be received on the destination port. A destination port cannot be a port mirroring source port at the same time. The destination port does not participate in any Layer 2 protocol, including Spanning-tree. Switching profile such as access or trunk profile cannot be applied on the destination port.

## Mirroring Sampled Ratio

You can configure the Mobility Access Switch to mirror at a ratio of one out of X packets (1:X) to the destination. The value of X can be between 0 and 2,047.

**Table 49: Sampled Ratio Values**

| Ratio (X value) | Description                                                        |
|-----------------|--------------------------------------------------------------------|
| 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.                 |

## Creating and Applying a Mirroring Profile to an Interface

### Using the CLI

```
(host) (config) # interface-profile mirroring-profile <profile-name>
 destination gigabitethernet <slot/module/port>
 ratio <0-2047>
 clone <source>
 no {...}
(host) (config) # interface gigabitethernet <slot/module/port>
 mirroring-in-profile <profile-name>
 mirroring-out-profile <profile-name>
```

The **mirroring-in-profile** is used for ingress traffic and the **mirroring-out-profile** is used for egress traffic.

### Sample Configuration

```
(host) (config) # interface-profile mirroring-profile MIRROR
 destination gigabitethernet 0/0/40
 ratio 10
 exit
(host) (config) # interface gigabitethernet 0/0/30
 mirroring-in-profile MIRROR
 mirroring-out-profile MIRROR
```

### Verifying Port Mirroring Configuration

```
(host) (config) #show mirroring

Mirroring Profile Name : MIRROR
Mirroring Ratio : 10
Mirroring Destination : GE0/0/40
Ingress mirrored ports : GE0/0/30
Egress mirrored ports : GE0/0/30

(host)# show interface-config gigabitethernet 0/0/30
gigabitethernet "0/0/30"

Parameter Value

<output truncated>
Ingress Port Mirroring Profile MIRROR
Egress Port Mirroring Profile MIRROR
<output truncated>
```

```
(host)# show interface-profile mirroring-profile MIRROR
Mirroring profile "MIRROR"

Parameter Value

gigabitethernet 0/0/30
Port mirroring ratio 10
```



This chapter describes the following topics:

- [Remote Monitoring \(RMON\) Overview on page 403](#)
- [Enabling RMON Service on page 403](#)
- [Configuring RMON Parameters on page 403](#)
- [Viewing RMON Active Configuration on page 406](#)

## Remote Monitoring (RMON) Overview

ArubaOS Mobility Access Switch supports RMON, which provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks (LANs). Monitoring devices (commonly called "probes") contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients. While both agent configuration and data collection use SNMP, RMON is designed to operate differently than other SNMP-based systems:

- Probes have more responsibility for data collection and processing, which reduces SNMP traffic and the processing load of the clients.
- Information is only transmitted to the management application when required, instead of continuous polling.

ArubaOS supports the following RMON groups:

- ethernet statistics
- history control
- ethernet history
- alarm
- event

## Enabling RMON Service

You can use the following command to enable RMON service on the Mobility Access Switch:

```
(host) (config) # service rmon
```

The **service rmon** command is disabled by default. 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 done. When the **service rmon** command is enabled, all the configurations done before would be applied.

## Configuring RMON Parameters

### Configuring the Alarm

[Table 50](#) describes the alarm parameters

**Table 50: Alarm Configuration Parameters**

Parameter	Description
alarm-profile	To associate an alarm profile.
monitor	Configures an OID to monitor.
owner	Configures an owner of this alarm entry.

You can use the following command to associate the alarm profile with the alarm entry:

```
(host) (config) #rmon alarm <alarm_index>
(host) (alarm_index) #alarm-profile <alarm-profile-name>
```

You can use the following command to monitor an interface or OID:

```
(host) (alarm_index) #monitor <oid>
```

You can use the following command to monitor OID on gigabitethernet interface:

```
(host) (alarm_index) #monitor gigabitethernet <slot/module/port> oid-type <oid_types>
```

You can use the following command to monitor OID on port-channel interface:

```
(host) (alarm_index) #monitor port-channel <port-channel id> oid-type <oid_types>
```

## Configuring the Alarm Profile

[Table 51](#) describes the alarm-profile parameters.

**Table 51: Alarm Profile Configuration Parameters**

Parameter	Description
falling-event	Associate an event index or profile to the falling event.
falling-threshold-value	Specifies the value at which the event is generated.
rising-event	Associate an event profile or index to the rising event.
rising-threshold-value	Specifies the value at which the event is generated.
sample-type	Specifies whether the sample type is either delta or absolute <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>
startup-alarm	Configures initial alarm (rising, falling, or either)

To configure the alarm variable, first you have to create an alarm profile. You can use the following command to create the alarm profile:

```
(host) (config) #rmon alarm-profile <profile-name>
 falling-event<event-index>
 falling-threshold-value <value>
 interval<interval>
 rising-event <event-index>
 rising-threshold-value <value>
 sample-type <absolute|delta>
 startup-alarm {falling|rising|rising-or-falling}
```

## Configuring Ethernet Statistics Index

[Table 52](#) describes the ethernet statistics index parameters.

**Table 52:** *Ethernet Statistics Index Configuration Parameters*

Parameter	Description
monitor	Configures an OID to monitor.
owner	Configure the owner of the etherstat entry.

You can use the following command to configure ethernet statistics collection on an interface:

```
(host) (config) # rmon etherstat <etherstat-index>
```

You can use the following command to monitor an OID:

```
(host) (etherstat_index) #monitor <oid>
```

You can use the following command to monitor OID on gigabitethernet interface:

```
(host) (etherstat_index) #monitor gigabitethernet <slot/module/port>
```

You can use the following command to monitor OID on port-channel interface:

```
(host) (etherstat_index) #monitor port-channel <port-channel id>
```

## Configuring History Group

[Table 53](#) describes the history group parameters.

**Table 53:** *History Group Configuration Parameters*

Parameter	Description
monitor	Configures the OID to monitor.
owner	Configures the owner of the history entry.
samples	Number of samples
sampling-interval	Interval of each sample

You can use the following command to create the history group profile:

```
(host) (config) #rmon history <history-index>
 samples <number>
 sampling-interval <interval>
 owner <owner>
```

You can use the following command to monitor an OID:

```
(host) (history_index) #monitor <oid>
```

You can use the following command to monitor OID on gigabitethernet interface:

```
(host) (history_index) #monitor gigabitethernet <slot/module/port>
```

You can use the following command to monitor OID on port-channel interface:

```
(host) (history_index) #monitor port-channel <port-channel id>
```

## Configuring Event Entry

[Table 54](#) describes the event entry parameters.

**Table 54:** Event Entry Configuration Parameters

Parameter	Description
description	Configures description of the event.
owner	Configures owner of the event.
Type	Specifies whether to send SNMPtrap or create log entry when the event occurs. <ul style="list-style-type: none"><li>• 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.</li><li>• When type is trap or log-and-trap, SNMP trap is generated.</li><li>• When type is none, no action is taken for this event.</li></ul>

You can use the following command to configure the event entry:

```
(host)(config)#rmon event <event-index>
```

You can use the following command to configure the event type:

```
(host)(event-index)#type
```

You can use the following command to clear the RMON log entries:

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

## Viewing RMON Active Configuration

You can use the following command to list the alarm-oids supported on device to use it 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
```

You can use the following command to display the RMON event table information:

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

RMON Event Table:

```

Event Index Type Last Seen Description Owner

1 log and Trap 10-25-2011@19-28-16 desc_log_1 admin
4 log - desc_log_2 guest
```

You can use the following command to display the log table information. The latest log entry will be displayed as the first one:

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

RMON Log Table:

```

Log Id Event Id Creation Time Description

1 3 3-22-2012@23-39-43 Rising threshold log: ifHCInOctets.455

```

You can use the following command to display the log table based on an event index:

```
(host)#show rmon log-table event <event-id> log <log-id>
```

You can use the following command to display the alarms on the device either briefly or detailed on alarm entry index basis:

```
(host)# show rmon alarms {brief | entry <index>}
```

The following command displays the details on the alarm on the device:

```
(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
```

You can use the following command to display the history table either briefly or detailed on history entry index basis:

```
(host)# show rmon history {brief | entry <index>}
```

The following example displays the history table information:

```
(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
```

## Viewing RMON Configuration

You can use the following list of commands to display the RMON configurations which may or may not get applied. For active configuration, see [Viewing RMON Active Configuration on page 406](#).

You can use the following command to display the configuration done for a specific alarm-profile:

```
(host)#show rmon-config alarm-profile [profile-name]
```

You can use the following command to display the configuration for a specific alarm entry:

```
(host)#show rmon-config alarm [index]
```

You can use the following command to display the configuration done for a specific etherstat index:

```
(host)#show rmon-config etherstat [index]
```

You can use the following command to display the configuration done for a specific event index.

```
(host)#show rmon-config event [index]
```

You can use the following command to display the configuration done for a specific history index:

```
(host)#show rmon-config history [index]
```

This chapter describes the following topics:

- [MIB and SNMP on page 409](#)
- [SNMP Parameters for Mobility Access Switch on page 409](#)
- [Logging on page 417](#)

## MIB and SNMP

ArubaOS Mobility Access Switch supports versions 1, 2c, and 3 of Simple Network Management Protocol (SNMP) for reporting purposes only. In other words, SNMP cannot be used for setting values in an Aruba system in the current Mobility Access Switch.




---

Aruba-specific management information bases (MIBs) describe the objects that can be managed using SNMP.

---

## SNMP Parameters for Mobility Access Switch

You can configure the following SNMP parameters for the Mobility Access Switch.

**Table 55:** *SNMP Parameters for the Mobility Access Switch*

Parameter	Description
Read Community Strings	Community strings used to authenticate requests for SNMP versions lower than version 3.
Enable Trap Generation	Activates the SNMP trap generation functionality. The configured SNMP trap receivers will receive the generated traps when this option is enabled.
Trap/Inform receivers	Host information about a trap receiver. This host needs to be running a trap receiver to receive and interpret the traps sent by the Mobility Access Switch. Configure the following for each host/trap receiver: <ul style="list-style-type: none"> <li>• IP address</li> <li>• SNMP version: can be 1, 2c, or 3.</li> <li>• Community string</li> <li>• UDP port on which the trap receiver is listening for traps. The default is the UDP port number 162. This is optional, and will use the default port number if not modified by the user.</li> </ul>
If you are using SNMPv3 to obtain values from the ArubaOS Mobility Access Switch, you can configure the following parameters:	
User name	Name of the user.
Authentication protocol	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: <ul style="list-style-type: none"> <li>• MD5: HMAC-MD5-96 Digest Authentication Protocol</li> <li>• SHA: HMAC-SHA-96 Digest Authentication Protocol</li> </ul>

Parameter	Description
Authentication protocol password	The (private) authentication key for use with the authentication protocol, if messages sent on behalf of this user can be authenticated. This is a string password for MD5 or SHA depending on the choice above.
Privacy protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This can take one of the following values: <ul style="list-style-type: none"> <li>• DES (Data Encryption Standard)</li> <li>• AES (Advanced Encryption Standard)</li> </ul> <b>NOTE:</b> Under DES, only CBC-DES Symmetric Encryption Protocol is supported.
Privacy protocol password	The (private) privacy key for use with the privacy protocol, if messages sent on behalf of this user can be encrypted/decrypted with AES or DES based on the privacy protocol selected.
Context	SNMPv3 context information used in SNMP agent.
Engine ID	Agent engine ID for SNMPv3.
SNMP Server Group	View access group entry for SNMPv3
View	SNMP view can be used to give restricted access to the MIB for the users. You can include or exclude the OIDs that are accessible to the users.

For the SNMP server parameters, see the following CLI command output:

```
(host) (config) #snmp-server ?
community Set read-only community string
context Create/Delete a context apart from default
enable Enable SNMP Traps
engine-id Engine ID of SNMP server in HEX.
group Define a User Security Model group
host Specify host address to receive SNMP notifications
inform SNMP Inform parameters
trap SNMP Trap parameters
user User Name configuration for the USM security model
view Define an SNMPv3 MIB view
<cr>
```

## Configuring SNMPv1/v2c Parameters

Execute the following command to configure the basic SNMP v1/v2c parameters:

```
(host) (config) #snmp-server community <string>
```

### Example

The following is a sample SNMP v1/v2c configuration:

```
(host) (config) #snmp-server community public
```

## Configuring SNMPv3 Parameters

You can use the SNMPv3 for advanced security options, such as authenticated or authenticated and encrypted security settings. You can also choose the unauthenticated settings.

Use one of the following system-defined groups for configuring v3 users with various security level settings or create a new group:

- ALLPRIV—Use this group for unauthenticated security settings.

- AUTHNOPRIV—Use this group for authenticated security settings.
- AUTHPRIV—Use this group for authenticated and encrypted security settings.

Execute the following commands to configure the basic SNMPv3 parameters:

```
(host) (config) #snmp-server group <group-name> {v1 | v2c | (v3 [auth|noauth|priv])}
(host) (config) #snmp-server user <user-name> group <name> {v1 | v2c | {v3[auth-prot {md5|sha}
<password>] [priv-prot {AES|DES} <password>]}}
```

## Example

You can use the following sample commands to configure SNMPv3:

```
(host) (config) #snmp-server group V3-Group v3 auth
(host) (config) # snmp-server user V3-User group V3-Group v3 auth-prot md5 abcd1234
```

For unauthenticated user configuration using the system-defined group, use the following command:

```
(host) (config) #snmp-server user V3-User1 group ALLPRIV v3
```

For authenticated user configuration using the system-defined group, use the following command:

```
(host) (config) #snmp-server user V3-User2 group AUTHNOPRIV v3 auth-prot md5 abc123
```

For authenticated and encrypted user configuration using the system-defined group, use the following command:

```
(host) (config) #snmp-server user V3-User3 group AUTHPRIV v3 auth-prot md5 password priv-prot
aes abc123
```

## Configuring SNMP Traps

Use the following commands to configure SNMP v1/v2c or v3 traps on the Mobility Access Switch:

```
(host) (config) #snmp-server enable trap
(host) (config) #snmp-server host <ipaddr> version {1 <community-string>} | {2c <community-
string>} | {3 <user-name>}
(host) (config) #snmp-server trap source <ipaddr>
```

To additionally configure informs, use the following command:

```
(host) (config) #snmp-server inform queue-length <size>
```

## Examples

To enable SNMP traps globally, use the following command:

```
(host) (config) #snmp-server enable trap
```

To configure SNMP v1 traps, use the following sample:

```
(host) (config) #snmp-server host 10.13.6.60 version 1 public
```

To configure SNMP v2c traps, use the following sample:

```
(host) (config) #snmp-server host 10.13.6.70 version 2c public
```

To configure SNMPv3 traps, use the following sample:

```
(host) (config) #snmp-server host 10.13.6.66 version 3 V3-User
```

To configure a trap source IP, use the following command:

```
(host) (config) #snmp-server trap source 10.13.7.80
```

To configure informs, use the following command:

```
(host) (config) #snmp-server inform queue-length 250
```

## Viewing SNMP Configuration Parameters

You can use the following show commands to view the SNMP configuration details on the Mobility Access Switch:

- **show snmp group-snmp:** View the SNMP Group information populated from the snmpd process.
- **show snmp group-trap:** View the SNMP Group trap information populated from the trapd process.
- **show snmp view:** View the View information with the included and excluded OID details.
- **show snmp context:** View the list of context names configured on the Mobility Access Switch.
- **show snmp community:** View the SNMP community table.
- **show snmp user-table:** View the user-table entries.
- **show snmp trap-hosts:** View the target trap host entries.
- **show snmp trap-group:** View 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.
- **show snmp notify filter profile-name:** View the SNMP Target profile names.
- **show snmp engine-id:** View the SNMP engine ID.
- **show snmp inform stats:** View the SNMP inform statistics.
- **show snmp trap-list:** View the list of SNMP traps supported and their status.
- **show snmp trap-queue:** View the list of SNMP traps in queue.

## Supported Standard MIBs

The following table gives the list of supported standard MIBs, supported tables in each MIB, and the scalars that are not supported in each MIB:

**Table 56:** *Supported MIBs*

MIB Name	Supported Tables	Scalars Not Supported
RFC1213-MIB	<ul style="list-style-type: none"> <li>• ipNetToMediaTable</li> <li>• tcp Globals</li> <li>• tcpConnTable</li> <li>• udp Globals</li> <li>• udpConnTable</li> <li>• sysinfo</li> </ul>	—
IF-MIB(RFC 1213, ifXTable RFC 2233, RFC 2863)	<ul style="list-style-type: none"> <li>• ifTable</li> <li>• ifXtable</li> <li>• ifTableLastChange</li> </ul>	<ul style="list-style-type: none"> <li>• ifOutDiscards</li> <li>• ifOutErrors</li> <li>• ifInUnknownProtos</li> <li>• ifInNUcastPkts</li> <li>• ifOutNUcastPkts</li> </ul>
EtherLike-MIB (RFC 3635)	<ul style="list-style-type: none"> <li>• dot3StatsTable</li> </ul>	<ul style="list-style-type: none"> <li>• dot3StatsSQETestErrors</li> <li>• dot3StatsSymbolErrors</li> <li>• dot3StatsEtherChipSet</li> <li>• dot3StatsCarrierSenseErrors</li> <li>• dot3StatsInternalMacTransmitErrors</li> <li>• dot3StatsRateControlAbility</li> <li>• dot3StatsRateControlStatus</li> <li>• dot3StatsAlignmentErrors</li> <li>• dot3StatsSingleCollisionFrames</li> </ul>

MIB Name	Supported Tables	Scalars Not Supported
ALARM-MIB-1 (RFC 3877)	<ul style="list-style-type: none"> <li>alarmModelTable</li> <li>alarmActiveStatsTable</li> <li>alarmClearTable</li> </ul>	—
NOTIFICATION-LOG(RFC3014)	<ul style="list-style-type: none"> <li>Notification MIB(Globals)</li> <li>nlmConfigLogTable</li> </ul>	—
SNMP-MPD-MIB(RFC 2572)		—
SNMP-FRAMEWORK-MIB(RFC 2571)	<ul style="list-style-type: none"> <li>snmpEngine</li> </ul>	—
SNMPv2-MIB (RFC 1907)	—	<ul style="list-style-type: none"> <li>snmplnTooBig</li> <li>snmplnNoSuchNames</li> <li>snmplnBadValues</li> <li>snmplnReadOnlys</li> <li>snmplnGenErrs</li> <li>snmplnTotalReqVars</li> <li>snmplnTotalSetVars</li> <li>snmplnGetRequests</li> <li>snmplnGetNexts</li> <li>snmplnSetRequests</li> <li>snmplnGetResponses</li> <li>snmplnTraps</li> <li>snmpOutTooBig</li> <li>snmpOutNoSuchNames</li> <li>snmpOutBadValues</li> <li>snmpOutGenErrs</li> <li>snmpOutGetRequests</li> <li>snmpOutGetNexts</li> <li>snmpOutSetRequests</li> <li>snmpOutGetResponses</li> <li>snmpOutTraps</li> </ul>
SNMP-TARGET-MIB (RFC 2573)	<ul style="list-style-type: none"> <li>snmpTargetObjects</li> <li>snmpTargetAddrTable</li> <li>snmpTargetParamsTable</li> </ul>	—
SNMP-NOTIFICATION-MIB(RFC 2573)	<ul style="list-style-type: none"> <li>snmpNotifyTable</li> <li>snmpNotifyFilterProfileTable</li> <li>snmpNotifyFilterTable</li> </ul>	—
Q-BRIDGE-MIB (RFC 4363)	<ul style="list-style-type: none"> <li>dot1qBase</li> <li>dot1qFdbTable</li> <li>dot1qTpFdbTable</li> <li>dot1qStaticUicastTable</li> <li>dot1qVlanStaticTable</li> </ul>	—
BRIDGE-MIB (RFC 4188)	<ul style="list-style-type: none"> <li>dot1dBase</li> <li>dot1dTpFdbTable</li> <li>dot1dStaticTable</li> <li>dot1dBasePortTable</li> </ul>	—

MIB Name	Supported Tables	Scalars Not Supported
PTOPO-MIB (RFC 2922)	<ul style="list-style-type: none"> <li>ptopoConnTable</li> </ul>	—
LLDP-MIB	<ul style="list-style-type: none"> <li>IldpPortConfigTable</li> <li>IldpConfigManAddrTable</li> <li>IldpStatsTxPortTable</li> <li>IldpStatsRxPortTable</li> <li>IldpLocPortTable</li> <li>IldpLocManAddrTable</li> <li>IldpRemTable</li> <li>IldpRemManAddrTable</li> </ul>	—
RMON-MIB (RFC 2819)	<ul style="list-style-type: none"> <li>etherStatsTable</li> <li>historyControlTable</li> <li>etherHistoryTable</li> <li>alarmTable</li> <li>eventTable</li> <li>logTable</li> </ul>	—
RMON2-MIB (RFC 4502)	<ul style="list-style-type: none"> <li>probeConfig</li> </ul>	—
HC-RMON-MIB (RFC 3273)	<ul style="list-style-type: none"> <li>etherStatsHighCapacityGroup</li> <li>etherHistoryHighCapacityGroup</li> </ul>	<ul style="list-style-type: none"> <li>etherStatsHighCapacityOverflowPkts64Octets</li> <li>etherStatsHighCapacityPkts64Octets</li> <li>etherStatsHighCapacityOverflowPkts65to127Octets</li> <li>etherStatsHighCapacityPkts65to127Octets</li> <li>etherStatsHighCapacityOverflowPkts128to255Octets</li> <li>etherStatsHighCapacityPkts128to255Octets</li> <li>etherStatsHighCapacityOverflowPkts256to511Octets</li> <li>etherStatsHighCapacityPkts256to511Octets</li> <li>etherStatsHighCapacityOverflowPkts512to1023Octets</li> <li>etherStatsHighCapacityPkts512to1023Octets</li> <li>etherStatsHighCapacityOverflowPkts1024to1518Octets</li> <li>etherStatsHighCapacityPkts1024to1518Octets</li> </ul>
OSPF-MIB	<ul style="list-style-type: none"> <li>ospfGeneralGroup</li> <li>ospfAreaTable</li> <li>ospfStubAreaTable</li> <li>ospfIfTable</li> <li>ospfNbrTable</li> <li>ospfLsdbTable</li> <li>ospfExtLsdbTable</li> </ul>	<ul style="list-style-type: none"> <li>ospfDemandExtensions</li> <li>ospfIfDemand</li> <li>ospfNbmaNbrPermanence</li> <li>ospfNbrHelloSuppressed</li> <li>ospfStubMetric</li> <li>ospfImportAsExtern</li> <li>ospfNbmaNbrPermanence</li> <li>ospfNbrHelloSuppressed</li> <li>ospfIfAuthKey</li> <li>ospfExtLsdbAdvertisement</li> <li>ospfLsdbAdvertisement</li> </ul>
ENTITY-MIB	<ul style="list-style-type: none"> <li>entityGeneral</li> <li>entPhysicalTable</li> <li>entLogicalTable</li> <li>entAliasMappingTable</li> <li>entPhysicalContainsTable</li> </ul>	<ul style="list-style-type: none"> <li>entPhysicalMfgName</li> <li>entPhysicalAssetID</li> <li>entPhysicalUri</li> <li>entPhysicalHardwareRev</li> <li>entPhysicalAlias</li> <li>entPhysicalMfgDate</li> <li>entLPMappingTable</li> </ul>



To get OID for ENTITY-MIB, a new MIB called ARUBA-VENDORTYPE has been added.

## Supported Enterprise MIBs

The following table gives the list of supported enterprise MIBs, supported tables in each MIB, and the scalars that are not supported in each MIB:

**Table 57:** *Supported Enterprise MIBs*

MIB Name	Supported Tables	Scalars Not Supported
ARUBA-SYSTEMEXT	<ul style="list-style-type: none"> <li>wlsxSysExtProcessorTable</li> <li>wlsxSysExtStorageTable</li> <li>wlsxSysExtMemoryTable</li> <li>wlsxSysExtCardTable</li> <li>wlsxSysExtFanTable</li> <li>wlsxSysExtPowerSupplyTable</li> </ul>	<ul style="list-style-type: none"> <li>wlsxSysExtSwitchMasterIp</li> <li>wlsxSysExtSwitchRole</li> </ul>
ARUBA-SWITCH	<ul style="list-style-type: none"> <li>wlsxSysXProcessorTable</li> <li>wlsxSysXStorageTable</li> <li>wlsxSysXMemoryTable</li> </ul>	<ul style="list-style-type: none"> <li>wlsxSwitchMasterIP</li> <li>wlsxSwitchRole</li> </ul>
ARUBA-USER	<ul style="list-style-type: none"> <li>wlsxUserTable</li> <li>wlsxUserSessionTimeTable</li> </ul>	—
ARUBA-IFEXT	<ul style="list-style-type: none"> <li>wlsxIfExtNPortTable</li> </ul>	—
ARUBA-POE	<ul style="list-style-type: none"> <li>wlsxPsePortTable</li> <li>wlsxPseSlotTable</li> </ul>	—
ARUBA-STACKING	<ul style="list-style-type: none"> <li>wlsxStackMemberTable</li> <li>wlsxStackProtoIfTable</li> <li>wlsxStackTopoTable</li> </ul>	—

## Supported Standard Traps

The following table gives the list of supported standard traps:

**Table 58:** *Standard Traps*

Supported Traps
<ul style="list-style-type: none"> <li>authenticationFailure</li> <li>coldStart</li> <li>linkDown</li> <li>linkUp</li> <li>warmStart</li> <li>ptopoConfigChange</li> <li>lldpRemTablesChange</li> <li>risingAlarm</li> <li>fallingAlarm</li> <li>ospfIfStateChange</li> <li>ospfNbrStateChange</li> <li>entConfigChange</li> </ul>

## Supported Enterprise Traps

The following table gives the list of supported enterprise traps:

**Table 59:** Supported Enterprise Traps

Supported Traps
<ul style="list-style-type: none"><li>● wlsxAuthMaxAclEntries</li><li>● wlsxAuthServerReqTimedOut</li><li>● wlsxColdStart</li><li>● wlsxFanFailure</li><li>● wlsxFanOK</li><li>● wlsxFanTrayInsertedTrap</li><li>● wlsxFanTrayRemovedTrap</li><li>● wlsxFlashSpaceOK</li><li>● wlsxIfLinkDownTrap (from ArubaOS 7.4.0.2 onwards)</li><li>● wlsxIfLinkUpTrap (from ArubaOS 7.4.0.2 onwards)</li><li>● wlsxInRangeVoltage</li><li>● wlsxInformQueueOverFlow</li><li>● wlsxLowMemory</li><li>● wlsxLowOnFlashSpace</li><li>● wlsxMemoryUsageOK</li><li>● wlsxNAuthMaxAclEntries</li><li>● wlsxNAuthServerIsDown</li><li>● wlsxNAuthServerIsUp</li><li>● wlsxNAuthServerReqTimedOut</li><li>● wlsxNFanFailure</li><li>● wlsxNGBICInserted</li><li>● wlsxNLowMemory</li><li>● wlsxNLowOnFlashSpace</li><li>● wlsxNOutOfRangeTemperature</li><li>● wlsxNOutOfRangeVoltage</li><li>● wlsxNProcessDied</li><li>● wlsxNUserEntryAuthenticated</li><li>● wlsxNUserEntryCreated</li><li>● wlsxNUserEntryDeAuthenticated</li><li>● wlsxNUserEntryDeleted</li><li>● wlsxNormalTemperature</li></ul>
<ul style="list-style-type: none"><li>● wlsxOutOfRangeTemperature</li><li>● wlsxOutOfRangeVoltage</li><li>● wlsxPowerSupplyFailureTrap</li><li>● wlsxPowerSupplyMissingTrap (From ArubaOS 7.4.0.3, the slot details of the ArubaStack are included in this trap)</li><li>● wlsxPowerSupplyOK</li><li>● wlsxPowerSupplyOKTrap</li><li>● wlsxProcessDied</li><li>● wlsxProcessRestart</li><li>● wlsxStackIfStateChangeTrap</li><li>● wlsxStackMacChangeTrap (from ArubaOS 7.4.1.1 onwards)</li><li>● wlsxStackTopologyChangeTrap</li><li>● wlsxUserAuthenticationFailed</li><li>● wlsxUserEntryAuthenticated</li><li>● wlsxUserEntryChanged</li><li>● wlsxUserEntryCreated</li><li>● wlsxUserEntryDeAuthenticated</li><li>● wlsxUserEntryDeleted</li><li>● wlsxVlanLinkDown</li><li>● wlsxVlanLinkUp</li><li>● wlsxWarmStart</li><li>● wlsxIfStateChangeTrap (Enhanced for BPDU guard feature)</li></ul>

## Logging

For each category or subcategory of message, you can set the logging level or severity level of the messages to be logged. [Table 60](#) lists the logging levels.

**Table 60:** *Logging Levels*

Logging Level	Description
Emergency	System is unusable
Alerts	Immediate action is needed.
Critical	Any critical conditions.
Errors	Error conditions.
Warning	Warning messages.
Notifications	Normal but signification conditions.
Informational	Messages of general interest to system users.
Debug	Messages containing information useful for debugging.

The default logging level for all categories is Warning. Within each logging level are several log types you can select.

- network
- security
- system
- user
- user debug



---

Starting from ArubaOS 7.4.1.7, users are restricted from configuring the **logging level debugging user debug** command for the **Stack Manager** process. This configuration is applicable only to the **Auth Manager** process.

---

The following table lists the terms and their definitions used in this guide.

---

**3DES**

Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

**3G**

Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.

**3GPP**

Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.

**4G**

Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

**802.11**

802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.

**802.11 bSec**

802.11 bSec is an alternative to 802.11 i. The difference between bSec and standard 802.11 i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC-MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11 i is upgraded to support SHA-256 and SHA-384.

**802.11a**

802.11 a provides specifications for wireless systems. Networks using 802.11 a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.

**802.11ac**

802.11 ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.

**802.11b**

802.11 b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase-Shift Keying (PSK) modulation method used in 802.11 standards, 802.11 b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multipath-propagation interference. 802.11 b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

---

**802.11d**

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

**802.11e**

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

**802.11g**

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

**802.11h**

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military RADAR systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

**802.11i**

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

**802.11j**

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a; the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

**802.11k**

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

**802.11m**

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

---

**802.11n**

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

**802.11r**

802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

**802.11u**

802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

**802.11v**

802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.

**802.1Q**

802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.

**802.1X**

802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.

**802.3af**

802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.

**802.3at**

802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.

**AAA**

Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

**ABR**

Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.

---

**AC**

Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.

**ACC**

Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.

**Access-Accept**

Response from the RADIUS server indicating successful authentication and containing authorization information.

**Access-Reject**

Response from RADIUS server indicating that a user is not authorized.

**Access-Request**

RADIUS packet sent to a RADIUS server requesting authorization.

**Accounting-Request**

RADIUS packet type sent to a RADIUS server containing accounting summary information.

**Accounting-Response**

RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

**ACE**

Access Control Entry. ACE is an element in an ACL that includes access control information.

**ACI**

Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.

**ACL**

Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

**Active Directory**

Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

**ActiveSync**

Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

---

**ad hoc network**

An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

**ADO**

Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

**ADP**

Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

**AES**

Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

**AIFSN**

Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

**AirGroup**

The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

**AirWave Management Client**

AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

**ALE**

Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises. This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or Instant clusters.

**ALG**

Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

---

**AM**

Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

**AMON**

Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

**AMP**

AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

**A-MPDU**

Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

**A-MSDU**

Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

**ANQP**

Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

**ANSI**

American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

**API**

Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

**app**

Short form for application. It generally refers to the application that is downloaded and used on mobile devices.

**ARM**

Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

---

**ARP**

Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

**Aruba Activate**

Aruba Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise network.

**ASCII**

American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

**band**

Band refers to a specified range of frequencies of electromagnetic radiation.

**BGP**

Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

**BLE**

Bluetooth Low Energy. The BLE functionality is offered by Bluetooth® to enable devices to run for long durations with low power consumption.

**BMC**

Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

**BPDU**

Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

**B-RAS**

Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

**BRE**

Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

**BSS**

Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

---

**BSSID**

Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID is generated randomly.

**BYOD**

Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

**CA**

Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

**CAC**

Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

**CALEA**

Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

**Campus AP**

Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

**captive portal**

A captive portal is a web page that allows the users to authenticate and sign in before connecting to a public-access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users.

**CCA**

Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

**CDP**

Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

**CDR**

Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added

---

through the network or charges for operator services, and so on.

**CEF**

Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension formatted as key-value pairs.

**CGI**

Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.

**CHAP**

Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.

**CIDR**

Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.

**ClearPass**

ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.

**ClearPass Guest**

ClearPass Guest is a configurable ClearPass application for secure visitor network access management.

**ClearPass Policy Manager**

ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.

**CLI**

Command-Line Interface. A console interface with a command line shell that allows users to execute text input as commands and convert these commands to appropriate functions.

**CN**

Common Name. CN is the primary name used to identify a certificate.

**CNA**

Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.

---

**CoA**

Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.

**CoS**

Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.

**CPE**

Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

**CPsec**

Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

**CPU**

Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

**CRC**

Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

**CRL**

Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

**cryptobinding**

Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

**CSA**

Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

**CSMA/CA**

Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

**CSR**

Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

---

**CSV**

Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

**CTS**

Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

**CW**

Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

**DAI**

Dynamic ARP inspection. A security feature that validates ARP packets in a network.

**DAS**

Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

**dB**

Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

**dBm**

Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

**DCB**

Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

**DCE**

Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.

**DCF**

Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.

**DDMO**

Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

---

**DES**

Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.

**designated router**

Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.

**destination NAT**

Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.

**DFS**

Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with RADAR systems.

**DFT**

Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.

**DHCP**

Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.

**DHCP snooping**

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.

**digital certificate**

A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth.

**Digital wireless pulse**

A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.

**Disconnect-Ack**

Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.

---

**Disconnect-Nak**

Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.

**Disconnect-Request**

Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

**distribution certificate**

Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

**DLNA**

Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

**DMO**

Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

**DN**

Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the "common name", which is the primary name used to identify the certificate.

**DNS**

Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

**DOCSIS**

Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

**DoS**

Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

**DPD**

Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

---

**DPI**

Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

**DRT**

Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

**DS**

Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

**DSCP**

Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

**DSL**

Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

**DSSS**

Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing the resistance to interference. See FHSS.

**DST**

Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

**DTE**

Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.

**DTIM**

Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.

**DTLS**

Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.

---

**dynamic authorization**

Dynamic authorization refers to the ability to make changes to a visitor account's session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

**dynamic NAT**

Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by masking the internal configuration of a private network.

**EAP**

Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

**EAP-FAST**

EAP – Flexible Authentication Secure Tunnel (tunneled).

**EAP-GTC**

EAP – Generic Token Card. (non-tunneled).

**EAP-MD5**

EAP – Method Digest 5. (non-tunneled).

**EAP-MSCHAP**

EAP Microsoft Challenge Handshake Authentication Protocol.

**EAP-MSCHAPv2**

EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

**EAPoL**

Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.

**EAP-PEAP**

EAP-Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).

**EAP-PWD**

EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.

**EAP-TLS**

EAP-Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.

---

**EAP-TTLS**

EAP-Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

**ECC**

Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

**ECDSA**

Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

**EDCA**

Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

**EIGRP**

Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

**EIRP**

Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

**ESI**

External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

**ESS**

Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

**ESSID**

Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

**Ethernet**

Ethernet is a network protocol for data transmission over LAN.

**EULA**

End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

---

**FCC**

Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

**FFT**

Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

**FHSS**

Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a random but predictable sequence. See also DSSS.

**FIB**

Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

**FIPS**

Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

**firewall**

Firewall is a network security system used for preventing unauthorized access to or from a private network.

**FQDN**

Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.

**FQLN**

Fully Qualified Location Name. FQLN is a device location identifier in the format: APname.Floor.Building.Campus.

**frequency allocation**

Use of radio frequency spectrum as regulated by governments.

**FSPL**

Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction.

**FTP**

File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.

---

**GARP**

Generic Attribute Registration Protocol. GARP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.

**GAS**

Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.

**gateway**

Gateway is a network node that allows traffic to flow in and out of the network.

**Gbps**

Gigabits per second.

**GBps**

Gigabytes per second.

**GET**

GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).

**GHz**

Gigahertz.

**GMT**

Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.

**goodput**

Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.

**GPS**

Global Positioning System. A satellite-based global navigation system.

**GRE**

Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.

**GTC**

Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.

---

**GVRP**

GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

**H2QP**

Hotspot 2.0 Query Protocol.

**hot zone**

Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

**hotspot**

Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet.

**HSPA**

High-Speed Packet Access.

**HT**

High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

**HTTP**

Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the w servers and browsers should take in response to various commands.

**HTTPS**

Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

**IAS**

Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

**ICMP**

Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

**IDS**

Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

**IEEE**

Institute of Electrical and Electronics Engineers.

---

**IGMP**

Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

**IGMP snooping**

IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

**IGP**

Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

**IGRP**

Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

**IKE**

Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

**IKEv1**

Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.

**IKEv2**

Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.

**IoT**

Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.

**IPM**

Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.

**IPS**

Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.

---

**IPsec**

Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.

**IPSG**

Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.

**IrDA**

An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.

**ISAKMP**

Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.

**ISP**

Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.

**JSON**

JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute-value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

**Kbps**

Kilobits per second.

**KBps**

Kilobytes per second.

**keepalive**

Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

**L2TP**

Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

**LACP**

Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

---

**LAG**

Link Aggregation Group . A LAG combines a number of physical ports together to make a single high-bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

**LAN**

Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

**LCD**

Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

**LDAP**

Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

**LDPC**

Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

**LEAP**

Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

**LED**

Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

**LEEF**

Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

**LI**

Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

**LLDP**

Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

**LLDP-MED**

LLDP-Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

---

**LMS**

Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

**LNS**

L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

**LTE**

Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

**MAB**

MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

**MAC**

Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

**MAM**

Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

**Mbps**

Megabits per second

**MBps**

Megabytes per second

**MCS**

Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

**MD4**

Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

**MD5**

Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

---

**MDAC**

Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

**MDM**

Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

**mDNS**

Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

**MFA**

Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

**MHz**

Megahertz

**MIB**

Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

**microwave**

Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

**MIMO**

Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

**MISO**

Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize data speed. The destination (receiver) has only one antenna.

**MLD**

Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

**MPDU**

MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

---

**MPLS**

Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

**MPPE**

Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

**MS-CHAP**

Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

**MS-CHAPv1**

Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

**MS-CHAPv2**

Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

**MSS**

Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

**MSSID**

Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

**MSTP**

Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

**MTU**

Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

**MU-MIMO**

Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

**MVRP**

Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

**mW**

milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

---

**NAC**

Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

**NAD**

Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

**NAK**

Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.

**NAP**

Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

**NAS**

Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial-in terminal server.

**NAT**

Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

**NetBIOS**

Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.

**netmask**

Netmask is a 32-bit mask used for segregating IP address into subnets. Netmask defines the class and range of IP addresses.

**NFC**

Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer-to-peer (P2P) network to exchange data.

**NIC**

Network Interface Card. NIC is a hardware component that allows a device to connect to the network.

---

**Nmap**

Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

**NMI**

Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.

**NMS**

Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

**NOE**

New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.

**NTP**

Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.

**OAuth**

Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third-party applications to access user information, without exposing the user credentials.

**OCSP**

Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

**OFDM**

Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.

**OID**

Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.

**OKC**

Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

**onboarding**

The process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters.

---

**OpenFlow**

OpenFlow is an open communications interface between control plane and the forwarding layers of a network.

**OpenFlow agent**

OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.

**Optical wireless**

Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.

**OSI**

Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.

**OSPF**

Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).

**OSPFv2**

Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.

**OUI**

Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.

**OVA**

Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.

**OVF**

Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.

**PAC**

Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.

---

**PAP**

Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

**PAPI**

Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

**PBR**

Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on policies configured by a network administrator.

**PDU**

Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control information that is delivered as a unit among peer entities of a network.

**PEAP**

Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

**PEF**

Policy Enforcement Firewall. PEF provides context-based controls to enforce application-layer security and prioritization.

**PFS**

Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

**PHB**

Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

**PIM**

Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

**PIN**

Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

**PKCS#n**

Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

---

**PKI**

Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

**PLMN**

Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

**PMK**

Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

**PoE**

Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

**PoE+**

Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

**POST**

Power On Self Test. An HTTP request method that requests data from a specified resource.

**PPP**

Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

**PPPoE**

Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

**PPTP**

Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

**private key**

The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

**PRNG**

Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

---

**PSK**

Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

**PSU**

Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

**public key**

The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

**PVST**

Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

**PVST+**

Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

**QoS**

Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

**RA**

Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.

**RADAR**

Radio Detection and Ranging. RADAR is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.

**RADIUS**

Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

**RAM**

Random Access Memory.

**RAPIDS**

Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.

---

**RARP**

Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.

**Regex**

Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.

**Registration Authority**

Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.

**Remote AP**

Remote AP. Remote AP extends the corporate network to users working from home, or at temporary work sites.

**REST**

Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.

**RF**

Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or RADAR signals.

**RFC**

Request For Comments. RFC is a commonly used format for the Internet standards documents.

**RFID**

Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.

**RIP**

Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.

**RJ45**

Registered Jack 45. RJ45 is a physical connector for network cables.

**RMON**

Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.

**RoW**

Rest of World. RoW or RW is an operating country code of a device.

---

**RSA**

Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

**RSSI**

Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.

**RSTP**

Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.

**RTCP**

RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.

**RTLS**

Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.

**RTP**

Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.

**RTS**

Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.

**RTSP**

Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

**RVI**

Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.

**RW**

Rest of World. RoW or RW is an operating country code of a device.

**SA**

Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.

**SAML**

Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

---

**SCEP**

Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.

**SCP**

Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.

**SCSI**

Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.

**SDN**

Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

**SDR**

Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

**SDU**

Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

**SD-WAN**

Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

**SFP**

The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

**SFP+**

Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

**SFTP**

Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

**SHA**

Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

---

**SIM**

Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

**SIP**

Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

**SIRT**

Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

**SKU**

Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

**SLAAC**

Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

**SMB**

Server Message Block or Small and Medium Business. Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

**SMS**

Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

**SMTP**

Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

**SNIR**

Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

**SNMP**

Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

**SNMPv1**

Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

---

**SNMPv2**

Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

**SNMPv2c**

Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

**SNMPv3**

Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

**SNR**

Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

**SNTP**

Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

**SOAP**

Simple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

**SoC**

System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

**source NAT**

Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

**SSH**

Secure Shell. SSH is a network protocol that provides secure access to a remote device.

**SSID**

Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

**SSL**

Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

---

**SSO**

Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

**STBC**

Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

**STM**

Station Management. STM is a process that handles AP management and user association.

**STP**

Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

**subnet**

Subnet is the logical division of an IP network.

**subscription**

A business model where a customer pays a certain amount as subscription price to obtain access to a product or service.

**SU-MIMO**

Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high-speed device during the allotted time slice.

**SVP**

SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

**SWAN**

Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

**TAC**

Technical Assistance Center.

**TACACS**

Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

---

**TACACS+**

Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

**TCP**

Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

**TCP/IP**

Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

**TFTP**

Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

**TIM**

Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

**TKIP**

Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next-generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

**TLS**

Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

**TLV**

Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

**ToS**

Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

**TPC**

Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

**TPM**

Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

---

**TSF**

Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

**TSPEC**

Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

**TSV**

Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

**TTL**

Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

**TTY**

TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

**TXOP**

Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

**UAM**

Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

**U-APSD**

Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

**UCC**

Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

**UDID**

Unique Device Identifier. UDID is used to identify an iOS device.

**UDP**

User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

---

**UDR**

User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

**UHF**

Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.

**UI**

User Interface.

**UMTS**

Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.

**UPnP**

Universal Plug and Play. UPnP is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

**URI**

Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.

**URL**

Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.

**USB**

Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.

**UTC**

Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.

**UWB**

Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.

**VA**

Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.

---

**VBR**

Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.

**VHT**

Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.

**VIA**

Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.

**VLAN**

Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.

**VM**

Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.

**VoIP**

Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

**VoWLAN**

Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

**VPN**

Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

**VRD**

Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

**VRF**

VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

---

**VRF Plan**

VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

**VRRP**

Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

**VSA**

Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

**VTP**

VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

**walled garden**

walled garden is feature that allows blocking of unauthorized users from accessing network resources.

**WAN**

Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

**WASP**

Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

**WAX**

Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

**W-CDMA**

Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

**web service**

Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

**WEP**

Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

---

**WFA**

Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

**WIDS**

Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

**Wi-Fi**

Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

**WiMAX**

Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

**WIP**

Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

**WIPS**

Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

**WISP**

Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

**WISPr**

Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

**WLAN**

Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

**WME**

Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC\_VO), video (AC\_VI), best effort (AC\_BE) and background (AC\_BK). See WMM.

---

**WMI**

Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

**WMM**

Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC\_VO), video (AC\_VI), best effort (AC\_BE), and background (AC\_BK).

**WPA**

Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

**WPA2**

Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

**WSDL**

Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

**WSP**

Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

**WWW**

World Wide Web.

**X.509**

X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

**XAuth**

Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

**XML**

Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

---

**XML-RPC**

XML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

**ZTP**

Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.