ArubaOS 6.4.3.1

Release Notes

aruba NETWORKS

Copyright Information

© 2015 Aruba Networks, Inc. All rights reserved. Aruba Networks®, Aruba NetworksTM (stylized), People Move Networks Must Follow®, Mobile Edge Architecture®, RFProtect®, Green Island®, ClientMatch®, Aruba Central®, Aruba Mobility Management System™, ETips™, Virtual Intranet Access™, Aruba Instant™, ArubaOS™, xSec™, ServiceEdge™, Aruba ClearPass Access Management System™, AirMesh™, AirWave™, Aruba@Work™, Cloud WiFi™, Aruba Cloud™, Adaptive Radio Management™, Mobility-Defined Networks™, Meridian™ and ArubaCareSM are trademarks of Aruba Networks, Inc. registered in the United States and foreign countries. Aruba Networks, Inc. reserves the right to change, modify, transfer or otherwise revise this publication and the product specifications without notice.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software fro Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved.This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS. Altering this device (such as painting it) voids the warranty.

Contents 3

Release Overview 23

Chapter Overview 23

Important Points to Remember 23

AP Settings Triggering a Radio Restart 23

Supported Browsers 24

Contacting Support 25

Features in 6.4.x Releases 27

Features Introduced in ArubaOS 6.4.3.1 27

Modified Commands 27

interface vlan 27

show interface vlan 27

Features Introduced in ArubaOS 6.4.3.0 27

AP-Platform 27

Support for the AP-205H Access Point 27

Support for the AP-228 Access Point 28

Support for the AP-277 Access Point 28

USB Modem Support for AP-210 Series and AP-220 Series 29

AP Console Access Using a Backup ESSID 29

ARM 29

Anyspot Client Probe Suppression 29

AP Scanning Optimization 29

Branch Controller 29

Authentication Survivability 29

Branch Controller Integration with Palo Alto Networks Firewalls 29

Monitor WAN Health 29
Per-Interface Bandwidth Contracts 30
Policy-Based Routing 30
PortFast and BPDU Guard 30
Uplink Routing using Next-Hop Lists 30
Virtual APs for WAN Link Failure 30
WAN Optimization 30
WebUI Enhancements for WAN 30
Zero Touch Provisioning 30
Client Match 31
BSS Transition Management Support 31
Multi-Media Sync-Up 31
Removing VBR Dependency on Probe Requests 31
Controller-Datapath 31
Wi-Fi Packet Capture in Split-Tunnel Forwarding Mode 31
Controller-Platform 31
7024 Controller 31
7205 Controller 32
DHCP Lease Limit on 7000 Series Controllers 32
AMON Message Size Changes on the Controller 32
Flexible Licensing for AP Controllers 32
Modem Support on 7000 Series Controllers 33
Serviceability 33
Username and Password Protection for the AP Console 33
PhoneHome-Lite 33
Security 33
AP-Group and AP-Name in Campus AP Whitelist 33
Centralized Control Plane Security Whitelist on CPPM 33
RadSec on RADIUS Servers 33

Configuring IKE Policies 33
Generating a Certificate Signing Request (CSR) 33
Voice and Video 34
UCC Score for Lync Media Classification 34
Lync SDN API 2.1 Support 34
WebUI Enhancements 34
Controller Health Monitoring 34
WLAN 34
Auto-tagging and Controller-based Policy 34
Maximum Number of iChat Users 34
mDNS AP VLAN Aggregation 34
mDNS-based Device Discovery of Apple TV 35
Mesh Support for 802.11ac 35
Multicast Response Propagation for mDNS 35
Features Introduced in ArubaOS 6.4.2.5 35
RADIUS Service-Type Attribute 35
Controller Authentication to CPPM 35
In the WebUI 35
In the CLI 36
Handling GARPs 36
In the CLI 36
NetGear AirCard 341U USB Modem Support 36
Modified Commands 36
show web-server profile 36
web-server profile 36
Features Introduced in ArubaOS 6.4.2.4 37
USB Storage for CSR and Key Files 37
AP Boot Prompt 37
Controller WebUI 37

Controller CLI 37
RAP Console 37
SFP/SFP+ modules 38
Modified Commands 38
show dot1x watermark 38
Features Introduced in ArubaOS 6.4.2.3 39
AP-2xx Series High Density Optimization 39
L2 GRE Tunnel Group 39
Important Points to Remember 39
Creating an L2 Tunnel Group 39
MLD Snooping 41
New Commands 41
show web-server statistics 41
Modified Commands 43
ids-general-profile 43
show web-server profile 44
web-server profile 44
Security Bulletin 44
Features Introduced in ArubaOS 6.4.2.2 44
Username Length Restriction 44
Features Introduced in ArubaOS 6.4.2.1 45
AP Power Mode on AP-220 Series 45
In the CLI 45
Important Points to Remember 45
Features Introduced in ArubaOS 6.4.2.0 46
AP-Platform 46
Support for the AP-210 Series 46
Enhanced Link Aggregation Support on AP-220 Series and AP-270 Series Access Points 46
Netgear AirCard 340U USB Modem Support 46

Netgear AirCard 341U USB Modem Support 46
VHT Support on AP-200 Series, AP-210 Series, AP-220 Series, and AP-270 Series Access Points 46
AP Regulatory 47
Channel 144 in Regulatory Domain Profile 47
Controller-Platform 47
Kernel Core Dump Enhancement 47
Web Content Classification 47
AP-Wireless 48
RTLS Station Message Frequency 48
Video Multicast Rate Optimization 48
Features Introduced in ArubaOS 6.4.1.0 48
AP-Platform 48
Support for AP-103H 48
Support for AP-200 Series 48
AP Regulatory 49
Downloadable Regulatory Table 49
Controller-Platform 49
7000 Series Controllers 49
AirGroup 49
AP Fast Failover Support for Bridge-mode Virtual AP 49
DHCP Lease Limit on 7000 Series Controllers 50
Selective Multicast Stream 50
Security 50
Authentication Profile based User Idle Timeout 50
Global Firewall Parameters 50
Features Introduced in ArubaOS 6.4.0.2 51
ArubaOS-AirWave Cross-Site Request Forgery Mitigation 51
Upgrade Recommendations 51
Fixed Software Versions 51

Frequently Asked Questions 51
EAP-MD5 Support 52
Features Introduced in ArubaOS 6.4.0.1 52
PhoneHome Reporting Enhancements 52
Features Introduced in ArubaOS 6.4.0.0 53
AP-Platform 53
Support for the AP-270 Series 53
Support for the AP-103 53
Hotspot 2.0 53
AP-220 Series Enhancements 54
AP-130 Series Functionality Improvements when Powered Over 802.3af (POE) 54
Franklin Wireless U770 4G Modem Support 54
Huawei E3276 LTE Modem Support 54
Authentication 54
Authentication Server Limits 54
EAP-MD5 Support 54
Controller-Platform 55
AirGroup 55
AppRF 2.0 56
Branch 57
Controller LLDP Support 58
High Availability 58
Features not Supported on 600 Series Controllers 59
Control Plane Bandwidth Contracts Values 60
Automatic GRE from IAP 60
DHCP Lease Limit 60
IPv6 60
Multicast Listener Discovery (MLDv2) Snooping 60
Static IPv6 GRE Tunnel Support 61

IPv6 Enhancements 61
VRRPv3 Support on Controllers 62
Security 62
Warning Message for Containment Features 62
Palo Alto Networks Firewall Integration 62
Application Single Sign-On Using L2 Network Information 63
802.11w Support 63
Ability to Disable Factory-Default IKE/IPsec Profiles 63
AOS/ClearPass Guest Login URL Hash 63
Authentication Server Load Balancing 63
Enhancements in the User Authentication Failure Traps 63
RADIUS Accounting on Multiple Servers 63
RADIUS Accounting for VIA and VPN Users 63
Spectrum Analysis 64
AP Platform Support for Spectrum Analysis 64
Voice and Video 64
Unified Communication and Collaboration 64
AP Support 64
Regulatory Updates 67
Regulatory Updates in ArubaOS 6.4.3.1 67
Regulatory Updates in ArubaOS 6.4.3.0 67
Regulatory Updates in ArubaOS 6.4.2.5 68
Regulatory Updates in ArubaOS 6.4.2.4 74
Regulatory Updates in ArubaOS 6.4.2.3 75
Regulatory Updates in ArubaOS 6.4.2.2 77
Regulatory Updates in ArubaOS 6.4.2.1 78
Regulatory Updates in ArubaOS 6.4.2.0 79
Regulatory Updates in ArubaOS 6.4.0.2 83

Regulatory Updates in ArubaOS 6.4.0.0 83

Resolved Issues **85**

Resolved Issues in ArubaOS 6.4.3.1 85

Air Management-IDS 85

AP-Datapath 85

Base OS Security 86

Captive Portal 86

Controller-Datapath 86

IPsec 87

Remote AP 87

Station Management 87

Resolved Issues in ArubaOS 6.4.3.0 88

AMON 88

AirGroup 88

Air Management-IDS 89

AP Datapath 90

90

AP-Platform 90

AP-Wireless 92

ARM 93

Authentication 93

Base OS Security 94

Captive Portal 95

Configuration 96

Controller-Datapath 96

Controller-Platform 98

IPsec 99

LDAP 99

Licensing 99
Local Database 100
Logging 100
Master-Local 100
Master-Redundancy 101
Mesh 101
Mobility 101
PhoneHome 102
PPTP 102
Radius 103
Remote AP 104
SNMP 105
Station Management 106
TACACS 107
Voice 107
VRRP 108
WebCC 108
WebUI 109
Resolved Issues in ArubaOS 6.4.2.5 110
AirGroup 110
AP-Datapath 111
AP-Platform 111
AP-Wireless 113
ARM 114
Base OS Security 115
Captive Portal 115
Configuration 115
Controller-Datapath 116
Controller-Platform 117

CPSec-Whitelist Management 117
IPsec 118
IPv6 118
Mobility 118
Radius 119
Remote AP 119
Station Management 119
Voice 120
VRRP 120
Web Content Classification 120
WebUI 121
WMM 121
Resolved Issues in ArubaOS 6.4.2.4 121
Advanced Monitoring 121
AirGroup 122
AP Datapath 122
AP-Platform 122
AP-Wireless 123
Authentication 123
Base OS Security 123
Configuration 124
Control Plane Security Whitelist Management 124
Controller-Datapath 124
Controller-Platform 125
DHCP 125
Guest Provisioning 125
IPv6 126
Port-Channel 126
Remote AP 126

Station Management 127
VRRP 127
Resolved Issues in ArubaOS 6.4.2.3 127
AirGroup 127
Air Management-IDS 128
AP-Datapath 128
AP-Platform 129
AP-Regulatory 130
AP-Wireless 130
ARM 132
Authentication 132
Base OS Security 133
Controller-Datapath 133
Controller-Platform 134
Mesh 135
Remote AP 136
Station Management 136
VRRP 136
Web Content Classification 137
WebUI 137
Wi-Fi Multimedia 137
Resolved Issues in ArubaOS 6.4.2.1 138
Activate 138
AirGroup 138
Air Management-IDS 138
AP-Platform 139
AP-Wireless 139
Base OS Security 140
Configuration 140

Controller-Datapath 141
Controller-Platform 142
HA-Lite 143
Hotspot-11u 143
Local Database 143
Mobility 143
Station Management 144
VRRP 144
WebUI 145
Resolved Issues in ArubaOS 6.4.2.0 145
802.1X 145
Air Management-IDS 145
AP-Platform 146
AP-Wireless 146
ARM 146
Base OS Security 147
Controller-Datapath 147
Controller-Platform 148
GRE 148
Licensing 148
LLDP 149
Policy Based Routing 149
QoS 149
Remote AP 150
Role/VLAN Derivation 150
Station Management 150
WebUI 151
Resolved Issues in ArubaOS 6.4.1.0 151
AirGroup 151

Air Management-IDS 153
AP Regulatory 153
AP-Platform 153
AP-Wireless 154
ARM 155
Authentication 155
Base OS Security 156
Captive Portal 157
Certificate Manager 157
Configuration 157
Controller-Datapath 158
Controller-Platform 159
DHCP 160
LLDP 161
Local Database 161
IPsec 161
Master-Redundancy 162
RADIUS 162
Remote AP 162
Role/VLAN Derivation 163
Routing 163
Startup Wizard 164
Station Management 164
Voice 164
WebUI 165
XML API 166
Resolved Issues in ArubaOS 6.4.0.3 166
Base OS Security 166
Resolved Issues in ArubaOS 6.4.0.2 166

Application Monitoring (AMON) 166
AP-Platform 167
AP-Regulatory 167
AP-Wireless 168
Base OS Security 168
Captive Portal 168
Controller-Datapath 169
Controller-Platform 169
IPsec 169
Mobility 170
RADIUS 170
Remote AP 170
Station Management 170
Voice 171
WebUI 171
Resolved Issues in ArubaOS 6.4.0.1 171
PhoneHome 171
Resolved Issues in ArubaOS 6.4.0.0 172
802.1X 172
AirGroup 172
Air Management-IDS 173
AP-Datapath 173
AP-Platform 174
AP Regulatory 177
AP-Wireless 178
ARM 183
Authentication 183
Base OS Security 183
Configuration 186

Captive Portal 186
Controller-Datapath 188
Controller-Platform 192
Control Plane Security 195
DHCP 195
Generic Routing Encapsulation 195
GSM 195
Guest Provisioning 196
HA-Lite 196
Hardware Management 196
IGMP Snooping 196
IPv6 197
Licensing 197
Local Database 197
Master-Redundancy 197
Mesh 198
Mobility 198
PPPoE 198
Remote AP 199
Role/VLAN Derivation 200
SNMP 200
Station Management 201
TACACS 201
VLAN 201
Voice 202
WebUI 203
WLAN Management System 204
XML API 205

Known Issues and Limitations 207
Known Issues and Limitations in ArubaOS 6.4.3.1 207
AP-Platform 207
AP-Wireless 208
ARM 209
Base OS Security 209
Captive Portal 210
Controller-Datapath 211
Controller-Platform 213
DDS 214
HA-Lite 214
Licensing 215
Master-Local 215
Voice 215
WebUI 216
Known Issues and Limitations in ArubaOS 6.4.3.0 216
AP-Wireless 216
Base OS Security 216
Configuration 217
Controller-Datapath 217
Controller-Platform 218
HA-Lite 218
Licensing 218
Monitoring 219
Radius 219
VRRP 219
Known Issues and Limitations in ArubaOS 6.4.2.5 219
AP-Datapath 220

AP-Platform 220
AP-Wireless 221
Base OS Security 221
Captive Portal 222
Controller-Platform 222
LLDP 223
Voice 223
Known Issues and Limitations in ArubaOS 6.4.2.4 223
No Support for Mesh in AP-200 Series 223
AP-Datapath 223
AP-Platform 224
AP-Wireless 224
Base OS Security 224
Controller-Datapath 225
Controller-Platform 225
Known Issues and Limitations in ArubaOS 6.4.2.3 225
Base OS Security 225
Controller-Datapath 226
Controller-Platform 226
HA-Lite 226
Port-Channel 226
Remote AP 227
Voice 227
Known Issues and Limitations in ArubaOS 6.4.2.1 227
AP Wireless 227
HA-Lite 227
Local Database 228
Remote AP 228
Known Issues and Limitations in ArubaOS 6.4.2.0 228

AP Wireless 228
AP Platform 228
Controller-Datapath 229
Known Issues and Limitations in ArubaOS 6.4.1.0 229
AP Regulatory 229
Controller-Datapath 229
Remote AP 230
WebUI 230
Known Issues and Limitations in ArubaOS 6.4.0.2 230
AP-Wireless 230
Controller-Platform 231
LLDP 231
Startup Wizard 231
Known Issues and Limitations in ArubaOS 6.4.0.0 231
AirGroup 232
AP-Platform 232
AP-Wireless 232
Configuration 232
Controller-Datapath 233
Controller-Platform 234
DHCP 234
Hardware-Management 235
IPSec 235
Local Database 235
LLDP 235
Master-Local 236
RADIUS 236
Remote AP 236
Station Management 237

WebUI 237
Issues Under Investigation 237
AP-Wireless 237
Controller–Datapath 238
Upgrade Procedure 239
Upgrade Caveats 239
Peer Controller Upgrade Requirement 240
Important Points to Remember 240
Installing the FIPS Version of ArubaOS 6.4.3.1 240
Before Installing FIPS Software 240
Important Points to Remember and Best Practices 240
Memory Requirements 241
Backing up Critical Data 242
Backup and Restore Compact Flash in the WebUI 242
Backup and Restore Compact Flash in the CLI 242
Upgrading in a Multi-Controller Network 243
Upgrading to ArubaOS 6.4.3.1 243
Install Using the WebUI 243
Upgrading From an Older version of ArubaOS 243
Upgrading From a Recent version of ArubaOS 244
Install Using the CLI 245
Upgrading From an Older Version of ArubaOS 245
Upgrading From a Recent Version of ArubaOS 245
Downgrading 247
Before You Begin 247
Downgrading Using the WebUI 247
Downgrading Using the CLI 248
Before You Call Technical Support 249

ArubaOS 6.4.3.1 is a software patch release that introduces fixes to the issues identified in previous releases.

NOTE

See the Upgrade Procedure on page 239 for instructions on how to upgrade your controller to this release.

Chapter Overview

- Features in 6.4.x Releases on page 27 provides a description of features and enhancements introduced in ArubaOS 6.4.x release versions.
- Regulatory Updates on page 67 describes the regulatory updates in ArubaOS 6.4.x release versions.
- Resolved Issues on page 85 describes the issues resolved in ArubaOS 6.4.x release versions.
- Known Issues and Limitations on page 207 describes the known and outstanding issues identified in ArubaOS 6.4.x release versions.
- Upgrade Procedure on page 239 describes the procedures for upgrading a controller to ArubaOS 6.4.3.1.

Important Points to Remember

If you modify the configuration of an AP, those changes take effect immediately; you do not need to reboot the controller or the AP for the changes to affect the current running configuration. Certain commands, however, automatically force the AP radio to restart.

AP Settings Triggering a Radio Restart

Changing the following settings triggers the radio to restart on the AP-200 Series, AP-210 Series, AP-220 Series, or AP-270 Series access points. When the radio restarts, wireless services will be briefly interrupted. Clients will automatically reconnect to the network once the radio is back up and running.

Table 1: *Profile Settings*

Profile	Settings
802.11a/802.11g Radio Profile	• Channel • Enable Channel Switch Announcement (CSA) • CSA Count • High throughput enable (radio) • Very high throughput enable (radio) • TurboQAM enable • Maximum distance (outdoor mesh setting) • Transmit EIRP • Advertise 802.11h Capabilities • Beacon Period / Beacon Regulate • Advertise 802.11d Capabilities
Virtual AP Profile	• Virtual AP enable • Forward Mode • Remote-AP operation

SSID Profile	• ESSID
	• Encryption
	• Enable Management Frame Protection
	• Require Management Frame Protection
	• Multiple Tx Replay Counters
	• Strict Spectralink Voice Protocol (SVP)
	• Wireless Multimedia (WMM) settings
	  ▪ Wireless Multimedia (WMM)
	  ▪ Wireless Multimedia U-APSD (WMM-UAPSD) Powersave
	  ▪ WMM TSPEC Min Inactivity Interval
	  ▪ Override DSCP mappings for WMM clients
	  ▪ DSCP mapping for WMM voice AC
	  ▪ DSCP mapping for WMM video AC
	  ▪ DSCP mapping for WMM best-effort AC
	  ▪ DSCP mapping for WMM background AC

High-throughput SSID Profile	• High throughput enable (SSID) • 40 MHz channel usage • Very High throughput enable (SSID) • 80 MHz channel usage (VHT)
802.11r Profile	• Advertise 802.11r Capability • 802.11r Mobility Domain ID • 802.11r R1 Key Duration • key-assignment (CLI only)
Hotspot 2.0 Profile	• Advertise Hotspot 2.0 Capability • RADIUS Chargeable User Identity (RFC4372) • RADIUS Location Data (RFC5580)

Supported Browsers

The following browsers are officially supported for use with ArubaOS 6.4.3.1 WebUI:

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or higher on Windows Vista, Windows 7, and MacOS
- Apple Safari 5.1.7 or higher on MacOS

Contacting Support

Table 2: *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	http://www.arubanetworks.com/support-services/contact-support/
Software Licensing Site	https://licensing.arubanetworks.com/
End of Support Information	http://www.arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	http://www.arubanetworks.com/support-services/security-bulletins/
Support Email Addresses	
Americas, EMEA, and APAC	support@arubanetworks.com
Security Incident Response Team (SIRT)	sirt@arubanetworks.com

This chapter describes features introduced in ArubaOS 6.4.x release versions. For more information about features introduced in ArubaOS 6.4.x, refer to the *ArubaOS 6.4.x User Guide*.

Features Introduced in ArubaOS 6.4.3.1

This section describes the new features and enhancements introduced in ArubaOS 6.4.3.1.

Modified Commands

The following commands are modified in ArubaOS 6.4.3.1.

interface vlan

The following new sub-parameter is introduced for the **option-82** parameter in the **interface vlan** command:

Parameter	Description	Default
`ap-name [essid]`	Allows a controller, when acting as a DHCP relay agent, to insert circuit specific information about the AP and SSID through which a client is connected, into a request that is forwarded to a DHCP server.	-

show interface vlan

The following new parameter is introduced as part of the output of the **show interface vlan** command:

Parameter	Description	Default
`DHCP Option-82 AP name and ESSID are configured on this Interface`	Displays the status of DHCP Option-82 if the AP-name and ESSID are configured on the interface.	-

Features Introduced in ArubaOS 6.4.3.0

This section describes the new features and enhancements introduced in ArubaOS 6.4.3.0.

AP-Platform

Support for the AP-205H Access Point

The AP-205H access point is a high-performance 802.11ac dual radio wired and wireless access point for hospitality and branch deployments. This device combines high-performance wireless mobility with Gigabit wired local access to deliver secure Wi-Fi network access to dormitories, hotel rooms, classrooms, medical clinics, and multi-tenant environments. MIMO (Multiple-Input Multiple-Output) technology enables the AP-205H to provide wireless 2.4 GHz 802.11n and 5 GHz 802.11n/ac functionality, while simultaneously

supporting existing 802.11a/b/g wireless services. The AP-205H access point works in conjunction with an Aruba controller.

The AP-205H provides the following capabilities:

- Dual wireless transceiver
- Protocol-independent networking functionality
- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor and spectrum analyzer
- Compatibility with IEEE 802.3af/at PoE
- Central management configuration and upgrades using a controller
- POE power sourcing to an attached POE network device
- Support for select USB peripherals

For more information, see *AP-205H Wireless Access Point Installation Guide*.

Support for the AP-228 Access Point

The AP-228 access point is a fully temperature hardened, water resistant, indoor rated, dual-radio IEEE 802.11ac access point. This access point use MIMO (Multiple-In Multiple-Out) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g/n wireless services. The AP-228 access point works in conjunction with an Aruba controller.

The AP-228 provides the following capabilities:

- Wireless transceiver
- Wireless access point (IEEE 802.11 a/b/g/n/ac)
- Wireless air monitor (IEEE 802.11 a/b/g/n/ac)
- Protocol-independent networking functionality
- Compatibility with IEEE 802.3at PoE
- Central management configuration and upgrades using a controller

For more information, see the *AP-228 Wireless Access Point Installation Guide*.

Support for the AP-277 Access Point

The AP-277 access point is an environmentally hardened, outdoor rated, dual-radio IEEE 802.11ac access point. This access point use MIMO (Multiple-In Multiple-Out) technology and other high throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g/n wireless services. The AP-277 access point works in conjunction with an Aruba controller.

The AP-277 provides the following capabilities:

- Wireless transceiver
- Wireless access point (IEEE 802.11 a/b/g/n/ac)
- Wireless air monitor (IEEE 802.11 a/b/g/n/ac)
- Protocol-independent networking functionality
- Compatibility with IEEE 802.3at PoE
- Central management configuration and upgrades using a controller

For more information, see the *AP-277 Wireless Access Point Installation Guide*.

USB Modem Support for AP-210 Series and AP-220 Series

The AP-210 Series and AP-220 Series access points now support all USB modems supported by other Aruba APs.

AP Console Access Using a Backup ESSID

This failover system allows users to access an AP console after the AP has disconnected from the controller. By advertising backup ESSID in either static or dynamic mode, the user is still able to access and debug the AP remotely through a virtual AP. Settings for this feature can be changed using the controller's WebUI or CLI.

ARM

Anyspot Client Probe Suppression

The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks. By reducing the frequency at which these messages are sent, this feature frees up network resources and improves network performance.

AP Scanning Optimization

The scanning algorithm is enhanced to reduce the delay between visits to some channel types, by changing their scan priority.

Branch Controller

ArubaOS supports distributed enterprises through the following features designed specifically for branch and remote offices.

NOTE

Throughout this document, the term **branch controller** will refer to a 7000 Series Cloud Services controller that has been configured via a branch config group created using the **Configuration>Branch>Smart Config** section of the ArubaOS WebUI.

Authentication Survivability

Authentication survivability allows controllers to provide authentication and authorization survivability when remote authentication servers are not accessible. It stores user access credentials, as well as Key Reply attributes, whenever clients are authenticated with external RADIUS servers or LDAP authentication servers.

When external authentication servers are not accessible, the controller uses its local survival server to continue providing authentication and authorization functions by using the user access credentials and Key Reply attributes that were stored earlier.

Branch Controller Integration with Palo Alto Networks Firewalls

Enable this feature on a master controller to securely redirect internet inbound traffic from branch or local controllers into the Palo Alto Networks (PAN) firewall. The Palo Alto Networks Large-Scale VPN (LSVPN) framework can integrate with a branch or local controller by establishing an IPsec tunnels between the firewall and the controller. Integrating a Palo Alto Networks firewall with a 7000 Series controller requires that all user traffic is routed, so it can be managed by a policy-based routing access control list. If PAN gateways are deployed across multiple datacenters, PAN devices must have a public IP or be behind a single NAT device so that reverse traffic comes back to the correct PAN gateway.

Monitor WAN Health

The health-check feature uses ping probes to measure WAN reachability and latency. Latency is calculated based on the round-trip time (RTT) of ping responses. The results of this health check appears in the WAN section of the Monitoring Dashboard.

Per-Interface Bandwidth Contracts

7000 Series and 7200 Seriescontrollers have the ability to classify and identify applications on the network. If a 7000 Series or 7200 Seriescontroller is configured as a branch controller, you can create bandwidth contracts to limit traffic for individual applications (or categories of applications) either sent from or received by a selected interface.

Policy-Based Routing

In ArubaOS 6.4.3.0, firewall policies support rules based on routing actions that can forward packets through an IPsec tunnel defined by the specified IPsec map, a device on a next hop list, GRE tunnel, or tunnel group.

PortFast and BPDU Guard

The PortFast feature is introduced to avoid network connectivity issues caused by delays in STP enabled ports moving from blocking-state to forwarding-state after transitioning from the listening and learning states.

BPDU Guard feature protects the port from receiving STP BPDUs.

Uplink Routing using Next-Hop Lists

A next-hop list provides redundancy for next-hop devices by forwarding the traffic to another next-hop device on the list if the higher-priority next-hop device fails. If the active next-hop device on the list becomes unreachable, traffic matching a policy-based routing ACL is forwarded using the highest-priority active next-hop on the list. If preemptive failover is enabled and a higher priority next-hop becomes reachable again, packets are again forwarded to the higher priority next-hop.

Virtual APs for WAN Link Failure

In the branch controller deployments, the local controllers are connected across the WAN link from the master controller to the RADIUS server. A WAN link outage will result in service outage as new users cannot be authenticated to 802.1X Virtual APs. This feature provides limited connectivity to branch controllers even when the WAN link is down. To provide connectivity when the WAN link is down, open and PSK SSID Virtual APs (VAPs) are available at all times and the user can connect to these VAPs instead of the main 802.1X Virtual AP.

WAN Optimization

WAN Optimization consists of IP payload data compression, which reduces the size of the data frames transmitted over a network link, thereby reducing the time required to transmit the frame across the network. Because the condensed frames take up less bandwidth, the network can transmit greater volumes of data. Internetworking devices employ lossless compression algorithms. These algorithms reproduce the original bit streams exactly, with no degradation or loss.

WebUI Enhancements for WAN

The WAN (Wide Area Network) dashboard, in the Dashboard section of the WebUI, is the landing page for the branch controller. The WAN dashboard provides the WAN summary details for VLANs such as status, throughput, latency, alerts, usage, and compression.

Zero Touch Provisioning

A managed node (MN) is an zero-touch provision (ZTP) controller that can automatically get its local and global configuration and license limits from a central controller. A local or branch controller with factory default settings can now gather the required information from the network and then provision itself automatically, like an AP. ZTP automates the configuration of local or branch controllers during initial installation without any user intervention.

Client Match

BSS Transition Management Support

The BSS Transition Management Support feature allows Client Match to steer devices using 802.11v BSS transition management standards for continuous wireless connectivity. This feature provides a seamless standards compatible method of device steering in wireless networks, as 802.11v BSS transition management support has become increasingly common in wireless devices.

Multi-Media Sync-Up

Client Match offers a tighter integration with multiple media-aware ALGs to provide better call quality for programs like Lync and Facetime. With Client Match's ability to understand various media protocols, clients are not steered to different APs in the middle of an active media session.

When the AP learns that the client is in a call, it will not attempt to steer the client to another AP until the controller indicates that the call has ended, allowing calls to run more smoothly without any disruptions to the ongoing media flow.

Removing VBR Dependency on Probe Requests

Client Match has shifted its dependency on probe requests to the AM data feed for virtual beacon report (VBR) data. Instead of relying solely on client background scans during probe requests, which can cause limitations due to low scanning frequency, Client Match uses AM data feeds to gain more continuous, comprehensive client RSSI feeds.

Controller-Datapath

Wi-Fi Packet Capture in Split-Tunnel Forwarding Mode

Starting with ArubaOS 6.4.3.0, the controller not only captures the egress traffic of the wireless client but also the ingress traffic in split-tunnel forwarding mode using the **packet-capture datapath wifi-client <client-mac> all** command.

Controller-Platform

7024 Controller

The 7024 controller is a wireless LAN controller that connects, controls, and intelligently integrates wireless Access Points (APs) and Air Monitors (AMs) into a wired LAN system.

There are two models of the 7024 controller that do not differ physically or functionally from each other.

- 7024-US—For the United States of America
- 7024-JP—For Japan
- 7024-RW—For the rest of the world

The 7024 controller has the following specification:

Table 3: *7024 Controller Specification*

Model	Access Ports	Number of APs Supported	Number of Users Supported
7024	• 24 x 10/100/1000BASE-T PoE/PoE+ • 2 x 10GBASE-X	32	2048

For more information, see *Aruba 7024* Controller *Installation Guide*.

7205 Controller

The 7205 controller is a wireless LAN controller that connects, controls, and intelligently integrates wireless Access Points (APs) and Air Monitors (AMs) into a wired LAN system.

There are two models of the 7205 controller that do not differ physically or functionally from each other.

- 7205-US—For the United States of America
- 7205-JP—For Japan
- 7205-RW—For the rest of the world

The 7205 controller has the following specification:

Table 4: *7205 Controller Specification*

Model	Ports	Number of APs Supported	Number of Users Supported
7205	• 4 x dual-media (10/100/1000BASE-T and 1000BASE-X) • 2 x 10GBASE-X	256	8192

For more information, see *Aruba 7205 Controller Installation Guide*.

DHCP Lease Limit on 7000 Series Controllers

The following table outlines the maximum number of DHCP leases supported on the 7024 and 7205 controllers.

Table 5: *DHCP Lease Limit*

Platform	DHCP Lease Limit
7024	1024
7205	4096

AMON Message Size Changes on the Controller

Data communication between Aruba controllers and AirWave servers has shifted from the SNMP model to the faster, more reliable, and scalable AMON model. Though the SNMP model can still be used to communicate data, users generally encounter delayed AirWave updates and high controller and process CPU usage.

The AMON packet size has been capped at a default value of 1500 bytes to reduce the amount of fragmentation and message loss that typically occurs in larger packet sizes, which can force customers to fall back to the SNMP model. Message size has been capped at 1400 bytes to allow for the addition of AMON headers and PAPI/UDP/IP headers. Each packet only contains one message to further reduce the amount of overall message loss, as the loss of even a single fragment can render an entire message invalid.

Flexible Licensing for AP Controllers

ArubaOS 6.4.3.0 offers flexible licensing support for controllers, which were previously restricted to set license counts. With this licensing scheme, which works with AP, PEFNG, and RFP licenses, customers can request licenses with a customizable license count. This customized license count is attached to a single key, simplifying the licensing process by reducing the number of licenses required for your system.

Modem Support on 7000 Series Controllers

The following USB modems are supported on the 7000 Series controllers:

- Netgear AirCard 340U USB modem for AT&T's LTE service.
- Netgear AirCard 341U USB modem for Sprint's LTE service.

For up-to-date information on inter-operation with popular Wi-Fi devices and other non-Wi-Fi peripherals, refer to the interoperability web page located here.

Serviceability

Username and Password Protection for the AP Console

The ArubaOS AP console username and password feature helps protect systems that manage highly sensitive information, like financial and banking institutions, by requiring users to login to the AP network with a username and password.

Under the default configuration, consoles do not have passwords. To protect your network, a username and password can be set while the AP is in enabled mode. The timeout feature is also supported as an added level of security. If there is no user input or activity during one timeout interval (default of 30 minutes), the user is logged out of the system. The timeout interval cannot be modified.

PhoneHome-Lite

PhoneHome-lite is an HTTPS-based tracking tool used to monitor WebCC feature usage on each controller. Aruba controllers communicate with Activate servers over a secure HTTPS SSL layer through the PhoneHome infrastructure to send information about which users have enabled WebCC. This usage data can then be analyzed to determine the scope of future WebCC feature licensing.

Security

AP-Group and AP-Name in Campus AP Whitelist

The Campus AP whitelist of a controller contains the AP-Group and AP-Name in addition to the MAC address of an AP. When CPSec is enabled, a campus AP uses the AP-Group and AP-Name from the Campus AP CPSec whitelist. If AP-Group and AP-Name is not defined, a campus AP uses "default" as AP-Group and its MAC address as AP-Name.

Centralized Control Plane Security Whitelist on CPPM

The control plane security whitelist is centralized with Clearpass Policy Manager (CPPM). A controller fetches the whitelist from CPPM instead of from the local database.

RadSec on RADIUS Servers

Enable RadSec to increase the level of security for authentication that takes place across unsecured networks such as the Internet. The RadSec enhancement is introduced to ensure RADIUS authentication and accounting data is transmitted safely and reliably across unsecure networks.

Configuring IKE Policies

A controller operating in FIPS mode is not permitted to configure Deffie-Hellman Group 1 and Group 2 group types.

Generating a Certificate Signing Request (CSR)

If the controller is operating in FIPS mode and the **CSR Type** is **rsa**, then the key length **1024** is not permitted.

Voice and Video

UCC Score for Lync Media Classification

Starting with ArubaOS 6.4.3.0, the controller supports UCC score for Lync calls prioritized using media classification. As part of this feature, Unified Communication Manager (UCM) supports the following:

- Real-time quality analysis for Lync voice and video calls (voice RTP streams only)
- Real-time computation of UCC score (delay, jitter, and packet loss) for Lync VoIP calls prioritized using media classification. The UCC score is computed by the AP in the downstream direction.
- Call Quality vs. Client Health chart in the UCC dashboard of the controller

NOTE

When VoIP calls are prioritized using media classification, end-to-end call quality metrics such as Mean Opinion Score (MOS), delay, jitter, and packet loss are not available.

Lync SDN API 2.1 Support

Starting with ArubaOS 6.4.3.0, the controller supports Lync SDN API version 2.1. As part of Lync SDN API 2.1, Lync SDN Manager (LSM) sends In-Call quality update messages to the controller. The In-Call quality update message provides visibility on the end-to-end delay, jitter, packet loss, and MOS periodically for VoIP calls that are active. In earlier versions of Lync SDN API, LSM sent end-to-end quality updates to the controller at the end of a VoIP call.

In addition, Lync SDN API 2.1 supports the following new features:

- A new XML schema which is supported from ArubaOS 6.4.3.0.
- Message forwarding enhancement - Ability to direct messages to specific controllers based on subnet or domain. Controllers now only receive events for relevant calls based on the calls' originating or terminating subnet or the SIP domain of the calling or called party.

WebUI Enhancements

Controller Health Monitoring

The Controller page displays details of the controllers and their health related information, such as CPU usage, memory usage, temperature, and fan speed.

WLAN

Auto-tagging and Controller-based Policy

AirGroup supports auto-tagging, which ensures that all the AirGroup users associated to an AP, its neighbors, AP-group, or AP-FQLN discover nearby AirGroup servers. By default, auto-tagging is disabled on all AirGroup servers. An administrator can enable auto-tagging for each AirGroup server separately and configure AP-name, AP-group, or AP-FQLN for auto-tagging. If auto-tagging is enabled, other location-based policy configuration for the AirGroup server on CPPM or CLI is not honored. Auto-tagging is applicable only for wireless AirGroup servers.

Maximum Number of iChat Users

The maximum number of iChat users is limited to 2000. Each iChat user is an mDNS server and their announcement messages are L2 multicast.

mDNS AP VLAN Aggregation

The mDNS AP VLAN aggregation allows the discovery of wired mDNS/SSDP devices which do not have L2 connectivity with the controller or which do not trunk in the controller. An AP, which is in the same VLAN as the

wired mDNS/SSDP device which does not trunk in the controller, receives and forwards the mDNS/SSDP packets from the wired mDNS/SSDP devices to the controller and from the controller to the wired mDNS/SSDP device. The AP forms a separate split tunnel with the controller and aggregates all mDNS/SSDP traffic to and from the controller.

mDNS-based Device Discovery of Apple TV

Apple devices support a Bluetooth-based device discovery mechanism, which allows an Apple device to discover an Apple TV that is within its Bluetooth range. AirGroup supports only mDNS-based device discovery and does not support Bluetooth-based device discovery mechanisms.

Mesh Support for 802.11ac

Mesh support has been added for all 802.11ac-capable access points. A number of new parameters have been added to the mesh high-throughput ssid profile to support this functionality.

Multicast Response Propagation for mDNS

The mDNS multicast response propagation allows services to multicast the response packet. This allows the existing users to instantly see a new user when a new user logs in. The mDNS response packet for iChat or Messages Application is multicast across all VLANs that are trunked in the controller.

Features Introduced in ArubaOS 6.4.2.5

This section describes the new feature enhancements introduced in ArubaOS 6.4.2.5.

RADIUS Service-Type Attribute

Starting with ArubaOS 6.4.2.5, the controller sends the following service-type attribute values for RADIUS authentication requests.

Table 6: *RADIUS Service-Type Attributes*

RADIUS Attribute	Authentication Type	Attribute Value
Service-Type	MAC	Call-Check
	802.1X	Framed
	Captive Portal	Login

The service-type-framed-user configuration of the RADIUS server overwrites all the attribute values to Framed irrespective of the authentication type. Existing deployments that depend upon this attribute for their third-party RADIUS integrations should make changes to support these new service types.

Controller Authentication to CPPM

The controller authentication to ClearPass Policy Manager (CPPM) is enhanced to use a configurable username and password instead of a support password. The support password is vulnerable to attacks as the server certificate presented by CPPM server is not validated.

In the WebUI

To configure controller authentication to CPPM:

1. Navigate to **Configuration** > **Security> Authentication> Servers**.
2. Under **Radius Server**, select the server name.

3. Enter the **cppm_username** and **cppm_password** parameters in the **CPPM credentials** field.
4. Click **Apply**.

In the CLI

To configure controller authentication to CPPM:

```
(host) (config) #aaa authentication-server radius <radius_server_name>
(host) (RADIUS Server "<radius_server_name>") #cppm username <username> password <password>
```

Handling GARPs

Gratuitous ARP (GARP) messages are not flooded from clients to wireless tunnels or wired interfaces. GARPs from Virtual APs using tunnel or decrypt-tunnel forwarding modes are dropped in the ingress when the **firewall optimize-dad-frames** command is set to enabled. This parameter is enabled by default.

In the CLI

The **firewall optimize-dad-frames** parameter is enabled by default. To disabled this parameter:

```
(host) (config) #no firewall optimize-dad-frames
```

To view the status of GARPs:

```
(host) #show firewall

Global firewall policies
------------------------
Policy                                          Action          Rate            Port
------                                          ------          ----            ----
Enforce TCP handshake before allowing data      Disabled
Prohibit RST replay attack                      Disabled
..
..
Optimize Duplicate Address Detection frames     Disabled
```

NetGear AirCard 341U USB Modem Support

ArubaOS 6.4.2.5 introduces support of the Netgear AirCard 341U USB modem on 7000 Seriescontrollers.

Modified Commands

The following commands are modified in ArubaOS 6.4.2.5.

show web-server profile

The following new parameter is introduced as part of the output of the **show web-server profile** command:

Parameter	Description	Default
`Enable bypass captive portal landing page`	Displays the status of the bypass captive portal landing page.	false

web-server profile

The following new parameter is introduced in the **web-server profile** command:

Parameter	Description	Default
`bypass-cp-landing-page`	Disables the bypass captive portal landing page. On disabling this feature, non-browser apps continue to request Captive Portal login page from the controller. **NOTE:** This increases the load of the **httpd** process of the controller. **NOTE:** The landing page contains the meta-refresh tag to reload the page using real browser applications.	enabled

Features Introduced in ArubaOS 6.4.2.4

This section describes the new feature enhancements introduced in ArubaOS 6.4.2.4.

USB Storage for CSR and Key Files

ArubaOS 6.4.2.4 introduces an enhancement to the custom certificate support for Remote AP (RAP) feature by storing the Certificate Signing Request (CSR) and private key from the RAP in a USB. To provision a RAP to store the CSR and private key in a USB, use one of the following options:

AP Boot Prompt

At the AP boot prompt, issue the **setenv usb_csr 1** and **setenv usb_type 100** commands.

NOTE

If this option is used to provision the RAP to store the files in the USB device, after the files are saved in the USB, enter the AP boot prompt to issue the **setenv usb_csr 0** command. This is mandatory.

Controller WebUI

To store the CSR and private key files from a RAP to a USB device:

1. Navigate to **Configuration** > **Wireless** > **AP Installation** > **Provisioning**.
2. Select the RAP, click **Provision**.
3. Under **USB Settings**, select the **USB Parameters** check box.
4. Select the **USB storage for CSR/Key** check box.
5. Select **Device Type** as **storage**.
6. Click **Apply and Reboot**.

Controller CLI

To store the CSR and private key files from a RAP to a USB device:

```
(host) (config) #provision-ap
(host) (AP provisioning) #read-bootinfo ap-name <ap name>
(host) (AP provisioning) #usb-csr
(host) (AP provisioning) #usb-type storage
```

RAP Console

To store the CSR and private key files from a RAP to a USB device:

1. Navigate to **Configuration** > **Management** > **Certificates**.
2. For **Store CSR and key in USB/Flash**, select **USB** from the drop-down list.

After the RAP is provisioned to store the CSR and private key in a USB, log in to the RAP console, export the CSR and private key files to the USB. A **.p12** certificate file format must be manually created as the RAP certificate in the USB to bring up the IKE/IPSEC connection.

SFP/SFP+ modules

ArubaOS 6.4.2.4 introduces support for the following SFP/SFP+ modules:

Table 7: *Supported SFP/SFP+ Modules*

SFP	Description
SFP-EX	Aruba SFP, 1000BASE-EX, LC Connector; 1550 nm pluggable GbE optic; up to 40,000 meters over single-mode fiber.
SFP-ZX	Aruba SFP, 1000BASE-ZX, LC Connector; 1310nm pluggable GbE optic; up to 70,000 meters over single-mode fiber.
SFP-10G-ZR	Aruba SFP, 10GBASE-ZR, LC Connector; 1550nm pluggable SFP+ optic; up to 80,000 meters over single-mode fiber.

Modified Commands

The following commands are modified in ArubaOS 6.4.2.4.

show dot1x watermark

The following new parameters are introduced in the **show dot1x watermark** command:

Parameter	Description	Range	Default

`table`
`active`
`pending`
	Table types:
	• **active**: Displays all current active sessions in the 802.1X queue and the corresponding user-age.
	• **pending**: Displays all pending sessions in the 802.1X queue, the duration for which the user is pending in the queue, and the corresponding user-age.
		–	–

The following examples show the outputs of the newly introduced **active** and **pending** parameters:

```
(host)# show dot1x watermark table active
Dot1x Active Table
------------------
MAC                User-Age (m:s)
---                --------------
11:11:11:11:11:cd 00:11
11:11:11:11:11:ce 00:10

(host)#  show dot1x watermark table pending
Dot1x Pending Table
-------------------
MAC                Time in PendingQ (s:ms) User-Age (m:s)
---                ----------------------- --------------
11:11:11:11:11:cd 20:236                   00:21
11:11:11:11:11:ce 20:196                   00:20
```

Features Introduced in ArubaOS 6.4.2.3

This section describes the new feature enhancements introduced in ArubaOS 6.4.2.3.

AP-2xx Series High Density Optimization

ArubaOS 6.4.2.3 introduces enhancements to the High-Density Mobility Solution for 802.11ac networks. It includes the following key enhancements to optimize the performance of the AP-200 Series, AP-210 Series, AP-220 Series, and AP-270 Series access points in high-density deployment with a large number of mobile devices:

- Enhancements to queuing, aggregation, and power-save handling to improve the overall system throughput when the AP-200 Series, AP-210 Series, AP-220 Series, or AP-270 Series access point is connected to a large number of mobile devices.
- Enhancements to the handling of voice and video packets in the presence of best-effort traffic.
- Enhancements to the handling of pure multicast traffic in high-density deployment.

L2 GRE Tunnel Group

The controller supports redundancy for L3 Generic Routing Encapsulation (GRE) tunnels. Starting with ArubaOS 6.4.2.3, the controller supports redundancy for L2 GRE tunnel as well. This feature enables automatic redirection of the user traffic to a standby tunnel when the primary tunnel goes down.

Creating multiple L2 tunnels to the remote site may result in network loops. To mitigate this issue, tunnel-group provides an active-standby mechanism where only one member tunnel is active at a time.

To enable this functionality, you must:

- configure the member tunnel and add them to the appropriate VLAN.
- enable tunnel keepalives on the tunnel interface.
- configure the tunnel-group and set the group type to L2.
- add the member tunnel to the group.

Important Points to Remember

- When an L2 member tunnel is added to the tunnel-group, the tunnel is used for data traffic only if it is the active member in the group. Standby member tunnels do not carry any data traffic. However, all member tunnels in the group continue to send and receive keepalive packets.
- The default value of tunnel group type is L3. When creating an L2 tunnel-group, set the tunnel-group type to L2. Only one type of member tunnels can be part of a tunnel-group, either L2 or L3.
- All member tunnels in a group must have the same VLAN membership.
- An L2 member tunnel can only be part of one tunnel-group.
- L2 tunnel-group is not interoperable with other vendors. You must setup L2 tunnel-groups between Aruba devices only.
- Tunnel-groups are required only for the member tunnels and not for the remote end points.

Creating an L2 Tunnel Group

A tunnel-group is identified by a name or number. You can add multiple tunnels to a tunnel-group. The order of the tunnels defined in the tunnel-group configuration specifies their standby precedence. The first member of the tunnel-group is the primary tunnel. When the first tunnel fails, the second tunnel carries the traffic. The third tunnel in the tunnel-group takes over if the second tunnel also fails. In the mean time, if the first tunnel comes up, it becomes the most eligible standby tunnel.

You can also enable or disable pre-emption as part of the tunnel-group configuration. Pre-emption is enabled by default. The pre-emption option automatically redirects the traffic whenever it detects an active tunnel with

a higher precedence in the tunnel-group. When pre-emption is disabled, the traffic gets redirected to a higher precedence tunnel only when the tunnel carrying the traffic fails.

You can configure an L2 tunnel-group using the CLI.

In the CLI

To configure an L2 tunnel-group, issue the following commands:

```
(host) (config) #tunnel-group <tungrpname>
(host) (config-tunnel-group)#mode {l2|l3}
```

Example

Following is the sample configuration:

```
(host) (config) #tunnel-group branch_1
(host) (config-tunnel-group)#mode l2
```

To view the operational status of all the tunnel-groups and its members, issue the following command:

```
(host) #show tunnel-group
```

Example

Following is the sample output of the **show tunnel-group** command:

```
(host) #show tunnel-group

Tunnel-Group Table Entries
--------------------------
Tunnel Group   Mode  Tunnel Group Id  Preemptive Failover   Active Tunnel Id  Tunnel Members
------------   ----  ---------------  --------------------  ----------------  --------------
branch_1       L2    16385            enabled               1                 10  11
```

To view the active member tunnel and all the member tunnels of the respective tunnel-group, issue the following command:

```
(host) #show datapath tunnel-group
```

Example

Following is the sample output of the **show datapath tunnel-group** command:

```
(host) #show datapath tunnel-group

Datapath Tunnel-Group Table Entries
-----------------------------------
Tunnel-Group  Active Tunnel        Members
------------  -------------  -------------------
16385         10             10  11
```

To view the standby member tunnels of the tunnel-group, issue the following command:

```
(host) #show datapath tunnel
```

Example

Following is the sample output of the **show datapath tunnel** command:

```
(host) #show datapath tunnel

+----+------+-----------------------------------------------------+
|SUM/|      |                                     |                |
|CPU | Addr | Description                                     Value |
+----+------+-----------------------------------------------------+
|    |      |                                                     |
| G  | [00] | Current Entries                                    10 |
| G  | [02] | High Water Mark                                    10 |
| G  | [03] | Maximum Entries                                32768 |
| G  | [04] | Total Entries                                      31 |
```

```
| G  | [06] | 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/Unknown Mcast,
D - Decrypt tunnel,  a - Reduce ARP packets in the air, e - EAPOL only
C - Prohibit new calls, P - Permanent, m - Convert multicast
n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel
V - enforce user vlan(open clients only)
H - Standby (HA-Lite)

#          Source       Destination    Prt  Type  MTU   VLAN       Acls
------  --------------  --------------  ---  ----  ----  ---- -------------------
10      192.0.2.1       198.51.100.1    47   1     1100  0    0    0    0    0
11      192.0.2.1       203.0.113.1     47   1     1100  0    0    0    0    0

BSSID              Decaps     Encaps     Heartbeats Cpu QSz Flags  EncapKBytes  DecapKBytes
----------------- ---------- ---------- ---------- --- --- ----- ------------- -----------
00:00:00:00:00:00          0          5          0  22   0 TEFPR
00:00:00:00:00:00          0          0          0  23   0 LEFPRH
```

In this example, the member tunnel 11 is a standby tunnel which is denoted by the **H** flag.

MLD Snooping

Starting with ArubaOS 6.4.2.3, Multicast Listener Discovery (MLD) snooping does not add IPv6 Solicited-Node multicast address or groups to the multicast table.

A Solicited-Node multicast address is an IPv6 multicast address valid within the local-link (example, an Ethernet segment or a Frame Relay cloud). Every IPv6 host has at least one such address per interface. Solicited-Node multicast addresses are used in Neighbor Discovery Protocol for obtaining the layer 2 link-layer addresses of other nodes.

New Commands

The following commands are introduced in ArubaOS 6.4.2.3.

show web-server statistics

This command displays the web server statistics.

Example

```
(host) #show web-server statistics

Web Server Statistics:
----------------------
Current Request Rate:            1 Req/Sec
Current Traffic Rate:            1 KB/Sec
Busy Connection Slots:           7
Available Connection Slots:      68
Total Requests Since Up Time:    284
Total Traffic Since Up Time:     1122 KB
Avg. Request Rate Since Up Time: 1 Req/Sec
Avg. Traffic Rate Since Up Time: 6144 Bytes/Sec
Server Scoreboard:               ______________KKKKKK_W______________

Scoreboard Key:
_ - Waiting for Connection, s - Starting up
```

```
R - Reading Request, W - Sending Reply
K - Keepalive, D - DNS Lookup
C - Closing connection, L - Logging
G - Gracefully finishing, I - Idle cleanup of worker
. - Open slot with no current process
```

The output of this command includes the following parameters.

Parameter	Description
`Current Request Rate`	HTTP/HTTPS request rate measured immediately within the last one second.
`Current Traffic Rate`	HTTP/HTTPS data transfer rate measured immediately within the last one second.
`Busy Connection Slots`	Number of simultaneous HTTP/HTTPS sessions currently being served. Each session occupies one slot from the total available slots configured in the **web-max-clients** parameter.
`Available Connection Slots`	Number of simultaneous HTTP/HTTPS sessions that can be served more than what is being served currently.
`Total Requests Since Up Time`	Total number of HTTP/HTTPS requests received by the web server since the server was up.
`Total Traffic Since Up Time`	Total number of HTTP/HTTPS traffic handled by the web server since the server was up.
`Avg. Request Rate Since Up Time`	Lifetime average of HTTP/HTTPS request rate. This is calculated by dividing the total number of requests received by the web server up-time.
`Avg. Traffic Rate Since Up Time`	Lifetime average of HTTP/HTTPS traffic rate. This is calculated by dividing the total of HTTP/HTTPS traffic by the web server up-time.
`Server Scoreboard`	Displays information of each worker thread of the web server.

Modified Commands

The following commands are modified in ArubaOS 6.4.2.3.

ids-general-profile

The following new parameters are introduced in the **ids-general-profile** command.

Parameter	Description	Range	Default

`frame-types-for-rssi`
`all`
`ba`
`ctrl`
`dhigh`
`dlow`
`dnull`
`mgmt`
`pr`
	Select frame types to be used in AM RSSI calculation.
	Frame types:
	all—All types of frames. This frame type overrides any other frame types.
	ba—Block ACK frame types.
	ctrl—All control frames except ACK.
	dhigh—Data frames more than 36 Mbps except null data frames.
	dlow—Data frames less than 36 Mbps except null data frames.
	dnull—Null data frames.
	mgmt—All management frames except probe request.
	pr—Probe request frames.
	NOTE: Configure this parameter under the supervision of Aruba Technical Support.
		—	ba, ctrl, dlow, dnull, mgmt, pr

`max-monitored-stations`	Maximum number of monitored stations. **NOTE:** This parameter is currently available on the AP-220 Series access points only. **NOTE:** Configure this parameter under the supervision of Aruba Technical Support.	1024-4096	1024
`max-unassociated-stations`	Maximum number of unassociated stations. **NOTE:** This parameter is currently available on the AP-220 Series access points only. **NOTE:** Configure this parameter under the supervision of Aruba Technical Support.	256-4096	256
`packet-snr-threshold`	Set the packet Signal to Noise Ratio (SNR) threshold. All packets with SNR below this threshold are dropped from IDS and ARM processing. No packets are dropped if the threshold is set to 0. **NOTE:** Configure this parameter under the supervision of Aruba Technical Support.	0-90 dB	0

The highlighted fields are newly introduced as part of the **show ids-general-profile** command.

```
(host) (config) #show ids general-profile Michael

IDS General Profile "Michael"
---------------------------
Parameter                                Value
---------                                -----
Adhoc AP Max Unseen Timeout              180 sec
Adhoc (IBSS) AP Inactivity Timeout       5 sec
AP Inactivity Timeout                    20 sec
AP Max Unseen Timeout                    600 sec
Frame Types for RSSI calculation         ba pr dlow dnull mgmt ctrl
IDS Event Generation on AP               none
Max Monitored Stations                   1024

Max Unassociated Stations                256
```

```
Min Potential AP Beacon Rate              25 %
Min Potential AP Monitor Time             2 sec
Mobility Manager RTLS                     false
Monitored Device Stats Update Interval    0 sec
Packet SNR Threshold                      0
Send Adhoc Info to Controller            true
Signature Quiet Time                      900 sec
STA Inactivity Timeout                    60 sec
STA Max Unseen Timeout                    600 sec
Stats Update Interval                     60 sec
Wired Containment                         true
Wired Containment of AP's Adj MACs        true
Wired Containment of Suspected L3 Rogue   false
Wireless Containment                      deauth-only
Debug Wireless Containment                false
WMS Client Monitoring                     all
```

show web-server profile

Starting with ArubaOS 6.4.2.3, the **show web-server** command is renamed to **show web-server profile**.

web-server profile

Starting with ArubaOS 6.4.2.3, the **web-server** command is renamed to **web-server profile**.

Security Bulletin

As part of CVE-2014-3566 security vulnerabilities and exposures, **SSLv3** transport layer security is disabled from ArubaOS 6.4.2.3 and later versions.

NOTE

Clients exclusively using SSLv3 will fail to access the Captive Portal or the controller WebUI. It is recommended to use TLSv1.0, TLSv1.1, and TLSv1.2 transport layer security.

To address this vulnerability, the following changes are introduced in the **web-server profile 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:
	• TLS v1.0
	• TLS v1.1
	• TLS v1.2
		—	tlsv1
			tlsv1.1
			tlsv1.2

Features Introduced in ArubaOS 6.4.2.2

This section describes the new feature enhancements introduced in ArubaOS 6.4.2.2.

Username Length Restriction

The maximum length of the controller management (SSH) username and password is restricted to 64 and 32 characters respectively.

Features Introduced in ArubaOS 6.4.2.1

This section describes the new feature enhancements introduced in ArubaOS 6.4.2.1.

AP Power Mode on AP-220 Series

Starting with ArubaOS 6.4.2.1, a new configuration parameter **ap-poe-power-optimization** is introduced. This parameter is available in the **ap provisioning-profile** command. When this parameter is set to **enabled**, the controller disables the USB and the Ethernet (eth1) ports of AP-220 Series access points. Once the ports are disabled, the AP runs in reduced power mode.

NOTE

Overriding the AP power mode sets the maximum power request for LLDP TLV to 17.1W instead of 19.0W.

In the CLI

Use the following commands to configure an AP to run in reduced power mode using the CLI:

```
(host) (config) #ap provisioning-profile default
(host) (Provisioning profile "default") #ap-poe-power-optimization enabled
```

Use the following command to verify the configuration using the CLI:

```
(host) (config) #show ap provisioning-profile default

Provisioning profile "default"
------------------------------
Parameter                                                        Value
---------                                                        -----
Remote-AP                                                        No
Master IP/FQDN                                                   N/A
PPPOE User Name                                                  N/A
PPPOE Password                                                   N/A
PPPOE Service Name                                               N/A
USB User Name                                                    N/A
USB Password                                                     N/A
USB Device Type                                                  none
USB Device Identifier                                            N/A
USB Dial String                                                  N/A
USB Initialization String                                        N/A
USB TTY device data path                                         N/A
USB TTY device control path                                      N/A
USB modeswitch parameters                                        N/A
Link Priority Ethernet                                           0
Link Priority Cellular                                           0
Cellular modem network preference                                auto
Username of AP so that AP can authenticate to 802.1x using PEAP  N/A
Password of AP so that AP can authenticate to 802.1x using PEAP  N/A
Uplink VLAN                                                      0
USB power mode                                                   auto
AP POE Power optimization                                        enabled
```

Important Points to Remember

- By default, the AP operates in normal mode with the USB and Ethernet ports enabled.
- Changing the **ap-poe-power-optimization** parameter requires a reboot of the AP.
- In case the AP has an external DC power source, the USB and Ethernet (eth1) ports are not disabled even after setting the **ap-poe-power-optimization** to **enabled**.

Features Introduced in ArubaOS 6.4.2.0

This section describes the new feature enhancements introduced in ArubaOS 6.4.2.0.

AP-Platform

Support for the AP-210 Series

The Aruba AP-210 Series (AP-214 and AP-215) wireless access points support the IEEE 802.11ac standard for high-performance WLAN. These access points use MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 802.11ac 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services. The AP-210 Series access points work only in conjunction with an Aruba Controller. The Aruba AP-210 Series access point provides the following capabilities:

- Wireless transceiver
- Protocol-independent networking functionality
- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- Compatibility with IEEE 802.3at PoE+ and 802.3af PoE
- Central management configuration and upgrades through a controller

For more information, see the *AP-210 Series Wireless Access Point Installation Guide*.

Enhanced Link Aggregation Support on AP-220 Series and AP-270 Series Access Points

The AP-220 Series (AP-224 and AP-225) and AP-270 Series (AP-274 and AP-275) wireless access points support link aggregation using either standard port-channel (configuration based) or Link Aggregation Control Protocol (protocol signaling based). These access points can optionally be deployed with LACP configuration to benefit from the higher (greater than 1 Gbps) aggregate throughput capabilities of the two radios.

ArubaOS 6.4.2.0 introduces the **AP LACP LMS map information** profile, a local profile that maps a LMS IP address to a GRE striping IP address. If the AP fails over to a standby or backup controller, the AP LACP LMS map information profile on the new controller defines the IP address that AP uses to terminate 802.11g radio tunnels on the new controller. This feature allows AP-220 Series or AP-270 Series access points to form a 802.11g radio tunnel to a backup controller in the event of a controller failover, even if the backup controller is in a different L3 network. In previous releases, the GRE striping IP address was defined in the global AP system profile, which did not allow APs to maintain GRE striping tunnels if the AP failed over to a backup controller in a different L3 network. The GRE striping IP address parameter is deprecated from the AP system profile in ArubaOS 6.4.2.0.

Netgear AirCard 340U USB Modem Support

ArubaOS 6.4.2.0 introduces support of the Netgear AirCard 340U USB modem for AT&T's LTE service on the RAP-3WN, RAP-108, RAP-109, and RAP-155.

Netgear AirCard 341U USB Modem Support

ArubaOS 6.4.2.0 introduces support of the Netgear AirCard 341U USB modem for Sprint's LTE service on the RAP-3WN, RAP-108, RAP-109, and RAP-155.

VHT Support on AP-200 Series, AP-210 Series, AP-220 Series, and AP-270 Series Access Points

This feature enables Very High Throughput (VHT) rates on the 2.4 GHz band, providing 256-QAM modulation and encoding that allows for 600 Mbit/sec performance over 802.11n networks. Maximum data rates are increased on the 2.4 GHz band through the addition of VHT Modulation and Coding Scheme (MCS) values 8

and 9, which support the highly efficient modulation rates in 256-QAM. Starting with ArubaOS 6.4.2.0, VHT is supported on AP-200 Series (AP-204 and AP-205), AP-210 Series (AP-214 and AP-215), AP-220 Series (AP-224 and AP-225), and AP-270 Series (AP-274 and AP-275) wireless access points on both 20 MHz and 40 MHz channels.

Using the controller CLI or WebUI, VHT MCS values 0-9 are enabled, overriding the existing high-throughput (HT) MCS values 0-7, which have a lower maximum data rate. However, this feature should be disabled if individual rate selection is required.

AP Regulatory

Channel 144 in Regulatory Domain Profile

If a Dynamic Frequency Selection (DFS) channel is enabled in the regulatory domain profile, an AP can use channel 144 as the primary or secondary channel. However, most clients do not support channel 144. When you enable a DFS channel:

- If the deployment is in 20 MHz mode, do not use channel 144 in a regulatory domain profile.
- If the deployment is in 40 MHz mode, do not use channel 140-144 in a regulatory domain profile.
- If the deployment is in 80 MHz mode, do not use channel 132-144 in a regulatory domain profile.

This is because most older clients do not support channel 144, even though they support DFS channels. An AP in 80 MHz or 40 MHz mode chooses:

- Channel 144 as the primary channel – Here, most clients do not connect to the AP.
- Channel 140 as the primary channel and channel 144 as the secondary channel – Here, most 802.11n clients do not connect to the AP over 40 MHz.

Controller-Platform

Kernel Core Dump Enhancement

ArubaOS 6.4.2.0 introduces the command **kernel coredump**. This command enables the controller to capture the snapshot of the working memory of the control plane when the control plane has terminated abnormally. After issuing this command, you may issue the **write memory** command to save the configuration. This will enable the kernel core dump feature across controller reboots.

Web Content Classification

NOTE

This feature is available for all customers with a PEF license to use during an early preview period. Eventually, Aruba intends to license this feature as an annual subscription. License enforcement time-line and pricing information will be made available once the SKUs and prices are finalized.

Currently, the AppRF feature displays a summary of all traffic in the controller. But a large amount of traffic on the controller is from the web, hence this release of ArubaOS introduces the implementation of the Web Content Classification (WebCC) feature. When the WebCC feature is enabled, all web traffic (http and https) is classified. The classification is done in the data path as the traffic flows through the controller.

This feature is supported on all 7000 Series controllers.

The current policy enforcement model relies on the L3/L4 information of the packet or L7 information with Deep Packet Inspection (DPI) support to apply rules. WebCC complements this as the user is allowed to apply firewall policies based on web content category and reputation.

Benefits of WebCC:

1. Prevention of malicious malware, spyware, or adware by blocking known dangerous Web sites

2. Visibility into web content category-level
3. Visibility into Web sites accessed by the user

AP-Wireless

RTLS Station Message Frequency

Currently, when configuring the RTLS server in **ap system-profile**, the valid range of values for **station-message-frequency** was 5-3600 seconds. There are deployments that might require this to be configurable to as frequently as 1 per second. Starting with ArubaOS 6.4.2.0, you can set the **station-message-frequency** parameter in the 1-3600 seconds range. Setting the frequency to 1 means a report would be sent for every station every second. A value of 5 would mean that reports for any particular station would be sent at 5 second intervals.

Important points to remember:

- Sending more frequent reports to the server can improve the accuracy of the location calculation.
- Configuring an AP to send reports more frequently adds additional load in terms of CPU usage.

Video Multicast Rate Optimization

The **Multicast Rate** parameter is renamed to **Video Multicast Rate Optimization**.

The **Video Multicast Rate Optimization** parameter overrides the configuration of the **BC/MC Rate Optimization** parameter for VI-tagged multicast traffic.

Features Introduced in ArubaOS 6.4.1.0

This section describes the new feature enhancements introduced in ArubaOS 6.4.1.0.

AP-Platform

Support for AP-103H

The Aruba AP-103H wireless access point supports the IEEE 802.11n standard for high-performance WLAN. It is a dual radio, 2x2:2 802.11n access point. This access point uses MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance 802.11n 2.4 GHz or 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services. AP-103H is equipped with a total of three active Ethernet ports (ENET 0-2). It is a wall-box type access point. The AP-103H access point works only with an Aruba controller.

The Aruba AP-103H access point provides the following capabilities:

- Wireless transceiver
- Protocol-independent networking functionality
- IEEE 802.11a/b/g/n operation as a wireless access point
- IEEE 802.11a/b/g/n operation as a wireless air monitor
- Compatibility with IEEE 802.3af PoE
- Central management configuration and upgrades through a controller

For more information, see the *Aruba AP-103H Wireless Access Point Installation Guide*.

Support for AP-200 Series

The Aruba AP-200 Series (AP-204 and AP-205) wireless access points support the IEEE 802.11ac and 802.11n standards for high-performance WLAN. It is a dual radio, 2x2:2 802.11ac access point. These access points use

MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance 802.11n 2.4 GHz and 802.11ac 5 GHz functionality while simultaneously supporting legacy 802.11a/b/g wireless services.

The Aruba AP-200 Series access point provides the following capabilities:

- Wireless transceiver
- Protocol-independent networking functionality
- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- Compatibility with IEEE 802.3af PoE
- Central management configuration and upgrades through a controller

For more information, see the *Aruba AP-200 Series Wireless Access Point Installation Guide*.

AP Regulatory

Downloadable Regulatory Table

The downloadable regulatory table features allows new regulatory approvals to be distributed without waiting for a new software patch and upgrade. A separate file called the Regulatory-Cert, containing AP regulatory information, will be released periodically on the customer support site. The Regulatory-Cert file can then be uploaded to the Aruba controller and pushed to deployed APs.

Controller-Platform

7000 Series Controllers

The Aruba 7000 Series controllers are an integrated controller platform. The platform acts as a software services platform targeting small to medium branch offices and enterprise networks.

The 7000 Series controllers include three models that provide varying levels of scalability.

Table 8: *Aruba 7000 Series Controllers*

Model	Number of APs Supported	Number of Users Supported
7005	16	1024
7010	32	2048
7030	64	4096

For more information, see the installation guide for each controller model.

AirGroup

The following AirGroup service changes are effective in ArubaOS 6.4.1.0:

- The **Chromecast** service is renamed to **DIAL**.
- The **googlecast** service is introduced.

AP Fast Failover Support for Bridge-mode Virtual AP

High Availability (HA) support for bridge mode in Campus AP is introduced in ArubaOS 6.4.1.0. In previous versions of ArubaOS the fast failover feature for Campus AP was supported using tunnel or decrypt mode. Now support has been extended to bridge mode as well.

NOTE

AP Fast Failover on bridge forwarding mode virtual AP is supported on 7200 Series controllers only.

DHCP Lease Limit on 7000 Series Controllers

The following table outlines the maximum number of DHCP leases supported on the new 7000 Series controllers.

Table 9: *DHCP Lease Limit*

Platform	DHCP Lease Limit
7005	512
7010	1024
7030	2048

Selective Multicast Stream

The selective multicast group is based only on the packets learned through Internet Group Management Protocol (IGMP).

- When the **broadcast-filter all** parameter is enabled, the controller would allow multicast packets to be forwarded only if the following conditions are met:
  - Packets originating from the wired side have a destination address range of 225.0.0.0 - 239.255.255.255
  - A station has subscribed to a multicast group.
- When IGMP snooping/proxy is disabled, the controller is not aware of the IGMP membership and drops the multicast flow.
- If Dynamic Multicast Optimization (DMO) is enabled, the packets are sent with the 802.11 unicast header.
- If AirGroup is enabled, mDNS (SSDP) packets are sent to the AirGroup application. The common address for mDNS is 224.0.0.251, and for SSDP is 239.255.255.250.

Security

Authentication Profile based User Idle Timeout

Starting with ArubaOS 6.4.1.0, the **user-idle-timeout** parameter in AAA profile accepts a value of 0. When a value of 0 is entered, the L3 user state is removed immediately upon disassociation. In other words, the controller deletes the user immediately after disassociation or disconnection from the wireless network. If RADIUS accounting is configured, the controller sends an accounting STOP message to the RADIUS server.

NOTE

A user idle timeout of 0 should not be configured for wired, split-tunnel, VIA, and VPN users. It is applicable only for wireless users in tunnel and decrypt-tunnel forwarding modes.

Global Firewall Parameters

NOTE

This feature works only when an L3 user entry exists on the controller.

Starting with ArubaOS 6.4.1.0, Address Resolution Protocol (ARP) and Gratuitous ARP packets from wired and wireless clients can be monitored or policed beyond a configured threshold value. The following new parameters are introduced as part of the global firewall parameters:

- **Monitor/police ARP attack**
- **Monitor/police Gratuitous ARP attack**

Additional options to drop excessive packets or blacklist a client are introduced.

NOTE

Blacklisting of wired clients is not supported.

Features Introduced in ArubaOS 6.4.0.2

This section describes the new feature enhancements introduced in ArubaOS 6.4.0.2.

ArubaOS-AirWave Cross-Site Request Forgery Mitigation

To defend against Cross-Site Request Forgery (CSRF) attacks, an enhancement is added to use randomly generated session-ID in HTTP transactions with the ArubaOS WebUI. As a consequence, AirWave must be upgraded to AirWave 7.7.10 so that it includes the session-ID in its requests.

Upgrade Recommendations

- Upgrade to AirWave 7.7.10 to maintain full functionality.
- Upgrade controllers to ArubaOS 6.4.0.2 to mitigate CSRF. Controllers that are not upgraded will continue to work with the upgraded AirWave 7.7.10, because controllers with older ArubaOS software image ignore the session-ID in the request.

Fixed Software Versions

- ArubaOS 6.4.0.2
- AirWave 7.7.10

Frequently Asked Questions

Q. What happens if I upgrade ArubaOS but not AirWave?

A. If you upgrade the controller to ArubaOS 6.4.0.2, AirWave must also be upgraded to version 7.7.10 to maintain full functionality. If the AirWave 7.7.10 patch is not applied, client monitoring, AppRF information, and push certificates will not work on the controller with the ArubaOS 6.4.0.2 software image.

Q. What happens if I upgrade to AirWave 7.7.10 but do not upgrade controllers to ArubaOS 6.4.0.2?

A. If you upgrade to AirWave 7.7.10, controllers that are not upgraded to ArubaOS 6.4.0.2 will continue to work with the upgraded AirWave 7.7.10, but will ignore the session-ID in the request.

Q. Where can I find more information on CSRF?

A. http://en.wikipedia.org/wiki/Cross-site_request_forgery

EAP-MD5 Support

The controller does not support EAP-MD5 authentication for wireless clients. In ArubaOS 6.3.x and ArubaOS 6.4, EAP-MD5 authentication for wired clients failed. This issue is fixed in ArubaOS 6.4.0.2.

Features Introduced in ArubaOS 6.4.0.1

This section describes the new feature enhancements introduced in ArubaOS 6.4.0.1.

PhoneHome Reporting Enhancements

The PhoneHome feature can be enabled by selecting the **Enable** option in the **Maintenance** > **File > Aruba TAC Server** section of the WebUI. When Auto PhoneHome is enabled, the first report occurs 7 days later. The Auto PhoneHome Report is disabled by default.

NOTE

The PhoneHome feature does not report any user information that includes client MAC addresses or user names.

The PhoneHome feature allows a controller to proactively report events such as hardware failures, software malfunctions, and other critical events. When PhoneHome is enabled on a controller, the customer support portal provides a summary of deployed APs and licenses that are linked to a specific controller. To view this information, you must enter a valid email address with a domain name associated with your controller in the **Maintenance > File > Aruba TAC Server** section of the controller WebUI. Access to this information also requires an active support contract and login access to the customer portal.

Previously, PhoneHome required reports to be sent over SMTP. However, starting with ArubaOS 6.4, controllers have the option to send PhoneHome reports over HTTPS to the Aruba Activate server.

If your controller is behind the proxy server and does not have direct access to the Internet, you can configure PhoneHome to send reports using an SMTP server. PhoneHome integration with Activate offers the following benefits:

- **Simpler configuration**—PhoneHome only requires you to configure the email ID of the network administrator managing the device, as Activate already has information to accurately identify your controller. This email address appears in the output of the command.
- **Smaller bandwidth requirements**—When the PhoneHome feature sends the report to the Activate server, the PhoneHome report is zipped into a smaller package, and then divided into smaller 1 MB pieces before being sent to the server using secure HTTPS. Only reports sent to Activate are zipped before they are sent, so reports sent to Activate use less bandwidth than a report sent to an SMTP server.
- **Enhanced error management**—If any individual portion of the report is not successfully received by the Activate server, PhoneHome makes up to three attempts to resend just that portion of the file, rather than resending the entire report. In contrast, reports sent via SMTP must be resent in their entirety if any portion is not received by the SMTP server.
- **Automatic removal of old reports**—Once the entire report is sent to the Activate server, Activate sends an acknowledgment to the controller, prompting the controller to delete its local copy of the report.
- The PhoneHome feature can be enabled or disabled using the **Maintenance** > **File > Aruba TAC Server** option in the WebUI. This can also be done through the **phonehome [enable | disable]** option in the CLI.

Features Introduced in ArubaOS 6.4.0.0

This section describes the new feature enhancements introduced in ArubaOS 6.4.0.0.

AP-Platform

Support for the AP-270 Series

The Aruba AP-270 Series (AP-274 and AP-275) wireless access points are environmentally hardened, outdoor rated, dual-radio IEEE 802.11ac wireless access points. These access points use MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g/n wireless services.

Support for the AP-103

The Aruba AP-103 wireless access point supports the IEEE 802.11n standard for high-performance WLAN. This access point uses MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high performance, 802.11n 2.4 GHz or 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services.

Hotspot 2.0

Hotspot 2.0 is a Wi-Fi Alliance Passpoint specification based on the 802.11u protocol that provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users the ability to roam between partner networks without additional authentication.

ArubaOS 6.4 supports Hotspot 2.0 with enhanced network discovery and selection. Clients can receive general information about the network identity, venue, and type via management frames from the Aruba AP. Clients can also query APs for information about the network's available IP address type (IPv4 or IPv6), roaming partners, and supported authentication methods, and receive that information in Information Elements from the AP.

ArubaOS 6.4 supports several ANQP and H2QP profile types for defining Hotspot data. The following table describes the profiles in the Hotspot profile set.

Table 10: *ANQP and H2QP Profiles referenced by an Advertisement Profile*

Profile	Description
Hotspot Advertisement profile	An advertisement profile defines a collection of ANQP and H2QP profiles. Each hotspot 2.0 profile is associated with one advertisement profile, which in turn references one of each type of the ANQP and H2QP profiles.
ANQP 3GPP Cellular Network profile	Use this profile to define priority information for a 3rd Generation Partnership Project (3GPP) Cellular Network used by hotspots that have roaming relationships with cellular operators.
ANQP Domain Name profile	Use this profile to specify the hotspot operator domain name.
ANQP IP Address Availability profile	Use this profile to specify the types of IPv4 and IPv6 IP addresses available in the hotspot network.
ANQP NAI Realm profile	This profile identifies and describes a Network Access Identifier (NAI) realm accessible using the AP, and the method that this NAI realm uses for authentication.
ANQP Network Authentication profile	Use the ANQP Network Authentication profile to define the authentication type used by the hotspot network.

Table 10: *ANQP and H2QP Profiles referenced by an Advertisement Profile*

Profile	Description
ANQP Roaming Consortium profile	Name of the ANQP Roaming Consortium profile to be associated with this WLAN advertisement profile.
ANQP Venue Name profile	Use this profile to specify the venue group and venue type information be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.
H2QP Connection Capability profile	Use this profile to specify the hotspot protocol and port capabilities.
H2QP Operating Class Indication profile	Use this profile to specify the channels on which the hotspot is capable of operating.
H2QP Operator Friendly Name profile	Use this profile to define the operator-friendly name sent by devices using this profile.
H2QP WAN Metrics profile	Use this profile to specify the WAN status and link metrics for your hotspot.

AP-220 Series Enhancements

The following enhancements have been made to the AP-220 Series access point:

- CAC and TSPEC handling
- Multi-client performance tuning

AP-130 Series Functionality Improvements when Powered Over 802.3af (POE)

Starting with ArubaOS 6.4, all features and both Ethernet ports of the AP-130 Series are supported when the AP is powered by 802.3af POE.

Franklin Wireless U770 4G Modem Support

ArubaOS 6.4 introduces support of the Franklin Wireless U770 4G USB cellular modem for the Sprint LTE service on the RAP-155.

Huawei E3276 LTE Modem Support

ArubaOS 6.4 introduces support of the Huawei E3276 LTE USB cellular modem on the RAP-3WN, RAP-108, RAP-109, and RAP-155.

Authentication

Authentication Server Limits

Starting with ArubaOS 6.4, a maximum of 128 each of LDAP, RADIUS, and TACACS servers can be configured on the controller.

EAP-MD5 Support

The controller does not support EAP-MD5 authentication for wireless clients. In ArubaOS 6.3.x and ArubaOS 6.4.x, EAP-MD5 authentication for wired clients fails. This issue is under investigation and expected to be fixed in the upcoming ArubaOS 6.3.x and ArubaOS 6.4.x patch releases.

Controller-Platform

AirGroup

Default Behavior Changes

Starting with ArubaOS 6.4, AirGroup is disabled by default. If you upgrade from an existing non-AirGroup version to AirGroup 6.4 or perform the fresh installation of ArubaOS 6.4, AirGroup is disabled by default. If you run an earlier version of ArubaOS with AirGroup enabled and upgrade to ArubaOS 6.4, the AirGroup feature is enabled.

The following AirGroup features are introduced in ArubaOS 6.4:

AirGroup DLNA UPnP Support

ArubaOS 6.4 introduces support for DLNA (Digital Living Network Alliance), a network standard that is derived from UPnP (Universal Plug and Play) in addition to the existing mDNS protocol. DLNA uses the Simple Service Discovery Protocol (SSDP) for service discovery on the network. DLNA provides the ability to share digital media between multimedia devices like Windows and Android, similar to how mDNS supports Zero Configuration Networking to Apple® devices and services.

ArubaOS 6.4 ensures that DLNA seamlessly works with the current mDNS implementation. All the features and policies that are applicable to mDNS are extended to DLNA. This ensures full interoperability between compliant devices.

AirGroup mDNS Static Records

AirGroup processes mDNS packets advertised by servers and creates the relevant cache entries. When a query comes from a user, AirGroup responds with the appropriate cache entries with the relevant policies applied. Starting with ArubaOS 6.4, AirGroup provides the ability for an administrator to add the mDNS static records to the cache.

Group Based Device Sharing

ArubaOS 6.4 AirGroup supports the sharing of AirGroup devices such as AppleTV or Printers to a **User Group** using CPPM. This is an enhancement to features that support device sharing based upon the user's username, user-role, and location.

AirGroup-WebUI Monitoring Dashboard Enhancements

This release of ArubaOS provides the following enhancements to the AirGroup WebUI:

- **Usage** – You can view the following enhancements in the **Usage** page of the WebUI:
  - The AirGroup service names in the **AirGroup** row are now clickable. If you click a service, you are redirected to the **Dashboard** > **AirGroup** page, which displays a list of AirGroup servers filtered by Service Name.
- **Clients** – You can view the following enhancements in the **Clients** page of the WebUI:
  - In **Dashboard** > **Clients**, a new **AirGroup** column is added to display the devices that are listed as mDNS, DLNA, or both. If a device does not support both **mDNS** and **DLNA**, this field is blank.
- **AirGroup** - You can view the following enhancements in the **AirGroup** page of the WebUI:
  - A new **AirGroup type** column is added that specifies if the type of the AirGroup device is mDNS, DLNA or both.
  - The MAC address of each AirGroup user and server is now clickable. If you click a MAC link, you are redirected to the **Dashboard** > **Clients** > **Summary page** > **AirGroup** tab. If an AirGroup user or AirGroup server is a wired trusted client, the MAC address is not clickable.

AirGroup-Limitations

The AirGroup feature has the following limitations in ArubaOS 6.4:

- AirGroup's DLNA discovery works across VLANs; however, media streaming from Windows Media Server does not work across VLANs. This limitation is a result of Digital Rights Management (DRM) support in Windows Media Server, which restricts media sharing across VLANs. Media streaming works only when both client and server are connected to the same VLAN.
- Android devices cannot discover Media Server while using the native music and video player applications and when they are connected across VLANs. For example, Samsung Tab 3 cannot discover Media Server on Samsung Galaxy S4 while using the native music and video player applications. Android devices can discover Media Server when they are connected in the same VLAN. This restriction is caused by Samsung devices.
- Xbox cannot be added as an extender to Windows clients using the Windows Media Center application with the AirGroup feature enabled. You need to disable the AirGroup feature before adding Xbox as an extender.

AppRF 2.0

The AppRF 2.0 feature improves application visibility and control by allowing you to configure and view access control list (ACL), bandwidth application, and application category-specific data. AppRF 2.0 supports a Deep Packet Inspection (DPI) engine for application detection for over a thousand applications. All wired and wireless traffic that traverses the controller can now be categorized and controlled by application and application category.

AppRF 2.0 provides the ability to:

- permit or deny an application or application category for a specific role. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.
- rate limit an application or application category, such as video streaming applications, for a specific role.
- mark different L2/L3 Quality of Service (QoS) tag for an application or application category for a user role. For example, you can mark video and voice sessions that originate from wireless users with different priorities so that traffic is prioritized accordingly in your network.

Policy Configuration

Access control lists now contain new application and application category options that let you permit or deny an application /application category on a given role.

Global Session ACL

A new session ACL has been added named "global-sacl." This session, by default, is in position one for every user role configured on the controller. The global-sacl session ACL has the following properties:

- Cannot be deleted.
- Always remains at position one in every role and its position cannot be modified.
- Contains only application rules.
- Can be modified in the WebUI and dashboard on a master controller.
- Any modifications to it result in the regeneration of ACEs of all roles.

Role Default Session ACL

You can configure role-specific application configuration using the WebUI and dashboard. For example, you can deny the Facebook application on the guest role using the dashboard without having to change the firewall configuration.

A new role session ACL named apprf-"role-name"-sacl has been added. This session, by default, is in position one for every user role configured on the controller.

The string "apprf" is added to the beginning and "sacl" to the end of a role's name to form a unique name for role default session ACL. This session ACL is in position 2 of the given user role after the global session ACL and takes the next higher priority after global policy rules.

The predefined role session ACL has the following properties:

- Cannot be deleted through the WebUI or CLI. It is only deleted automatically when the corresponding role is deleted.
- Always remains at position 2 in every role and its position cannot be modified.
- Contains only application rules.
- Can be modified using the WebUI or dashboard on a master controller; however, any modification results in the regeneration of ACEs for that role.
- Cannot be applied to any other role.

Bandwidth Contract Configuration

Bandwidth contract configuration lets you configure bandwidth contracts for both the global or application-specific levels.

Global Bandwidth Contract Configuration

You can configure bandwidth contracts to limit application and application categories on an application or global level.

Role-Specific Bandwidth Contracts

Application-specific bandwidth contracts (unlike "generic" bandwidth contracts) allow you to control or reserve rates for specific applications only on a per-role basis. An optional exclude list is provided that allows you to exclude applications or application categories on which a generic user/role bandwidth contract is not applied. The exclude list enables you to give specific enterprise applications priority over other user traffic.

Important points regarding bandwidth contracts include:

- Application bandwidth contracts are per-role by default.
- When an application bandwidth contract is configured for both a category and an application within the category, always apply the most specific bandwidth contract.

AppRF Dashboard Application Visibility

The AppRF Dashboard Application Visibility feature allows you to configure both application and application category policies within a given user role.

The **AppRF** page on the **Dashboard** tab displays the PEF summary of all the sessions in the controller aggregated by users, devices, destinations, applications, WLANs, and roles. The elements are now represented in box charts instead of pie charts.

NOTE

Applications and application categories containers are only displayed on 7200 Series controllers. The remaining controller platforms will retain ArubaOS 6.3.x.x firewall charts (i.e. without new application classification box chart).

Branch

Centralized BID Allocation

In a master-local controller setup, the master controller runs the BID allocation algorithm and allocates BID to the branches that terminate on it and to the local controllers. The master controller saves the BIDs in its memory IAP database to avoid the collision of BID (per subnet), whereas the local controller saves the BIDs only in its memory data structures. The IAP manager in the local controller forwards only the new register request (branch coming for the first time with BIDs as -1) message to the master controller. For an existing branch's register request, the local controller tries to honor the requested BIDs first. The master and local

communication is within the existing IPsec tunnel. The master controller gets the register request and allocates BIDs using the BID allocation algorithm. Finally, the master controller sends back the allocated BIDs to the local controller, and the local controller updates its data structure and sends the response to the IAP.

General guidelines for upgrading from an existing IAP-VPN release to ArubaOS 6.4:

1. Ensure that all the branches are upgraded to Instant 4.0.
2. Upgrade the data center to ArubaOS 6.4.

NOTE

If you have a master-local setup; upgrade the master controller first and then the local controller.

3. Ensure that the IAP-VPN branches are always configured using authorized tools like AirWave/Athena, otherwise you must trust all branches or the required branch using the following command:

   ```
   iap trusted-branch-db allow-all
   ```

   or

   ```
   iap trusted-branch-db add mac-address<mac-address>
   ```

NOTE

Instant versions earlier than 4.0 also need the previous command to be executed in order for the controller to come up with ArubaOS 6.4.

Controller LLDP Support

ArubaOS 6.4 provides support for Link Layer Discovery Protocol (LLDP) on controllers to advertise identity information and capabilities to other nodes on the network, and store the information discovered about the neighbors.

High Availability

This section describes High Availability features added or modified in ArubaOS 6.4.

High Availability Configuration Using the WebUI

The high availability profiles introduced in ArubaOS 6.3 can now be configured using the **Configuration > Advanced Services Redundancy** window of the ArubaOS 6.4 WebUI. In previous releases, high availability profiles were configured in the **HA** section of the **Configuration > Advanced Services > All Profile Management** window. This section of the WebUI is removed in ArubaOS 6.4.

Client State Synchronization

State synchronization improves failover performance by synchronizing client authentication state information from the active controller to the standby controller, allowing clients to authenticate on the standby controller without repeating the complete 802.1X authentication process. This feature requires you to configure the high availability group profile with a pre-shared key. The controllers use this key to establish the IPsec tunnels through which they send state synchronization information.

The state synchronization feature limits each high availability group to one IPv4 standby controller and one IPv6 standby controller, or one pair of dual-mode IPv4 and IPv6 controllers. Therefore, this feature can only be enabled in high-availability deployments that use the following topologies for each IPv4 or IPv6 controller pair:

- **Active/Active Model**: In this model, two controllers are deployed in dual mode. Controller one acts as a standby for the APs served by controller two, and vice-versa. Each controller in this deployment model supports approximately 50% of its total AP capacity, so if one controller fails, all the APs served by that controller will fail over to the other controller, thereby providing high availability redundancy to all APs in the cluster.

- **Active/Standby Model**: In this model, the active controller supports up to 100% of its rated capacity of APs, while the other controller in standby mode is idle. If the active controller fails, all APs served by the active controller will fail over to the standby controller.

High Availability Inter-controller Heartbeats

The high availability inter-controller heartbeat feature allows faster AP failover from an active controller to a standby controller, especially in situations where the active controller reboots or loses connectivity to the network.

The inter-controller heartbeat feature works independently from the AP mechanism that sends heartbeats from the AP to the controller. If enabled, the inter-controller heartbeat feature supersedes the AP's heartbeat to its controller. As a result, if a standby controller detects missed inter-controller heartbeats from the active controller, it triggers the standby APs to fail over to the standby controller, even if those APs have not detected any missed heartbeats between the APs and the APs' active controller.

CAUTION

Use this feature with caution in deployments where the active and standby controllers are separated over high-latency WAN links.

When this feature is enabled, the standby controller starts sending regular heartbeats to an AP's active controller as soon as the AP has an UP status on the standby controller. The standby controller initially flags the active controller as *unreachable*, but changes its status to *reachable* as soon as the active controller sends a heartbeat response. If the active controller later becomes unreachable for the number of heartbeats defined by the heartbeat threshold (by default, five missed heartbeats), the standby controller immediately detects this error, and informs the APs using the standby controller to fail over from the active controller to the standby controller. If, however, the standby controller never receives an initial heartbeat response from the active controller, and therefore never marks the active controller as initially reachable, the standby controller will not initiate a failover.

Extended Standby Controller Capacity

The standby controller over-subscription feature allows a standby controller to support connections to standby APs beyond the controller's original rated AP capacity. This feature is an enhancement from the high availability feature introduced in ArubaOS 6.3, which requires the standby controller have an AP capacity equal to or greater than the total AP capacity of all the active controllers it supports.

Starting with ArubaOS 6.4, a 7200 Series controller acting as a standby controller can oversubscribe to standby APs by up to four times that controller's rated AP capacity, and a standby M3 controller module or 3600 controller can oversubscribe by up to two times its rated AP capacity, as long as the tunnels consuming the standby APs do not exceed the maximum tunnel capacity for that standby controller.

NOTE

3200XM, 3400, and 600 Series controllers do not support this feature.

Features not Supported on 600 Series Controllers

The 600 Series controller platforms do not support the following features in ArubaOS 6.4.

- AirGroup
- AppRF 1.0/Firewall Visibility
- IF-MAP
- AP Image Preload
- Centralized Image Upgrade
- IAP-VPN

Control Plane Bandwidth Contracts Values

Beginning with ArubaOS 6.4, control plane bandwidth contracts are configured in packets per second (pps) instead of bits per second (bps). This makes performance more predictable. The bandwidth contract range is now 1 to 65536 pps. Additionally, show commands related to control plane bandwidth contracts display pps. The formula used to convert bps to pps is **pps=bps/(256 x 8)**.

Automatic GRE from IAP

ArubaOS 6.4 introduces automatic GRE tunnel formation between the controller and Instant access points. Manual configuration of GRE is no longer required on the controller. This feature uses the existing IPSec connection with the controller to send control information to set up the GRE tunnel. Since the GRE control information is exchanged through a secure tunnel, security and authentication is addressed.

DHCP Lease Limit

The following table provides the maximum number of DHCP leases supported per controller platform.

Table 11: *DHCP Lease Limit*

Platform	DHCP Lease Limit
620	256
650/651	512
3200XM	512
3400	512
3600, M3	512
7210	5120
7220	10240
7240	15360

IPv6

This section describes IPv6 features added or modified in ArubaOS 6.4.

Multicast Listener Discovery (MLDv2) Snooping

This release of ArubaOS supports Source Specific Multicast (SSM) and Dynamic Multicast Optimization (DMO) as part of the IPv6 MLDv2 feature.

Source Specific Multicast

The Source Specific Multicast (SSM) supports delivery of multicast packets that originate only from a specific source address requested by the receiver. You can forward multicast streams to the clients if the source and group match the client subscribed source group pairs (S,G).

The controller supports the following IPv6 multicast source filtering modes:

- Include - In Include mode, the reception of packets sent to a specified multicast address is enabled only from the source addresses listed in the source list. The default IPv6 SSM address range is FF3X::4000:1 – FF3X::FFFF:FFFF, and the hosts subscribing to SSM groups can only be in the Include mode.
- Exclude - In Exclude mode, the reception of packets sent to a specific multicast address is enabled from all source addresses. If there is a client in the Exclude mode, the subscription is treated as an MLDv1 join.

Dynamic Multicast Optimization

In a scenario where multiple clients are associated to an AP and one client subscribes to a multicast stream, all clients associated to the AP receive the stream, as the packets are directed to the multicast MAC address. To restrict the multicast stream to only subscribed clients, Dynamic Multicast Optimization (DMO) sends the stream to the unicast MAC address of the subscribed clients. DMO is currently supported for both IPv4 and IPv6.

Understanding MLDv2 Limitations

The following are the MLDv2 limitations:

- Controller cannot route multicast packets.
- For mobility clients, MLD proxy should be used.
- VLAN pool scenario stream is forwarded to clients in both the VLANs even if the client from one of the VLANs is subscribed.
- DMO is not applicable for wired clients in controllers.

Static IPv6 GRE Tunnel Support

Static IPv6 L2/L3 GRE tunnels can be established between Aruba devices and other devices that support IPv6 GRE tunnels. IPv4 and IPv6 L2 GRE tunnels carry both IPv6 and IPv4 traffic. The IPv6 traffic can also be redirected over the IPv4 L3 GRE tunnel.

The following options for directing traffic into the tunnel are introduced for IPv6:

- Static route—Redirects traffic to the IP address of the tunnel.
- Firewall policy (session-based ACL)—Redirects traffic to the specified tunnel ID.

NOTE

If a VLAN interface has multiple IPv6 addresses configured, one of them is used as the tunnel source IPv6 address. If the selected IPv6 address is deleted from the VLAN interface, then the tunnel source IP is re-configured with the next available IPv6 address.

Important Points to Remember

- By default, a GRE Tunnel Interface is in IPv4 L3 mode.
- IPv6 configurations are allowed on an IPv4 Tunnel only if the tunnel mode is set to IPv6. Similarly, IPv4 configurations are allowed on an IPv6 Tunnel only if the tunnel mode is set to IP.

Understanding Static IPv6 GRE Tunnel Limitations

ArubaOS does not support the following functions for Static IPv6 GRE Tunnels:

- IPv6 autoconfiguration and IPv6 Neighbor Discovery mechanisms do not apply to IPv6 tunnels.
- Tunnel encapsulation limit and MTU discovery options on the IPv6 tunnels.
- IPv6 GRE for a master-local setup cannot be used as IPsec is not supported in this release.

IGMPv3 Support

ArubaOS 6.4 supports IGMPv3 functionality, which makes Aruba controller aware of Source Specific Multicast (SSM) and optimizes network bandwidth. The SSM functionality is an extension of IP multicast where the datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. By default, the multicast group range of 232.0.0.0 through 232.255.255.255 (232/8) is reserved for SSM by IANA (Internet Assigned Numbers Authority).

IPv6 Enhancements

This release of ArubaOS provides the following IPv6 enhancements on the AP:

- DNS based ipv6 controller discovery
- FTP support for image upgrade in an IPv6 network
- DHCPv6 client support

VRRPv3 Support on Controllers

Virtual Router Redundancy Protocol (VRRP) eliminates a single point of failure by providing an election mechanism among the controllers to elect a master controller. The master controller owns the configured virtual IPv6 address for the VRRP instance. When the master controller becomes unavailable, a backup controller steps in as the master and takes ownership of the virtual IPv6 address.

VRRPv2 support over IPv4 is already present on the Aruba Mobility Controllers. VRRPv3 support over IPv6 is introduced in the current version of ArubaOS.

Depending on your redundancy solution, you can configure the VRRP parameters on your master and local controllers. The following parameters are added in this release:

- IP version - Select IPv4 \ IPv6 from the drop-down list.
- IP \ IPv6 Address - Based on the selection made in the IP version field, either IP Address \ IPv6 Address is displayed. This is the virtual IP address that is owned by the elected VRRP master. Ensure that the same IP address and VRRP ID is used on each member of the redundant pair. Note: The IP address must be unique and cannot be the loopback address of the controller. Only one global IPv6 address can be configured on a VRRP instance.

NOTE

The IP address must be unique and cannot be the loopback address of the controller. Only one global IPv6 address can be configured on a VRRP instance.

Understanding VRRP Limitations

- It is not recommended to enable preemption on the master redundancy model. If preemption is disabled and there is a failover, the new primary controller remains the primary controller even when the original master is active again. The new primary controller does not revert to its original state unless forced by the administrator. Disabling preemption prevents the master from “flapping” between two controllers and allows the administrator to investigate the cause of the outage.
- VRRP v2 over IPv4 supports the master-master redundancy model. However, this support is not available in VRRP v3 over IPv6. This model will be supported once support for IPsec over IPv6 is added. Currently only master-local and local-local redundancy are supported.

Security

Warning Message for Containment Features

The feature for enabling wireless containment using the **IDS Unauthorized Device** profile and **IDS Impersonation** profile may be in violation of certain Federal Communications Commission (FCC) regulatory statutes. To address this, a warning message is issued each time the feature is enabled.

Palo Alto Networks Firewall Integration

The User-Identification (User-ID) feature of the Palo Alto Networks (PAN) firewall allows network administrators to configure and enforce firewall policies based on user and user groups. User-ID identifies the user on the network based on the IP address of the device that the user is logged in to. Additionally, firewall policy can be applied based on the type of device the user is using to connect to the network. Since the Aruba controller maintains the network and user information of the clients on the network, it is the best source to provide the information for the User-ID feature on the PAN firewall.

Application Single Sign-On Using L2 Network Information

This feature allows single sign-on (SSO) for different web-based applications using Layer 2 authentication information. Single sign-on for web-based applications uses Security Assertion Markup Language (SAML), which happens between the web service provider and an identity provider (IDP) that the web server trusts. A request made from the client to a web server is redirected to the IDP for authentication. If the user has already been authenticated using L2 credentials, the IDP server already knows the authentication details and returns a SAML response, redirecting the client browser to the web-based application. The user enters the web-based application without needing to enter the credentials again.

Enabling application SSO using L2 network information requires configuration on the controller and on the IDP server. The Aruba ClearPass Policy Manager (CPPM) is the only IDP supported.

802.11w Support

ArubaOS supports the IEEE 802.11w standard, also known as Management Frame Protection (MFP). MFP makes it difficult for an attacker to deny service by spoofing Deauth and Disassoc management frames.

MFP is configured on a virtual AP (VAP) as part of the **wlan ssid-profile**. There are two parameters that can be configured, **mfp-capable** and **mfp-required**. Both parameters are disabled by default.

Ability to Disable Factory-Default IKE/IPsec Profiles

This feature enables you to disable default IKE policies, default IPsec dynamic maps, and site-to-site IPsec maps. You can do this by using the **crypto isakmp policy**, **crypto dynamic-map**, and **crypto-local ipsec-map** CLI commands. Alternatively, you can use the WebUI and navigate to **Advanced Services > VPN Services > IPSEC** and **Advanced Services > VPN Services > Site-To-Site**.

AOS/ClearPass Guest Login URL Hash

This feature enhances the security for the ClearPass Guest login URL. A new parameter called **url_hash_key** (disabled by default) is added to the Captive Portal profile so that ClearPass can trust and ensure that the client MAC address in the redirect URL has not been tampered by anyone.

Authentication Server Load Balancing

Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers, thus avoiding any one particular authentication server from being overloaded. Authentication Server Load Balancing functionality enables the Aruba Mobility Controller to perform load balancing of authentication requests destined to external authentication servers (Radius/LDAP etc). This prevents any one authentication server from having to handle the full load during heavy authentication periods, such as at the start of the business day.

Enhancements in the User Authentication Failure Traps

The output of the **show snmp trap-queue** command has been enhanced to support information such as Server IP address, user MAC, AP name, authentication failure details, authentication request time out, authentication server down, and up traps messages that are sent to the host.

RADIUS Accounting on Multiple Servers

ArubaOS 6.4 provides support for the controllers to send RADIUS accounting to multiple RADIUS servers. The controller notifies all the RADIUS servers to track the status of authenticated users. Accounting messages are sent to all the servers configured in the server group in a sequential order.

RADIUS Accounting for VIA and VPN Users

RADIUS Accounting is now supported for VIA and VPN users. A knob has been added in the **AAA Authentication VIA Auth profile** and the **AAA Authentication VPN profile** to enable this feature.

Spectrum Analysis

AP Platform Support for Spectrum Analysis

Starting with ArubaOS 6.3.1.0 and ArubaOS 6.4, AP-120 Series access points do not support the spectrum analysis feature, and cannot be configured as a spectrum monitor or hybrid AP.

Voice and Video

Unified Communication and Collaboration

This section describes the Unified Communication and Collaboration (UCC) feature introduced in ArubaOS 6.4. The Unified Communications Manager (UCM) is the core solution component of this feature. UCC addresses the onslaught of mobile devices that use voice, video, and collaboration applications. This reduces the cost of voice infrastructure for communication and collaboration needs.

UCC continues to support all existing functionality provided by ArubaOS 6.3.x. Following are the new sub-features introduced in ArubaOS 6.4:

- UCC Dashboard in the WebUI
- UCC **show** commands
- UCC— AirWave Integration
- Changes to Call Admission Control
- Per User Role Lync Call Prioritization
- Dynamically Open Firewall for UCC Clients using STUN
- UCC Call Quality Metrics

AP Support

ArubaOS 6.3.x.x will be the last release to support the RAP-5 access point. ArubaOS 6.3 will be supported at least through October 31st 2018. Individual AP support dates will vary based on their end of sale date. See the Aruba end of support page at http://www.arubanetworks.com/support-services/end-of-life-products/ for additional details.

Table 12: *AP Support*

AP Model	End of Sale Dates (Standard Variants)	Last ArubaOS Version Supported
AP-60, AP-61, AP-65, AP-65WB, AP-70 (All Variants)	31-May-2011	ArubaOS 6.3
AP-85 (All Variants)	30-Apr-2013	ArubaOS 6.3
AP-120, AP-121 (802.11a/b/g)	31-Jan-2012	ArubaOS 6.4
AP-120, AP-121 (802.11a/n or 802.11b/g/n)	31-Jan-2012	ArubaOS 6.4
AP-124, AP-125 (802.11a/b/g)	1-Aug-2013	ArubaOS 6.4
AP-124, AP-125 (802.11a/n and 802.11b/g/n)	1-Aug-2013	ArubaOS 6.4

Table 12: *AP Support*

AP Model	End of Sale Dates (Standard Variants)	Last ArubaOS Version Supported
RAP-2WG	31-Oct-2013	ArubaOS 6.3
RAP-5WN	31-Oct-2013	ArubaOS 6.3
RAP-5	31-Jan-2012	ArubaOS 6.3

Chapter 3
Regulatory Updates

This chapter describes the regulatory updates in ArubaOS 6.4.x release versions.

NOTE

Contact your local Aruba sales representative on device availability and support for the countries listed in the following tables.

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the controller command-line interface and issue the command **show ap allowed-channels country-code <country-code> ap-type <ap-model>**.

Regulatory Updates in ArubaOS 6.4.3.1

The following Downloadable Regulatory Table (DRT) file versions are supported in ArubaOS 6.4.3.1:

- DRT-1.0_49422
- DRT-1.0_49596

For a complete list of countries certified with different AP models, refer to the respective DRT release notes at support.arubanetworks.com.

Regulatory Updates in ArubaOS 6.4.3.0

The following Downloadable Regulatory Table (DRT) file versions are supported in ArubaOS 6.4.3.0:

- DRT-1.0_48902
- DRT-1.0_49142

For a complete list of countries certified with different AP models, refer to the respective DRT release notes at support.arubanetworks.com.

Regulatory Updates in ArubaOS 6.4.2.5

The following table describes regulatory enhancements introduced in ArubaOS 6.4.2.5 (Reg-DRT-1.0_48188, Reg-DRT-1.0_48460, and Reg-DRT-1.0_48713).

Table 13: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Aland Islands	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Albania	• Support added for AP-103H • Support added for AP-175P • Support added for AP-225 • Support added for RAP-108
Andorra	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Argentina	• Support added for AP-103H • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support updated for AP-224 and AP-225
Aruba	Support added for AP-225
Australia	UNII-3 band enabled for: • AP-204 and AP-205 • AP-214 and AP-215 • AP-224 and AP-225 Support added for AP-277
Bahrain	Support added for AP-277
Bangladesh	Support added for AP-224 and AP-225
Barbados	Support added for AP-225
Brazil	Support added for AP-214 and AP-215

Table 13: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Canada	Support added for AP-205H
China	Support updated for RAP-3WN
Columbia	Support added for AP-214 and AP-215
Costa Rica	• Support updated for AP-103 and AP-103H • Support updated for RAP-3WN and RAP-3WNP
Ecuador	• Support added for AP-135 • Support added for AP-204 and AP-205
Egypt	• Support updated for AP-92, AP-93, and AP-93H • Support updated for AP-114 and AP-115 • Support updated for AP-124 and AP-125 • Support updated for AP-134 and AP-135 • Support updated for AP-175P • Support updated for AP-204 and AP-205 • Support updated for AP-224 and AP-225 • Support updated for AP-274 and AP-275
El Salvador	Support added for AP-114 and AP-115
Faroe Islands	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
French Guiana	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP

Table 13: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
French Southern Territories	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Greenland	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Grenada	Support added for AP-225
Guatemala	Support added for AP-114 and AP-115
Guernsey	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Island of Man	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP

Table 13: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Jersey	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Jordan	• Support added for AP-225 • Support added for AP-277
Kenya	Support added for AP-103
Kuwait	• Support added for AP-93 • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-215
Martinique	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Mexico	Support added for AP-214
Monaco	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Morocco	Support added for AP-205

Table 13: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
New Zealand	UNII-3 band enabled for: • AP-204 and AP-205 • AP-214 and AP-215 • AP-224 and AP-225 Support added for AP-277
Oman	• Support updated for AP-93 • Support added for AP-103 • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for AP-274 and AP-275 • Support added for AP-277
Panama	Support added for AP-205
Peru	Support added for AP-274
Philippines	Support added for AP-277
Reunion	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Saint Barthelemy	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Saint Lucia	Support added for AP-225

Table 13: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Saint Martin	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
San Marino	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Saint Pierre and Miquelon	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Saudi Arabia	Support added for AP-277
Singapore	Support added for AP-277
Svalbard and Jan Mayen	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP
Thailand	Support updated for AP-214 and AP-215

Table 13: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
United States of America	• Support updated for AP-103 • FCC DFS channels 52-64 added for AP-274 and AP-275
Vietnam	Support added for AP-215
Wallis and Futuna	• Support added for AP-93 • Support added for AP-103 and AP-103H • Support added for AP-105 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-175P • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-224 and AP-225 • Support added for RAP-108 and RAP-109 • Support added for RAP-3WNP

Regulatory Updates in ArubaOS 6.4.2.4

The following table describes regulatory enhancements introduced in ArubaOS 6.4.2.4.

Table 14: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Algeria	Support added for AP-205
Brazil	Support added for AP-92 and AP-93
Jamaica	Support added for AP-225
Morocco	Support added for RAP-3WN and RAP-3WNP
Malaysia	Support added for AP-214
Oman	• Support added for RAP-109 • Support added for RAP-155
Peru	• Support added for RAP-3WNP • Support added for RAP-108 • Support added for AP-204 and AP-205 • Support added for AP-275
Russia	• Support added for AP-103 and AP-103H • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215 • Support added for AP-274 and AP-275
South Korea	Support added for AP-103H
Taiwan	Support added for AP-274 and AP-275

Table 14: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Tunisia	Support added for AP-105
United Arab Emirates	Support added for AP-214
Zimbabwe	• Support added for AP-103 • Support added for AP-205

Regulatory Updates in ArubaOS 6.4.2.3

The following table describes regulatory enhancements introduced in ArubaOS 6.4.2.3.

Table 15: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Australia	Support added for AP-214 and AP-215
Bolivia	Support added for AP-135
Botswana	Support added for AP-135
Brazil	Support added for RAP-155 and RAP-155P
Canada	• DFS channels added for AP-214 and AP-215 • DFS channels added for AP-274 and AP-275
China	Support added for RAP-3WN and RAP-3WNP
Costa Rica	• Support added for RAP-3WN and RAP-3WNP • Support added for RAP-108 and RAP-109 • Support added for AP-114 and AP-115 • Support added for AP-204 and AP-205 • Support added for AP-224 and AP-225 • Support added for AP-274 and AP-275
ETSI Country Domains	• MAX-EIRP updated for AP-204 and AP-205 • MAX-EIRP updated for AP-214 and AP-215
Indonesia	• Support added for AP-103H • Support added for AP-204 • Support added for AP-215
Japan	Support added for AP-274 and AP-275
Jordan	Support added for AP-103
Kazakhstan	• Support added for RAP-108 and RAP-109 • Support added for RAP-155 and RAP-155P

Table 15: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Kenya	• Support added for AP-115 • Support added for AP-205 • Support added for AP-215 • Support added for AP-225 • Support added for AP-275
Kuwait	Support added for AP-225
Lebanon	Support added for AP-225
Macau	• Support added for AP-103 • Support added for AP-103H
Macedonia	Support added for AP-225
Malaysia	• Support added for AP-103H • Support added for AP-215
Mexico	• Support added for AP-103 and AP-103H • Support added for RAP-155 and RAP-155P • Support added for AP-215 • Support added for AP-224 and AP-225
Morocco	Support added for AP-225
Namibia	Support added for AP-224 and AP-225
New Zealand	Support added for AP-214 and AP-215
Nigeria	Support added for AP-225
Panama	• Support added for AP-135 • Support added for AP-225
Peru	• Support added for RAP-3WN • Support added for AP-103 and AP-103H • Support added for RAP-108 • Support added for RAP-109 • Support added for AP-114 and AP-115 • Support added for AP-135 • Support added for AP-225
Serbia	Support added for AP-225
Singapore	Support added for AP-204
South Africa	• Support added for AP-134 and AP-135 • Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215
Taiwan	Support added for AP-103H

Table 15: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Ukraine	• Support added for RAP-3WN and RAP-3WNP • Support added for AP-224 and AP-225
United Arab Emirates	• Support added for AP-204 • Support added for AP-205 • Support added for AP-215
Vietnam	• Support added for AP-104 • Support added for RAP-155P • Support added for AP-205

Regulatory Updates in ArubaOS 6.4.2.2

The following table describes regulatory enhancements introduced in ArubaOS 6.4.2.2.

Table 16: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Argentina	Support added for AP-204 and AP-205
Bahrain	Support added for AP-225
Brazil	Support added for AP-204 and AP-205
Costa Rica	Support added for RAP-108 and RAP-109
Egypt	Support added for AP-103H
Indonesia	• Support removed for AP-105 • Support added for RAP-108 and RAP-109 • Support added for AP-115 • Support removed for AP-135 • Support added for RAP-155 and RAP-155P • Support added for AP-175P • Support added for AP-225
Israel	• Support added for AP-103 and AP-104 • Support added for AP-204 and AP-205
Japan	Support added for AP-274 and AP-275
Mexico	• Support added for RAP-155 and RAP-155P • Support added for AP-275
Philippines	Support added for AP-214 and AP-215
Saudi Arabia	• Support added for AP-105 • Support added for AP-214 and AP-215
South Korea	Support added for AP-214 and AP-215

Table 16: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Sri Lanka	• Support added for AP-105 • Channel 144 removed for AP-105 • Support added for AP-135 • Channel 144 removed for AP-135 • Support added for AP-225
Taiwan	• Support added for AP-214 and AP-215 • Channel 165 removed for AP-214 and AP-215
Ukraine	Support added for AP-214 and AP-215
Uruguay	• Support added for AP-135 • Support added for AP-225
Vietnam	Support added for AP-104

Regulatory Updates in ArubaOS 6.4.2.1

The following table describes regulatory enhancements introduced in ArubaOS 6.4.2.1.

Table 17: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Argentina	Support added for AP-274 and AP-275
Australia	Support added for AP-103H
Bolivia	Support added for AP-225
Botswana	Support added for AP-225
Brazil	Support added for AP-103
Canada	DFS channels added for AP-204 and AP-205
Chile	• Support added for AP-103H • Support added for AP-214 and AP-215
China	Support added for AP-214 and AP-215
Hong Kong	• Support added for AP-103H • Support added for AP-214 and AP-215
India	• Support added for AP-204 and AP-205 • Support added for AP-214 and AP-215
Japan	Support added for AP-103H
Malaysia	Support added for AP-204 and AP-205

Table 17: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Mauritius	Support added for AP-135
Mexico	Support added for AP-204 and AP-205
Morocco	Support added for AP-225
New Zealand	Support added for AP-103H
Philippines	Support added for AP-103H
Qatar	Support added for AP-214 and AP-215
Saudi Arabia	Support added for AP-103H
Singapore	• Support added for AP-214 and AP-215 • Support added for AP-103H
South Africa	• Support added for AP-103H • Support added for AP-204 and AP-205
South Korea	• Support added for AP-204 and AP-205 • Support added for AP-274 and AP-275
Taiwan	• Support added for AP-103 • Support added for AP-204 and AP-205
Ukraine	Support added for AP-103H
United Arab Emirates	Support added for AP-103H
Venezuela	Channels 36-48 for 802.11a 80MHz (outdoor) for AP-225

Regulatory Updates in ArubaOS 6.4.2.0

The following table describes regulatory enhancements introduced in ArubaOS 6.4.2.0.

Table 18: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Argentina	Support added for AP-103
Australia	Support added for AP-204 and AP-205
Austria	• Support added for AP-103H • Support added for AP-214 and AP-215
Bahamas	• Support added for AP-204 and AP-205 • Support added for AP-224 and AP-225 • Support added for AP-274 and AP-275

Regulatory Domain	Regulatory Changes
Belgium	• Support added for AP-103H • Support added for AP-214 and AP-215
Bosnia/Herzegovina	Support added for AP-103H
Bulgaria	• Support added for AP-103H • Support added for AP-214 and AP-215
Canada	• Support added for AP-103H • Support added for AP-214 and AP-215
Chile	Support added for AP-274 and AP-275
China	Support added for AP-275
Colombia	• DFS channels added for AP-224 and AP-225 • Support added for AP-103H
Croatia	• Support added for AP-103H • Support added for AP-214 and AP-215
Cyprus	Support added for AP-103H
Czech Republic	• Support added for AP-103H • Support added for AP-214 and AP-215
Denmark	• Support added for AP-103H • Support added for AP-214 and AP-215
Dominican Republic	DFS channels added for AP-224 and AP-225
Estonia	• Support added for AP-103H • Support added for AP-214 and AP-215
Finland	• Support added for AP-103H • Support added for AP-214 and AP-215
France	• Support added for AP-103H • Support added for AP-214 and AP-215
Germany	• Support added for AP-103H • Support added for AP-214 and AP-215
Hong Kong	• Support added for AP-204 • Channels 141-165 enabled for AP-120, AP-121, AP-124, and AP-125 • Support added for AP-224 and AP-225
Hungary	• Support added for AP-103H • Support added for AP-214 and AP-215
India	Support added for AP-274 and AP-275
Ireland	• Support added for AP-103H • Support added for AP-214 and AP-215

Regulatory Domain	Regulatory Changes
Israel	• Support added for AP-204 and AP-205 • Support ended for 802.11g 40MHz (indoor) 8-12 and 9-13 for all APs • Support ended for 802.11g 40MHz (outdoor) 8-12 and 9-13 for all APs
Italy	• Support added for AP-103H • Support added for AP-214 and AP-215
Japan	Support added for AP-204 and AP-205
Latvia	• Support added for AP-103H • Support added for AP-214 and AP-215
Lithuania	• Support added for AP-103H • Support added for AP-214 and AP-215
Luxembourg	• Support added for AP-103H • Support added for AP-214 and AP-215
Macedonia	• Support added for AP-204 and AP-205 • Support added for AP-103H
Malta	• Support added for AP-103H • Support added for AP-214 and AP-215
Maritime	• Support added for AP-68 • Support added for AP-92, AP-93, and AP-93H • Support added for AP-103H, AP-104, and AP-105 • Support added for AP-120, AP-121, AP-124, and AP-125 • Support added for AP-134 and AP-135 • Support added for AP-175DC, AP-175AC, and AP-175P • Support added for AP-204 and AP-205 • Support added for AP-224 and AP-225 • Support added for RAP-3WN and RAP-3WNP
Maritime Offshore	• Support added for AP-68 • Support added for AP-92, AP-93, and AP-93H • Support added for AP-103H, AP-104, and AP-105 • Support added for AP-120, AP-121, AP-124, and AP-125 • Support added for AP-134 and AP-135 • Support added for AP-175DC, AP-175AC, AP-175P • Support added for AP-204 and AP-205 • Support added for AP-224 and AP-225 • Support added for RAP-3WN and RAP-3WNP
Mauritius	Support added for AP-224 and AP-225
Mexico	Support added for AP-103
Montenegro	Support added for AP-103H
Netherlands	• Support added for AP-103H • Support added for AP-214 and AP-215
New Zealand	Support added for AP-204 and AP-205

Regulatory Domain	Regulatory Changes
Philippines	• Support added for RAP-108 • Support added for AP-204 and AP-205
Poland	• Support added for AP-103H • Support added for AP-214 and AP-215
Portugal	• Support added for AP-103H • Support added for AP-214 and AP-215
Puerto Rico	• DFS channels added for AP-224 and AP-225 • Support added for AP-103H • Support added for AP-274 and AP-275
Qatar	Support added for AP-204 and AP-205
Romania	• Support added for AP-103H • Support added for AP-214 and AP-215
Saudi Arabia	Support added for AP-204 and AP-205
Slovakia	• Support added for AP-103H • Support added for AP-214 and AP-215
Slovenia	• Support added for AP-103H • Support added for AP-214 and AP-215
South Africa	Support added for AP-274 and AP-275
South Korea	Support added for AP-274 and AP-275
Sweden	Support added for AP-103H
Thailand	Support added for AP-103H
Ukraine	Support added for AP-204 and AP-205
United Kingdom	• Support added for AP-103H • Support added for AP-214 and AP-215
United States of America	• Support added for AP-103H • Support added for AP-214 and AP-215
Venezuela	Support added for AP-225
Vietnam	• Support added for AP-225 • Support added for AP-115

Regulatory Updates in ArubaOS 6.4.0.2

The following table describes regulatory enhancements introduced in ArubaOS 6.4.0.2.

Table 19: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
India	Support added for AP-175DC
Senegal	Support added for AP-134 and AP-135

Regulatory Updates in ArubaOS 6.4.0.0

The following table describes regulatory enhancements introduced in ArubaOS 6.4.0.0.

Table 20: *Regulatory Domain Updates*

Regulatory Domain	Regulatory Changes
Argentina, Brazil, Chile, India, Indonesia, Israel, Mexico, Philippines, Russia, Taiwan, Trinidad and Tobago, and Ukraine	Support added for AP-224 and AP-225
Argentina, Uruguay, and Vietnam	Support added for AP-92 and AP-93
Argentina, Chile, and Israel	Support added for RAP-3WN and RAP-3WNP
Argentina, Chile, Israel, and Taiwan	Support added for RAP-108 and RAP-109
Australia, Argentina, Brazil, Chile, China, Colombia, Egypt, Hong Kong, India, Indonesia, Israel, Malaysia, Mexico, New Zealand, Qatar, Russia, Saudi Arabia, Singapore, South Korea, South Africa, Taiwan, Thailand, Trinidad and Tobago, UAE, and Ukraine	Support added for AP-114 and AP-115
Australia, Chile, China, Egypt, Hong Kong, India, Indonesia, Israel, Japan, Malaysia, Mexico, New Zealand, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Taiwan, Thailand, and Ukraine	Support added for RAP-155 and RAP-155P

Regulatory Domain	Regulatory Changes
China	Support added for AP-224
Costa Rica	Support added for AP-134 and AP-135
Indonesia	Support added for AP-175
Nigeria	Support added for AP-105
Serbia and Montenegro	In addition to the **CS** country code used for both Serbia and Montenegro combined, ArubaOS now supports the **RS** country code for Serbia and the **ME** country code for Montenegro.
Thailand, Indonesia	Support added for the RAP-109
Uruguay	Support added for AP-104 and AP-105

The following example shows indoor, outdoor, and DFS channels supported by an AP-105 in the **United States** domain.

```
(host) #show ap allowed-channels country-code us ap-type 105
Allowed Channels for AP Type 105 Country Code "US" Country "United States"
-------------------------------------------------------------------------
PHY Type                 Allowed Channels
--------                 ----------------
802.11g (indoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)         36 40 44 48 52 56 60 64 100 104 108 112 116 132 136 140 149 153 157
161 165
802.11g (outdoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)        52 56 60 64 100 104 108 112 116 132 136 140 149 153 157 161 165
802.11g 40MHz (indoor)   1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)   36-40 44-48 52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11g 40MHz (outdoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)  52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11a (DFS)            52 56 60 64 100 104 108 112 116 132 136 140
```

This chapter describes the issues resolved in ArubaOS 6.4.x release versions.

Resolved Issues in ArubaOS 6.4.3.1

The following issues are resolved in ArubaOS 6.4.3.1.

Air Management-IDS

Table 21: *Air Management-IDS Fixed Issues*

Bug ID	Description
114740 114768 114891 115069 115914	**Symptom:** The WMS process crashed in a controller. This issue is resolved by addressing the WMS exiting/restarting at startup due to key file corruption. **Scenario:** This issue occurred in 7210 controllers running ArubaOS 6.4.3.0. **Platform:** 7210 controllers. **Reported Version:** ArubaOS 6.4.3.0.

AP-Datapath

Table 22: *AP-Datapath Fixed Issues*

Bug ID	Description
113962	**Symptom:** When a client started roaming from one AP to another, the phones got stuck at Key1. This issue is resolved by making improvements to the wireless drivers. **Scenario:** This issue was observed in Netlink phones after the controller was upgraded from 6.1.3.4 to 6.3.1.14. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.14.
114412	**Symptom:** Multiple AP-135 access points crashed simultaneously with the reboot reason **Reboot Reason: Reboot caused by kernel panic: assert**. This issue is resolved by removing unnecessary messages from the datapath. **Scenario:** This issue occurred in AP-135 access points connected to 7240 controllers running ArubaOS 6.3.1.6. **Platform:** AP-135 access points. **Reported Version:** ArubaOS 6.3.1.6.
115460	**Symptom:** Access Control Lists (ACLs) using firewall rules with domain names did not work with AP-205 access points. This issue is resolved by modifying the data sequence. **Scenario:** This issue was caused by a failed DNS resolution. This issue was observed in AP-205 access points connected to controllers running ArubaOS 6.4.2.5 in a split-tunnel mode. **Platform:** AP-205 access points. **Reported Version:** ArubaOS 6.4.2.5.

Base OS Security

Table 23: *Base OS Security Fixed Issues*

Bug ID	Description
113301 114278	**Symptom**: The **extifmgr** process crashed in the controller. The fix ensures that there is no memory corruption and the **extifmgr** process remains stable. **Scenario**: The **extifmgr** process crashed due to a memory corruption for a response to an HTTP error. This process is responsible to send HTTP User Agent strings and mDNS broadcast information to ClearPass Policy Manager. This issue was observed in the local controller of a master-local topology. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.

Captive Portal

Table 24: *Captive Portal Fixed Issues*

Bug ID	Description
115484	**Symptom**: When a custom background image was used in the captive portal configuration, the background was not displayed although the functionality of captive portal worked as expected. This issue is resolved by changing how the background image is utilized in the captive portal. **Scenario**: This issue occurred when a custom background image was used for captive portal. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.0.

Controller-Datapath

Table 25: *Controller-Datapath Fixed Issues*

Bug ID	Description
110452 116139	**Symptom:** There was an unexpected drastic increase followed by a decrease in the datapath CPU utilization. This issue is resolved by adding a mechanism to avoid loops during the lookup for sessions in pending delete state. **Scenario:** This issue was observed in 7220 controllers running ArubaOS 6.4.2.2. This issue was observed during either of the following conditions: • If DPI was enabled and if there was a large number of sessions • In situations where hash collisions occurred in the session table and a non-IP frame (like ARP) was received but the session corresponding to that frame was linked after a session in pending delete state. **Platform:** 7220 controllers. **Reported Version:** ArubaOS 6.4.2.2.
112676 115547	**Symptom**: A controller crashed and rebooted. The log files for the event listed the reason for the reboot as **datapath timeout**. This issue is resolved by making internal code changes. **Scenario**: This issue was observed when the **show datapath ipv6-mcast destination** command was issued. This issue was observed in 7220 controllers running ArubaOS 6.4.2.5 in a master-local topology. **Platform:** 7220 controllers. **Reported Version:** ArubaOS 6.4.2.5.

IPsec

Table 26: *IPsec Fixed Issues*

Bug ID	Description
115373	**Symptom:** After a successful authentication, the controller did not send back a class-attribute to the authentication server in radius-accounting packets. This issue is resolved by making internal code changes. **Scenario:** This issue was observed with VIA/VPN users connected to a 7220 controllers running ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.

Remote AP

Table 27: *Remote AP Fixed Issues*

Bug ID	Description
112421 114593 115813 115885	**Symptom**: Wireless clients that associated to a RAPv3 network failed to access the internet in split-tunnel forwarding mode. The fix ensures that the wireless clients can access the internet successfully. **Scenario**: This issue was observed when performing a full global configuration synchronization of the master controller with the local controller, the bridge forwarding mode ACLs could have got re-arranged in the AP. A full global configuration synchronization occurs when there is a loss of master-local connectivity or when a local controller joins a new master controller. This issue was observed in controllers running ArubaOS 6.4.0.0 or later versions. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.0.

Station Management

Table 28: *Station Management Fixed Issues*

Bug ID	Description
114442	**Symptom:** A 7240 controller stopped responding and crashed. The log files for the event listed the reason as **STM Arithmetic exception**. A check is added to avoid memory overrun in the Station Management (STM) process of the controller during a memory copy function. **Scenario:** This issue was observed when an access point sent corrupted PAPI packets to the controller. This resulted in the corruption of the STM license table. This issue was observed in controllers running ArubaOS 6.3.1.13 or 6.4.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.13.

Resolved Issues in ArubaOS 6.4.3.0

ArubaOS 6.4.3.0 is a maintenance release that includes a fix for CVE-2015-0286 and CVE-2015-0292. Additionally, the following issues are resolved in ArubaOS 6.4.3.0.

AMON

Table 29: *AMON Fixed Issues*

Bug ID	Description
107732	**Symptom**: In the **Dashboard > Performance**, clients check for retried frames on **To Client** and **From Client** displayed large percentages. This issue is resolved by implementing internal code changes. **Scenario**: This issue was observed in 7240 controllers running ArubaOS 6.4.1.0 in a master-local topology. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.1.0.

AirGroup

Table 30: *AirGroup Fixed Issues*

Bug ID	Description
91690	**Symptom**: Clients were unable to use AirGroup services to connect to other iChat clients. The fix ensures that iChat and unsolicited responses for iChat are supported from this release. **Scenario**: This issue was observed in ArubaOS 6.3.0.1, and is triggered because AirGroup does not support unsolicited advertisements required by iChat. As a result, clients were unable to immediately discover each other when they logged in to the network using Bonjour. **Platform:** 3400 controllers. **Reported Version:** ArubaOS 6.3.0.1.
96675	**Symptom:** Local controllers handling multicast Domain Name System (mDNS) process crashed. To resolve this issue, the cache entries and memory used for the device that sends an mDNS response packet with a time-to-live (TTL) value as zero are cleared. **Scenario:** This issue was observed when a controller received mDNS response packets, and the value of TTL was set to zero. This issue was observed in ArubaOS 6.3, but was not specific to any controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.0.0.
104089 104090 104091 104152	**Symptom:** When devices roamed from one controller to another and then left the network, the internal cache records of AirGroup was cleared, but references were not cleared. Subsequent access to resources using the references crashed a controller. This issue is resolved by clearing the references when clearing the cache records. **Scenario:** This issue occurred when AirGroup was enabled, AirGroup domain was configured, and devices roamed from one controller to another and left the network. This issue was observed in 7240 controllers running ArubaOS 6.4.1.0 **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.1.0.

Table 30: *AirGroup Fixed Issues*

Bug ID	Description
108014	**Symptom:** Occasionally, an incorrect last queried time was displayed in the output of the **show airgroup user verbose** command. This issue is resolved by not updating the timestamp to a default value whenever an invalid mDNS packet is received and by displaying an empty timestamp when all received packets are invalid mDNS packets. **Scenario:** This issue was observed when an invalid mDNS or DLNA packet was received and the default last queried time was displayed. This issue was not limited to any specific controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.9
110305	**Symptom:** Memory leakage was observed on a controller. This issue is resolved by freeing the unused memory. **Scenario:** The memory leak occurred when the **allowall** service was disabled and AirGroup received mDNS response packets that contained a pointer record with an unique **service-id**. **Platform:** 7210 controllers. **Reported Version:** ArubaOS 6.4.1.0.
110283	**Symptom:** The discovery of the printer proxy servers failed and the clients did not connect to AirPrint printers. This issue is resolved by improving how a controller queries for printer information. **Scenario:** This issue was observed when the printer/proxy servers did not respond with all mDNS records for a wildcard query. This issue was not specific to any controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.13.

Air Management-IDS

Table 31: *Air Management-IDS Fixed Issues*

Bug ID	Description
103304	**Symptom**: A rogue AP was detected with match-type unknown and match mac 00:00:00:00:00:00. This issue is resolved by performing a MAC Organizationally Unique Identifier (OUI) compare only if the gateway MAC of an AP is set to non-zeros. **Scenario**: This issue occurred when an access point was trunked to listen to frames from multiple (tagged) VLANs. An issue during AP startup, in rare cases, allowed a malformed MAC address to be marked as a gateway MAC for rogue classification purposes. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.8.
104711	**Symptom**: Real Time Location Server (RTLS) received multiple station messages with invalid client MAC OUIs in controllers with AP-105 access points. This issue is resolved by implementing internal code changes. **Scenario**: This issues was observed when corrupt block acknowledgment frames were transmitted by AP-105 access points to its clients. As a result, a controller created client entries with invalid MAC addresses. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.5.

AP Datapath

Table 32: *AP Datapath Fixed Issues*

Bug ID	Description
99655	**Symptom:** Gratuitous ARP triggered responses, which caused station buffer overflow. This issue is resolved by changing the Gratuitous ARP to the gateway IP, so that all stations receive the packet, but only gateways are able to respond. This avoids unnecessary ARP learning. **Scenario:** This issue was observed when a Gratuitous ARP was sent from a RAP to update the uplink switch/router MAC table. This caused devices in the same network to send ARP responses which lead to client MAC table overflow. This issue was observed in ArubaOS 6.2.1.5. **Platform:** AP-105. **Reported Version:** ArubaOS 6.2.1.5.
112086	**Symptom:** Clients connected to a remote AP in bridge forwarding mode lost connectivity and showed the wrong ESSID in the user table of a controller because of a corrupt AP bridge table. This issue is resolved by ensuring that the AP reads the VLAN information of the offline Virtual AP (VAP) in the ArubaOS 6.1 format. **Scenario:** This issue was observed when a controller was upgraded from ArubaOS 6.1. to ArubaOS 6.3 . This issue occurred because the format of the offline VAP was different between ArubaOS 6.1 and ArubaOS 6.3 which caused the APs to not read the stored offline information in the ArubaOS 6.1 format. This issue was observed in controllers running ArubaOS 6.3. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.14.

AP-Platform

Table 33: *AP-Platform Fixed Issues*

Bug ID	Description
96944	**Symptom:** When an AP and standby controller were on the same subnet, the IPSEC tunnel setup failed. This issue is resolved by not adding the host route when a master or standby controller has an AP on the same subnet. **Scenario:** This issue was observed when an AP and standby controller were on the same subnet. This issue was observed in controllers running ArubaOS version 6.4 or lower but was not specific to any controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.3.
98691	**Symptom:** The status of an access point showed down in the master controller although it was up in the local controller. This issue is resolved by adding master-local periodic AP state synchronization. **Scenario:** This issue occurred when the master and local controllers in a master-local topology were upgraded to ArubaOS 6.3.1.5. This issue occurred in 7200 Series controllers running ArubaOS 6.3.1.4. **Platform:** 7200 Series controllers. **Reported Version:** ArubaOS 6.3.1.4.
100768	**Symptom:** The configuration command **logging level debugging ap-debug** did not run after rebooting a controller and it had to be reconfigured. This issue is resolved by sending debug level request message to syslogdwrap when initializing the SAPM. **Scenario:** This issue occurred when the SAPM was initializing and it did not send debug level request to syslogdwrap. Hence, the SAPM did not send the debug level configure log message to the access points. This issue was observed in controllers running ArubaOS 6.4.0.3 but was not specific to any controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.0.

Table 33: *AP-Platform Fixed Issues*

Bug ID	Description
103362	**Symptom:** All active APs on a local controller displayed the status as down on a master controller. Fixing the LMS list processing in the Station Management (STM) process for restart cases resolved this issue. **Scenario:** After an STM restart, the LMS list for the master controller was not updated in STM. This issue was observed in master-local topology. This issue was not limited to any specific controller model and was observed in controllers running ArubaOS 6.4.1.0 or 6.3.1.8. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.8.
105930	**Symptom:** When the **show ap debug client-stats** command was executed and there was no response from the AP, an internal process was blocked. This issue is resolved by modifying the implementation of the **show ap debug client-stats** command to avoid internal processes from being blocked. **Scenario:** This issue was observed when a message was sent to the AP after the command was executed and if the response was larger than the network MTU size then it was fragmented. If there was an issue with the network, the response did not reach the controller, so the controller waited until timeout limit was reached. During this time frame, no other AP messages were processed which caused other APs to reboot. This issue was observed in APs connected to controllers running ArubaOS 6.3 or later versions. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.9
106500	**Symptom:** A controller accepted GRE-Stripping and AP-Wired-Port configuration if AP-System profile was mapped at the end. This issue is resolved by checking the ap-group, ap-name, ap system-profile, ap wired-ap profile, and ap wired-port profile when the aplacp is enabled. **Scenario:** This issue occurred when the ap-system profile or enet1-port profile was mapped to ap-group profile and ap-name profile. A controller did not check the configuration and displayed an error message. This issue occurred in AP-225 access points connected to controllers running ArubaOS 6.4.1.0. **Platform:** AP-225 **Reported Version:** ArubaOS 6.4.1.0.
112791 113519	**Symptom:** When the **show ap debug client-stats** command was executed, incorrect goodput values were displayed in the controller UI. This issue is resolved by adding a check to count non-null data frames only. **Scenario:** This issue was observed when goodput was computed using management and data frames instead of data frames. This issue was observed in AP-200 Series access points connected to controllers running ArubaOS 6.4.2.4. **Platform:** AP-200 Series access points. **Reported Version:** ArubaOS 6.4.2.4.
113715	**Symptom:** An access point rebootstraped when there were many clients connected in the network, which caused high traffic. This issue is resolved by prioritizing the access point heartbeat messages. **Scenario:** This issue was observed in AP-61 Series, AP-90 Series, AP-120 Series access points connected to controllers running ArubaOS 6.3.1.9. **Platform:** AP-60 Series, AP-90 Series, AP-120 Series. **Reported Version:** ArubaOS 6.3.1.9.
113989 112157	**Symptom:** A AP-205 access point rebooted randomly. The log files listed the reason for the reboot as **kernel panic: Fatal exception**. This issue is resolved by introducing a bypass NULL pointer check to initialize transmit beamforming link on the default VAP. **Scenario:** This issue was observed when the driver radio reset initialized data structures and NULL pointer was accessed. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.

AP-Wireless

Table 34: *AP-Wireless Fixed Issues*

Bug ID	Description
98692 99914 100459 101862 103013 106065	**Symptom:** AP-220 Series access points stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel panic: Fatal exception**. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in AP-220 Series access points connected to 7210 controller running ArubaOS 6.4.0.2 in a master-local topology where the APs terminated on both the controllers in campus mode. **Platform:** AP-220 Series. **Reported Version:** ArubaOS 6.4.0.2.
99678	**Symptom:** A AP-175 access point rebooted continuously. This issue is resolved by setting a default channel to avoid crash when the channel configuration has an error. **Scenario:** This issue was observed when the country-code was set to South Africa (SA) and when the SAPD process set an unsupported channel to the AP driver. **Platform:** AP-175. **Reported Version:** ArubaOS 6.2.1.1.
100251	**Symptom:** An access point rebooted with error **unhandled kernel unaligned access**. This issue is resolved by implementing Internal code changes in the Linux kernel. **Scenario:** This issue was observed in AP-125 access points connected to controllers running ArubaOS 6.3.1.5. **Platform:** AP-125. **Reported Version:** ArubaOS 6.3.1.5.
105089	**Symptom:** The wireless clients experienced packet loss when connected to the AP-135/AP-105 access points where the multicast was using DMO. This issue is resolved by reducing the retry tx rate for AP-104/AP-105/AP-135/AP-134 at DMO mode. **Scenario:** This issue was observed in AP-135/AP-105 where the DMO enables an SSID profile and the client does not send ACK packets when receiving high 11n rate data. **Platform:** AP-135. **Reported Version:** ArubaOS 6.4.1.0.
108694	**Symptom:** Some clients were unable to pass traffic after adding net-destination to the role. This issue is resolved by updating the ACL synchronization between STM, authentication, and AP. **Scenario:** This issue occurred after adding net-destination to the user role. This issue occurred in AP-105 access points connected to M3 controllers running ArubaOS 6.1.3.9. **Platform:** AP-105. **Reported Version:** ArubaOS 6.1.3.9.
110195	**Symptom:** Windows 8 and Windows 10 clients were unable to switch between guest network and corporate network. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in AP-105 access points connected to 3200 controllers running ArubaOS 6.3.1.10 in a master-standby topology. **Platform:** AP-105. **Reported Version:** ArubaOS 6.3.1.10.

Table 34: *AP-Wireless Fixed Issues*

Bug ID	Description
110581	**Symptom**: An access point crashed and the log files for the event listed the reason for the crash as **kernel page fault at virtual address 00000000, epc == c08f2734, ra == c08f4be**. This issue is resolved by implementing internal code changes. **Scenario**: This issue was observed in AP-105 access points connected to controllers running ArubaOS 6.3.1.13. **Platform**: AP-105. **Reported Version**: ArubaOS 6.3.1.13.
111596	**Symptom:** A AP-225 access point had uneven per-client throughput for 802.11ac clients. This issue is resolved by changing the queuing mechanism for stations to provide better airtime for all clients. **Scenario:** This issue was observed in AP-225 access points running ArubaOS 6.4.x version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3.
112077	**Symptom:** Radar detection was triggered when operating on DFS channel. This issue is resolved by updating when radar detection is triggered to eliminate false detection. **Scenario:** This issue occurred in AP-215 access points connected to controllers running ArubaOS 6.4.2.3 when the DFS channel was the operating channel. **Platform:** AP-215. **Reported Version:** ArubaOS 6.4.2.3.

ARM

Table 35: *ARM Fixed Issues*

Bug ID	Description
112958	**Symptom:** Low throughput was observed on clients. This issue is resolved by implementing code changes in the accounting algorithm to improve the performance. **Scenario:** This issue was observed in a standalone master topology when ATF was enabled. This issue was observed in AP-125, AP-135, and AP-224 access points connected to 7210 controllers running ArubaOS 6.3.1.x. **Platform:** 7210 controllers, AP-125, AP-135, and AP-224. **Reported Version:**ArubaOS 6.3.1.9.

Authentication

Table 36: *Authentication Fixed Issues*

Bug ID	Description
96285	**Symptom:** A correct role was not assigned to a user when the XML API changed the user role. This issue is resolved by sending a notification to the Campus AP (CAP) in the bridge mode during External Captive Portal (ECP) event of role change. **Scenario:** This issue was observed when a client was connected to the CAP in the bridge mode. This issue occurred in controllers running ArubaOS 6.3.1.2 and was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.2.

Base OS Security

Table 37: *Base OS Security Fixed Issues*

Bug ID	Description
93550	**Symptom:** Running the **aaa test-server** command for a TACACS authentication server displayed **AAA server timeout** in spite of successful authentication. The fix ensures that the command displays **Authentication Successful** for a successful TACACS server. **Scenario:** This issue was not limited to any specific controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.0.
102480	**Symptom:** When a wired user moved to a new port and VLAN, the port switched to the initial role and did not repeat L2 authentication. The fix ensures that the old user entries including the ipuser entries are deleted. **Scenario:** This issue was observed when a user moved from one controller to another and the DMZ controller observed the user traffic from the second GRE tunnel. L2 authentication was not initiated because the VLAN was different. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.5.
104056	**Symptom:** The authentication process crashed when deriving DHCP-option based UDR. Hence, users were listed in deny-all role and failed authentication. This issue is resolved by changing how the authentication process handles DHCP packets when the client-host address contains all zeros. **Scenario:** This issue occurred in 3400 controllers running ArubaOS 6.1.3.13. **Platform:** 3400 controllers. **Reported Version:** ArubaOS 6.1.3.13.
106261	**Symptom:** The authentication module crashed on a local controller while trying to print the IP address of an access point after deleting the SAP entry. This issue is resolved by printing the IP address of an access point by using its local copy. **Scenario:** This issue occurred in a 6000 controller running ArubaOS 6.4.2.0 in master-local topology. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.0.
106682	**Symptom:** A user entry was deleted with the radius accounting terminate-cause **Lost-Service**. This issue is resolved by changing the radius accounting terminate-cause to **Idle-Timeout** in the radius accounting stop packet. The fix changes the behavior of the terminate-cause to be consistent with how an administrator views the system operation. **Scenario:** This issue occurred when a client silently roamed away or triggered STM timeout. This issue was not specific to any controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.
109507 109726	**Symptom:** A 802.1X client failed authentication with an external RADIUS server. This issue is resolved by changing the authentication server name to a non-case sensitive name. **Scenario:** When 802.1X clients terminate on an external RADIUS server, multiple RADIUS messages are exchanged with the external RADIUS server. All these messages must be sent to the same authentication server. There was an issue when the authentication process compared the authentication server name while sending the second RADIUS message to the authentication server. This caused the client to fail authentication. This issue was observed in controllers running ArubaOS 6.4.2.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2.

Table 37: *Base OS Security Fixed Issues*

Bug ID	Description
109835	**Symptom:** The Tunnel-Private-Group-ID radius attribute was displayed incorrectly in the logs when this attribute was sent by the radius server with the Tag field set. This issue is resolved by implementing internal code changes. **Scenario:** This issue was not specific to any controller or release version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.8.
109838	**Symptom:** A controller displayed an incorrect number of net destinations in the WebUI. The fix ensures that the controller displays the correct number of net destinations in the WebUI. **Scenario:** This issue occurred when there was a space before the net destination name. This issue was observed in controllers running ArubaOS 6.3.x and was not limited to any specific controller model. **Platform:** All platform. **Reported Version:** ArubaOS 6.3.1.12.
111762	**Symptom:** The output of the **show running-config** command displayed the Network Time Protocol (NTP) MD5 secret key in plain text. The fix ensures that the NTP MD5 secret key is not displayed in plain text. **Scenario:** This issue was observed when the **encrypt enable** command was enabled. This issue was not limited to a specific controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.13.

Captive Portal

Table 38: *Captive Portal Fixed Issues*

Bug ID	Description
93927	**Symptom:** The output of the **show datapath user** command displayed a user entry but it was not present in the control plane. The fix ensures that the user entry is part of the control plane. **Scenario:** This issue occurred when WLAN was configured in the tunnel mode and was observed in controllers running ArubaOS 6.2 or later. **Platform:** 7200 Series controllers. **Reported Version:** ArubaOS 6.2.1.3.
113370	**Symptom:** Microsoft Windows 8/8.1 clients failed to redirect to the Wireless Internet Service Provider roaming (WISPr) portal page when the clients choose an open browser. This issue is resolved by bypassing the landing page for WISPr user-agent. **Scenario:** This issue occurred with Windows clients connected to AP-225 access points that were connected to 7005 controllers running ArubaOS 6.4.2.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2.

Configuration

Table 39: *Configuration Fixed Issues*

Bug ID	Description
94559	**Symptom**: An ACL configured by the user could not be edited or deleted. This issue is resolved by ensuring that the flag is reset when the ACLs generated for the whitelist configuration are re-used after removing the whitelist. **Scenario**: This issue was observed when a user configuration was whitelisted in Captive Portal profiles in controllers running ArubaOS 6.2 or later versions. **Platform:** 7200 Series controllers. **Reported Version:** ArubaOS 6.2.1.4.
99459	**Symptom**: When the **show running-config** or **show ip access-list** command was executed, the **next-hop-list** parameter was not displayed. This issue was resolved by removing the option to configure **next-hop-list**. **Scenario**: This issue was observed when the **next-hop-list** parameter was configured under session ACL and the parameter was not supported. This issue was observed in 3400 controllers running ArubaOS 6.3.1.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.4.

Controller-Datapath

Table 40: *Controller-Datapath Fixed Issues*

Bug ID	Description
90937	**Symptom:** Application gmail drive was not classified to appID 906. This issue is resolved by integrating the new Qosmos version. The original gmail drive application is deprecated and classified as google_docs with appID 1489. **Scenario:** This issue occurred after DPI was enabled and a client accessed the gmail drive application. This issue was observed in controllers running ArubaOS 6.4.0.0 but was not specific to any controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.0.
94965	**Symptom:** A 7210 controller crashed. The logs for this error listed the reason for the crash as **datapath timeout**. This issue is resolved by adding a length check to ensure that the Wi-Fi fragments have at least 8 bytes of payload, else the Wifi packed is dropped. **Scenario:** The issue was observed in 7210 controllers running ArubaOS 6.3.1.1 in a master-local topology. **Platform:** 7210 controllers. **Reported Version:** ArubaOS 6.3.1.1.
96227	**Symptom:** Access points dropped heartbeat messages to the controller and rebooted. This issue is resolved by introducing the **arp** and **grat-arp** parameters to drop or blacklist the clients that are including unnecessary ARP traffic. **Scenario:** This issue occurred due to large number of unnecessary ARP traffic and was observed on 7200 Series controllers running ArubaOS 6.3.1.2 or later. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.2.

Table 40: *Controller-Datapath Fixed Issues*

Bug ID	Description
99251	**Symptom:** Users were not redirected to the captive portal page. This issue is resolved by adding checks to prevent the IP address of a controller from being added to the whitelist. **Scenario:** This issue was observed when the IP address of a controller was added as a whitelist IP. As a result, the policy to redirect the traffic did not take effect and captive portal stopped working. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.3.
112065	**Symptom:** A controller stopped responding and rebooted. The log files for the event listed the reason as **datapath timeout**. This issue is resolved by removing manual speed configuration and configuring the 1GE port on the remote device connected to the 1GE uplink port of the controller to auto-negotiate the speed. **Scenario:** This issue occurred because the 1GE uplink port on a 7200 Series controller that was configured to auto-negotiate the speed but had resolved to half-duplex because the speed on the remote port was configured manually. However, the uplink port accepted only unidirectional traffic. During high Rx traffic, all the packets in transmission were blocked and triggered datapath timeout. This issue was observed on 7200 Series controllers running ArubaOS 6.3.x or later. **Platform:** 7200 Series controller. **Reported Version:** ArubaOS 6.3.1.14.
112899	**Symptom:** A controller stopped responding and rebooted unexpectedly. The log files for the event list the reason for the reboot as **datapath exception**. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in 7030 controllers running ArubaOS 6.4.2.4. **Platform:**7030 controllers. **Reported Version:** ArubaOS 6.4.2.4.
114177	**Symptom:** A controller crashed due to a datapath exception. The fix ensures that there is no datapath exception if a race condition occurs. **Scenario:** This issue may be observed with Microsoft® Lync voice or video calls. This issue occurred due to a race condition. The race condition may have occurred during Media Classification of Lync voice or video calls. This issue was observed in controllers running ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.

Controller-Platform

Table 41: *Controller-Platform Fixed Issues*

Bug ID	Description
96819	**Symptom:** A user cannot transfer files using SCP to or from a controller on MAC devices. The fix ensures that the SCP copy operation is successful. **Scenario:** This issue is not limited to any specific controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.2.0.0.
101835	**Symptom:** A controller displayed the error message error **Unable to set ip_dst_cache**. This issue is resolved by removing the incorrect error message from the FAPPS module. **Scenario:** This issue occurred in 7000 Series controllers running ArubaOS 6.4.0.0. **Platform:** 7000 Series controllers. **Reported Version:** ArubaOS 6.4.0.0.
103416	**Symptom:** A master controller rebooted and remained in **cpboot** state. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in 3600 controllers running ArubaOS 6.3.1.5 in a master-local topology. **Platform:** 3600 controllers. **Reported Version:** ArubaOS 6.3.1.5.
106690	**Symptom:** An ACL with a destination as Netdestination vrrp_ip applied on a port was not hit on a local controller. This issue is resolved by changing how the FPAPPS module handles messages with wrong ACL name from the authentication module. **Scenario:** This issue occurred during 802.1X authentication of wired and wireless clients. This issue occurred because of a miss configuration of an ACL name which included a space at the end. This issue was observed in master–local network topology. This issue was not limited to any specific controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.5.
111191 111276 111467	**Symptom:** HRTimers failed because of a corrupted stack. This issue is resolved by not tampering the stack frame under certain conditions like after a context save but before invoking interrupt handlers. **Scenario:** This issue was observed in 7000 Series and 7200 Series controllers but was not specific to any ArubaOS version. **Platform:** 7000 Series and 7200 Series controllers. **Reported Version:** ArubaOS 6.3.1.7.
113078	**Symptom:** The output of the **show lldp neighbor interface gigabitethernet <interface number>** command displayed **interface <interface number> invalid** for certain interfaces. This issue is resolved by Implementing internal code changes. **Scenario:** This issue occurred because the GSM component published the information to LLDP using the incorrect slot. This issue was observed on controllers running ArubaOS 6.4.2.3 or later but was not specific to any controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3.
113750	**Symptom:** Users observed that the NTP sync failed with the configured servers. This issue is resolved by adding a periodic timer (15 seconds) to check if the network is up and then performing a NTP sync. **Scenario:** This issue occurred if a NTP sync was performed before an IPSec tunnel was established. This issue was observed in 7010 controllers running ArubaOS 6.4.2.5. **Platform:** 7010 controllers. **Reported Version:** ArubaOS 6.4.2.5.

IPsec

Table 42: *IPsec Fixed Issues*

Bug ID	Description
113559	**Symptom:** RAPs came up using the default Aruba certificates although **crypto isakmp block-aruba-ca enable** was configured in a controller. This issue is resolved by adding a check for **block_aruba_ca** when checking against the device certificates. **Scenario:** This issue was observed when RAPs terminated on a controller. This issue was not specific to any controller or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3.
113688	**Symptom:** The Internet Key Exchange (IKE) process did not respond. This issue is resolved by adding checks to ensure that IKE Dead Peer Detection (DPD) keepalives are not transmitted. **Scenario:** This issue was observed when an access point was deployed as a RAP in Pre-Shared Key (PSK) mode. This issue was caused by high volume of IKE DPD messages that resulted in high CPU utilization. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.

LDAP

Table 43: *LDAP Fixed Issues*

Bug ID	Description
90859	**Symptom:** A controller intermittently disconnected from the LDAP server because the LDAP server reset its TCP connection. This issue is resolved by establishing a TCP connection for each user and binding it by using admin-dn and password. After the user is authenticated, the connection binds the actual user. **Scenario:** This issue was triggered by null binds created when the controller established TCP/SSK connections in advance, so that they can be used whenever a user joined the network. This issue occurred in a 3000 Series controllers running ArubaOS 6.1.3.10. **Platform:** 3000 Series controllers. **Reported Version:** ArubaOS 6.1.3.10.

Licensing

Table 44: *Licensing Fixed Issues*

Bug ID	Description
103538	**Symptom:** A controller generated the following license warning message: **300145: <WARN> |licensemgr| Licenses sent by the server will expire in 29 days**. These were false warning messages and the fix ensures that the controller generates only legitimate warning messages. **Scenario:** This issue was observed when a controller was upgraded to ArubaOS 6.3.1.8 or later version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.8.

Local Database

Table 45: *Local Database Fixed Issues*

Bug ID	Description
113458 113472 115482	**Symptom:** A controller rebooted frequently due to a **udbserver** module crash. This issue is resolved by making internal code changes. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.

Logging

Table 46: *Logging Fixed Issues*

Bug ID	Description
112397 113428	**Symptom:** A controller generated the following Web Content Classification (WebCC) error message: **syslogdwrap[1838]: PAPI_Send: sendto WEB Content Classification failed: No such file or directory Message Code 1003 Sequence Num is 23418**. The fix ensures that the controller stops generating this error message. **Scenario:** This issue occurred although WebCC process was not running on the controller. This issue was observed in M3 and 3000 Series controllers running ArubaOS 6.4.x.x. **Platform:** M3 and 3000 Series controllers. **Reported Version:** ArubaOS 6.4.2.3.

Master-Local

Table 47: *Master -Local Fixed Issues*

Bug ID	Description
100526	**Symptom:** When the **aaa user fast-age** feature was enabled, all the existing ip-users were removed from the table. The fix ensures that existing ip users are not removed when **aaa user fast-age** is configured. **Scenario:** This issue was observed when **aaa user fast-age** feature was configured. This issue was not limited to any specific controller model and was observed in ArubaOS 6.2 and above. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.5.
111482	**Symptom:** An Access Control List (ACL) that had a system defined **vrrp_ip** alias failed to synchronize with the local controller. This issue is resolved by adding a dummy netdestination with the IP address of the controller during initialization. When the vrrp configuration is applied, the netdestination is updated with the configured VRRP IP address. The **vrrp_ip** netdestination exists even if VRRP is not configured. **Scenario:** This issue occurred in controllers running ArubaOS 6.3.1.13. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.13.

Master-Redundancy

Table 48: *Master-Redundancy Fixed Issues*

Bug ID	Description
101012	**Symptom:** Old user derivative rules (UDRs) were not pushed from a master controller to a standby controller. This issue is resolved by always performing full synchronization between master and standby controllers. **Scenario:** This issue occurred only for the old UDR rules that were configured on the master controller. Newly created UDRs were pushed correctly from a master controller to a standby controller. This issue was observed with partial configuration synchronization of global configuration from master and standby controllers. This issue was not limited to any specific to controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.1.3.7.
104636	**Symptom:** Local database failed to synchronize after 1010th attempt. The logs for the event listed the reason as **Last failure cause: Standby switch did not acknowledge the local user database transfer**. The fix ensures that the local database synchronizes after 1010th attempt. **Scenario:** Internal code errors in the **dbsync** process caused this issue. This issue was observed in controllers running ArubaOS 6.3.x in master-standby topology. **Platform:** 7220 controller **Reported Version:** ArubaOS 6.3.1.8.

Mesh

Table 49: *Mesh Fixed Issues*

Bug ID	Description
114108	**Symptom:** A mesh point was unable to build a mesh link with the mesh portal after upgrading the ArubaOS version in a controller from ArubaOS 6.3.1.13 to ArubaOS 6.4.2.4. This issue is resolved by using maximum EIRP to transmit frames when a mesh point does not get the registration table from a controller. **Scenario:** This issue occurred when the ArubaOS version was upgraded in a controller from a version prior to ArubaOS 6.4.2.0 to a version after ArubaOS 6.4.2.0 or when a mesh point was re-provisioned with ArubaOS version after ArubaOS 6.4.2.0. **Platform:** All 802.11n access points. **Reported Version:** ArubaOS 6.4.2.4.

Mobility

Table 50: *Mobility Fixed Issues*

Bug ID	Description
102540	**Symptom:** The IP Mobility module crashed on a controller. This issue is resolved by implementing code level changes to correct the error message. **Scenario:** An incorrect error message was displayed in the IP Mobility module. This issue was observed in 3400 controllers running ArubaOS 6.2.1.7. **Platform:** 3400 controllers. **Reported Version:** ArubaOS 6.1.3.7.

PhoneHome

Table 51: *PhoneHome Fixed Issues*

Bug ID	Description
96219	**Symptom:** Issuing the **no phonehome smtp** command removed SMTP as the transport protocol but did not rollback to the default HTTPS mode. The fix ensures that PhoneHome rolled back to the default HTTPS mode. **Scenario:** This issue was observed when SMTP was deleted as the transport protocol. This issue was observed in controllers running ArubaOS 6.4 or later versions. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.0.
96901	**Symptom:** The auto-report of the PhoneHome statistics was displayed incorrectly in the output of the **show phonehome stats** command though the report was sent successfully. This issue is resolved by incrementing the auto-report count even if the report sent is a duplicate. **Scenario:** This issue occurred when auto-report was triggered from support mode. This issue was observed in controllers running ArubaOS 6.4.0.1. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.1.

PPTP

Table 52: *PPTP Fixed Issues*

Bug ID	Description
107265 113011	**Symptom:** Server-Derived Rules (SDR) failed to work for Point-to-Point Tunneling Protocol (PPTP) clients. The fix ensures that the server-group is referenced correctly for L3 users performing SDR. **Scenario:** This issue was observed when SDR was configured for VPN clients using PPTP. This issue was observed in controllers running ArubaOS 6.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.

Radius

Table 53: *Radius Fixed Issues*

Bug ID	Description
93689	**Symptom:** When clients executed a script on their windows phone for 802.1X authentication, the controller sent an **EAP Failure** message. This issue is resolved by removing the EAP-Failure messages when the client timed out during 802.1X authentication. **Scenario:** This issue was not limited to any specific controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.1.3.8.
94086	**Symptom:** User-Name (attribute value pairs) in the radius accounting packets contained FQDN/domain name although the **trim-fqdn** was enabled. This issue is resolved by trimming the FQDN/domain name when composing the radius accounting packet. **Scenario:** This issue was observed when the radius interim accounting and trim-fqdn was enabled. This issue was not limited to any specific controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.1.1.1.
110230	**Symptom:** The **Class Identifier** attribute was not present in the RADIUS accounting messages sent from a controller to the RADIUS accounting server. This issue is resolved by copying the appropriate authserver for the user, from the key cache. **Scenario:** This issue was observed during 802.1X authentication. This issue was observed in 7210 controllers running ArubaOS 6.4.1.0. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.1.0.
110970	**Symptom:** A controller sent accounting requests with Unknown in Location-ID field and N/A in Group field. This issue is resolved by caching the ap-name and ap-group. **Scenario:** This issue occurred when an access point rebooted. This issue was observed in controllers running 6.4.2.2 but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2

Remote AP

Table 54: *Remote AP Fixed Issues*

Bug ID	Description
102205	**Symptom:** Sierra U320 modem was not functional. This issue is resolved by configuring the **ap provisioning-profile**, with the following values: • **usb-type** - sierrausbnet • **usb-dev** - 0x11990fff • **usb-init** - AT+CGDCONT=1,'IP','telstra.internet' • **usb-tty** - ttyUSB2 **Scenario:** This issue was observed in RAP-155 running ArubaOS 6.3.1.6. **Platform:** RAP-155. **Reported Version:** ArubaOS 6.3.1.6.
103995	**Symptom:** When an user executed the **show datapath bridge ap-name** command it returned multiple entries that were similar and displayed a **Not enough memory to complete** error message. This issue is resolved by ensuring an entry is not added twice in the AP bridge table. **Scenario:** This issue occured only when access points were configured as RAPs with Point-to-Point Protocol over Ethernet (PPPoE) enabled. This issue was not limited to any controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.6.
107527	**Symptom:** A wired bridge user was mapped with incorrect ACLs even though the wired bridge user was mapped with correct user role. This issue is resolved by overloading the ingress field with wired port and fetching the correct AAA profile. **Scenario:** This issue was observed in remote APs connected to controllers running ArubaOS 6.3.1.8. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.8.

SNMP

Table 55: *SNMP Fixed Issues*

Bug ID	Description
91537	**Symptom:** AirWave displayed the status of a controller as DOWN due to SNMP request timeouts. This issue is resolved by reducing the SNMP timeout value for the **STM** and **WMS** processes which prevents an increase in the wait time of the SNMP queue. **Scenario:** The SNMP request time out was caused because there was an increase in the SNMP request queue from AirWave, while the **SNMPD** process waited for a response from the **WMS**/**STM** process that was busy. **Platform:** All platforms. **Reported Version:** ArubaOS 6.2.1.4.
112681	**Symptom:** SNMP trap was not sent to servers which had IP address, x.42.x.x. This issue is resolved by changing the behavior of the IPv6 address look up. **Scenario:** This issue was observed in controllers configured to send SNMP trap to hosts with 42 in the IP address. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.
111767	**Symptom:** SNMP configuration errors like **Configuration error: Only support physical Interface 24577 in snmpGetIfEthTable, snmp_switch.c:591** were logged. This issue is resolved by disabling debug log. **Scenario:** This issue occurred when SNMP debug was enabled using the **logging level warnings system subcat snmp** command or when an SNMP walk was performed. This issue was observed in controllers running ArubaOS 6.3.1.0, but was not specific to any controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.0.
111813	**Symptom:** SNMP **walk** and **get** stopped working. This issue is resolved by making sure that socket flags are correct when **snmp-server source controller-ip** is disabled in a controller. **Scenario:** This issue was observed when IPv6 was disabled and when the **snmp-server source controller-ip** command was executed to enable/disable the SNMP server, which triggered socket flags to fail. **Platform:** All platforms. **Reported Version:** ArubaOS 6.1.3.7.

Station Management

Table 56: *Station Management Fixed Issues*

Bug ID	Description
95648	**Symptom:** When the clients associated to an AP exceeded the maximum number of clients allowed, the log file displayed a message - **AP is resource constrained**, which was applicable to other scenarios as well. This issue is resolved by adding a new message - **AP is resource constrained-Max Clients associated** in the log file. **Scenario:** This issue was observed when multiple scenarios shared the same error code. **Platform:** All platforms. **Reported Version:** ArubaOS 6.1.1.1.
102035	**Symptom:** STM crashed in a local controller. This issue is resolved by adding sanity checks to STA number. **Scenario:** This issue occurred in 7210 controllers in the master-standby topology when a corrupt or malformed packet had wrong STA number and the STM used the number directly without checking upper boundary. **Platform:** All platforms. **Reported Version:** ArubaOS 6.2.1.0.
102144	**Symptom:** Active APs of a local controller were not displayed on the master controller. This issue is resolved by introducing a new action to handle this race condition. **Scenario:** This issue was triggered by a race condition which resulted in creating session entries before IPsec tunnel and Network Address Translation (NAT) rules were created. The session removal mechanism did not remove the session entries without NAT flags. This issue was observed in controllers running ArubaOS 6.2.1.x or later. **Platform:** All platforms. **Reported Version:** ArubaOS 6.2.1.0.
107998	**Symptom:** When an SNMP walk was performed, a standalone master controller returned an incorrect value for the number of clients associated per ESSID. This issue is resolved by correcting the client count calculation for SNMP. **Scenario:** This issue was observed in 7240 controllers running ArubaOS 6.4.1.0. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.1.0
112850	**Symptom:** The STM module in a controller crashed when the ap-lacp-profile was modified. The fix ensures that the STM does not crash when the ap-lacp-profile is modified. **Scenario:** This issue occurred when the STM tried to apply a modified ap-lacp-profile to non-functional access points. Non-functional access points have a duplicate name, do not belong to a group, do not have a license, or so on. This issue occurred in non-functional AP-200 Series access points connected to controllers running ArubaOS 6.4.2.3. **Platform:** AP-220 Series access points. **Reported Version:** ArubaOS 6.4.2.3.

TACACS

Table 57: *TACACS Fixed Issues*

Bug ID	Description
100762	**Symptom:** A user cannot delete a TACACS server group that is referenced but was taken out of the **AAA** profile. The fix ensures that the reference to the old server group is decremented. **Scenario:** This issue was observed in M3 controllers running ArubaOS 6.1.3.9. **Platform:** All platforms. **Reported Version:** ArubaOS 6.1.3.9.
105653	**Symptom:** The management authentication did not work when it was configured with TACACS server. This issue was resolved by resetting the file descriptor. **Scenario:** This issue occurred when there was a delay in response from TACACS server due to network congestion. This issue was not specific to any controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:**ArubaOS 6.3.1.5

Voice

Table 58: *Voice Fixed Issues*

Bug ID	Description
90888	**Symptom:** The **show voice real-time-analysis** command failed to display any result for voice calls between Microsoft® Lync clients. The fix ensures that the controller displays Real-time Transport Analysis (RTPA) report. **Scenario:** This issue was observed when Microsoft Lync clients were connected to the same Remote AP (RAP) in split-tunnel forwarding mode. In such cases, the voice packets were locally routed through the RAP without forwarding it to the controller. As a result, the controller failed to display any RTPA report. This issue was observed in controllers running ArubaOS 6.4. **Platform:** All platforms. **Reported Version**: ArubaOS 6.4.
94546 94641	**Symptom:** The CDR for NOE phones was in an **ALERTING** state when a call was disconnected by the caller before it was accepted. The fix ensures that the CDR is terminated when the **RING_OFF** event is triggered in for New Office Environment (NOE) Application Layer gateway (ALG). **Scenario:** This issue occurred when an NOE call was received by a wireless client connected to the controller from a wired client outside the controller. This issue was observed in controllers running ArubaOS 6.1 or later versions. **Platform:** All platforms. **Reported Version:** ArubaOS 6.1.

VRRP

Table 59: *VRRP Fixed Issues*

Bug ID	Description
109845	**Symptom:** After upgrading a controller to ArubaOS 6.4.2.2, the VRRP routed through L2 GRE tunnel for non-routable VLAN was in backup state. This fix ensures that the status of the tunnel is retrieved before proceeding with lookup for master transition when the tunnel is UP. If **operstate** of the VRRP VLAN is UP and the tunnel state is DOWN, the VRRP routed through tunnel will fail-over to master in 120 seconds. **Scenario:** This issue was observed when VRRP instances in the tunneled VLANs was in backup state and was not being handled while receiving the link status of the VLAN. This issue was observed in 650 and 7210 controllers running ArubaOS 6.4.2.2. **Platform:** 650 and 7210 controllers. **Reported Version:** ArubaOS 6.4.2.2.

WebCC

Table 60: *WebCC Fixed Issues*

Bug ID	Description
104189	**Symptom:** The WebCC process in the controller crashed randomly. The fix ensures that the WebCC process does not crash when enabling and disabling repeatedly in quick succession. **Scenario:** This issue was observed when enabling and disabling the WebCC feature repeatedly in quick succession. This issue was observed on 7000 Series and 7200 Series controllers running ArubaOS 6.4.2.x or later. **Platform:** 7000 Series and 7200 Series controllers. **Reported Version:** ArubaOS 6.4.2.0.
104650	**Symptom:** When the **clear web-cc stats** command was executed, the **DB entries** field was cleared. The fix ensures that the **DB entries** field is not cleared when the command is executed. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.0.
104772	**Symptom:** Bandwidth contract was not applied when an URL belonged to multiple categories and a matching WebCC Advance Classification Engine (ACE) did not exist. This issue is resolved by enforcing a WebCC category based on bandwidth contracts for traffic that mapped to multiple categories. **Scenario:** This issue was observed on 7000 Series and 7200 Series controllers running ArubaOS 6.4.2.x or later. **Platform:** 7000 Series and 7200 Series controllers. **Reported Version:** ArubaOS 6.4.2.0.

WebUI

Table 61: *WebUI Fixed Issues*

Bug ID	Description
76432	**Symptom**: In the **Client detail** page, the trend was not displayed for **Frame Rates To Client** or **Frame Rates From Client**. This issue is resolved by implementing internal code changes. **Scenario**: This issue was not limited to a specific controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.2.0.0.
90915	**Symptom:** A spectrum analysis recording did not display the correct channels in the swept spectrogram chart when that recording was played back using the RFPlayback Tool. This issue is resolved by using the correct color value for the unavailable data. **Scenario:** This issue occurred when the RFPlayback tool played a spectrum analysis recording created by a 3000 Series controller running ArubaOS 6.1.3.6. **Platform:** All platforms. **Reported Version:** ArubaOS 6.1.3.6.
95610 100668 104486	**Symptom:** When a client was in bridge mode, the IP address of the bridge was not displayed on the dashboard. To resolve this issue, the STM notifies the IP address of the bridge to AMON and user device after receiving it from the authentication manager in the GSM mac_user channel. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.3, but was not specific to any controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.
97281	**Symptom:** Users were unable to configure the extended ACLs using the WebUI. This issue is resolved by removing the PEF license for extended ACLs, which restricted users from configuring the ACL. **Scenario:** This issue was observed when PEF license was not installed. This issue was not limited to any specific controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.3.
97789	**Symptom:** Controllers running ArubaOS 6.4 or later versions failed to copy an ArubaOS image using Windows TFTP and displayed an error message **Error determining new default boot partition version**. The fix ensures that the ArubaOS image copies successfully using Windows TFTP. **Scenario:** This issue occurred when copying an ArubaOS image to the non-boot partition of a controller using Windows TFTP. This issue occurred in controllers running ArubaOS 6.4 or later versions, but was limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.0.
101390	**Symptom:** A user was not able to copy files to a USB drive that was connected to the slot 1 of a controller by using the WebUI. This issue is resolved by changing the validation condition of partition of the USB drive. **Scenario:** This issue was observed in 7010 controllers running ArubaOS 6.4.1.0. A 7010 controller has two USB slots. **Platform:** 7010 controller. **Reported Version:** ArubaOS 6.4.1.0.
103187	**Symptom:** Capital letters were not accepted in the **E-mail address** field of GPP page. A user was unable to create a guest user through GPP login by using capital letters in email address. This issue is resolved by allowing capital letters in email address. **Scenario:** This issue occurred in controllers running ArubaOS 6.2.1.4, but was not limited to any specific controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.2.1.4.

Table 61: *WebUI Fixed Issues*

Bug ID	Description
111348	**Symptom:** The banner does not appear correctly in the WebUI of a controller. The fix ensures that a controller displays the banner correctly. **Scenario:** This issue occurred when quotation marks were used for banner alignment in the CLI. This issue was not limited to a specific controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.1.0.
112333	**Symptom:** When uploading the VIA installer file on a controller, the error message **Error uploading VIA installer. Not enough free space** was displayed. With the fix, the VIA installer installs successfully. **Scenario:** This issue occurred even if there was sufficient disk space in a controller. This issue was observed in 7030 controllers running ArubaOS 6.4.2.4. **Reported Version:** ArubaOS 6.4.2.4.
112631	**Symptom:** When creating a guest user account with a phone number that is less than 10 digits, a controller displayed validation error and the CLI did not validate the phone number. This issue is resolved by removing the digit limitation of a phone number and allowing phone numbers with any number of digits. **Scenario:** This issue occurred in controllers running ArubaOS 6.3.1.9, but was not specific to any controller model. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.9.

Resolved Issues in ArubaOS 6.4.2.5

The following issues are resolved in ArubaOS 6.4.2.5.

AirGroup

Table 62: *AirGroup Fixed Issues*

Bug ID	Description
109808	**Symptom:** When a query was initially executed or refreshed, mDNS used the IP as the source IP and as a result some servers were not discovered. This issue is resolved by using the VLAN IP as the source IP for mDNS queries. **Scenario:** This issue was observed in 7200 controllers running ArubaOS 6.3.1.13. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.13.
112905 113652 113577 113084 113663 113515	**Symptom:**Controller rebooted due to memory leak in the **mDNS** process. This issue is resolved by making code level changes to appropriately handle the AirGroup timers. **Scenario:** This issue was observed due to the error in AirGourp timer settings. This issue was observed in 7240 controllers running ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:**ArubaOS 6.4.2.4.

AP-Datapath

Table 63: *AP-Datapath Fixed Issues*

Bug ID	Description
103230	**Symptom:** An AP crashed when a client associated a BSS which had an ACL with domain SA or DA. This issue is resolved by making internal code changes to fix the byte-order issue in AP-205. **Scenario:** This issue was observed in AP-205 access points connected to 3600controllers running ArubaOS 6.4.1.10. **Platform:**AP-205 access points. **Reported Version:**ArubaOS 6.4.1.0.
111273	**Symptom:** Clients connected to AP-215 access points were unable to pass traffic in the bridge mode. This issue is resolved by implementing internal code changes. **Scenario:** This issue was seen for clients in authenticated role. This issue was observed after upgrading the AP-215 access point from ArubaOS 6.3.x to ArubaOS 6.4.2.2. **Platform:** AP-215 access point. **Reported Version:**ArubaOS 6.4.2.2.

AP-Platform

Table 64: *AP-Platform Fixed Issues*

Bug ID	Description
106364	**Symptom:**AP-124 rebooted randomly. The log files listed the reason for the reboot as **PCI ERROR [MR_WABT]: PCI master abort detected on write**. This issue is resolved by making internal code changes. **Scenario:** This issue was observed in AP-124 access points when connected to a controller as a campus AP or to a mesh network. This issue was observed in M3controllers running ArubaOS 6.3.1.5. **Platform:**M3controller. **Reported Version:**ArubaOS 6.3.1.3.
107806	**Symptom:** Some Gratuitous ARP (GARP) packets from a client, that was associated with a bridge forwarding mode SSID, had an incorrect VLAN ID. This issue is resolved by sending the GARP packets with the correct VLAN ID when the client successfully associates with a bridge forwarding mode SSID. **Scenario:** This issue occurred in 7210controllers running ArubaOS 6.2.1.7. **Platform:** 7210controller. **Reported Version:** ArubaOS 6.2.1.7.
106472 111504 112382	**Symptom:**AP-110 Series access points rebooted unexpectedly. This issue is resolved by setting valid limits for radio calibration data. **Scenario:** This issue occurred when the radio calibration data was set incorrectly. This issue was observed in AP-110 Series access points connected to controllers running ArubaOS 6.3.x. **Platform:** AP-110 Series access points. **Reported Version:** ArubaOS 6.3.x.0.
108013	**Symptom:**AP-125 access points are not able to get an IPv6 address through Stateless Address Auto Configuration (SLAAC) when M bit is enabled on the IPv6 router. The fix ensures that AP-125 access points ignore the M flag. **Scenario:** This issue is observed in networks where AP-125 access points are deployed, and the M bit is enabled on IPv6 router. The M bit is enabled to obtain an IPv6 address from DHCPv6, but AP-125 access points do not support DHCPv6. **Platform:**AP-125 access points. **Reported Version:** ArubaOS 6.4.2.5.

Table 64: *AP-Platform Fixed Issues*

Bug ID	Description
108299 108352 113793	**Symptom:** Wireless clients failed to connect to a remote AP after an AP failover. The **show auth-tracebuf** command displayed the following event: **received eapol-pkt before assos**. This issue is resolved by updating the tunnel IP of the virtual APs in **always** or **persistent** mode with the correct local management switch (LMS) IP. **Scenario:** This issue occurred due to AP failover in a master local setup when LMS was configured and at least one virtual AP was configured with **rap-operation** parameter set to **always** or **persistent**. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.0.
109542	**Symptom:** The access point rebooted multiple times due to Station Management (STM) module crash. This issue is resolved by parsing AIE (ARUBA STM IE) first when processing association and re-association requests. **Scenario:** This issue was observed when the client sent malformed association request to STM. This issue was observed in AP-220 Series access point running ArubaOS 6.4.1.0. **Platform:**AP-200 Series access points. **Reported Version:** ArubaOS 6.4.1.0.
110095	**Symptom:** An AP did not renew its DHCP lease when the old DHCP server was out of service. This issue is resolved by updating the DHCP server IP in the DHCP acknowledgment packet. **Scenario:** This issue was observed when an AP sent a DHCP renewal message to the old DHCP server even when it was not present in the network. This issue was observed in APs connected to controllers running ArubaOS 6.3.1.x. **Platform:** 3600 controller. **Reported Version:** ArubaOS 6.3.1.x.
110157	**Symptom:** The **show ap radio-database** command did not display the E flag for 802.11ac channel bonding. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.x and 6.4.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2.
111261	**Symptom:** AP-114/AP-115 sent a pause frame when the ingress packet-flow was high. This issue is resolved by disabling L2 flow control on AP-114/AP-115. **Scenario:** This issue occurred on AP-114/AP-115 access points connected to 7220 controllers running ArubaOS 6.3.1.17. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.7.
112781	**Symptom:** An AP-205 access point rebootstrapped and periodically displayed the **RC_ERROR_IKEP2_PKT1** error in the event logs. This issue is resolved by modifying the IPSec tunnel state machine on the AP. **Scenario:** This issue was observed when HA was enabled on the AP-205 and the AP moved to an incorrect state. **Platform:**AP-205 access point. **Reported Version:** ArubaOS 6.4.2.2.

AP-Wireless

Table 65: *AP-Wireless Fixed Issues*

Bug ID	Description
100425 104516 113890 113891 114126	**Symptom:** Traffic was stopped for a few seconds and then resumed by an access point with the error message **Kernel Panic: Fatal exception Badness at net/sched/sch_generic.c:269**. Sometimes, the access point rebooted. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in AP-215/AP-225 access points connected to 7210 controllers running ArubaOS 6.4.1.0. **Platform:** AP-215/AP-225 **Reported Version:** ArubaOS 6.4.1.0.
103421	**Symptom:** An AP crashed and rebooted. The log files listed the reason for the reboot as **ar7240 data bus error: cause 0x50808008**. This issue is resolved by making code level changes in the wireless driver. **Scenario:** This issue was observed in AP-68P access points connected to controllers running ArubaOS 6.3.1.2. **Platform:** AP-68P access point. **Reported Version:** ArubaOS 6.3.1.2.
108810	**Symptom:** Multicast rate optimization did not work per VAP. This issue is resolved by making multicast rate optimization work per VAP. **Scenario:** This issue occurred in AP-200 Series access points connected to controllers running ArubaOS 6.3. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.1.0
109856	**Symptom:** Clients connected to bridge mode SSID could not send traffic randomly. This issue occurred because the group key from the AP station management was assigned to the wireless driver and the wireless driver cleared the TX PN of the key when ARM changed the Tx power. This issue is resolved by ignoring the same group key request in the wireless driver. **Scenario:** This issue was observed in AP-135 access points connected to 650 controllers running ArubaOS 6.4.2.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2
110481	**Symptom:** Sometimes, an AP-225 access point buffered packets for too long. A driver update in the AP has resolved this issue. **Scenario:** This issue occurred when the AP buffered packets for an 802.11b client. The issue was found in APs running ArubaOS 6.4.2.0. **Platform:** All platforms. **Reported Version:**ArubaOS 6.4.2.0.
111019	**Symptom:** Broadcom based access points did not reset client idle time to zero on null data packets. The fix ensures that the idle time is reset on receiving null/qos-null data packets. **Scenario:** This issue was observed in AP-225 access points connected to 650controllers running ArubaOS 6.4.2.3. **Platform:** AP-225 access point. **Reported Version:**ArubaOS 6.4.2.3.
111381	**Symptom:** Bridge mode clients did not send traffic until the AP-103 access point was rebooted. This issue is resolved by updating the key that exists in the cache. **Scenario:** This issue was observed in AP-103 access points connected to 7210controllers running ArubaOS 6.4.1.0. **Platform:** AP-103 access point. **Reported Version:**ArubaOS 6.4.1.0.

Table 65: *AP-Wireless Fixed Issues*

Bug ID	Description
111854	**Symptom:** AP-125 sent many Block Acknowledge Retry (BAR) requests to the client because it did not receive Block Acknowledge (BA) from the client. This issue is resolved by reducing the retry counts per BAR frames. **Scenario:** This issue was observed in clients when the **Allow the computer to turn off this device to save power** NIC power management option was enabled. This issue was observed in AP-125/AP-105 connected to controllers running ArubaOS 6.3.1.9. **Platform:**AP-125 and AP-105 access points. **Reported Version:**ArubaOS 6.3.1.9.
111913	**Symptom:** Clients frequently lost connectivity to AP-105 access point because the AP detected a false RADAR and moved to another channel. The fix ensures that a RADAR chirp detection support is added for AP-105, to avoid false RADAR detection. **Scenario:** This issue was observed in AP-105 operating in DFS channel. This issue was observed in AP-104, AP-105, AP-92, and AP-93 access points connected to M3 controllers running ArubaOS 6.1.3.11. **Platform:** AP-104, AP-105, AP-92, and AP-93 access points. **Reported Version:** ArubaOS 6.1.3.11.
112960	**Symptom:** Clients had issues when sending traffic because of sequence number mismatch between the AP and the client. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when the MPDU aggregation was enabled. This issue is not specific to any controller or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.
113381 113974	**Symptom:** Wireless clients experienced connectivity loss when they associated with 802.11ac-capable access points. The fix ensures that there is no connectivity loss when associated with 802.11ac-capable access points. **Scenario:** Some packets in 802.11ac-capable access points have callbacks associated with them. These callbacks help in clearing node memory after de-authentication. This issue was observed when the callback entries failed to clear from the callback table of the AP. This issue was seen on all 802.11ac-capable access points running ArubaOS 6.4.2.3. **Platform:** AP-200 Series, AP-210 Series, AP-220 Series, and AP-270 Series access points. **Reported Version:**ArubaOS 6.4.2.3.

ARM

Table 66: *ARM Fixed Issues*

Bug ID	Description
111543	**Symptom:** Adaptive Radio Management (ARM) failed to work for Egypt country domain. Changes in the internal code ensures that ARM works correctly for Egypt country domain. **Scenario:** This issue was seen when 40 MHz assignment is enabled in ARM profile. This issue was observed in 802.11n and 802.11ac-capable access points running ArubaOS 6.3.1.14. **Platform:** 802.11n and 802.11ac-capable access points. **Reported Version:**ArubaOS 6.3.1.14.
111603	**Symptom:** ARM error log **ARM Process| Unexpected (arm process) runtime error at dot11v_btm_req_cb, 75, Unable to find STA** occurred for 802.11v capable clients. This issue is resolved by changing the message severity level to debugging. **Scenario:** This issue occurred for 802.11v capable clients when the clients did not respond to 802.11v BTM request and leave the network. **Platform:** All platforms. **Reported Version:**ArubaOS 6.4.2.3.

Base OS Security

Table 67: *Base OS Security Fixed Issues*

Bug ID	Description
109918	**Symptom:** Users were unable to add ACL rules with the netservice **web** after they upgraded from ArubaOS 6.4.2.1 to 6.4.2.2. The fix ensures that after an upgrade, the netservice **web** is automatically renamed to **svc-web** in all the ACL rules using the service **web**. **Scenario:** This issue occurred when the netservice **web** was renamed to **svc-web** in ArubaOS 6.4.2.2. **Platform:** 7210 controller. **Reported Version:**ArubaOS 6.4.2.2.
103227 103355	**Symptom:** The **ssh mgmt-auth public-key** parameter was disabled on the master controller but was not synchronized on the local controller when the value in the **cfg sync-type** command was set as **complete**. This issue is resolved by including the **no ssh mgmt-auth public-key** parameter in the running-config when the **ssh mgmt-auth public-key** parameter is disabled. **Scenario:** This issue occurred in a master-local setup due to the absence of a trigger on the local controller to delete **ssh mgmt-auth public-key**. This issue was not limited to any specific controller or ArubaOS version. **Platform:** 7220 controller. **Reported Version:** ArubaOS 6.3.1.7.
111030	**Symptom:** A controller classified a Microsoft® Lumia Windows 8.1 mobile phone as Android in the user table. The fix ensures that the device is classified as Windows Phone. **Scenario:** This issue was observed in 7210 controllers running ArubaOS 6.3.x or 6.4.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2.

Captive Portal

Table 68: *Captive Portal Fixed Issues*

Bug ID	Description
107681 109842	**Symptom:** There was a delay in displaying the Captive Portal login page or Captive Portal authentication page for wireless clients. This issue occurred because of high CPU utilization when the number of entries in the AAA device id cache exceeded twice the maximum number of users. This issue is resolved by disabling devtype classification in the AAA profile. **Scenario:** This issue occurred when wireless clients were connected in split-tunnel mode with device classification enabled. This issue occurred in AP-93 access points connected to 7220 controllers running ArubaOS 6.3.1.8. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.8.

Configuration

Table 69: *Configuration Fixed Issues*

Bug ID	Description
106791	**Symptom:** A RADIUS key was not synchronized with the standby controller. This issue is resolved by making changes to the key values in the RADIUS profile to accept a string length of more than 256 characters. **Scenario:** This issue occured if the clear text key length was 110 characters, whereas the encrypted length was more than 256 characters. This issue is observed in standby controllers in a master-standby topology running ArubaOS 6.3.1.8. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.8.

Controller-Datapath

Table 70: *Controller-Datapath Fixed Issues*

Bug ID	Description
102315	**Symptom:** When packets were reordered, the first fragment was received last, but all the fragments were sent out. As a result, the fragment context could not be released resulting in very low download speed over site-to-site VPN.This issue is resolved by deleting the fragment context immediately instead of them going through the aging process. **Scenario:** This issue was observed in a WAN between master and local controllers. This issue was observed in all controllers running ArubaOS 6.2.x version onwards. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.7.
108007	**Symptom:** An AP was not able to connect to a master controller. The fix ensures that the PAPI packet reassembly is handled correctly. **Scenario:** This issue was observed when AP-225 tried to connect to a 3600controller running ArubaOS 6.3.1.9. This issue is observed in a topology where the AP and the master controller are in different locations and are connected through IPsec tunnel. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.9.
108398	**Symptom:** Gratuitous ARP packets were flooded in the wifi tunnel. This issue is resolved by making code level changes to the dhcp router entries in the datapath. **Scenario:** This issue is observed in 7240controllers running ArubaOS 6.4.0.2. **Platform:** 7240controllers. **Reported Version:** ArubaOS 6.4.0.2.
110705	**Symptom:** The controller stopped responding and rebooted unexpectedly. The log files for the event listed the reason as **datapath exception**. This issue is resolved by implementing internal code changes. **Scenario:** This issue occurred when a Point-to-Point Tunneling Protocol (PPTP) client connected and passed traffic through the PPTP tunnel. This issue was observed on 7220 and 7240controllers running ArubaOS 6.3.1.12 or 6.3.1.13. **Platform:** 7220 and 7240controllers. **Reported Version:** ArubaOS 6.3.1.13.

Controller-Platform

Table 71: *Controller-Platform Fixed Issues*

Bug ID	Description
104139 104729 107907 108026 108194 109894 109896 109897 109898 110158 112021 112023	**Symptom:** WMS and database modules rebooted unexpectedly. This issue is resolved by implementing internal code changes. **Scenario**: This issue was observed in all controllers running ArubaOS 6.3.x and later versions. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.6.
108690	**Symptom:** On rebooting the controller, static routes were deleted from the controller. This issue was resolved by saving the system generated configuration file correctly for the **interface tunnel** command. **Scenario**: This issue was seen when the controller had IPv4 GRE tunnels configured and the system generated a **config.cfg** file in which an incorrect syntax for the **interface tunnel** command was executed. This issue was observed in controllers running ArubaOS 6.4.2.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.
112959	**Symptom:** A controller rebooted with the reboot cause **Nanny rebooted machine - low on free memory**. Internal code changes are implemented to free the allocated memory of refresh query packet after sending it out. **Scenario**: This issue was not limited to any specific controller model and was observed in ArubaOS 6.4.0.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4.

CPSec-Whitelist Management

Table 72: *CPSec-Whitelist Management Fixed Issues*

Bug ID	Description
103909	**Symptom:** An AP was not listed in the AP database. Database synchronization or modification also failed to list the AP. This issue is resolved by adding validation code in the database synchronization mechanism to validate each entry before sending the synchronization response. This change ensures that rest of the synchronization does not fail because of an entry, and a corrupt entry is not synchronized to the other controllers. **Scenario**: This issue occurred due to invalid entries in the AP whitelist database or any corruption in the database entry. Invalid or corrupt entries were populated in the AP whitelist database when the master controller code was drastically different from the local controller code. This issue was observed on controllers running ArubaOS 6.3.x and 6.4.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.1.0.

IPsec

Table 73: *IPsec Fixed Issues*

Bug ID	Description
105112 109796	**Symptom:** The management protocol [IKE] in the VPN module crashed when revocation check of certificates was performed multiple times. This issue is resolved by ensuring that the exchange element in IKE is set to NULL for all the corresponding requests of that exchange, when exchange is freed. **Scenario:** This issue was observed when the exchange element was set to NULL for only one of the multiple requests, when exchange was freed. This issue was not limited to a specific model or release version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.8.
111100	**Symptom:**ArubaOS did not support uplink failover within a site-to-site tunnel prior to ArubaOS 6.3.1.15. This issue is resolved by implementing changes that improve the way old IKEv2/IPsec security association (SA) states are deleted before a new SA is established. **Scenario:** This issue occured in controllers using IKEv2-PSK SA authentication methods for site-to-site VPNs. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.14.

IPv6

Table 74: *IPv6 Fixed Issues*

Bug ID	Description
112636	**Symptom:** The customer was unable to get an IP address using the IPv6 Neighbor Discovery (ND) protocol or Router Advertisement (RA) when the **Broadcast-filter ARP** parameter was enabled. To resolve this issue a check is introduced to observe if the MAC address obtained after unicast conversion is similar to the source MAC of the packet. If it is, then the packet is not sent to the tunnel or as multicast, depending on whether **Suppress ARP** parameter is enabled on the vlan. **Scenario:** This issue was observed when the M3controller was upgraded from ArubaOS 6.3.1.6 to 6.3.1.14. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.14.

Mobility

Table 75: *Mobility Fixed Issues*

Bug ID	Description
108282	**Symptom:** Clients were not categorized under the correct VLAN even though: • L3 mobility feature is enabled • **no ip mobile proxy auth-sta-roam-only** parameter is configured • anchor table is configured in the mobility domain This issue is resolved by performing a vlan look-up from anchor table when **no ip mobile proxy auth-sta-roam-only** is configured. **Scenario:** This issue was observed in mobility controllers running ArubaOS 6.3 and 6.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.1.0.

Radius

Table 76: *Radius Fixed Issues*

Bug ID	Description
107322 108890 112153	**Symptom:** Radius requests were directly sent to the last authentication server in an authentication server-group if the previous attempt to authenticate the client failed on each authentication server once. This issue is resolved by clearing the saved authentication server names if the authentication fails against all authentication servers. **Scenario:** This issue occurred on 7210controllers running ArubaOS 6.4.2.0. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.0.

Remote AP

Table 77: *Remote AP Fixed Issues*

Bug ID	Description
104073	**Symptom:** The user could not reconnect to the 3G up-link sites after upgrading from ArubaOS 5.x to 6.x. The fix ensures that the Sierra driver on the IAP is updated to maintain compatibility. **Scenario:** This issue was observed in RAP-5s connected to M3controllers running ArubaOS 6.3.1.8. **Platform:** M3controller. **Reported Version:**ArubaOS 6.3.1.8.
109380	**Symptom:** When the **show ap debug usb ap-name <ap name>** was executed on a RAP the output did not display Supported Network Services, Firmware Version, and ESN Number. The fix ensures that these values are displayed when the **show ap debug usb ap-name <ap name>** is executed. **Scenario:** This issue was observed in UML-295 modems connected to RAP-5WN/RAP-155 running ArubaOS 6.3.1.12. **Platform:** RAPs supporting UML-295 modems. **Reported Version:**ArubaOS 6.3.1.12.

Station Management

Table 78: *Station Management Fixed Issues*

Bug ID	Description
112713	**Symptom:** APs rebootstrapped unexpectedly. The log files for the event listed the reason as **Bootstrap requested by STM**. Enhancement in the wireless driver ensures that the AP stops rebootstrapping. **Scenario:** This issue was observed when the AP was upgraded to ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:**ArubaOS 6.4.2.4.

Voice

Table 79: *Voice Fixed Issues*

Bug ID	Description
108539	**Symptom:** The UCM process crashed on the controller. Internal code changes ensures the UCM process does not crash on the controller. **Scenario:** This issue was seen for H.323 VoIP calls which had junk codec values for the UCM module to process this call. This issue was observed in controllers running ArubaOS 6.4.0.3-HDMSx2. **Platform:** All platforms. **Reported Version:**ArubaOS 6.4.0.3-HDMSx2.

VRRP

Table 80: *VRRP Fixed Issues*

Bug ID	Description
111451	**Symptom:** On adding the sixty-third VRRP instance on the controller, the WebUI and CLI got stuck showing the VRRP instance in an infinite loop. This issue is fixed by changing a software logical error. **Scenario:** This issue was seen because of a software logical error. This issue was seen in controllers running ArubaOS 6.3.1.x or 6.4.x. **Platform:** All platforms. **Reported Version:**ArubaOS 6.3.1.8.

Web Content Classification

Table 81: *Web Content Classification Fixed Issues*

Bug ID	Description
110873	**Symptom:** The Web Content Classification (WebCC) process on the controller stopped responding and crashed. The fix ensures that the controller does not crash even if there is a "**%**" string in the URL. **Scenario:** This issue was caused when the URL contained the "**%**" string. This issue is observed in 7220controllers running ArubaOS 6.4.2.3. **Platform:**7220controller. **Reported Version:**ArubaOS 6.4.2.3.

WebUI

Table 82: *WebUI Fixed Issues*

Bug ID	Description
102077 106193	**Symptom:** A **Script error in browser** message was displayed in the **Configuration > Networks > Port > Port-channel** page of the controller WebUI. This issue is resolved by making internal code changes. **Scenario:** This issue occurred when the controller did not have a PEF license. This issue was observed in 7200 Series controllers and is not limited to any ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3.
111971	**Symptom:** When a controller reloaded the destination alias and **sso-sacl** were not displayed. This issue is resolved by adding a DNS resolve request re-try per SSO URL every 20 seconds, if the resolution for that URL is not done. **Scenario:** This issue was observed in 7210 controllers running ArubaOS 6.4.2.3. **Platform:** 7210 controller. **Reported Version:** ArubaOS 6.4.2.3.

WMM

Table 83: *WMM Fixed Issues*

Bug ID	Description
111647	**Symptom:** The count of Tx WMM [VO] dropped packets increased without a voice client. The Tx WMM [VO] dropped packets count was determined from BAR frame Tx statistics. When a BAR frame was transmitted but a corresponding BA frame was not received from a client, the Tx WMM [VO] dropped packets count was incremented. This issue is resolved by: • counting only the data frames into Tx WMM [priority] dropped statistics if a frame transmission fails. • not counting the transmitting management or control frame into Tx WMM [VO] or Tx WMM [BE] statistics. **Scenario:** This issue occurred in AP-135 and AP-125 access points connected to controllers running ArubaOS 6.3.1.9. **Platform:**AP-135 and AP-125. **Reported Version:**ArubaOS 6.3.1.9.

Resolved Issues in ArubaOS 6.4.2.4

ArubaOS 6.4.2.4 is a software patch release that includes a fix for CVE-2015-1388. Additionally, the following issues are resolved in ArubaOS 6.4.2.4.

Advanced Monitoring

Table 84: *Advanced Monitoring (AMON) Fixed Issues*

Bug ID	Description
107631	**Symptom:** The controller displayed incorrect values for the **Health(%)**, **Speed**, and **Max Speed** parameters of a wireless client. The fix ensures that the controller displays the correct values. **Scenario:** This issue was observed in clients that associated with AP-200 Series access points running ArubaOS 6.4.2.0.

AirGroup

Table 85: *AirGroup Fixed Issues*

Bug ID	Description
102706 108029	**Symptom:** Loss of wired connectivity was observed for a short duration when the MAC address table was polluted on the L3 switch. This issue is resolved by ensuring that the source MAC address in the response packet and the MAC address of the controller that is sending the packet are identical. **Scenario:** This issue was observed in a controller–L3 switch–controller topology where both the controllers were in the same AirGroup domain. This issue was observed on controllers running ArubaOS 6.3.1.7.
108316	**Symptom:** When a refresh query is sent by the controller, a few printers did not respond with the complete set of records (SRV/A/AAAA/TXT). This issue is fixed by sending both the queries, qtype and qclass, with the value ANY. **Scenario:** This issue was observed when the controller sent an mDNS query with qtype value as PTR and qclass value as ANY, but some HP and Epson printers did not respond with all the records (SRV/A/AAAA/TXT). This issue was observed in controllers running ArubaOS 6.3.x versions.
111099	**Symptom:** False radar detects were observed on the 80 MHz channel during IPERF and multicast video streaming. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in AP-225 access points connected to 7210 controllers running ArubaOS 6.4.2.3.

AP Datapath

Table 86: *AP Datapath Fixed Issues*

Bug ID	Description
110566	**Symptom:** An FTP file download failed because the TCP connection was reset and clients were disconnected. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when a large file was simultaneously requested by the clients over FTP.

AP-Platform

Table 87: *AP-Platform Fixed Issues*

Bug ID	Description
109925	**Symptom:** A mesh point failed to establish a link with the mesh portal. Adding the **wpa-supplement** process resolved this issue. **Scenario:** This issue was observed in the 6.3.1.x FIPS version because it did not include the **wpa-supplement** process for mesh. This issue was observed in AP-85 connected to controllers running ArubaOS 6.3.1.1 - ArubaOS 6.3.1.13.

AP-Wireless

Table 88: *AP-Wireless Fixed Issues*

Bug ID	Description
109237	**Symptom:** AP-274 access point transmitted data at 1 Mbps rate although the SSID profile was not configured with 1 Mbps transmission rate. The fix ensures that the access point transmits data as per the SSID profile configuration. **Scenario:** This issue was observed in access points with the Broadcom chip-set running ArubaOS 6.4.2.2.

Authentication

Table 89: *Authentication Fixed Issues*

Bug ID	Description
96286	**Symptom:** The username was missing in RADIUS accounting **start** packets. This issue is resolved by avoiding the use of Pairwise Master Key (PMK) information saved in the user copy, in the absence of PMK cache. **Scenario:** This issue was observed when PMK information saved in the user copy was used to authenticate a client although the server did not have the client credentials. This issue was observed in controllers running ArubaOS 6.3.1.2 or later versions.

Base OS Security

Table 90: *Base OS Security Fixed Issues*

Bug ID	Description
107252	**Symptom:** A memory leak was observed in the **authentication** process of the controller. The fix ensures that there is no memory leak in the **authentication** process of the controller. **Scenario:** This issue was observed in the LDAP server keepalive/connection operation of the controller. This issue was observed in controllers running ArubaOS 6.3.1.5.
107953 108101 108752 109485 110354 110693	**Symptom:** The authentication process on a controller stopped responding and crashed. The log files for the event listed the reason as **auth module aborted**. This issue was resolved by making internal code changes to ensure that the freed memory is not used. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.2.2.
109038	**Symptom:** A local controller crashed on multiple modules and rebooted due to an authentication memory leak. The log files for the event listed the reason for the crash as **Nanny rebooted machine - fpapps process died**. This issue is resolved by implementing internal code changes to address the memory leak in the Authentication module. **Scenario:** This issue was observed in 7240 controllers deployed in a master local topology and running ArubaOS 6.4.2.0.
109982 109988	**Symptom:** The **extifmgr** process crashes while sending IF-MAP requests. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in 7000 Series, 3000 Series, and M3 controllers running ArubaOS 6.3.x and 6.4.x.

Configuration

Table 91: *Configuration Fixed Issues*

Bug ID	Description
108271	**Symptom:** When a controller was out of memory and the **write memory** command was executed , Layer 2/Layer 3 configurations were not captured. This resulted in network outage of controllers or APs. This issue is resolved by adding defense checks to prevent incomplete Layer 2/Layer 3 configurations when the **write memory** command is executed and the controller is low on memory. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.5 in a master local topology.

Control Plane Security Whitelist Management

Table 92: *Control Plane Security Whitelist Management Fixed Issues*

Bug ID	Description
107118	**Symptom:** The datapath route cache was corrupted because the IP address of a switch was assigned as the inner IP address of a RAP. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when RAPs terminated on controllers running ArubaOS 6.3.1.8.

Controller-Datapath

Table 93: *Controller-Datapath Fixed Issues*

Bug ID	Description
106870 107973 107974 109521 109919	**Symptom:** A controller stopped responding and rebooted. The log files for the event listed the reason as **datapath exception**. Changes in the datapath module code fixed this issue. **Scenario:** This issue was observed in 3600 controllers running ArubaOS 6.3.1.9.
108221	**Symptom:** The local controller stopped responding and rebooted. The log files for the event listed the reason as **datapath timeout**. Changes in the internal ArubaOS code fixed this issue. **Scenario:** This issue was observed in a large scale WLAN network where the number of users joining and leaving the network was high and per-user bandwidth contract was configured for a given role. This issue was seen on a master-local topology. This issue was observed in controllers running ArubaOS 6.4.2.0.

Controller-Platform

Table 94: *Controller-Platform Fixed Issues*

Bug ID	Description
106254	**Symptom:** The system log recorded multiple instances of a particular port reaching the maximum bridge entry limit. The fix ensures that the log file is updated with the correct port information sent from the datapath to the control plane. **Scenario:** This issue was observed when STP was enabled in the network. This issue was observed in M3 and 6000 Series controllers running ArubaOS 6.3.1.5.
108536 108794 108797 109386 110061 110072 110723 111313 111452 111557 111981 115410	**Symptom:** A 7200 Series controller rebooted unexpectedly. The log file for the event listed the reason as **Reboot Cause: kernel panic**. This issue is resolved with internal code changes. **Scenario**: This issue occurred when captive portal was enabled on the controller. This issue was observed on 7200 Series controllers running any version of ArubaOS.
109123 109414 111751	**Symptom:** A controller became unresponsive. The log files listed the reason for the event as **Halt reboot (Intent:cause:register 13:86:0)**. **Scenario:** This issue was observed in 3000 Series controllers running ArubaOS 6.3.1.13.
111549	**Symptom:** A local controller crashed and rebooted. The log files listed the reason for the crash as **Hard Watchdog reset**. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in XLP chipset with AP-105, AP-125, AP-135, and AP-115 access points connected to controllers running ArubaOS 6.4.2.3.

DHCP

Table 95: *DHCP Fixed Issues*

Bug ID	Description
107621 111499	**Symptom:** The DHCP packet forwarded by a controller had an incorrect BSSID value (zero) in option-82. Internal code changes avoided corruption in the BSSID value. **Scenario:** This issue was observed when option-82 was configured on a controller acting as a DHCP relay agent. This issue was observed in 7200 Series controllers running ArubaOS 6.4.2.2.

Guest Provisioning

Table 96: *Guest Provisioning Fixed Issues*

Bug ID	Description
107175	**Symptom:** Guest users failed to get an IP address from an external DHCP server. The fix ensures that guest users successfully get an IP address from the DHCP server. **Scenario:** This issue was seen under the following circumstances: • Guest provisioning users has **guest-access-email** enabled. • The **util_proc** process crashed on the controller. This issue was not limited to any specific controller model or ArubaOS release version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.9.

IPv6

Table 97: *IPv6 Fixed Issues*

Bug ID	Description
107993	**Symptom:** The controller flooded ICMPv6 Neighbor Solicitation (NS) packets to different VLANs. A Duplicate Address Detection (DAD) message was sent as a multicast packet instead of a unicast packet. The fix ensures that the controller sends a DAD message as a unicast packet: • if **broadcast-filter arp** is enabled, a DAD message is sent as a unicast packet to the station if the target address is already present in the user table. • if **supress-arp** is also enabled, a DAD message is not sent over the Wi-Fi tunnel if the address is not present in the user table. **Scenario:** This issue was observed when VLAN pooling was enabled for the VLAN and the DAD message was sent as a multicast packet over the Wi-Fi network. This issue was observed in controllers running ArubaOS 6.4.0.2.

Port-Channel

Table 98: *Port-Channel Fixed Issues*

Bug ID	Description
110563	**Symptom:** The Link Aggregation Control Protocol (LACP) timed out. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in M3 controllers connected to routers that use LACP over 1 Gigabit Ethernet links.

Remote AP

Table 99: *Remote AP Fixed Issues*

Bug ID	Description
107975	**Symptom:** RAP-155 did not reboot after failing over from Ethernet to a cellular link connected to Huawei® K4505 modem. This issue is resolved by making code level changes to the USB initialization script. **Scenario:** This issue was observed in RAP-155 when a USB-mode switch failed while disconnecting storage devices. This issue was observed in 7210 controllers running ArubaOS 6.3.1.10.
108770	**Symptom:** In a master local topology, when the IAP master failover occurred, the new GRE tunnel was deleted. This issue is resolved by deleting the branch with the old IP, before the branch with the same VC key creates a GRE tunnel. **Scenario:** This issue was observed when IAP established a VPN tunnel and registered to the controller with the same VC key and a different inner IP, for the same branch.

Station Management

Table 100: *Station Management Fixed Issues*

Bug ID	Description
105294 111346 111955 112262 114518	**Symptom:** Clients were continually de-authenticated with the message, **Denied: AP Ageout** until the AP was rebooted. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in ArubaOS 6.4.2.3 with HA enabled but was not limited to a specific controller model or AP.
107737	**Symptom:** Multiple error messages like **sta non-NULL for aid:12(LE:0xdc0) mismatched-MAC** occurred in access points. This issue is fixed by changing the level of the log messages to debug log-level. **Scenario:** This issue was observed in 7240 controllers running ArubaOS 6.4.2.0.
109619	**Symptom:** Clients were unable to associate with an AP and the log files for the event listed the reason as **AP is resource constrained**. This issue is resolved by disabling the per-radio 11r settings, but only if there are no other 802.11r enabled VAPs on the radio. **Scenario:** This issue was observed when 802.11r was enabled in the SSID profile and the user was connected to the AP for the first time. This issue was observed in 7200 Series controllers running ArubaOS 6.3.1.10.

VRRP

Table 101: *VRRP Fixed Issues*

Bug ID	Description
111161	**Symptom:** The VRRP state transitioned unexpectedly between master and backup. The issue is resolved by increasing the control plane packet processing priority on the controller. **Scenario:** This issue was observed after 7210 controller was upgraded from ArubaOS 6.3.1.5 to ArubaOS 6.4.2.2.

Resolved Issues in ArubaOS 6.4.2.3

The following issues are resolved in ArubaOS 6.4.2.3.

AirGroup

Table 102: *AirGroup Fixed Issues*

Bug ID	Description
106505	**Symptom:** A controller sent multiple authentication requests for AirGroup users to the CPPM server when it did not receive a response from the CPPM server. This issue is resolved with internal code changes. **Scenario:** This issue was not limited to a specific controller model or ArubaOS release version.
106912 107807 107810 108929	**Symptom:** Memory leakage was observed on a controller. This issue is resolved by freeing the unused memory. **Scenario:** The memory leak occurred when the **allowall** service was disabled and AirGroup received mDNS response packets that contained a pointer record with an unique **service-id**.

Air Management-IDS

Table 103: *Air Management-IDS Fixed Issues*

Bug ID	Description
89705	**Symptom:** Log messages on the controller incorrectly warned of a TKIP DoS attack from a valid client. This issue is resolved with internal code changes. **Scenario:** The current TKIP attack detection code incorrectly identified certain types of (normal) packet exchanges as a TKIP DoS attack. This issue was observed in a master-local topology and occurred on all controllers running ArubaOS 6.x.
101919	**Symptom:** The WLAN Management System (WMS) process was busy. This issue is resolved by changing the way the WMS process queues are handled. **Scenario:** This issue was observed when the same MAC address was reused between clients and their hosted soft APs. This issue was observed in 6000 Series controllers running ArubaOS 6.2.1.0.
103000	**Symptom:** A controller continuously generated the following error message: **An internal system error has occurred at file aeroscout.c function rtls_send_message line 188 error sendto failed**. Adding extra checks and validation to avoid memory corruption fixed this issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.0.3.
106128	**Symptom:** The controller displayed incorrect properties for a valid AP when a rogue AP was spoofing it. The fix ensures that the controller does not allow a spoofing AP to change the properties of a valid AP. **Scenario:** A rouge AP sent spoofed probe response frames from a Virtual AP to a client. The controller allowed these spoofed frames to change the SSID and encryption type of the Virtual AP. This issue was observed in a master-local topology and was not limited to any specific controller model or ArubaOS release version.

AP-Datapath

Table 104: *AP-Datapath Fixed Issues*

Bug ID	Description
102588 103545	**Symptom:** Clients using bridge or split-tunnel forwarding mode did not get the correct role although the user-table displayed the correct role assignment. The fix ensures that the client retains the **initial-role** till the new role configuration becomes available on the AP. **Scenario:** When a downloadable-role or a manually configured role took time to propagate on the AP, the client was assigned the **logon** role on the AP. This issue was observed in controllers running ArubaOS 6.4.1.0.
110070	**Symptom:** Clients associated with AP-205 were unable to get IP addresses. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when 802.1Q VLAN tagging was enabled. This issue was observed in AP-205 access points connected to controllers running ArubaOS 6.4.2.3.

AP-Platform

Table 105: *AP-Platform Fixed Issues*

Bug ID	Description
104186	**Symptom:** On the controller WebUI, the **Rx Frames to Me** parameter value was zero. The fix ensures that the WebUI shows the correct non-zero value when the AP's radio has clients associated to it. **Scenario:** This issue was specific to AP-125 on controllers running ArubaOS 6.3.1.8.
104786 108566 109126 109127 109128	**Symptom:** An AP kernel crashed on the DFS channel. The log files indicated the reboot reason as **Kernel unaligned instruction access**. Changes in the internal ArubaOS code fixed this issue. **Scenario:** This issue was observed with DFS channel in AP-65 and AP-70 running ArubaOS 6.3.1.6.
105120	**Symptom:** An AP provisioned with LMS and backup-LMS IP in **ap system-profile** initially terminated on primary LMS IP. When the switch associated with the AP and the controller was rebooted, the AP did not re-associate with the primary controller unless the AP was manually rebooted. This issue is resolved by limiting the number of LMS IP used in AP memory to two. **Scenario:** This issue was observed in a setup where: • Both LMS and backup-LMS existed in **ap system-profile**. • An AP received at least three different LMS IPs during reboot. In this case, the first IP was the master controller IP, the second IP was the server IP, and the third IP was the DNS resolution of aruba-master. • Control plane security was enabled and RAP was included. This issue was triggered when the number of LMS IPs in AP memory was not set correctly. **NOTE:** Before upgrading to ArubaOS 6.4.2.3, If a customer uses static master configuration for an AP, make sure the AP gets no more than two different LMS IP. Either make the server IP same as master or make the DNS IP same as master.
106096	**Symptom:** The radios on AP-270 Series access points were not enabled after receiving power through a PoE+ source. This issue is resolved by resending the **Hello** message with the correct PoE flag after detecting a change in power. **Scenario:** An AP started with power profile 2 and switched to power profile 1 when 25.5 W power was negotiated through Link Layer Discovery Protocol (LLDP). Prior to ArubaOS 6.4.2.0, LLDP negotiation started immediately, and the AP switched to power profile 1 before it sent a **Hello** or **Keep Alive** message to the controller. The controller was only aware that the AP was powered from a PoE+ source and radios were brought up normally. This behavior changed in ArubaOS 6.4.2.0, and the LLDP negotiation started only after the AP received the configuration from the controller. The AP eventually received PoE+ power but after the **Hello** message was sent with the PoE flag. This issue was observed on AP-270 Series access points running ArubaOS 6.4.2.0.
107214 108284 108415 108858 109185 109233	**Symptom:** AP Management modules were not in sync with APs, as a result the APs pointed to the wrong LMS. The fix ensures that information related to the primary LMS is passed to the AP Management module, to be synchronized. **Scenario:** This issue occurred when APs failed over from a primary LMS to a standby LMS. If the AP failover recurred, SAPD identified the primary LMS, but STM identified the secondary as primary. This issue was observed in ArubaOS versions 6.4.1.0 and later, but was not limited to any specific controller model.
110165	**Symptom:** Clients connecting to an AP-205 failed to load the captive portal page. The fix ensures that the captive portal page loads successfully. **Scenario:** This issue was seen when an AP-205 was configured as a Remote AP (RAP) in split-tunnel forwarding mode. This issue was observed on AP-205 access points running ArubaOS 6.4.2.2.
110550 110551	**Symptom:** The output of the **show ap debug system-status ap-name** command hanged and displayed incomplete information. Changes in the internal code fixed this issue. **Scenario:** The output of this command hanged when the **paging** feature was enabled on the controller CLI. On disabling **paging**, the command displayed incomplete information. This issue was observed in APs and controllers running ArubaOS 6.4.2.2.

AP-Regulatory

Table 106: *AP-Regulatory Fixed Issues*

Bug ID	Description
106698	**Symptom:** Some RF signals erroneously triggered RADAR events. This issue is resolved by adding a check to ensure that the pulse interval is within the prescribed limit. **Scenario:** This issue was observed in AP-225 access points operating on Dynamic Frequency Selection (DFS) channels and running ArubaOS 6.4.1.0.

AP-Wireless

Table 107: *AP-Wireless Fixed Issues*

Bug ID	Description
97709 103855 106485 106681 107161 107555	**Symptom:** Multiple APs rebooted unexpectedly on the controller. Internal code changes in the wireless driver of the AP fixed this issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.8.
103973	**Symptom:** Multicast video on the clients froze when spectrum monitoring was enabled on the radio serving the client. This issue is resolved by disabling the spectrum monitoring and promiscuous mode in the decrypt-tunnel forwarding mode when a video or voice call is in progress. **Scenario:** This issue occurred when spectrum monitoring was enabled on AP radio. The radio did not receive client data when Fast Fourier Transforms (FFTs) were enabled. As a result, Internet Group Management Protocol (IGMP) messages were lost. This issue was observed on AP-220 Series access points running ArubaOS 6.4.x.x.
96308 103991 105074 105212 105628 106467 108995 110880	**Symptom:** Listed below are some of the symptoms related to this issue: • When streaming multicast video to a large number of clients connected to AP-200 Series access points, the video froze on some of the Windows Media Player clients. • A client connected to AP-200 Series access point lost L3 connectivity to the default gateway, but retained association with the AP and was able to ping other clients on the same subnet. • When a large number of clients tried to associate with AP-200 Series access point in the presence of interference, some clients had difficulty in associating or passing traffic. • A Windows client connected to AP-200 Series access point showed **Limited connectivity** with the yellow "**!**" sign. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in 7200 Series controllers running ArubaOS 6.4.0.2.
104507	**Symptom:** Multicast video streaming stopped responding on Windows Media Player clients. This issue is resolved by changing the value of the non-DFS 5 GHz channel to the value of 2 GHz channel. **Scenario:** This issue occurred when the number of clients on an AP scaled beyond 20.
104447	**Symptom:** On AP-220 Series access point, the transmit power was fluctuating in the 3 dB range. Changes in the internal code fixed this issue. **Scenario:** This issue was observed in AP-220 Series access points when a pre-defined power index had inconsistency between different units.
104833 106906 107628 110210	**Symptom:** AP-225 access point crashed multiple times. This issue is resolved by adding checks to ensure that the packet is valid before processing. **Scenario:** This issue was triggered due to an invalid packet. This issue was observed on AP-225 running ArubaOS 6.4.x.x. **Platform:** AP-225. **Reported Version:** ArubaOS 6.4.1.

Table 107: *AP-Wireless Fixed Issues*

Bug ID	Description
105613	**Symptom:** An intermittent connectivity problem occurred between clients and AP-225. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in AP-225 access points using 2.4 GHz radio.
105925	**Symptom:** When a user moved away from an AP, the transfer rates did not reduce. Internal code changes fixed issues with rate adaptation. **Scenario:** This issue occurred when the Aggregation MAC Protocol Data Unit (AMPDU) was disabled. This issue was observed in controllers running ArubaOS 6.1.3.9.
106540	**Symptom:** A driver log showed low tx power for AP-105 access point. This issue is resolved by correcting the algorithm to get the tx power of AP-105 access point after the first beacon. **Scenario:** This issue was observed in AP-105 access points connected to controllers running ArubaOS 6.3.1.9.
106709	**Symptom:** MacBook Air users experienced packet loss when they connected to APs, which resulted in video pixelation. This issue is resolved by setting the **interference-immunity** parameter to 0. **Scenario:** This issue was observed with access points connected to 7210 controllers running ArubaOS 6.4.1.0.
107110	**Symptom:** The performance of access points dropped in networks with a large number of ESSIDs and multicast packets. This issue is resolved by detecting and recovering the out-of-synchronization power save status between the BSSID and the associated clients. **Scenario:** This issue was observed when the broadcast filter option was disabled in a network with multiple WEP ESSIDs in the same VLAN and large number of multicast packets. This issue was observed in AP-225 access points connected to controllers running ArubaOS 6.4.2.2 or earlier versions.
107197	**Symptom:** The calls made between Vocera badges were sometimes of bad quality when connected to a 2.4 GHz radio. This issue is resolved by retaining legacy packets even if the **in_transit** counter is above the threshold although there are no high threshold or very high threshold clients. **Scenario:** This issue was observed in an AP-105 access point connected to controllers running ArubaOS 6.3.1.9.
108839	**Symptom:** Intel clients disconnected randomly. The fix ensures that deauthorization of UAPSD clients follows the correct path instead of randomly disconnecting from the legacy power save queue. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.0.3 in a master local topology.
109191	**Symptom:** Multiple AP-220 Series access points stopped responding and rebooted. The log files for the event listed the reason as **kernel panic: Fatal exception in interrupt**. Improvements in the wireless driver of the AP fixed this issue. **Scenario:** This issue was caused due to fragmented multicast packets. This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.x.
109211 107991 109656 110457 110655	**Symptom:** In the beacon, high-throughput persisted even though high-throughput was disabled in the configuration. This issue is resolved by removing the logic to update all VAPs when high-throughput configuration is changed on one VAP. **Scenario:** This issue was observed in AP-225 access points connected to controllers running ArubaOS 6.4.2.2 when the **high-throughput-enable** parameter was disabled in **ht-ssid-profile**.

Table 107: *AP-Wireless Fixed Issues*

Bug ID	Description
109627	**Symptom:** SSIDs that there were not configured on the controller were displayed in mobiles devices. This issue is resolved by modifying the Traffic Indication Map (TIM) offset and updating the firmware. **Scenario:** This issue was observed in 7210 controllers running ArubaOS 6.4.1.0 when hidden SSIDs were configured in a standalone master topology.
104694 109975	**Symptom:** A high memory utilization was observed on AP-225 when clients associated to this AP. Improvements in the wireless driver of the AP fixed this issue. **Scenario:** This issue occurred when packets were locked in the Broadcast/Multicast queue of the AP resulting in high memory utilization. This issue was observed in AP-225 access points running a beta version of ArubaOS 6.4.2.3.
110619 105941	**Symptom:** 802.11ac clients experienced high packet loss when associated to an AP-225 access point. Improvements in the wireless driver of the AP fixed this issue. **Scenario:** This issue occurred when 802.11ac clients associated to a WPA2-PSK SSID in power save mode. This issue was observed in AP-225 access points running a beta version of ArubaOS 6.4.2.3.

ARM

Table 108: *ARM Fixed Issues*

Bug ID	Description
108540	**Symptom:** The memory available on the controller is reduced due to a memory leak in the ARM process. This issue is fixed by implementing internal code changes. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.0.3.

Authentication

Table 109: *Authentication Fixed Issues*

Bug ID	Description
101664	**Symptom:** On rebooting the controller, the management user account that was created for certificate-based GUI access was deleted. This issue is fixed by storing the username with quotes. **Scenario:** This issue was observed when the management user account created for the certificate-based GUI access contained a space in the username.
107114	**Symptom:** 802.1X clients failed to authenticate. The fix ensures that 802.11r enabled tunnel-mode clients in the **ActivedotxStation** table are appropriately handled during fast-roaming. **Scenario:** This issue was observed when 802.11r enabled tunnel-mode clients roamed between access points. This issue was not specific to any controller model or ArubaOS release version.

Base OS Security

Table 110: *Base OS Security Fixed Issues*

Bug ID	Description
105188	**Symptom:** When users roamed to a new AP with the same ESSID but with different VAP and AAA profiles, their roles did not change. This issue is resolved by deleting the IP user entry when there is a change in the AAA profile, so that new properties are applied. **Scenario:** This issue was observed when the SSID profile was the same for APs in different groups but the VAP and AAA profiles were different. This issue was observed in 7240 controllers running ArubaOS 6.4.1.0.
105705	**Symptom**: Invalid station entries were created when the **aaa user add** command was executed to change a user role on the controller. The fix reduces the number of invalid station entries on the controller. **Scenario:** This issue was observed on an M3 controller running ArubaOS 6.3.1.7 when the **show station- table** command was executed or the maximum user capacity was reached due to invalid station entries.
105873	**Symptom:** The **authentication** process leaked memory while sending out the RADIUS accounting **START** message. This issue is resolved by freeing the memory in the **authentication** process. **Scenario:** This issue was observed in an M3 controller running ArubaOS 6.1.3.2.
105952	**Symptom:** After the controller rebooted, a AAA user derivation rule name that was configured with spaces was missing from the current configuration. This issue is resolved by addressing the space in the profile name. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.5 or earlier.
107069 109547	**Symptom:** A memory leak was observed in the **Authentication** module when the downloadable role was used. The fix ensures that the memory is cleared after it is used. **Scenario:** This issue was observed when role download was enabled using the **Configuration** > **Security** > **Authentication** > **AAA Profiles** option and the RADIUS response also contained a downloadable role with an Aruba vendor-specific attribute (VSA). This issue was observed in controllers running ArubaOS 6.4.1.0.

Controller-Datapath

Table 111: *Controller-Datapath Fixed Issues*

Bug ID	Description
101587 104272 104273 104505	**Symptom:** A controller rebooted and crashed while reassembling the fragments received from a mesh AP. Changes to the recursive IP packet assembly resolved this issue. **Scenario:** This issue occurred due to a misconfiguration between a controller running ArubaOS 6.3.1.5 and a mesh AP.
107310 110293 110405	**Symptom:** A controller authenticated the clients successfully, but the DNS resolution failed. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when **Media Classification** was enabled. To disable **Media Classification**, remove **classify-media** from the ACLs and/or disable **allow-stun** in the firewall. This issue was observed in 600 Series, M3, and 7200 Series controller running ArubaOS 6.4.X.0.

Controller-Platform

Table 112: *Controller-Platform Fixed Issues*

Bug ID	Description
95071 95444 97548 97835 98115 98262 104276 107166 107964	**Symptom**: When a show command was executed from a standby controller running ArubaOS 6.3.1.1, a **Module Configuration Manager is Busy** error message was triggered. This issue is resolved by making code level changes to prevent deadlock scenarios between database backup processes. **Scenario**: This issue was observed in a standby 3600 controller in a master-standby topology.
100208 107938	**Symptom**: A DHCP client in an access point sent **debugging** log messages when the logging level was set to **information** and flooded the syslog server. This issue is resolved by implementing internal code changes. The DHCP logs are associated with logging configuration and these logs are available when DHCP debug logs are enabled. **Scenario**: This issue was observed in controllers running ArubaOS 6.4.0.2.
102943 105329 105905 106616	**Symptom:** A master controller rebooted and remained in **CPboot** state. The log files for the event listed the reason as **Hard Watchdog reset**. Changes in the internal code of ArubaOS fixed this issue. **Scenario:** This issue was observed in 3000 Series and M3 controllers running ArubaOS 6.3.1.5 and later.
103416 104932 106115 106630 106868 107052 107273 107283 107874 107996 108033 108224 108256 108621 108853 109410 109416 109474 109673	**Symptom:** A controller stopped responding and there was no corresponding entry in the log file. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in 3600 controllers running ArubaOS 6.3.1.9.
106253	**Symptom:** The **show cpu current** command displayed an incorrect CPU utilization status. The value returned for the first iteration was incorrect whereas the values for the later iterations were correct. This issue is resolved by implementing internal code changes. **Scenario:** This issue occurred due to inconsistency in the value displayed. This issue was not limited to a specific controller model or ArubaOS release version.
106314 106426 106771 109022	**Symptom:** A master controller was slow and did not respond to some output commands. Processes such as **CFGM**, **STM**, and **WMS** stopped responding. This issue is fixed by restricting the **WMS** database from exceeding the threshold. **Scenario:** This issue occurred due to low memory on the controller and was observed in a master-local topology. This issue was observed in controllers running ArubaOS 6.3.x and 6.4.x.

Table 112: *Controller-Platform Fixed Issues*

Bug ID	Description
106573 107888 108040 108320 108471 108986 110411	**Symptom:** The **DOGMA** process (watchdog process monitor) on the controller continued to be in the **INITIALIZING** state. Changes in the internal code fixed this issue. **Scenario:** As soon as the controller was rebooted, the **show process monitor statistics** command displayed the **DOGMA** process in the **INITIALIZING** state. This issue was observed in 7000 Series and 7200 Series controllers running ArubaOS 6.4.x.
108533	**Symptom:** After logs were introduced to track the crashes in the firewall-visibility process caused by DNS cache, there was an increase in the errors logged. This issue is resolved by introducing a delay logic to reduce the number of errors logged for the firewall-visibility process and by increasing the maximum number of mappings value. **Scenario:** This issue was observed when the number of IP address mappings to DNS name increased beyond the permitted value. This issue was not limited to a specific controller model or ArubaOS release version.
108739 109461	**Symptom:** In rare cases, a 7005 controller can power off due to a false temperature exception. You must manually power on the controller to bring it back online. The fix ensures that the controller remains powered on. **Scenario:** This issue was found in very few 7005 controllers running ArubaOS 6.4.1.0 or later versions.
108989 107285 109051 109052 109490 109492 109493 109494	**Symptom:** A memory leak was observed when the Web Content Classification (WebCC) feature was enabled without executing the **ip name-server** command. This issue is resolved by configuring the IP name server before enabling the WebCC feature. **Scenario:** This issue was observed in 7240 controllers running ArubaOS 6.4.2.0.

Mesh

Table 113: *Mesh Fixed Issues*

Bug ID	Description
104660 108414	**Symptom:** A mesh AP stopped responding and rebooted. The log files for the event listed the reason as **kernel BUG at aruba_wlc.c**. Changes in the internal ArubaOS code fixed this issue. **Scenario:** This issue was observed in AP-270 Series running ArubaOS 6.4.x.

Remote AP

Table 114: *Remote AP Fixed Issues*

Bug ID	Description
103850	**Symptom:** A Huawei® E160 USB modem stopped responding as it did not synchronize with the RAP. This issue is resolved by making code level changes to delay the modem boot-up process of the Huawei® E160 USB modem. **Scenario:** This issue was observed when RAP-109 access points terminated on controllers in the RAP mode. This issue was not limited to a specific controller model and was observed in ArubaOS 6.4.1 in a master-local topology.
105024	**Symptom:** When the up-link IP address of the RAP was set in the 192.168.11.x range, and if the RAP was not rebooted, it disconnected from the network. Enhancements to the internal code fixed this issue. **Scenario:** This issue was observed when you upgrade the RAP to ArubaOS 6.3.1.2.
105739	**Symptom:** A RAP-3WN remote access point did not associate with Huawei® E3276-S150 USB modem. This issue is resolved by modifying the initialization script for Huawei® E3276-S150 USB modem. **Scenario:** This issue occurred when the **usb-init** string was not saved correctly for this modem. This issue was observed on a RAP-3WN remote access point running ArubaOS 6.4.0.3. **Platform:** RAP-3WN. **Reported Version:** ArubaOS 6.4.0.3.

Station Management

Table 115: *Station Management Fixed Issues*

Bug ID	Description
103452	**Symptom:** When a client previously associated with an AP-225 left, its record showed up in the **show ap remote debug association** and the **show ap association** commands. The stale record was not removed. This issue is fixed by implementing internal code changes. **Scenario:** This issue was observed in AP-220 Series access points where many clients were connected. This issue was observed in AP-220 Series access points running ArubaOS 6.4.0.2.
106411	**Symptom:** The station management process on the local controller crashed and caused all APs to fail over to the master controller. Internal code changes in the station management process fixed this issue. **Scenario:** This issue was seen in a master-local topology and was not limited to any specific controller model or ArubaOS release version.

VRRP

Table 116: *VRRP Fixed Issues*

Bug ID	Description
108693 110519	**Symptom:** After upgrading the controllers to ArubaOS 6.4.2.2, the VRRP instances were still in the backup state. To resolve this issue, the VRRP state machine is restarted based on the link status instead of Spanning Tree Protocol (STP) state convergence, when STP is globally enabled but not on the VRRP VLAN. **Scenario:** This issue was seen when STP was globally enabled on a master-standby topology but the VRRP VLAN was not part of STP. This issue was observed in controllers running ArubaOS 6.4.2.2.

Web Content Classification

Table 117: *WebCC Fixed Issues*

Bug ID	Description
109930	**Symptom:** The Web Content Classification (WebCC) process on the controller stopped responding and crashed. Changes in the internal code fixed this issue. **Scenario:** This issue was observed in 7220 controller running ArubaOS 6.4.2.2.

WebUI

Table 118: *WebUI Fixed Issues*

Bug ID	Description
101933 106412	**Symptom:** An error occurred when a user tried to open the WebUI of the controller with Fully Qualified Domain Name (FQDN) or IP address in the compatibility view mode of Internet Explorer 9 or higher version. This issue is resolved by overriding the compatibility mode. The page loads in the standard mode. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.5 or higher version.
101989	**Symptom:** The controller displayed the status of an AP as inactive when an administrator tried to view the client activity under the **Monitoring** tab of the controller WebUI. Changes in the internal ArubaOS code fixed this issue. **Scenario:** This issue was observed in 3400 controllers running ArubaOS 6.2.1.x. or 6.3.1.x.
104118 105173 105679 106987 107548 108324 108984	**Symptom:** On the **Monitoring > NETWORK > All Access Points** page of the controller WebUI, the **2.4 GHz clients** displayed an incorrect client count as compared to the output of the **show ap association** command. This issue is resolved by making internal code changes. **Scenario:** This issue was observed in a master standalone controller running ArubaOS 6.4.1.0 or later versions.
105664 109546 113316 113926 114006	**Symptom:** The user was unable to upload the captive portal page to a controller. This issue is resolved by correcting the free flash space calculation. **Scenario:** This issue was observed when a user tried to load custom XML files to the captive portal page. This issue occurred due to miscalculation of the flash memory size. This issue was observed in controllers running ArubaOS 6.4.2 or earlier versions.

Wi-Fi Multimedia

Table 119: *Wi-Fi Multimedia Fixed Issues*

Bug ID	Description
101501 107735	**Symptom:** The quality of the Lync calls was poor and the Mean Opinion Score (MOS) was low when multiple users were in power saving mode and some of the users received downstream UDP traffic at 10 Mbps. **Scenario:** This issue was observed in AP-200 Series and AP-220 Series in tunnel and decrypt tunnel forwarding mode running ArubaOS 6.3.1.8, 6.4.0.3, or 6.4.1.0.

Resolved Issues in ArubaOS 6.4.2.1

The following issues are resolved in ArubaOS 6.4.2.1.

Activate

Table 120: *Activate Fixed Issues*

Bug ID	Description
105345	**Symptom:** When the active whitelist feature was enabled and the controller downloaded the whitelist from the Active Server, the customer's account credentials were logged in the active logs. These logs were enabled only when the logging level was set to debugging. The fix ensures that the logs retrieving the activate HTTP message content are removed. **Scenario:** This issue was observed in controllers running ArubaOS 6.3 and later versions.

AirGroup

Table 121: *AirGroup Fixed Issues*

Bug ID	Description
102648 108406	**Symptom:** The **mDNS** process crashed frequently. This issue is resolved by making code level changes to obtain the switch MAC address in a robust manner. **Scenario:** This issue was observed in 7200 Series controllers running ArubaOS 6.4.0.3.

Air Management-IDS

Table 122: *Air Management-IDS Fixed Issues*

Bug ID	Description
106242	**Symptom:** The initial RSSI (Received Signal Strength Indication) value was incorrect for some wireless client entries in the AP. When creating the client entry, the AP checks if the frame was sent by the client device. If not, the controller does not update the RSSI value, and it remains unset until a frame is seen from the client device. This check resolved the issue. **Scenario:** This issue occurred only when an AP2STA (AP to station) frame was used to create the client entry. Though this frame was not initiated from the wireless client, the AP incorrectly used the RSSI from this frame to set the RSSI value for the wireless client. This issue was not limited to any specific controller model or ArubaOS release version.

AP-Platform

Table 123: *AP-Platform Fixed Issues*

Bug ID	Description
102260	**Symptom:** Although multiple Virtual Access Points (VAPs) were enabled, only one VAP could be configured. This issue is resolved by making code level changes to the VAP configuration. **Scenario:** This issue was observed when multiple VAPs were enabled on a single radio. This issue was observed when the **show ap debug received-config** command was issued.
104520 104726 105296 105627 106396 106609 107104 108006 113246 113603 114050	**Symptom:** The status of an AP was displayed as UP on the local controller, but as DOWN on the master controller. The fix ensures that when there is no change in the value of the master switch IP, an update from the IKE module is rejected. **Scenario:** This issue was observed in M3 and 3600 controllers running ArubaOS 6.3.1.5 in a master standby local topology.
105417 106186	**Symptom:** Although wireless clients were associated to an AP, they failed to transmit data. This issue is resolved by making code level changes to enable **dos-prevention**, thereby ensuring that the entities in the AP are synchronized. **Scenario:** This issue was observed when the **dos-prevention** parameter in the **wlan virtual-ap** command was disabled. This issue was triggered when the client sent a **DISASSOC** frame to the AP. This issue was observed in all AP platforms running ArubaOS 6.4.1 or later versions.
105529	**Symptom:** When the AP restarted, the Enet1 port was used as the new active uplink. Also, the AP did not boot. This issue is fixed by ensuring that the Enet0 port is used as the primary active link. **Scenario:** This issue was observed in an AP-224/AP-225 when the Enet1 port was connected to a laptop or a projector and the AP was using the static IP address.

AP-Wireless

Table 124: *AP-Wireless Fixed Issues*

Bug ID	Description
104160 104278 104279	**Symptom:** An error occurred when the hardware chip set was unable to perform self-offset calibration in 1 ms. This issue is resolved by removing unnecessary driver logs when there is a channel switch failure. **Scenario:** This issue occurred when the volume of error messages per day was high on the syslog server. This issue was observed in AP-115 and RAP-155 running ArubaOS 6.3.0 or later versions.
104254 104922 106118 106704 106966108361	**Symptom:** After upgrading to ArubaOS 6.4.1.0, access points de-authenticated clients with the error message **Station Up Message controller Timed Out**. Internal code changes ensure valid authentication of clients by access points. **Scenario:** Clients were unable to connect to the SSID after the controller was upgraded to ArubaOS 6.4.1.0. This issue was observed on M3 controllers running ArubaOS 6.4.1.0.
105528	**Symptom:** A Dell laptop did not connect to an AP-225 and EAP exchange failed. This issue is resolved by fixing the capability in the beacon when HT is disabled. **Scenario:** This issue was observed in an AP-225 connected to controllers running ArubaOS 6.3.1.5.

Base OS Security

Table 125: *Base OS Security Fixed Issues*

Bug ID	Description
101355	**Symptom:** The controller was not completely compliant with RFC3576 because the state attribute was not processed and sent back to the server. With this fix, the controller adheres to RFC3576. **Scenario:** This issue occurred when the Change of authorization (CoA) request packet contained a state attribute but the controller was not placing that state attribute in the CoA-Ack. This issue was not limited to a specific controller model or ArubaOS release version.
102632	**Symptom:** EAP-TLS termination displayed a **certificate verification failed** error message when the controller was upgraded from ArubaOS 6.1 to ArubaOS 6.3. Changes in the certificate verification to support a partial chain fixed this issue. **Scenario:** This issue was observed when the CA-certificate that was used for verification did not have the full chain to the Root CA. This issue was observed when the controller was configured with EAP-TLS termination running ArubaOS 6.2 or later versions.
105418	**Symptom:** A flaw in OpenSSL SSL/TLS server could allow a man-in-the-middle attacker to force a downgrade to TLS 1.0 even if both the server and client support a higher protocol version. This issue is resolved with internal code changes. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.x and ArubaOS 6.4.x.
106066 106572	**Symptom:** The **authentication** process crashed in 7240 controller. This issue is resolved with internal code changes. **Scenario:** This issue was observed in a 7240 controller running ArubaOS 6.3.1.5.

Configuration

Table 126: *Configuration Fixed Issues*

Bug ID	Description
95535 95582 99325 99934 104674	**Symptom:** The ACL configuration on the local controller went out of sync intermittently with the master controller. The fix ensures that when centralized licensing is enabled and if PEFNG license is installed, the ACL configuration associated with the license is not changed even if the PEFNG license is temporarily unavailable. **Scenario:** This issue occurred when there was a change in licenses. This issue was observed in controllers running ArubaOS 6.3.1.2 or later versions in a master-local topology.
105688	**Symptom:** The access control entries were corrupt after the controller rebooted. This issue is resolved by updating the CFGM module. **Scenario:** This issue was observed in a master redundancy topology after the controller was reloaded. This issue was observed in ArubaOS 6.4.0.3, but is not limited to any specific controller model.

Controller-Datapath

Table 127: *Controller-Datapath Fixed Issues*

Bug ID	Description
103223	**Symptom:** When the **netservice** command with end port 65535 was executed followed by **no netservice** command, an infinite loop of the **no netservice** command executed. This caused the controller to reboot. Internal code changes ensure that the controller does not reboot after executing **netservice** with end port 65535 followed by the **no netservice** command. **Scenario:** This issue was observed when **netservice** or **no netservice** commands were executed with end port value as 65535. This issue was observed in controllers running ArubaOS 6.3.x or later versions.
104097	**Symptom:** Controllers were unable to see ping requests, which resulted in ping responses being dropped. This issue is resolved by disabling the **firewall enable-stateful-icmp** parameter by default. **Scenario:** This issue was observed when the firewall checked for the unsolicited ICMP echo replies and dropped them if there were no ICMP echo request sessions. This issue was observed in 7200 Series controllers and M3 controllers running ArubaOS 6.4.1.0 and above.

Controller-Platform

Table 128: *Controller-Platform Fixed Issues*

Bug ID	Description
95993 96671 97943 98502 100384 101190 101795 101852 103097 103689 104252 104638 105502	**Symptom:** The **firewall-visibility** process crashed on a local controller. The process restarts and recovers on its own. **Scenario:** This issue was observed after a controller was running for a long time, possibly due to overflow of an internal data structure. This issue was not limited to any specific controller model or ArubaOS release version.
103736 102443 102930 103798 103968 104828 105499 106614	**Symptom:** A controller stopped responding and rebooted. The log files for the event listed the reason as **kernel module crash**. This issue is resolved by enabling the watchdog petting all and watchdog respawn features. **Scenario:** This issue was observed when the **watchdog** process crashed. This issue was observed in a 7240 controller running ArubaOS 6.4.0.2.
103937	**Symptom:** Establishing an SSH session to the controller failed randomly with error message **ssh_exchange_identification: Connection closed by remote host**. SSH sessions were either stale or NoTTY (non-interactive session) where an SSH session did not exist but the underlying TCP connection existed. This issue is resolved by: • Performing a graceful log out for all SSH sessions whose terminal was closed earlier without logging out. This clears NoTTY sessions. • Setting the parameter **ClientAliveCountMax** to 7200 and parameter **ClientAliveInterval** to 0, which terminates SSH sessions that are idle for 7200 seconds (2 hours) on the controller without killing the respective process from the shell. Disable keep alive on the SSH client so that the channel remains idle during inactivity. **Scenario:** This issue was observed because of stale SSH processes (with NoTTY) which were unresponsive for a long time.
104929	**Symptom:** A 7240 controller crashed when the **show ap tech-support ap-name** command was executed. This issue is resolved by modifying the **show ap tech-support ap-name** command from asynchronous mode to synchronous mode. **Scenario:** This issue was observed in APs connected to an IPv4 network and in 7240 controllers running ArubaOS 6.4.0.2.
106963	**Symptom:** A 7005 controller had incorrect license limits for AP, Policy Enforcement Firewall Next Generation (PEFNG), and RF Protect (RFP) licenses. The correct license limit of 16 AP, 16 PEFNG, and 16 RFP is fixed in this release. **Scenario:** A 7005 controller license was erroneously set to 32 AP, 32 PEFNG, and 32 RFP whereas the system tested limits are 16 AP, 16 PEFNG, and 16 RFP. This bug accepted more than the tested limits. This issue was observed in a 7005 controller running ArubaOS 6.4.1.0 or 6.4.2.0. **NOTE:** If you have not yet upgraded to ArubaOS 6.4.2.1 and are running ArubaOS 6.4.1.0 or 6.4.2.0, it is not recommended to over-provision the 7005 controller with more than the system tested limits to avoid any issues with future software upgrades.

HA-Lite

Table 129: *HA-Lite Fixed Issues*

Bug ID	Description
105535	**Symptom:** The APs switched between active and standby controller unexpectedly due to heart beats being missed between the controllers. The issue is resolved by making internal code changes. **Scenario:** This issues was observed in 7240 controllers running ArubaOS 6.4.2.0.
105915	**Symptom:** When using fast failover, the Eth-1 wired session did not fail over. This issue is resolved by setting the **cp->enable** flag based on the **wired-port-profile** or **wired-ap-profile** configuration. **Scenario:** This issue was observed when HA failed over from active to standby in controllers running ArubaOS 6.4.

Hotspot-11u

Table 130: *Hotspot-11u Fixed Issues*

Bug ID	Description
105976	**Symptom:** Although the **hs2-profile** was removed from the **wlan virtual-ap** profile, Hotspot 2.0 was not disabled completely. This issue is resolved by introducing handlers. **Scenario:** This issue was observed in an AP-225 connected to controllers running ArubaOS 6.4.2.

Local Database

Table 131: *Local Database Fixed Issues*

Bug ID	Description
104157	**Symptom:** A controller crashed due to lack of flash space. This issue is resolved by setting a size limit on log files stored in the flash memory of the controller. **Scenario:** This issue was observed when log files occupied most of the flash space due to multiple crashes in the database server. This issue was not limited to any specific controller model or ArubaOS release version.

Mobility

Table 132: *Mobility Fixed Issues*

Bug ID	Description
101517	**Symptom:** A controller set the L3 mobility roaming state incorrectly as Home Switch/Foreign VLAN instead of Home Switch/Home VLAN when the user roamed between two SSIDs. This issue is resolved by stopping the association timer on the L3 mobility client. **Scenario:** This issue was observed when L3 mobility was enabled with a single WAN controller having two SSIDs, one SSID with L3 mobility enabled and the other with L3 mobility disabled.

Station Management

Table 133: *Station Management Fixed Issues*

Bug ID	Description
102223 106169	**Symptom:** When the **show ap association** command was executed, the association table listed invalid entries. These entries were not displayed when the **show user ap-name** and **show ap debug client-table ap-name** commands were executed. The fix ensures that the **send_ageout** parameter is called when the new node is not created and a counter is added to track the old SAP entry. **Scenario:** This issue was observed when there were a large number of mobile users. This issue was observed in AP-92, AP-105, AP-125, and AP-2255 access points connected to 7210 controller running ArubaOS 6.3.1.7.
102241	**Symptom:** The Station Management (STM) process crashed on the master controller when the **ap wipe out flash** command was executed. This issue is resolved by relaying the correct message to the local controller. **Scenario:** This issue was observed if an AP was present on the local controller and the **ap wipe out flash** command was executed on the master controller running the FIPS version of ArubaOS. This issue was observed on controllers running any version of FIPS ArubaOS.
104639	**Symptom:** Wireless clients unexpectedly failed to be in 802.11r enabled WLAN. The clients failed because the station management process crashed on the access point. Changes in the internal code of the station management module ensure that clients roam seamlessly in an 802.11r enabled WLAN. **Scenario:** This issue was observed when an 802.11r-capable wireless client roams from one AP to another with the same or different ESSID. In addition, this issue lasted until the client manually switched to another ESSID. This issue was observed in controllers running ArubaOS 6.3.1.8 or later versions.
105240	**Symptom:** The **stm add blacklist-client** command failed to add more than 512 entries whereas the previous versions of ArubaOS allowed up to 4096 entries to be added. This issue is resolved by adding a limit parameter to the client blacklist function, and allowing 4096 or 512 entries as required. **Scenario:** This issue was observed on controllers running ArubaOS 6.4.2.1.

VRRP

Table 134: *VRRP Fixed Issues*

Bug ID	Description
103093	**Symptom:** Although Virtual Router Redundancy Protocol (VRRP) preemption was disabled on the controllers, the actual master controller did not remain as standby after it came up. The fix ensures that the actual master controller waits for the correct master rollover time calculation before assuming the role of the master controller again. **Scenario:** This issue was observed in Aruba7210 controllers when a master controller rebooted and took the role of the master controller instead of remaining in the standby role. This issue occurred due to an incorrect timing calculation on **Higher priority Standby**.

WebUI

Table 135: *WebUI Fixed Issues*

Bug ID	Description
96082	**Symptom:** The Received Signal Strength Indicator (RSSI) value of a client was displayed incorrectly in the **Client Monitoring** page of the WebUI. This issue is resolved by making code level changes to ensure that the correct value is displayed on all browsers. **Scenario:** This issue was observed when accessing the controller's WebUI using the Google Chrome browser. This issue was observed in controllers running ArubaOS 6.4.
100284	**Symptom:** When a MAC address with two octets was searched from the RAP whitelist database of the controller WebUI, the search returned zero result although the MAC address was present in the whitelist database. The user entered the complete MAC address when querying a whitelist-db entry. Code level changes in the search API fixed this issue and the user can now use a partial MAC address. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.6.

Resolved Issues in ArubaOS 6.4.2.0

The following issues are resolved in ArubaOS 6.4.2.0.

802.1X

Table 136: *802.1X Fixed Issues*

Bug ID	Description
103635	**Symptom:** When an 11r client with tunnel-mode roamed from one AP to another AP, the data traffic from the client sometimes stopped. This issue is resolved by setting a key at the controller datapath for 11r tunnel-mode stations. **Scenario:** This issue was observed when 11r clients with tunnel forwarding mode enabled roamed between APs. This issue was observed in controllers running ArubaOS 6.3.1.6. This issue was not limited to any specific controller model.

Air Management-IDS

Table 137: *Air Management-IDS Fixed Issues*

Bug ID	Description
102715	**Symptom:** An Ekahau/RTLS server did not parse tag frames forwarded to the server from AP-225, AP-275, or AP-205. This issue is fixed adding an extra two bytes of padding in the forwarded frame, as the server expects. The padding is added by default, but it can be configured under the AP system profile. **Scenario:** This issue was observed when using tag forwarding to Ekahau/RTLS servers from AP-225, AP-275, or AP-205 connected to controllers running ArubaOS 6.4.x. The issue does not affect Aeroscout tag forwarding.

AP-Platform

Table 138: *AP-Platform Fixed Issues*

Bug ID	Description
98995	**Symptom:** AP-70 crashed when scanning an unsupported channel. This issue is resolved by changing the channel in the Singapore (SG) country code and not allowing AP-70 to scan an unsupported channel. **Scenario:** This issue was observed in AP-70 Series devices connected to a controller running ArubaOS 6.2.1.3.

AP-Wireless

Table 139: *AP-Wireless Fixed Issues*

Bug ID	Description
102301	**Symptom**: AP-225 rebooted unexpectedly. The log files listed the reason for the reboot as **Out of Memory error**. The fix ensures that the accounting error that causes AP reboot is addressed. **Scenario**: This issue was observed when UDP bidirectional traffic was sent using the **iperf** command, which resulted in an increase in traffic and RX queue. This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.7.
102631	**Symptom**: When running a down-link test with best effort (BE) traffic to one client and voice traffic to another client, the voice traffic dropped to 10-12 %. This issue is fixed by setting the packet size for the UDP test to 1260 bytes or enabling MTU discovery, and not limiting the MTU to 1500 bytes. **Scenario:** This issue occurred when significant packets dropped before reaching the wireless driver. This issue was observed in a Server-Controller-AP-Client topology with AP-225 devices.

ARM

Table 140: *ARM Fixed Issues*

Bug ID	Description
95771	**Symptom:** Scan reject did not occur when VO traffic existed. This issue is fixed by setting 802.1d priority for VO Traffic in ASAP module. **Scenario:** This issue was observed in AP-225 devices connected to controllers running ArubaOS 6.4.0.0.

Base OS Security

Table 141: *Base OS Security Fixed Issues*

Bug ID	Description
99882	**Symptom:** The down-link packets to WPA-TKIP clients randomly stopped on 7200 Series controllers. The fix ensures that issues related to support single replay counter with TKIP, which is independent of the WMM priority of the packet is addressed. **Scenario:** The issue was observed when a client used TKIP with WMM enabled. This led to the locking of WMM queues which resulted in the client losing network connectivity.
101269	**Symptom:** The output of the **show rights** command displayed only a partial list of session ACLs. This issue is resolved by correcting the scanning function that fetches the output in batches. **Scenario:** This issue was observed when a large number of ACLs with a large number of policies were configured under a role. This issue was observed in controllers running ArubaOS 6.3.1.4 or later. This issue was not limited to any specific controller model.
101594	**Symptom:** When **snmpwalk** is used to query the **nUser6Name** Object Identifier(OID), some addresses were not retrieved. Internal code changes ensure that the subsequent IPv6 address for the same station MAC on the controller is retrieved. **Scenario:** This issue was observed when there were consecutive IPv6 addresses for the same station MAC on the controller and subsequent IPv6 address were not retrieved.

Controller-Datapath

Table 142: *Controller-Datapath Fixed Issues*

Bug ID	Description
100922	**Symptom:** Accessing Microsoft® SharePoint using Microsoft Internet Explorer timed out. Correcting the TCP Maximum Segment Size (MSS) on the controller fixed the issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.2 or later. This issue was not limited to any specific controller model.
101392	**Symptom:** In a controller, a user did not appear immediately in the user-table when connected. Traffic passed through only after the user appeared in the user-table. This issue is resolved by deleting the oldest 5% of total entries during devid_cache table full condition instead of deleting only one entry, so that the table-full condition is not reached for consecutive new users. **Scenario:** This issue was observed in 7200 Series controllers running ArubaOS 6.3.1.3. This issue might be observed in earlier ArubaOS releases too when the devid_cache table is full and new users (who are not present in the devid-cache) come in at approximately 10 users per second. This issue was not limited to any specific controller model, but the scenario is more likely to occur on 7200 Series controllers where the maximum users are higher. Maximum devid_cache is twice the max-users and SQL sorting operations take longer along with the number of entries present.
103514	**Symptom:** After the user upgraded ArubaOS 6.4.1.0, the input error bytes on 10Gb physical interfaces were increasing. This issue is resolved by disabling 802.3 Ethernet frame length error checks on 10Gb physical interfaces. **Scenario:** This issue was observed on 7210 Series controllers running ArubaOS 6.4.0.0. This issue was observed when the 802.3 Ethernet frame length received did not match the actual number of data bytes received.

Controller-Platform

Table 143: *Controller-Platform Fixed Issues*

Bug ID	Description
100679	**Symptom:** A controller crashed and rebooted with hardware watchdog reset. Internal code changes fixed this issue. **Scenario:** This issue was observed in 620, 650, 3200, 3400, 3600, and M3 controllers, but was not limited to any specific ArubaOS version.
101003	**Symptom:** Centralized image upgrade over TFTP did not work if the image file was in sub-directory. Centralized upgrade over TFTP worked if the image file was in root directory. Changes in the internal code fixed this issue. **NOTE:** The present implementation does not support absolute path. The TFTP server typically runs in sandbox. Only relative path is supported. **Scenario:** The download function ignored the file-path in case of download from a TFTP server. This issue was not limited to any specific controller model or ArubaOS release version.
102725 103483 103558	**Symptom:** The **fpapps** module that handles port channel management crashed and the controller rebooted. This issue is resolved by deleting a section of debug code that was not required. **Scenario:** This issue was caused due to the debug code added to fix bug ID 95129 and was observed on controllers running ArubaOS 6.3.1.7, 6.1.3.13, and 6.4.1.0.
103715	**Symptom:** The fans in the 7010 controller ran very fast and were noisy even at room temperature. This issue is resolved by fixing the fan controller algorithm to have finer granularity of RPM control vs PoE power. **Scenario:** This issue was observed in the controller although there was not much PoE load. This issue is specific to 7010 controllers running ArubaOS 6.4.1.0.

GRE

Table 144: *GRE Fixed Issues*

Bug ID	Description
103336	**Symptom:** The tunnel went down due to keep-alive failure. This issue is resolved by modifying the keep-alive process to avoid packet loss. **Scenario:** This issue was observed when the tunnel endpoints were not in the same VLAN as the uplink VLAN through which controllers were connected. This issue was observed in controllers running ArubaOS 6.3.1.8 and was not limited to any specific controller model.

Licensing

Table 145: *Licensing Fixed Issues*

Bug ID	Description
101443 103325	**Symptom:** RAPs did not come up after upgrading from ArubaOS 6.3.1.1 (or prior) to ArubaOS 6.3.1.2 (or later). This issue is resolved by enabling the RAP feature if AP licenses exist. **Scenario:** This issue was observed when centralized licensing was enabled with RAPs and controllers were upgraded from ArubaOS 6.3.1.1 (or prior) to ArubaOS 6.3.1.2 (or later). The RAP feature bit was enabled in the cached bitmap on controllers running ArubaOS 6.3.1.2, which caused the upgrade issue.

LLDP

Table 146: *LLDP Fixed Issues*

Bug ID	Description
102431	**Symptom:** When AP-225 was connected to a switch with a long (more than 50 m) Ethernet cable, it always worked in restricted mode even though the switch secured 19 W power by LLDP. This issue is resolved by enforcing AP-225 to work in unrestricted mode if switch can secure 19 W power by LLDP. **Scenario:** This issue was not limited to any specific controller model or release version.
103548	**Symptom:** LLDP packets were sent on boot and prior to configuration push. This issue is fixed by, not sending LLDP TLVs when AP boots, sending three mandatory TLVs (chassis subtype, port subtype and TTL) and one Aruba TLV on boot, and sending the configured TLVs after the AP receives the configuration from the controller. **Scenario:** This issue was observed on controllers running ArubaOS version prior to 6.4.2.0.

Policy Based Routing

Table 147: *Policy Based Routing Fixed Issues*

Bug ID	Description
104169	**Symptom:** The user was unable to add SRC-NAT using the Web UI when ESI policy was enabled. This issue is resolved by adding the **NAT Pool** option in the Web UI, for ESI policy. **Scenario:** This issue is observed in ArubaOS 6.3.x and 6.4.x.

QoS

Table 148: *QoS Fixed Issues*

Bug ID	Description
103363	**Symptom:** When the DSCP value on outer GRE IP was not set, voice quality issue was observed with Vocera badges. This issue is resolved by copying the inner DSCP value to the outer DSCP field when packet is GRE encapsulated. **Scenario:** This issue was observed only when WEP was enabled and not for other encryption modes. This issue was not limited to any specific controller model.

Remote AP

Table 149: *Remote AP Fixed Issues*

Bug ID	Description
99635	**Symptom:** A Huawei® E160 USB modem was not functional because it lost synchronization with the RAP. This issue is resolved by making code level changes to delay the modem boot-up process for E160. **Scenario:** This issue was observed when the RAP connected to the USB modem was hard rebooted.
101526	**Symptom:** The Remote AP Authorization Profile feature was not functional when the RAP was upgraded from ArubaOS 6.2.1.0 to ArubaOS 6.3.1.6. This issue is resolved by changing the code to perform AP authorization against RAP whitelist instead of local-userdb-ap. **Scenario:** This issue was observed when the flag status of the RAPs did not change to Rc2 even after they were authorized by the Captive Portal user. As a result, the configuration download was incomplete. This issue was observed in ArubaOS 6.3 and above.
101767	**Symptom:** The Huawei® EC177 modem was not functional as it incorrectly executed script of another modem. This issue is resolved by scanning the modem twice to get the updated product ID (modem mode ID). **Scenario:** This issue was observed when the AP did not wait until the completion of mode-switch process for EC177. This resulted in the same product ID for both Huawei E392 and EC177.
102267	**Symptom:** The **IAPMGR** process crashed on the controller. This issue is resolved by removing the assert statement in an erroneous condition. **Scenario:** This issue was observed on controllers running ArubaOS 6.4 with IAPs in VPN configuration.

Role/VLAN Derivation

Table 150: *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
103090	**Symptom:** In a network that has internal and DMZ controllers and the internal controller tunnels packets from the clients through the L2 GRE tunnel to the DMZ controller, UDR rules were not applied when a user moved as a wired user over GRE tunnel from the internal controller to the DMZ controller. This issue is resolved with internal code changes. **Scenario:** This issue was observed when using L2 GRE tunnel to send the client traffic from internal controller to DMZ controller. This issue was observed on 3600 Series controller running ArubaOS 6.3.1.8.

Station Management

Table 151: *Station Management Fixed Issues*

Bug ID	Description
103452	**Symptom:** When a client previously associated to AP-225 left, its record showed up in show ap remote debug association table and show ap association table. This record was stale and was not removed. This issue is fixed by increasing the scb number so that the buffer reclaiming logic is not triggered often and modifying the notification to STM so that the driver does not delete a record until ageout arrives from AP STM. **Scenario:** This issue was observed in busy AP-225 where many clients were connected and the reclaiming logic was triggered. This issue was observed in AP-225 connected to controllers running ArubaOS 6.4.0.2.

WebUI

Table 152: *WebUI Fixed Issues*

Bug ID	Description
103384	**Symptom:** The user was unable to add port Access Control Lists (ACL) using the WebUI. This issue was fixed by making changes to the port values. **Scenario:** This issue occurred if the minimum port value was more than the maximum port value and this issue is observed on 3600 controllers running ArubaOS 6.3.1.5.

Resolved Issues in ArubaOS 6.4.1.0

The following issues are resolved in ArubaOS 6.4.1.0.

AirGroup

Table 153: *AirGroup Fixed Issues*

Bug ID	Description
96233 96235 96236	**Symptom:** An Apple® TV got dropped off from the AirGroup server list as the device got deleted from the controller cache table due to expiry of mDNS address record (A or AAAA). The fix ensures that the device is deleted from the controller cache table only if the IP address of the device matches with the expired mDNS address records (A and AAAA). **Scenario:** When an Apple TV acted as a sleep proxy server for other mDNS devices connected in the network, it advertised the address records and services of these mDNS devices. When the advertised address records of the sleeping device expired , the apple TV that acted as the sleep proxy server got deleted incorrectly. This issue is not limited to any specific controller model or ArubaOS release version.
97685	**Symptom:** AirGroup did not adhere to the global RADIUS settings when the **ip radius source-interface [loopback | vlan]** command was issued. The fix ensures that the global RADIUS configuration overrides the IP address used for sending AirGroup RADIUS requests. **Scenario:** This issue is not limited to any specific controller model or ArubaOS release version.
97771	**Symptom:** When the user tried to access Google® Chromecast the following error was displayed, **selected device is no longer online**. This issue is resolved by ensuring that the MAC multicast address for Simple Service Discovery Protocol (SSDP) packets is generated correctly. **Scenario:** This issue was observed if a user tried to connect to Chromecast when Airgroup service was enabled. This issue was caused because the controller was not receiving DLNA response from Chromecast for multicast DLNA queries, resulting in missing cache entries on the controller for DIAL service from Chromecast. This issue is observed in all controllers running ArubaOS 6.4 and later.

Table 153: *AirGroup Fixed Issues*

Bug ID	Description
100002	**Symptom:** The CPPM server was flooded with AirGroup authorization requests from the controller. The fix ensures that the controller does not send AirGroup authorization requests if an AirGroup device changes its IP address. **Scenario**: This issue was observed on controllers running ArubaOS 6.3 and later. This issue is observed when a controller sends out RADIUS requests each time an AirGroup user changes the IP address.
102063 102064 102258 102455 102457 102740 102741 102743 102745 102746 102877 102934 102935 102936 102938 102939 102940 103782 104023 104024 104025 104026 104027 104140 106264 106265 106266 106267 106269 107187 107449 107542 107618 108417 108474 109328 109382 109685 112446 112447 113388	**Symptom:** The multicast Domain Name System (mDNS) process of AirGroup crashed and restarted on M3 controller. The logs for the event listed the reason for the crash as **Nanny rebooted machine - low on free memory**. Internal code changes are implemented to ensure the memory leak was removed. **Scenario:** A memory leak occurred every time the user sent a query and controller responded with the relevant mDNS records. This issue was observed in M3 controller running ArubaOS 6.3.1.7.

Air Management-IDS

Table 154: *Air Management-IDS Fixed Issues*

Bug ID	Description
90630	**Symptom:** Log messages incorrectly warn of a Block ACK (BA) DoS attack from a valid client. Changes in the internal code have fixed this issue. **Scenario:** This issue was identified in a 6000 controller running ArubaOS 6.2.0.2 in a master-local topology.
96206	**Symptom:** The WMS module periodically failed to respond to SNMP requests when it removed monitored devices that were not in use. This issue is resolved by optimizing the WMS station check and AP removal process. **Scenario:** This issue occurred in large networks with many monitored devices, when the table size became large in the WMS module, and the WMS module failed to respond to the SNMP poll requests. This issue was not limited to any specific controller model or ArubaOS release version.

AP Regulatory

Table 155: *AP Regulatory Fixed Issues*

Bug ID	Description
98303	**Symptom**: Incorrect max EIRP value was displayed for AP-104. This issue is resolved by correcting the regulatory limit for EU countries. **Scenario**: This issue was observed in AP-104 access points running ArubaOS 6.3.1.x due to incorrect value defined for the regulatory limit for EU countries.
98628	**Symptom:** MaxEIRP for RAP-3WN/ RAP-3WNP was inconsistent due to wrong maximum tx-power setting. The fix ensures that the regulatory and hardware limits are correctly set. **Scenario:** This issue was observed when the value of configured tx-power was larger than the MaxEIRP.

AP-Platform

Table 156: *AP-Platform Fixed Issues*

Bug ID	Description
95472 96239	**Symptom:** When an AP was configured with a static IP address, the Link Aggregation Control Protocol (LACP) on AP-220 Series access points was not functional. This issue is resolved by initiating a LACP negotiation when an AP with a static IP is identified. **Scenario:** This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.3 and 6.4.0.1 when configured with a static IP.
95893	**Symptom:** When an AP sent a DHCP request, it received an IP address 0.0.0.0 from the Preboot Execution Environment (PXE) server. Though the AP accepted this IP address, the AP could not communicate further and rebooted. The fix ensures that the PXE acknowledgment is ignored and the AP receives a valid IP address. **Scenario:** This issue was observed in deployment scenarios that have a DHCP server and multiple PXE servers. This issue was observed in APs running ArubaOS 6.3 or earlier.
96051 96754 98008	**Symptom:** AP-115 access points rebooted unexpectedly. This issue is resolved by adding a device queue status check before sending data to an Ethernet driver. **Scenario:** A crash occurred when the throughput was high on Ethernet connected to a 100/10M switch. This issue was observed in AP-114 and AP-115 access points running ArubaOS 6.3.x and later versions.

Table 156: *AP-Platform Fixed Issues*

Bug ID	Description
97544	**Symptom:** RAP-109 could not be used on un-restricted controllers that do not have Japan country code. This issue is resolved by mapping the country code in AP regulatory domain profile to the AP regulatory domain enforcement. **Scenario:** This issue was observed when the Instant AP with Japan Stock-Keeping Unit (SKU) was converted to Remote AP running ArubaOS 6.3.1.3.
100586	**Symptom:** AP-120 Series (802.11 a/b/g) access point models stopped working after upgrading to ArubaOS 6.4.x. Support for AP-120 Series (802.11 a/b/g) access point models are enabled in ArubaOS 6.4.x. **Scenario:** This issue was observed in AP-120 Series (802.11 a/b/g) access point models running ArubaOS 6.4.x.

AP-Wireless

Table 157: *AP-Wireless Fixed Issues*

Bug ID	Description
83716	**Symptom:** Some of the IEEE 802.11g beacon transmit rates were not supported by AP-220 Series access point. This issue is resolved by allowing beacon transmit rates support for non-basic IEEE 802.11g. **Scenario:** This issue was triggered when non-basic IEEE 802.11g rate was not allowed on AP-220 Series access point. This issue was observed in AP-220 Series devices and AP-270 Series running ArubaOS 6.3.x, 6.4.x or earlier versions.
88940	**Symptom:** A crash was observed on APs when the status of the channel was set inappropriately by the process handling the AP management. This issue is resolved by selecting the first channel of the current 802.11 band, using the auto-channel option. **Scenario:** This issue was observed when a standard RAP or CAP was configured at the Dynamic Frequency Selection (DFS) channel. This issue is observed in AP-70 connected to controllers running ArubaOS 6.3.1.2.
94482 96677	**Symptom:** An AP crashed due to an internal Watchdog timeout. This issue is resolved by reducing the wait time, and rebooting the AP to recover from that state. **Scenario:** This issue occurred within one of the reset functions in the Ethernet driver where there was a long wait, which exceeded the watchdog timeout, causing AP failure.
96751	**Symptom:** An AP continuously crashed and rebooted due to out of memory. Disabling wireless and rogue AP containment features in the Intrusion Detection System (IDS) profile resolved this issue. **Scenario:** This issue occurred when wireless and rogue AP containment features were enabled on the IDS profile. This issue was observed on AP-220 Series running ArubaOS 6.3.1.2 version.
97428	**Symptom**: Users were unable to access the network as the old DHCP route-cache entry was not modified by the new DHCP cache route on Aruba Remote APs (RAP). The fix ensures that the old route cache entry is replaced by the new route cache. **Scenario**: This issue was observed when IPs were assigned to clients through DHCP on RAP. This issue was observed in RAPs running ArubaOS 6.4.x.

Table 157: *AP-Wireless Fixed Issues*

Bug ID	Description
99833 100559	**Symptom:** When more than 120 customers were connected in the bridge mode, broadcast packets were dropped and customers lost connectivity. This fix ensures that the broadcast packet handling is modified to resolve the issue. **Scenario:** This issue was observed when the frequency of customers trying to connect to the APs was high. This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.2.
99922	**Symptom:** AP-220 Series access points displayed more than actual number of associated stations. When reclaiming the client data structures, there was inconsistency between driver and AP processes which is now resolved. **Scenario:** This issue was observed when the value of the parameter **max-clients** was set to 255 and the count of the associated and non-associated stations exceeded the maximum value. This issue was observed in AP-220 Series access points connected to controllers running ArubaOS 6.3.x and later versions.
100652 100731	**Symptom:** AP-225 access point was not transmitting multicast streams. This issue is resolved by fixing the accounting problem. **Scenario:** This issue was observed when the counter used to track the buffered multicast frames was not decremented when invalid frames in the buffers were discarded. When the counter reached the maximum outstanding multicast frames, no more multicast frames were allowed for transmission.

ARM

Table 158: *ARM Fixed Issues*

Bug ID	Description
97585	**Symptom:** The **show ap arm client-match history** command displayed that a client was steered to a radio with less than -70 dBm. This was a display error. ARM log does not record the correct signal strength. The fix ensures that the ARM log always notes the signal strength that is used to make client match decision. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.2 or later versions.

Authentication

Table 159: *Authentication Fixed Issues*

Bug ID	Description
96492	**Symptom**: When 802.1X authentication was in progress, two key1 packets were sent out during key exchange. This issue is resolved by making code level changes to ensure that only one key1 packet is sent out during key exchange. **Scenario**: This issue was observed when machine authentication was enabled and when user authentication was processed. During this process if the machine authentication details were found in the cache, key1 was sent out again for the second time. This issue is not limited to any specific controller model or ArubaOS release version.

Base OS Security

Table 160: *Base OS Security Fixed Issues*

Bug ID	Description
88563 96465	**Symptom:** Some cipher suites were not working when the operations were offloaded to hardware. This issue was resolved by disabling the cipher suites which were not working with the hardware engine. **Scenario:** This issue was observed during any crypto operation that uses Diffie–Hellman key exchange.
92817	**Symptom:** Wireless clients were blacklisted even when the rate of the IP Session did not exceed the threshold value set. This issue is resolved by increasing the storage of the threshold to16 bits. **Scenario:** This issue was observed when the threshold of the IP Session rate was set to a value greater than 255. This issue was observed in controllers running ArubaOS 6.x.
95367	**Symptom:** Issuing the **show rules <role-name>** command from the controller's CLI resulted in an internal module (Authentication) crash. Ensuring that Access Control Lists (ACLs) are not configured with spaces in the code resolved the issue. **Scenario:** This issue was observed when a large number of ACL was configured with spaces in their names. This was not limited to any specific controller model or ArubaOS release version.
96755	**Symptom:** Wired 802.1X using EAP-MD5 authentication failed. This issue is resolved by the modifying the authentication code to allow the wired-clients that perform authentication using EAP-MD5 authentication framework. **Scenario:** This Issue was observed when wired clients connected directly either to the controller or to the Ethernet port of a Campus AP or Remote AP. This issue was not limited to a specific controller model or ArubaOS release version.
96980	**Symptom:** Customer faced connectivity issues with Pre-Shared Key (PSK), Mac Authentication, and VLAN Derivation as key1 packet was sent out twice. This issue is resolved by introducing serialized Mac Authentication and PSK. **Scenario:** This issue occurred when PSK and Mac Authentication were parallely processed, but PSK was initiated before MAC Authentication VLAN update. This issue was observed in ArubaOS 6.3.1.1.
98492	**Symptom:** When the customer roamed from a demilitarized zone (DMZ) to an internal controller, the display showed wireless instead of wired. This issue is resolved by checking the tunnel through which the user is connected and changing the user to wired. **Scenario:** This issue was observed when the customer routed traffic from an internal controller to DMZ using the L2 GRE Tunnel. This issue was observed in 3600 controllers running ArubaOS 6.2.1.3.
100248	**Symptom:** The Authentication module crashed on a 7210 controller. This issue is resolved by adding preventive checks that prevent a wired user with zero MAC address, and by adding logs and error stats counters to identify occurrence of such crashes. **Scenario:** This issue was observed in a network where the Remote AP and a wired user were on the same controller. This issue is specific to 7210 controllers running ArubaOS 6.4.0.3.

Captive Portal

Table 161: *Captive Portal Fixed Issues*

Bug ID	Description
98992	**Symptom:** After upgrading from ArubaOS 6.1.3.9 to ArubaOS 6.3.1.4, captive portal redirect was not sent, so CP Authentication could not be completed. This issue is resolved by introducing forward lookup mechanism to check if CP Authentication has been configured multiple times for the same client. If multiple CP Authentications are detected, they are redirected until the captive portal configuration is complete. **Scenario:** This issue was observed only when multiple CP Authentication configurations were created. This issue was observed in controllers running ArubaOS 6.4 and ArubaOS 6.3.1.3 or later versions.

Certificate Manager

Table 162: *Certificate Manager Fixed Issues*

Bug ID	Description
98565	**Symptom:** When the customer tried to upload a CA Certificate, an error message was displayed - **Not a CA certificate**. This issue is resolved by making code level changes to check if CA is set to true when the certificate is uploaded. **Scenario:** This issue was observed when the customer tried to upload a RAP custom certificate.

Configuration

Table 163: *Configuration Fixed Issues*

Bug ID	Description
95535 95582 99934 100234	**Symptom**: The ACL configuration on the local controller went out of sync intermittently with the master controller. The fix ensures that when centralized licensing is enabled and if PEFNG license is installed, the ACL configuration associated with the license is not be changed even if the PEFNG license is not available temporarily. **Scenario**: This issue occurred when there was a change in licenses. This issue was observed in controllers running ArubaOS 6.3 in a master-local topology.

Controller-Datapath

Table 164: *Controller-Datapath Fixed Issues*

Bug ID	Description
84585 92227 92228 92883 94200 96860 98380	**Symptom:** Traffic failed to pass a network with heavy traffic (such as high levels of packet replication), when AES-CCM or another encryption/decryption modes were enabled. This issue is resolved by increasing the estimated time for packet processing, in the datapath. **Scenario:** This issue was identified on 7200 Series controller connected to 2000 APs when Gratuitous ARP messages were replicated and sent to clients.
93582	**Symptom:** A 7210 controller crashed. The logs for the event listed the reason for the crash as **datapath timeout**. Ensuring that the destination UDP port of the packet is PAPI port while processing Application Level Gateway (ALG) module resolved this issue. **Scenario:** This issue was observed in 7210 controllers running ArubaOS 6.3.1.0.
97223	**Symptom:** An L3 GRE tunnel between an Aruba controller and a Cisco device was not restored when there was a keep-alive failure. The fix ensures that Aruba and Cisco devices use the same protocol number in the GRE keep-alive packets. **Scenario:** This issue was observed when Aruba and Cisco devices used different protocol numbers in GRE keep-alive packets, and both the devices dropped the keep-alive packets sent by the other as the protocol number was unknown. This issue was not limited to any specific controller model and was observed in ArubaOS 6.4.x.
97434	**Symptom:** High volume of Address Resolution Protocol (ARPs) requests triggered an increase in datapath utilization, which resulted in service impact. This issue is resolved by introducing the **arp** and **grat-arp** parameters to drop or blacklist the clients that are sending excessive ARPs. **Scenario:** This issue was observed when a client excessively scanned and dropped the Internet Control Message Protocol (ICMP) packets. This issue was observed in a local M3 controller running ArubaOS 6.4.x, in a master-local topology.
98499 100392 100393	**Symptom**: Controllers crashed multiple times. The log files for the event listed the reason for the reboot as datapath exception. **Scenario**: When a wireless user generated encrypted wifi fragments, these fragments were sent to the security engine for decryption, which returned results that were out-of-order and some of them had decryption errors. The fix ensures that the wifi fragments out-of-order decryption errors are handled correctly.
98500	**Symptom:** A legacy platform controller crashed when it received more than three Aggregated Mac Service Data Unit (A-MSDU) fragments. To resolve this issue, a check is introduced in the controller to drop the packets when more than three A-MSDU fragments were received. **Scenario:** This issue was observed when a wireless client sent aggregated A-MSDU packets to the AP which was further fragmented to more than three packets and sent to the controller. This issue was specific to legacy platform controllers (6000 Series controllers platforms with XLR/XLS processors and 650 controllers) running ArubaOS 6.3 and 6.4.
99483	**Symptom:** When AMSDU-TX was enabled, one of the packets were incorrectly freed and another packets failed, which lead to double incarnation of the same buffer and the system crashed. The fix ensures that the buffers are freed correctly. **Scenario:** This issue was observed in controllers running ArubaOS 6.3 or later, and was not limited to any specific controller model
100084	**Symptom:** Unknown ARP (ARP without user entry in datapath) requests were flooded in RAP wired tunnels. This issue is resolved by changing the behavior of the unknown ARPs from flooding in RAP wired tunnels. **Scenario:** This issue was observed in all controllers running ArubaOS 6.3.1.6 or later.

Controller-Platform

Table 165: *Controller-Platform Fixed Issues*

Bug ID	Description
74428 88758	**Symptom:** On dual-media RJ45 ports 0/0/0 and 0/0/1, if the port speed was forced from/to 1 Gbps to/from 10/100 Mbps when traffic was flowing, traffic forwarding on the port stopped in an unintended manner. This issue is resolved by disabling the port to stop the traffic on the port before changing the speed and re-enabling the port after changing the speed. **Scenario:** This issue was observed in 7200 Series controllers running ArubaOS 6.2 in configurations or topologies where traffic is flowing.
76059 85289 92255 93467 93827 95431 96293 96791 96827 98196 99287 99360 99362 99472 99568 100857 100858 101476	**Symptom:** A controller rebooted unexpectedly. The log files for the event listed the reason as **Reboot Cause: kernel panic**. The fix ensures that the **httpd** process resumes immediately after crashing. **Scenario:** This issue was seen in 7200 Series controller having a high density of IPv4 captive-portal users configured. This resulted in a high number of **httpd** processes running on the controller. This issue was observed in ArubaOS 6.2 or later versions.
91097 96923	**Symptom:** A local controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as **Mobility Processor update**. The fix ensures that the controller does not reboot unexpectedly by making code level changes to the primary and secondary NOR flash boot partition. **Scenario:** This issue was observed in controllers running ArubaOS 6.1.3.9.
91541 94045 95079	**Symptom:** A controller rebooted due to low memory. Changes to the controller software fixed this issue. **Scenario:** This issue occurred when there was a continuous traffic inflow terminating on the control plane. This resulted in an internal component of the ArubaOS software to take up high memory. This issue was observed in 600 Series, 3000 Series, and M3 controllers running ArubaOS 6.1 or later versions.
94427 96347 97456 97468 97938 98425 98656 99448 99919	**Symptom:** An M3 controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as **User pushed reset** error. The issue is resolved by removing the lock contention. **Scenario:** This issue was observed due to panic dump or SOS crash, which was a result of jumbo packet or packet corruption. This issue was observed in M3, 3200, 3400, and 3600 controllers, but was not limited to any specific ArubaOS release version.
96712 99920	**Symptom:** A local controller rebooted unexpectedly during terminal/ssh related operation. The log files for the event listed the reason for the reboot as **Kernel panic**. Internal changes in the ArubaOS code fixed this issue. **Scenario:** This issue was observed in 7240 controllers running ArubaOS 6.2.1.4.

Table 165: *Controller-Platform Fixed Issues*

Bug ID	Description
97237	**Symptom:** A controller rebooted because of memory leak in the module that handles address, route, and interface related configurations and notifications on the system. This issue is resolved by fixing the memory leak in the flow. **Scenario:** Memory leak occurred when an interface or STP states changed frequently with PAPI error. This issue was observed on 651 controller running ArubaOS 6.2.1.6 or later.
97388 97658 98373	**Symptom:** Some access points went down when the controller to which they were connected rebooted. This issue is resolved by ensuring that the boot partition information is updated in the secondary bank of the controller. **Scenario:** This issue occurred when the controller rebooted due to a watchdog reset. This issue was not limited to any specific controller model or ArubaOS release version.
97411 97816 98419 98686 98688	**Symptom:** Local handling Station Management (STM) and WLAN Management System (WMS) processes crashed, with **0x01 exit** status. The fix ensures that during a specific table backup, the database does not get corrupted. **Scenario:** This issue occurs due to database table corruption. This issue was observed in controllers running ArubaOS 6.3 and ArubaOS 6.4.
95835 98034 98202 99342	**Symptom:** A controller stopped responding and rebooted. The log files for the event listed the reason as **softwatchdog reset**. This issue is resolved by removing the various race condition in the panic dump path and reimplementing the watchdog framework. **Scenario:** This issue was seen during datapath core dump. This issue was observed on 7200 Series controller running ArubaOS 6.3.1.2.
98873 100421	**Symptom:** A 650 controller crashed during reboot. The log files for the event listed the reason as **address error on CPU4**. This issue is resolved by reverting the sos_download sequence in rcS script. **Scenario:** This issue was observed in 650 controller running ArubaOS 6.2.1.5.
99106	**Symptom:** A large number of **Only Bottom slots can arbitrate** debug messages were generated and as a result the controller console was flooded with these redundant messages. The issue is fixed by disabling these redundant messages in the arbitration algorithm. **Scenario:** This issue was observed in M3 controllers and is not limited to any ArubaOS version.
99208 99210 99211 99212 99213	**Symptom:** A controller crashes due to memory leak in PIM after a long uptime (for example, 90 days). The fix ensures that there are no memory leaks in PIM module. **Scenario:** This issue is observed when IGMP snooping or proxy is enabled and users perform multicast streaming. This issue occurs when the user's DHCP pool range is too vast (more than 2 million addresses). This issue is not limited to any specific controller model or ArubaOS version.

DHCP

Table 166: *DHCP Fixed Issues*

Bug ID	Description
96117 96433	**Symptom:** Some wireless clients experienced delay in obtaining an IP address. This issue is fixed by disabling the DDNS (Dynamic Domain Name system) update logic within Dynamic Host Configuration Protocol (DHCP). **Scenario:** This issue occurred when the DHCP pool was configured with the domain name and the Domain Name System (DNS) server was configured on the controller, using **ip name-server** command. This resulted in DDNS update of the host and delayed the response for the DHCP request. This issue was not limited to any specific controller model or ArubaOS release version.

LLDP

Table 167: *LLDP Fixed Issues*

Bug ID	Description
100439	**Symptom:** Clients were unable to disable the 802.3 TLV power in the AP LLDP configuration. This results in PoE allocation issue on the switches. The fix allows the customer to enable/disable the 802.3 power Type Length Value (TLV). **Scenario:** This issue was observed in 7210 controllers running ArubaOS 6.2.1.7.

Local Database

Table 168: *Local Database Fixed Issues*

Bug ID	Description
95277	**Symptom:** Any RAP whitelist entry with special characters failed to synchronize with any controller, and synchronization failed for subsequent whitelist entries. The issue is resolved by correcting the handling of special characters for every field in RAP and CPSEC whitelist entries so that synchronization can happens properly. **Scenario:** This issue was observed where RAP and CPSEC whitelist entries are synchronized on controllers running ArubaOS 6.3.1.2.

IPsec

Table 169: *IPsec Fixed Issues*

Bug ID	Description
97775 100139	**Symptom:** If a user entered a wrong password, the VIA application did not prompt thrice for a password retry. This issue is resolved by sending the **XAUTH STATUS FAIL** message to the VIA client before deleting the IKE/IPSec session of the VIA client. **Scenario:** This issue was observed in controllers running ArubaOS 6.2, 6.3, or 6.4. The issue was caused when the controller did not send **XAUTH STATUS FAIL** to the VIA client.
98901	**Symptom:** An internal process (ISAKMPD) crashed on the controller. This issue is fixed by properly allocating the Process Application Programming Interface (PAPI) message that is sent from ISAKMPD process to the Instant Access Point (IAP) manager. **Scenario:** This issue occurred when the IAPs terminated on the controller and established IKE/IPsec connections with the controller. This issue was more likely to happen on M3, 3600, and 3200 controller models than on 7200 Series controller models, and occurred on ArubaOS running 6.3 or later.
99675	**Symptom:** ISAKMPD process crashed on master controller when maximum number of RAP limit was reached and a new user had to be added. This issue is resolved by reworking the debug infra code to remove the tight loop. **Scenario:** This issue was observed when more than 2 supported RAPS terminated on a controller. This resulted in ISAKMPD process sitting in a tight loop.

Master-Redundancy

Table 170: *Master -Redundancy Fixed Issues*

Bug ID	Description
98005	**Symptom:** After centralized licensing was enabled, the standby master displayed **UPDATE REQUIRED** message. This issue is resolved by ignoring the RAP bit when checking if a new license type has been added. **Scenario:** This issue was observed when the centralized licensing was enabled and the master controller had embedded AP licenses. This issue was not limited to a specific controller model but is observed in ArubaOS 6.3.1.3, when the master controller has embedded AP licenses.
98663	**Symptom:** Error messages were displayed when database synchronization was taking place in 600 Series controllers. This issue is resolved by removing support for **iapmgr**. **Scenario:** This issue was observed in 600 Series controllers. The issue is caused when the user upgrades to ArubaOS 6.3 and executes the **write erase all** command.

RADIUS

Table 171: *RADIUS Fixed Issues*

Bug ID	Description
93578	**Symptom:** In the **show auth-trace buff** command output, the number of RADIUS request packets jumped from 127 to 65408. This issue is fixed by changing the data type of the variable used in the command output. **Scenario:** This issue occurred due to an incorrect value that was displayed in the command output. This issue was not limited to any specific controller model or ArubaOS version.
96038	**Symptom:** Sometimes, the user name was missing in the RADIUS accounting **STOP** messages sent from the controller. The fix ensures that a check is added for user entries with multiple IP addresses before revoking authentication. **Scenario:** This issue was observed when the controller revoked authentication for user entries with multiple IP addresses. This issue was not limited to any specific controller model or ArubaOS release version.

Remote AP

Table 172: *Remote AP Fixed Issues*

Bug ID	Description
95572	**Symptom:** All clients, wired and wireless, connected to Remote AP (RAP), were unable to pass traffic locally with source NAT in split-tunnel forwarding mode. The fix ensures that the entries in the route-cache table are aged out correctly. **Scenario:** This issue was observed when the route-cache table reached the max size as the aging was not working. This issues was observed when the 3200XM controller was upgraded from ArubaOS 6.1.3.6 to ArubaOS 6.3.1.2.
97009	**Symptom:** A RAP failed to establish a PPPoE connection when the RAP's up-link port was VLAN tagged. The fix ensures that the RAP can establish a PPPoE connection with VLAN tag. **Scenario:** This issue was observed in RAPs running ArubaOS 6.3.1.3.
99466	**Symptom:** The output of the **show iap table** command incorrectly displayed the status of iap (branch) as UP with older tunnel inner ip, after the isakmpd process crashed. The fix ensures that the status of the iap(branch) is updated properly with the new inner ip. **Scenario:** This issue is observed in controllers running ArubaOS 6.3 and 6.4.

Role/VLAN Derivation

Table 173: *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
89236 94936 96005 99978	**Symptom:** Incorrect VLAN derived for mac-auth derived role-based VLAN. This issue is resolved by deriving the mac-auth derived role-based VLAN from the L2 user-role. **Scenario:** This issue was observed when a user entry existed, user entry was assigned to mac-auth derived role-based VLAN, and the client re-associated. A user was assigned to the default VLAN instead of the mac-auth derived role-based VLAN because mac-auth was skipped for the existing mac-authenticated user-entry.
94423	**Symptom:** There was a mismatch between the device id stored in the user table and the AP cache. The fix ensures that the information retrieved from **show user** command and device id cache display the information received in the first packet. **Scenario:** This issue was observed when the device id cache was not updated by the AP, but when the **show user** command was executed, the updated device id cache was displayed. This issue was not limited to any specific controller model or release version.
97117	**Symptom:** When the RADIUS server returned multiple Vendor Specific Attributes (VSAs), ArubaOS did not check these attributes or set user roles. This issue is fixed by verifying the list of attributes before matching them with the rules. **Scenario:** This issue was observed when a user tried to set a role using the VSA attributes that were returned from the RADIUS server. This issue was observed in 3400 controllers running ArubaOS 6.2.1.4.
99745 100008 100198 100435	**Symptom:** Role/VLAN derived from SDR and UDR were incorrect since they matched only the first rule. This issue is resolved by correcting the logical error in code to make sure role/VLAN derivation for SDR and UDR works correctly. **Scenario:** This issue occurred only when SDR and UDR was configured with multiple rules.

Routing

Table 174: *Routing Fixed Issues*

Bug ID	Description
94746	**Symptom:** When the loopback IP address was used as the controller-ip, the controller was not reachable from a wired network after reboot for a specific configuration and timing. The controller was reachable only from the same subnet to which the controller's uplink belongs. This issue was not seen when a VLAN interface was used as the controller-ip. This issue is resolved by maintaining the correct sequence for appropriate execution of the two internal threads . **Scenario:** This issue was observed when two threads in an internal process tried to modify the kernel default route information and lost the sequence of execution. This issue was seen in 7200 Series controllers running ArubaOS 6.3.1.0.

Startup Wizard

Table 175: *Startup Wizard Fixed Issues*

Bug ID	Description
98110	**Symptom:** Mobility Controller **Setup Wizard** page was stuck with Java script error when you clicked **Next** on the **VLANs and IP Interfaces** tab of the controller's WebUI. Changes in the internal XML code fixed this issue. **Scenario:** This issue was not limited to any specific controller model and was observed in ArubaOS 6.4.0.2.
98159	**Symptom: Campus WLAN Wizard** page was stuck in **Role Assignment** step when you clicked **Next** on the **Authentication Server** step of the controller's WebUI using Microsoft® Internet Explorer 10 or Internet Explorer 11. Changes in the internal XML code fixed this issue. **Scenario:** This issue is not limited to any specific controller model and is observed in ArubaOS 6.4.0.2.

Station Management

Table 176: *Station Management Fixed Issues*

Bug ID	Description
86620 88646	**Symptom:** The **show ap association client-mac** command showed client MAC addresses for clients that aged out beyond the idle timeout value. This issue is resolved by making code level changes to station table in the Station Management module. **Scenario:** This issue was not limited to any specific controller model or ArubaOS release version.
96910	**Symptom:** The SNMP query on the objects, **wlanAPRxDataBytes64** and **wlanAPTxDataBytes64** returned incorrect values for AP-225. This issue is resolved by making code level changes to the read function in the AP driver. **Scenario:** This issue was observed when the statistics in the AP driver was parsed incorrectly. This issue was observed in AP-225 access points running ArubaOS 6.3.x and later versions.

Voice

Table 177: *Voice Fixed Issues*

Bug ID	Description
95566	**Symptom:** When two parties made a VoIP call using Microsoft® Lync 2013, media classification running on the controller prioritized the media session with wrong DSCP values. The fix ensures that the WMM value is read from the TUNNEL Entry rather than the Bridge Entry, so that the value is correct. **Scenario:** The DSCP values configured under the ssid-profile did not take effect. This issue occurred when the initial VLAN and the assigned VLAN were different. This issue was observed on M3 controllers running ArubaOS 6.1.3.10.

WebUI

Table 178: *WebUI Fixed Issues*

Bug ID	Description
94818	**Symptom: AP Group** name did not support special characters. With this fix, you can create an **AP Group** name with the following special characters: **" / > < : } { + _) (* & ^ % $ # @ ! [ ] ; , . /**. **Scenario:** This issue was seen when you create an **AP Group** from the **Configuration > WIRELESS > AP Configuration** page of the controller's WebUI. This issue was not limited to any specific controller or release version.
95185	**Symptom:** Collecting the **logs.tar** with **tech-support** logs from the controller's WebUI failed with **Error running report... Error: receiving data from CLI, interrupted system call** error message. The fix ensures that the session is kept active till the logs are ready to be downloaded. **Scenario:** This issue was not seen under the following cases: • Downloading the **logs.tar** without **tech-support** log from the WebUI. • Downloading the **logs.tar** with **tech-support** logs from the CLI. This issue was observed in 7220 controller running ArubaOS 6.3.1.2.
98939	**Symptom:** The user was unable to access the **Monitoring > Summary** page on a controller GUI using Internet Explorer 9 (IE 9). This issue is resolved by implementing internal code changes that ensures the Web UI loads correctly. **Scenario:** This issue was observed when the controller was upgraded to ArubaOS 6.3.1.4-FIPS. This issue was caused by a missing **DOCTYPE** HTML code in the **Monitoring > Summary** page. Alternatively, the user can access the **Monitoring > Summary** page using Google Chrome or Mozilla Firefox. This issue is not limited to any specific controller model or ArubaOS version.
99356	**Symptom:** The WebUI incorrectly displayed that the interface was selected under IGMP in the **Network > IP > IP Interface > Edit VLAN** page even though a port channel was configured in the CLI. The fix ensures that the WebUI correctly displays the configured port channel when IGMP proxy is configured on a VLAN interface. **Scenario:** This issue was observed when the ip igmp **proxy port-channel** command was executed on a VLAN interface. This issue was observed in all the controller platforms.
99471	**Symptom:** The WebUI could not disable IGMP proxy when it was enabled under IGMP in the **Network > IP > IP Interface > Edit VLAN** page. The fix adds a new **Enable IGMP** checkbox under VLAN to enable or disable the IGMP options selected. **Scenario:** The WebUI did not allow disabling both IGMP snooping and IGMP proxy together once either of the radio buttons was selected. This issue was not limited to any specific controller model or ArubaOS version.
99961 100373 100771	**Symptom:** Remote AP settings were missing in the controller WebUI under the **Configuration->Wireless->AP Installation > Provision** page. The remote AP license check is removed to fix this issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.1.6.
100051	**Symptom:** Banner text on login page of the controller’s WebUI was incorrectly aligned. The fix ensures that the banner text is aligned correctly. **Scenario:** This issue was observed when a controller was upgraded to ArubaOS 6.3.x.

XML API

Table 179: *XML API Fixed Issues*

Bug ID	Description
97102 99101	**Symptom:** RADIUS accounting START message did not trigger for clients when a user was added using XML-API. To resolve this issue, the **check-for-accounting** parameter has been introduced in the Captive Portal configuration. This parameter helps in bypassing the check for Captive Portal profile role, by toggling between older versions of ArubaOS and ArubaOS 6.3 or later versions. **Scenario:** This issue was observed only when a user was added before the authentication was complete. This issue was not limited to any specific controller model or ArubaOS release version.

Resolved Issues in ArubaOS 6.4.0.3

The following issues were resolved in ArubaOS 6.4.0.3.

Base OS Security

Table 180: *Base OS Security Fixed Issue*

Bug ID	Description
99070	**Symptom:** An Aruba controller's WebUI and captive-portal were vulnerable to an OpenSSL TLS heartbeat read overrun attack. For more information on this vulnerability, read the OpenSSL Security Advisory. The TLS heartbeat in the current OpenSSL version 1.0.1c is disabled so that any heartbeat request will be ignored by the controller. This change fixed the issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.3 or later versions.

Resolved Issues in ArubaOS 6.4.0.2

The following issues were resolved in ArubaOS 6.4.0.2.

Application Monitoring (AMON)

Table 181: *AMON Fixed Issues*

Bug ID	Description
94570	**Symptom:** Incorrect roles were displayed in the WebUI dashboard for the clients connected to RAPs in split-tunnel mode. This issue was resolved by resetting the flag that populates the client role value in the dashboard. **Scenario:** This issue was not limited to any specific controller model or release version.

AP-Platform

Table 182: *AP-Platform Fixed Issues*

Bug ID	Description
95893	**Symptom:** When an AP sent a DHCP request, it received an IP address 0.0.0.0 from the Preboot Execution Environment (PXE) server. Though the AP accepted this IP address, the AP could not communicate further and rebooted. The fix ensures that the PXE acknowledgment is ignored and the AP receives a valid IP address. **Scenario:** This issue was observed in deployment scenarios that have a DHCP server and multiple PXE servers. This issue was observed in APs running ArubaOS 6.3 or earlier.
96051 96754 98008	**Symptom:** AP-115 access points rebooted unexpectedly. This issue is resolved by adding a device queue status check before sending data to an Ethernet driver. **Scenario:** A crash occurred when the throughput was high on Ethernet connected to a 100/10M switch. This issue was observed in AP-114 and AP-115 access points running ArubaOS 6.3.x and later versions.
96239 95472	**Symptom:** When an AP was configured with a static IP address, the Link Aggregation Control Protocol (LACP) on AP-220 Series access points was not functional. This issue is resolved by initiating a LACP negotiation when an AP with a static IP is identified. **Scenario:** This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.3 and 6.4.0.1 when configured with a static IP.
96913	**Symptom:** When a controller was upgraded from ArubaOS 3.4.4.3 and above, or ArubaOS 5.0.x (5.0.3.1 or later), or ArubaOS 6.0.x (6.0.1.0 or later) to ArubaOS 6.4.0.1, APs failed to upgrade to ArubaOS 6.4.0.1. A defensive check is made in affected API so that PAPI messages which are smaller than PAPI header size are handled properly in ArubaOS 6.0.x compared to ArubaOS 5.0.x. **Scenario:** This issue was observed in APs running ArubaOS 3.x, or ArubaOS 5.0.x (5.0.3.1 or later) or ArubaOS 6.0.x (6.0.1.0 or later). APs running ArubaOS 6.1 and later versions are not impacted.
97544	**Symptom:**RAP-109 could not be used on un-restricted controllers that do not have Japan country code. This issue is resolved by mapping the country code in AP regulatory domain profile to the AP regulatory domain enforcement. **Scenario:** This issue was observed when the Instant AP with Japan Stock-Keeping Unit (SKU) was converted to Remote AP running ArubaOS 6.3.1.3.

AP-Regulatory

Table 183: *AP-Regulatory Fixed Issues*

Bug ID	Description
95759	**Symptom:** RADAR detection and channel change events were observed in APs on Russia country code. The issue is fixed by correcting the country domain code for Russia. **Scenario:** This issue was not limited to any specific AP model or ArubaOS release version.

AP-Wireless

Table 184: *AP-Wireless Fixed Issues*

Bug ID	Description
86184	**Symptom:** Wireless clients were unable to associate to an access point on the 5 GHz radio. This issue is resolved by making code level changes to ensure that an APs channel is changed after radar detection. **Scenario:** This issue was observed when a channel change in an access point failed after a Dynamic Frequency Selection (DFS) radar signature detection. This issue was observed in AP-125 running ArubaOS 6.1.x, 6.2.x, 6.3.x.
96751	**Symptom:** An AP continuously crashed and rebooted due to out of memory. Disabling wireless and rogue AP containment features in the **Intrusion Detection System (IDS**) profile resolved this issue. **Scenario:** This issue occurred when wireless and rogue AP containment features were enabled on the IDS profile. This issue was observed on AP-220 Series running ArubaOS 6.3.1.2 version.
97818	**Symptom:** Zebra® QL 420 Plus mobile printer did not associate with AP-220 Series access points. Improvements in the wireless driver of the AP in ArubaOS 6.4.0.2 resolved the issue. **Scenario:** This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.2 or later versions.

Base OS Security

Table 185: *Base OS Security Fixed Issues*

Bug ID	Description
93537	**Symptom:** Wireless clients did not get a Dynamic Host Configuration (DHCP) IP. This issue is resolved by enabling both IP Mobility and MAC authentication, so that user gets an IP address even if the MAC authentication fails due to configuration error or connectivity issues. **Scenario**: This issue was observed when L3 mobility was configured on the controller and MAC authentication failed for the client, which caused mobile IP to drop packets from the client. This issue was not limited to any specific controller model or release version.
96458	**Symptom:** A controller rebooted with the reboot cause **Nanny rebooted machine - low on free memory**. This issue is resolved by freeing the memory that was leaking in the authentication module. **Scenario:** This issue was observed for VPN users when the **cert-cn-lookup** parameter was disabled under **aaa authentication vpn** profile. This issue was not limited to a specific controller model or release version.
96755	**Symptom:** Wired 802.1X using EAP-MD5 authentication failed. This issue is resolved by the modifying the authentication code to allow the wired-clients that perform authentication using EAP-MD5 authentication framework. **Scenario:** This Issue was observed when wired clients connected directly either to the controller or to the Ethernet port of a Campus AP or Remote AP. This issue was not limited to a specific controller model or release version.

Captive Portal

Table 186: *Captive Portal Fixed Issues*

Bug ID	Description
92927 94414 97765	**Symptom:** When Apple® iOS 7 clients tried to connect through the Captive Portal profile, the users were not redirected to the next page even after a successful authentication. A change in the redirect URL has fixed this issue. **Scenario:** This issue was observed only in clients using Apple iOS 7 devices.

Controller-Datapath

Table 187: *Controller-Datapath Fixed Issues*

Bug ID	Description
92657	**Symptom:** Although the **prohibit-arp-spoofing** parameter was disabled in firewall, clients were getting blacklisted with reason **ARP spoofing**. Controlling the action on ARP-spoofing only by the **prohibit-arp-spoof** parameter and on ip-spoofing only by the firewall **prohibit-ip-spoof** parameter fixed the issue. **Scenario:** This issue was not limited to a specific controller model or release version.
93582	**Symptom:** A7210 controller crashed. The logs for the event listed the reason for the crash as **datapath timeout**. Ensuring that the destination UDP port of the packet is PAPI port while processing Application Level Gateway (ALG) module resolved this issue. **Scenario:** This issue was observed in 7210 controllers running ArubaOS 6.3.1.0.
95939 96156	**Symptom**: The local controller crashed as buffer allocation requests were queued to a single processor that resulted in high CPU utilization. This issue is resolved by distributing allocation requests to different CPUs to balance the load across all processors. **Scenario**: This issue was observed in 7200 Series controllers running ArubaOS 6.3.

Controller-Platform

Table 188: *Controller-Platform Fixed Issues*

Bug ID	Description
96420 88234 91172 93465 93913 94754 95664 97384 97761	**Symptom:** A local controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as **Kernel Panic**. This issue is resolved by making code level changes to handle chained buffer punts to the CPU. **Scenario:** This issue was observed when the local controller received an Aggregate MAC Service Data Unit (AMSDU) packet sent by the clients as fragmented multiple packets which triggered internal conditions. This issue was observed in 3600 controllers running ArubaOS 6.3.1.2.

IPsec

Table 189: *IPsec Fixed Issues*

Bug ID	Description
95634 97749	**Symptom:** Site-to-Site IPsec VPN tunnels randomly lost connectivity on a 7210 controller. This issue is resolved by making code level changes to ensure that the key length matches. **Scenario:** This issue was observed when there were 500 or more remote sites terminating IPsec VPN tunnels on a 7210 controller running ArubaOS 6.3.1.2.

Mobility

Table 190: *Mobility Fixed Issues*

Bug ID	Description
83927	**Symptom:** When the primary HA went down, the alternate HA did not become the home agent for a roaming client although the **auth-sta-roam** parameter was disabled. This issue is resolved by creating a user-entry on the alternate HA using user information from the primary HA when the primary HA goes down. **Scenario:** This issue was observed on controllers running ArubaOS 6.3 in a setup containing an HA, FA, and an alternate HA with L3 mobility enabled and the **auth-sta-roam** parameter disabled.
96207 96214 96222 96555	**Symptom:** The client did not receive an IP address through DHCP, and could not pass traffic when L3 mobility was enabled on the controller. This issue is resolved by clearing the state machine of the affected client. **Scenario:** This issue was observed when the client roamed from a Virtual AP (VAP) in which the **mobile-ip** parameter was enabled to a VAP in which the **mobile-ip** parameter was disabled. This issue was observed in ArubaOS 6.3 and later versions, but was not limited to a specific controller model.

RADIUS

Table 191: *RADIUS Fixed Issues*

Bug ID	Description
96038	**Symptom:** Sometimes, the user name was missing in the RADIUS accounting **STOP** messages sent from the controller. The fix ensures that a check is added for user entries with multiple IP addresses before revoking authentication. **Scenario:** This issue was observed when the controller revoked authentication for user entries with multiple IP addresses. This issue was not limited to any specific controller model or release version.

Remote AP

Table 192: *Remote AP Fixed Issues*

Bug ID	Description
97009	**Symptom:** A RAP failed to establish a PPPoE connection when the RAP's up-link port was VLAN tagged. The fix ensures that the RAP can establish a PPPoE connection with VLAN tag. **Scenario:** This issue was observed in RAPs running ArubaOS 6.3.1.3.

Station Management

Table 193: *Station Management Fixed Issues*

Bug ID	Description
86620 88646	**Symptom**: The **show ap association client-mac** command showed client MAC addresses for clients that aged out beyond the idle timeout value. This issue is resolved by making code level changes to station table in the STM module. **Scenario**: This issue was not limited to a specific controller or ArubaOS release version.

Voice

Table 194: *Voice Fixed Issues*

Bug ID	Description
94038 94600	**Symptom:** The **show voice call-cdrs** and **show voice client-status** commands displayed incorrect state transitions for consulted, transfer, and speaker announced call scenarios. The fix ensures the state transitions for New Office Environment (NOE) application layer gateway. **Scenario:** This issue was observed in an NOE deployed voice environment with controllers running ArubaOS 6.1 or later versions.

WebUI

Table 195: *WebUI Fixed Issues*

Bug ID	Description
68464 94529 94961	**Symptom:** The user was forced out of a WebUI session with the **Session is invalid** message. This issue is resolved by fixing the timing issue for the exact session ID from cookies in the https request. **Scenario:** This issue was observed when a web page of the parent domain name was accessed previously from the same browser. This issue was not limited to any specific controller model or release version.
96465	**Symptom:** Some cipher suites were not working when the operations were offloaded to hardware. This issue was resolved by disabling the cipher suites which were not working with the hardware engine. **Symptom:** This issue was observed during any crypto operation that uses DH key exchange**.**
94818	**Symptom: AP Group** name did not support special characters. With this fix, you can create an **AP Group** name with the following special characters: **" / > < : } { + _) (* & ^ % $ # @ ! [ ] ; , . /**. **Scenario:** This issue was seen when you create an **AP Group** from the **Configuration > WIRELESS > AP Configuration** page of the controller's WebUI. This issue was not limited to any specific controller or release version.

Resolved Issues in ArubaOS 6.4.0.1

The following issues were resolved in ArubaOS 6.4.0.1:

PhoneHome

Table 196: *PhoneHome Fixed Issues*

Bug ID	Description
96789	**Symptom**: Starting with ArubaOS 6.4.0.1, PhoneHome automatic reporting is disabled by default. This is a change in behavior from ArubaOS 6.4.0.0, as this feature was automatically enabled when the controller upgraded to ArubaOS 6.4.0.0. **Scenario**: This change in behavior impacts controllers upgrading to ArubaOS 6.4.0.1.

Resolved Issues in ArubaOS 6.4.0.0

The following issues were resolved in ArubaOS 6.4.0.0.

802.1X

Table 197: *802.1X Fixed Issues*

Bug ID	Description
89106	**Symptom**: A configured CLASS attribute was missing from the accounting messages sent from the RADIUS server to clients when previously idle clients reconnected to the network. **Scenario**: This issue occurred in a deployment using RADIUS accounting, where the RADIUS server pushed CLASS attributes in the access-accept messages for 802.1X authentication. When an idle user timed out from the network, ArubaOS deleted the CLASS attribute for the user along with rest of the user data. This issue is resolved with the introduction of the **delete-keycache** parameter in the 802.1X authentication profile, which, when enabled, deletes the user keycache when the client's user entries get deleted. This forces the client to complete a full 802.1X authentication process when the client reconnects after an idle timeout, so the CLASS attributes are again be sent by the RADIUS servers.
92564	**Symptom**: Clients experienced authentication failure when they used 802.1 x authentication. This issue is resolved by increasing the stack size. **Scenario**: The issue occurred due to stack overflow, which caused memory corruption. This issue was observed in 600 Series controllers and 3000 Series controllers running ArubaOS 6.1 and 6.2.

AirGroup

Table 198: *AirGroup Fixed Issues*

Bug ID	Description
88522 92368	**Symptom:** The multicast Domain Name System (mDNS) process of AirGroup crashed and restarted on a controller. This issue is resolved by blocking the memory leak to ensure that the controller is not crashing when the maximum number of servers and users supported on each platform is exceeded. **Scenario:** This issue was triggered when the number of AirGroup users exceeded the limit specified on a platform. This issue was observed in the controllers except 600 Series controllers running earlier versions of ArubaOS 6.4.

Air Management-IDS

Table 199: *Air Management-IDS Fixed Issues*

Bug ID	Description
84148	**Symptom:** The **show wms client** command took a long time to return output. This issue is fixed by retrieving wms client information from the in-memory data structures, instead of sending queries to the database. **Scenario:** This issue occurred when the **show wms client** command was executed. This issue was not limited to any specific controller model or release version.
90330	**Symptom:** An adhoc AP was classified to be manually contained, but it would not be contained unless the **protect from adhoc** feature was also enabled. This issue is resolved by changes that ensure an adhoc AP marked for containment is correctly contained. **Scenario:** This issue was observed in controllers running ArubaOS 6.2 or later.
92070	**Symptom:** The age field in the Real-Time Location System (RTLS) station report sent by an AP was sometimes reset although the station was no longer being heard by the AP. **Scenario:** This issue occurred when the detecting AP can no longer hear frames from the station, but it can still hear frames sent by other APs to the station. This issue could occur on a controller running ArubaOS 6.1 or later.
93912	**Symptom:** Issuing the **show wms client probe** command did not return any output and instead it displayed the **WMS module busy** message after a timeout period. Executing the command with the MAC address of the client fixed this issue. **Scenario:** This issue is observed when there was a large number of entries in the WLAN Management System (WMS) table. This issue is not limited to any specific controller model or ArubaOS version.

AP-Datapath

Table 200: *AP-Datapath Fixed Issues*

Bug ID	Description
90645	**Symptom:** The **show datapath session ap-name command** output did not display **ap-name** option. The command output is now displayed correctly even if the **ap-name** parameter is used. **Scenario:** This issue was observed in controllers running ArubaOS 6.2.1.3 and was not limited to any specific controller model.
94067	**Symptom:** The VLAN in the wired AP is different from the AP's native VLAN. **Scenario:** This issue occurred on the AP-93H device connected to controllers running any ArubaOS version. This issue occurred because the wired driver did not support the extra two bytes used by the internal switch chip.

AP-Platform

Table 201: *AP-Platform Fixed Issues*

Bug ID	Description
86096	**Symptom:** When multiple DNS servers were configured in a local RAP DHCP pool, only the first server in the DNS server list was available to the DHCP client. **Scenario**: This issue was observed in RAPs that were configured to use a local DHCP server and were running ArubaOS 6.2 or 6.3. This issue occurred due to incorrect handling of the DNS servers configured by SAPD.
86112	**Symptom**: The APs went to an inactive state. Changes in the internal code fixed this issue. **Scenario:** This issue was observed when the **named-vlan** parameter was configured in **wlan virtual-ap <name>** command and when all the VLAN IDs were greater than 4064. This issue was not limited to any specific controller model or ArubaOS version.
87775	**Symptom:** A Remote AP (RAP) crashed due to incorrect watchdog feeding. The issue is resolved by ensuring that the hardware watchdog feeding is done periodically. **Scenario:** This issue was observed in RAP-5WN and AP-120 Series access points running ArubaOS 6.3 or earlier versions when there was a high traffic flow in the network.
87857	**Symptom**: Fragmented configuration packets sent from the controller to the AP can cause the AP to come up with the "D:" (dirty) flag. Improvements to how ArubaOS handles out-of-order packets resolve this issue. **Scenario**: This issue is triggered by network congestion or breaks in the connection between the controller and AP.
88288 88568 89040 89135 89137 89252 89254 89255 90021 90028 90495 90604 91016 91392 91393 91755 92585 93336	**Symptom**: 802.11n-capable APs unexpectedly stopped responding and rebooted. Log files for the event listed the reason for the crash as **kernel panic** or **kernel page fault**. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue occurred on AP-125, AP-135, and AP-105 access points running ArubaOS 6.3.0.1.
88389 89882 90175 90332	**Symptom:** 802.11n-capable access points unexpectedly rebooted. The log files for the event listed the reason for the reboot as **kernel page fault**. Improvements in the wireless driver of the AP resolved this issue. **Scenario:** This issue was observed when an 802.11n-capable campus AP was in bridge forwarding mode and there was a connectivity issue between the AP and the controller. This issue was observed in 802.11n-capable access points running any version of ArubaOS.
88504 92678	**Symptom:** No output was displayed when the **show ap config ap-group <ap-group>** command was executed. Increasing the buffer size of SAPM (an AP management module in STM) resolved this issue. **Scenario:** This issue was observed on controllers running ArubaOS 6.3.x.x.

Table 201: *AP-Platform Fixed Issues*

Bug ID	Description
88813 89594	**Symptom:** The **show ap allowed-max-EIRP** command displayed incorrect information for AP-220 Series access points. This display issue is resolved by increasing the buffer size that stores Effective Isotropic Radiated Power (EIRP) information. **Scenario:** This issue was observed in 3200 Series controllers and 3400 Series controllers running ArubaOS 6.3.x.
89016	**Symptom**: The SNMP OID **wlanStaAccessPointESSID** had no value when a client roamed from a down AP to an active AP. Improvements to internal processes that manage layer-2 roaming resolve this issue. **Scenario**: This issue was observed when clients roamed between APs running ArubaOS 6.2.
89041	**Symptom:** A 802.11n-capable access point unexpectedly rebooted or failed to respond. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue was observed when a client disconnected from the network. The issue occurred on 802.11n access points running ArubaOS 6.3.0.1.
89042	**Symptom**: An access point crashed and rebooted frequently. The log files for the event listed the reason for the crash as **kernel panic**. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue was observed in 802.11n access points running ArubaOS 6.3.0.1.
89043 89054 89045	**Symptom**: 802.11n- capable access points unexpectedly rebooted or failed to respond. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario**: This issue was observed on 802.11n-capable access points running ArubaOS 6.3.0.1.
89514 92163 93504	**Symptom:** AP-220 Series access point rebooted repeatedly when connected to a Power over Ethernet (PoE) switch without storing a reboot reason code in the flash memory of the AP. Design changes to the AP-220 Series access point code resolved the issue. **Scenario:** This issue was observed on AP-220 Series access points running ArubaOS 6.3.x or later versions.
89691 94047	**Symptom**: APs stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel page fault**. A change in the route cache has fixed this issue. **Scenario**: This issue occurred when the deletion of the route cache was interrupted. This issue was not limited to any specific controller model or release version.
90854	**Symptom:** On multiport APs (such the AP-93H), the APs bridge priority was configured as 8000 by default. This caused the AP to become a root bridge, when connected to a switch, and the AP became slow. **Scenario:** Starting in ArubaOS 6.4, the default value has been set to 61440 (0xF000), which avoids this issue.
91803	**Symptom:**AP-120 Series controller failed unexpectedly. **Scenario:** This issue occurred on AP-120 Series controller running on ArubaOS 6.3.10. It was due to the AP's memory is low due to heavy traffic or many clients.

Table 201: *AP-Platform Fixed Issues*

Bug ID	Description
88793 91804 92194 92195 92700 92749 93080 93140 93695 93798 93845 93997	**Symptom:** APs stopped responding and crashed due to a higher utilization of memory caused by the client traffic. A change in the AP memory management resolved this issue. **Scenario:** This issue was observed in ArubaOS 6.2 and later versions, but was not limited to a specific controller model.
91820	**Symptom:** An AP crashed and rebooted frequently and the log file for the event listed the reason for the reboot as **Kernel Panic**. Updates to the wireless driver fixed this issue. **Scenario:** This issue occurred while receiving and freeing the buffer memory. This issue was observed in AP-135 access points running ArubaOS 6.3.1.0.
91937	**Symptom:** AP-92 and AP-93 access points were unable to come up with ArubaOS 6.3.x.x-FIPS. ArubaOS 6.3.x.x-FIPS now supports AP-92 and AP-93 access points. **Scenario:** When upgrading to ArubaOS 6.3.x.x.-FIPS, the image size was too big to fit into AP-92's or AP-93's 8 MB flash, and hence was rejecting these access points to come up although these access points required to be supported with 16 MB flash. **NOTE:** Due to the infrastructure limitation, to support 16 MB flash, the code block for 8 MB flash had to be removed as well. So, AP-92 and AP-93 access points with 8 MB flash will also come up with ArubaOS 6.3.x.x-FIPS but it is not supported. Only the AP-92 and AP-93 access points with 16 MB flash are supported with ArubaOS 6.3.x.x-FIPS.
91963	**Symptom:** An AP rebootstrapped with the **Wrong cookie in request** error after a failover from one controller to another. This issue is fixed by enhancements to drop the error message if an AP detected a cookie mismatch when the error message came from a different controller than current the LMS. **Scenario:** This issue occurred after a failover of an AP from one controller to another, and when the AP received the messages from old controller and incorrectly identified as a cookie mismatch. This issue was observed in controllers in a master-local topology with an LMS and a backup LMS configured.
92245	**Symptom:** An AP did not respond with "**aruba_valid_rx_sig: Freed packet on list at ath_rx_tasklet+0x138/0x2880……**" message and needed a manual power cycle to restore the normal status. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.4. **Scenario:** This issue occurred when the buffer was corrupted in wireless driver. This issue was observed in AP-125 model access points associated to controllers running ArubaOS 6.3.1.
92348	**Symptom:** Upstream traffic flow was interrupted and caused IP connectivity issues on MAC OS clients. This issue is fixed by setting the maximum number of MAC service data units (MSDUs) in one aggregate-MSDU (A-MSDU) to 2 and disabling the de-aggregation of AMSDU for tunnel mode VAP. **Scenario:** This issue occurred when the maximum number of MSDUs in one A-MSDU was set to 3, which was not supported in the AP driver. This issue was observed in MacBook Air clients associated with AP-225 access points running ArubaOS 6.3.1.0.
92572	**Symptom:** APs stopped responding and crashed due to a higher utilization of memory caused by the client traffic. A change in the AP memory management has resolved this issue. **Scenario:** This issue was observed in ArubaOS 6.2 and later versions, but is not specific to any controller model.

Table 201: *AP-Platform Fixed Issues*

Bug ID	Description
93012 95172	**Symptom:** Sometimes, a low voice call quality was observed on the clients. This issue is resolved by suspending any off-channel AP operation and ensuring that the voice calls are given higher priority. **Scenario:** This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.0 and earlier versions.
93067	**Symptom:** The authorization for users was unexpectedly revoked and the **show ap client trail-info** CLI command displayed the reason as **Ptk Challenge Failed**. Sending the Extensible Authentication Protocol over LAN (EAPoL) packets as best effort traffic instead of voice traffic resolved this issue. **Scenario:** This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.1 when the virtual AP is configured with WPA-802.1X-AES encryption.
93715 93380 93744 95259 95619 96726 96856 97738 99276	**Symptom:** An unexpected reboot of an AP-220 Series AP occurred due to a kernel panic. Internal software changes resolved this issue. **Scenario:** This reboot was triggered by VAP deletion and can occur upon mode change when all VAPs are deleted. The crash was caused because the PCI device is put to sleep when all the VAPs are deleted but ArubaOS accessed the PCI device before it woke up. This issue was limited to AP-220 Series APs running any version of ArubaOS.
94189	**Symptom:** The enet1 interface of AP-135 did not power up when connected to a data switch. Starting with ArubaOS 6.4, the AP-130 Series supports full functionality when powered by an 802.3af Power over Ethernet (PoE) power source. **Scenario:** The issue was observed when the AP was connected to an 802.3af PoE power source. This issue was observed in AP-135 access points, but is not specific to any version of ArubaOS.
94279 94720	**Symptom:** A regulatory mismatch was observed on non-US controllers after an IAP was converted to a controller based AP. This issue is resolved by adding a new rule to verify the RW domain and accept RW APs on non-US controllers. **Scenario:** This issue was observed in IAP-224, IAP-225-RW, IAP-114, and IAP-115-RW.
94456	**Symptom:** Users observed AP reboot issues with two source mac addresses from the same port. This issue is fixed by not allowing ICMPv6 packets before Ethernet 1 is bonded even when it is UP. **Scenario:** This issue occurred when Ethernet 1 acted as uplink on an AP and the first ICMPv6 packet was sent with source MAC address of Ethernet 1. However, the successive ICMPv6 packets were sent with the source MAC of Ethernet 0 and caused AP reboot. This issue was not limited to any AP, controller models, and ArubaOS release version.

AP Regulatory

Table 202: *AP Regulatory Fixed Issues*

Bug ID	Description
86764	**Symptom:** The output of the **show ap allowed channels** command incorrectly displayed that 5 GHZ channels were supported on AP-68 and AP-68P. This issue is resolved by modifying the allowed channel list for AP-68 and AP-68P. **Scenario:** This issue was observed in AP-68 and AP-68P running ArubaOS versions 6.1.x, 6.2.x, or 6.3.
90995	**Symptom:** The Effective Isotropic Radiated Power (EIRP) was inconsistent and in some instances greater than the MaxEIRP, for HT20 and W52. This issue is resolved by updating the algorithm to consider the maximum EIRP for all modulation schemes. **Scenario:** This issue was observed in M3 controllers running ArubaOS 6.1.3.6.

AP-Wireless

Table 203: *AP-Wireless Fixed Issues*

Bug ID	Description
67847	**Symptom:** APs unexpectedly rebooted and the log files listed the reason for reboot as **Data BUS error**. A change in the exception handling module has fixed this issue. **Scenario:** This issue was observed in AP-120 Series and AP-68P devices connected to controllers running ArubaOS 6.3.1.2. **Duplicate Bugs:** 69062, 69346, 71530, 74352, 74687, 74792, 75212, 75792, 75944, 76142, 76217, 76715, 77273, 77275, 78118, 80735, 82147, 83242, 83243, 83244, 83624, 83833, 84170, 84339, 84511, 85015, 85054, 85086, 85367, 85959, 88515, 89136, 89253, 89256, 89816, 90603, 91084, 92871, 92877, 92878, 92879, 93923.
69424 71334 74646 75248 75874 78978 78981 79891 80054 85753 87250 87360 88619 88620 88989 89537 91689 92641 92975 93079 93455 93811 91689	**Symptom:** When upgraded to ArubaOS 6.2, AP-125 crashed and rebooted. Reallocating the ArubaOS loading address in memory fixed the issue. **Scenario:** This issue was observed when upgrading to ArubaOS 6.2 from ArubaOS 6.1.3.2 and later in any deployment with an AP-125.
86398	**Symptom**: The output of the **show ap debug system-status** command showed an unexpectedly large increase in the buffers in use for queue 8. Changes in how unfinished frames are queued prevents an error that allowed this counter to increment more than once per frame. **Scenario**: This occurred in AP-135 and AP-115 access points running ArubaOS 6.3.x.x, and managing multicast traffic without Dynamic Multicast Optimization (DMO).
86456	**Symptom**: A controller running ArubaOS 6.3 with an AP-125 running as a RAP rebooted unexpectedly. This was caused when the AP received a BC/MC auth frame and failed. **Scenario**: This issue occurred on an AP-125 access point running ArubaOS 6.3.
86584	**Symptom:** The AP-225 did not support prioritization for multicast traffic. **Scenario:** This issue was observed on theAP-220 Series running ArubaOS 6.3.x.
88282	**Symptom**: AP-220 Series access points running ArubaOS 6.3.0.1 stopped responding and rebooted. The log files for the event listed the reason for the crash as **kernel panic: Fatal exception**. ArubaOS memory improvements resolve this issue. **Scenario**: This issue occurred in a master-local 7200 Series controller topology where the AP-220 Series AP terminated on both the controllers in campus mode.

Table 203: *AP-Wireless Fixed Issues*

Bug ID	Description
88328	**Symptom:** Wireless clients experienced packet loss when connecting to remote AP that was in bridge mode. The fix ensures that some buffer is reserved for transmitting unicast traffic. **Scenario:** This issue was observed in AP-105 running ArubaOS 6.1.3.8 when there was a huge multicast or broadcast traffic in the network.
88385 94033	**Symptom**: Bridge mode users (802.1x and PSK) are randomly unable to associate to a RAP. Adding reference count for messages between authentication and Station management processes to avoid incorrect order of messages resolved this issue. **Scenario**: This issue occurred because of the incorrect order of messages between authentication and station management processes. This issue was observed in controllers running ArubaOS 6.3.0.1 or later.
88741	**Symptom:** Throughput degradation was observed on the AP-225. **Scenario:** This issue was caused by an internal ArubaOS malfunction and was observed only in AP-225.
88771 88772 91086	**Symptom:** 802.11n capable access points stopped responding and rebooted. The log files for the event listed the reason for the crash as kernel page fault. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1. **Scenario:** This issue was observed only in 802.11n capable access points running ArubaOS 6.3.0.1.
88827 93771	Symptom: An AP stopped responding and reset. Log files listed the reason for the event as **ath_bstuck_tasklet: Radio 1 stuck beacon; resetting**. Changes in the ArubaOS 6.4 channel change and radio reset routines prevent this error. **Scenario**: This issue occurred in an AP-125 running ArubaOS 6.2.1.3, and was not associated with any controller model.
89442 93804	**Symptom:** The AP-220 Series controllers crashed frequently. Log files listed the reason for the event as **Kernel Panic: Unable to handle kernel paging request**. **Scenario:** This issue occurred when the radio mode was altered between Monitor and Infrastructure. This issue was observed only in AP-220 Series controllers running ArubaOS 6.3.1.2.
88631 88044 88569 88843 89044 89046 89053 89058 89325 89326 89811 89901 90890 92076 92336 92786 93335	**Symptom:** An access point stopped responding and continuously rebooted. Improvements in the wireless driver of the AP fixed this issue. **Scenario:** This issue was observed in AP-220 Series running ArubaOS 6.3.0.1 when clients disconnected from the network.
89460	**Symptom:** When APs used adjacent DFS channels, the AP-135 falsely detected RADAR and exhausted all DFS channels. If no non-DFS were enabled, the AP stopped responding to clients. **Scenario:** This issue was observed in an AP-135 running ArubaOS 6.3.x and 6.2.x. It was caused when APs used adjacent DFS channels.

Table 203: *AP-Wireless Fixed Issues*

Bug ID	Description
89735 89970 90572 91140 91560 91620 92017 92428 93373	**Symptom:** The Ethernet interface of an 802.11ac capable AP restarted frequently. Changes in the internal code fixed this issue. **Scenario:** This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.0 and later versions.
90960	**Symptom**: Microsoft® Surface Pro and Surface RT clients were unable to acquire an IP address or correctly populate the ARP table with a MAC address when connecting to an AP using 20 MHz channels on 2.4 GHz or 5 GHz radios. This issue is resolved by channel scanning improvements to APs in 20 MHz mode. **Scenario**: This issue was triggered when Microsoft Surface clients running Windows 8 or Windows 8.1 connected to 20 MHz APs running ArubaOS 6.1.3.8.
91192	**Symptom**: Poor performance was observed in clients connecting to an AP due to non-WiFi interference. Implementing the Cell-Size-Reduction feature in AP-220 Series along with deauthorizing clients when they are about to go out of the desired cell range resolved this issue. **Scenario**: This issue was observed in AP-220 Series connected to controllers running ArubaOS 6.3.1.1 or earlier.
91373	**Symptom:** MacBook clients were unable to pass traffic on the network. This issue was resolved by changes to ArubaOS that require APs to send data frames to all connected clients. **Scenario:** This issue was observed in AP-220 Series access points that were upgraded to ArubaOS 6.3.1.0, and was triggered by virtual APs being enabled or disabled, either manually (by network administrators) or automatically, as a part of the regular AP startup process.
91374	**Symptom**: Latency issues occur when clients are connected to a single AP. **Scenario:** This issue occurred on an AP-225 access point on a controller running ArubaOS 6.3.1 and later. This occurred when clients go into PS mode.
91379 91449 91454 91480 94171 94238 94413	**Symptom:** AP-220 Series device unexpectedly crashed. Using the correct structure to fill the information in the outgoing response frame resolved this issue. **Scenario:** The 802.11k enabled client that sent a Neighbor Report Request frame caused the AP-220 Series device to crash when the packet was freed. This issue was observed in controllers running ArubaOS 6.3.x or later.
91856	**Symptom:** Certain 802.11b clients did not communicate with 802.11n-capable access points. Improvements in the wireless driver of 802.11n-capable access points resolved this issue. **Scenario:** This issue was observed when Denso® 802.11b handy terminals communicated with 802.11n-capable access points on channel 7. This issue was not limited to a specific controller model or release version.

Table 203: *AP-Wireless Fixed Issues*

Bug ID	Description
91770 91802 91805 91946 92052 92102 92260 92550 92552 92554 92555 92557 92559 92561 92562 92736 92788 92790 92873 92976 92977 93756 93757 93963	**Symptom:** AP-135 stopped responding and rebooted. Improvements to the wireless driver in ArubaOS 6.1.3.2 resolved the issue. **Scenario:** This issue occurred when the buffer was corrupted in the wireless driver. This issue was observed in AP-135 running ArubaOS 6.3.1.0.
92346	**Symptom**: When the 80 MHz option is enabled in the RF arm-profile, HT Capabilities in beacon only show 20 MHz support. **Scenario:** This issue occurred on controllers with AP-225 access points running ArubaOS6.3.1 and later.
92626	**Symptom:** An AP crashed and the log files for the event listed the reason for the crash as **kernel panic**. This issue is fixed by referencing the valid memory. **Scenario:** This issue occurred when an invalid memory was referenced. This issue occurred in AP-225 access points running ArubaOS 6.3.1.1.
92775 96408	**Symptom:** Wireless clients received Automatic Private IP Address (APIPA) when associated to AP-225. Improvements in the wireless driver of the AP fixed the issue. **Scenario:** This issue was seen when wireless clients associated to encryption-enabled tunnel-mode Virtual AP (VAP) on the AP-225 and there was one or more bridge or decrypt-tunnel VAPs configured with encryption mode set to **static-wep**.
93113	**Symptom:** Windows 7 clients using Intel 4965 NIC intermittently stopped passing traffic when connected to AP-225. Changes in the internal code resolved this issue. **Scenario:** This issue occurred on AP-225 running ArubaOS 6.3.1.1.
93288	**Symptom:** Some clients with low signal strength had trouble sending packets to an AP. Implementing the Cell-Size-Reduction feature on AP-220 Series along with deauthorizing clients when they are about to go out of the desired cell range resolved this issue. **Scenario:** This issue was observed in AP-220 Series connected to controllers running ArubaOS 6.3.1.1 or earlier.
93476	**Symptom:** Sporadic input/output control errors were seen in the logs of many APs. Changes in the internal code resolved this issue. **Scenario:** This issue was observed when the authentication manager tries to set the keys for previous association, then station sends deauthentication, or the AP disconnects the station.

Table 203: *AP-Wireless Fixed Issues*

Bug ID	Description
93710 94370	**Symptom:** Vocera clients associated to an AP were unable to communicate with the Vocera server. This issue was resolved by limiting the multicast transmission rate so that the unicast transmission is not affected. **Scenario:** This issue occurred when multicast traffic blocked hardware and software queues resulting in unicast packets being dropped. This issue is observed in AP-225 connected to controllers running ArubaOS 6.3.1.1.
93996	**Symptom:** AP-120 Series access point rebooted unexpectedly. This issue is resolved by making changes to the internal code to avoid a potential condition that causes an infinite loop and NMI watchdog condition which causes the AP to reboot. **Scenario:** This issue occurred in AP-120 Series devices connected to controllers running ArubaOS 6.3.1.0.
94059 94520 95057 95106 95107	**Symptom:** An AP rebooted due to unhandled kernel unaligned access. **Scenario:** This issue was observed in AP-120 Series access points when the controllers were upgraded from ArubaOS 6.1.3.7 to 6.1.3.9, but is not limited to any specific controller model.
94117	**Symptom**: Clients are unable to connect to a SSID when the **Local Probe Request Threshold** setting in the SSID profile (which defines the SNR threshold below which incoming probe requests are ignored) is set to a value of 25 dB. This issue is resolved by changes that allow the AP to respond to probe requests with the same dB value as the local probe request threshold. **Scenario**: This issue was triggered in ArubaOS 6.3.1.x because when the Local Probe Request Threshold setting had a value of 25 dB in this setting, the AP did not respond to probe requests with SNR higher than 35 dB. As a result, APs did not respond to authentication requests from the clients, preventing them from associating to the AP.
94155 94249	**Symptom:** AP-225 device rebooted unexpectedly when connected to a PoE. This issue is resolved by making code level changes in the index table. **Scenario:** This issue occurred due to the drastic peak in power when AP-225 is connected to 3af PoE (Power over Ethernet) and operates in low-power mode. This issue was observed in AP-225 connected to controllers running ArubaOS.
94164 94534	**Symptom:** Wireless clients were unable to connect to an AP through the G band when the WPA2 authentication scheme was used. This issue is resolved by changing the initial value of VHT (Very High Throughput) to **0**. **Scenario:** This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.1.
94198	**Symptom:** An AP rebooted unexpectedly with the log error message out of memory. **Scenario:** This issue occurred on the AP-120 Series running ArubaOS 6.3.1.0.
95006	**Symptom:** IOS devices faced connectivity issues after upgrading from 6.1.3.8 to 6.3.1.2.This issue is resolved by revising the received signal strength indication (RSSI) threshold value that triggers the handoff assist. **Scenario:** This issue was observed in controllers running ArubaOS 6.2 and 6.3 when the RSSI dropped below the defined threshold value.

ARM

Table 204: *ARM Fixed Issues*

Bug ID	Description
93312	**Symptom:** When location server was configured on the controller, a connected Air Monitor (AM) mode AP did not generate a probe report unless the location-feed flag was manually set through the AP console. **Scenario:** This issue occurred could occur on any model of AP operating in AM mode running ArubaOS 6.3.x.x.

Authentication

Table 205: *Authentication Fixed Issues*

Bug ID	Description
94629	**Symptom:** The clients connected to RAPs lost connectivity when the process handling the AP management and user association crashed. This fix ensures that the AP management and user association process does not crash. **Scenario:** This issue was observed in controllers running ArubaOS 6.3 and 6.4.
94964	**Symptom:** Captive Portal users were forced to re-authenticate every 5-10 minutes as users were not sending the IPv6 traffic. This issue is resolved by making code level changes in the authentication module. **Scenario:** This issue was observed when wired users connected to an AP and IPv6 was enabled on the controller. This issue was limited only to release versions that supported IPv6 features.

Base OS Security

Table 206: *Base OS Security Fixed Issues*

Bug ID	Description
86141 93351 93726	**Symptom:** Issuing the **show global-user-table list** command displayed duplicate client information. Ignoring the master controller IP query in Local Management Switch (LMS) list fixed the issue. **Scenario:** This issue was observed in a VRRP or master-local deployment where the master controller queried itself and the LMS list resulted in duplicate client information. This issue was observed in controllers running ArubaOS 6.3.X.0.
86867	**Symptom:** When a user-role and the ACL that have the same name and were configured as the ip access-group on the interface for APs/RAPs, the AP/RAP traffic was hitting the user-role ACL instead of the ip access-group ACL. **Scenario:** This issue was observed on controllers running ArubaOS 6.2.1.2.
87405	**Symptom:** Firewall policies were not enforced on certain client traffic when the clients were connected to a RAP in wired mode and configured with a static IP. This issue is resolved by ensuring that the sessions established with untrusted users are deleted and recreated to apply the firewall policies correctly. **Scenario:** This issue was observed when the traffic was initiated by a device or server connected to the controller with an idle client. This issue was not limited to any specific controller model or release version.

Table 206: *Base OS Security Fixed Issues*

Bug ID	Description
87742	**Symptom:** AP group information was not present in the RADIUS packet when the radio was disabled on the AP. The fix ensures that the AP group information is correctly populated in the RADIUS packet even when the radio is disabled. **Scenario:** This issue occurred when the wired clients were connected to the AP where BSSIDs were unavailable due to a disabled radio. This issue was not limited to any specific controller model or release version.
88271	**Symptom**: It was not possible to configure a **deny any any protocol** access control list (ACL) that overrode a statically configured **permit any any protocol** ACL. This issue is resolved by improvements that allow a user-defined ACL to take precedence over a static ACL entry. **Scenario**: This issue was observed on a controller running ArubaOS 6.3.0.1.
89453	**Symptom**: The **show rights** command did not display all the user roles configured in the controller. The output of this command now displays all the user roles configured in the controller. **Scenario** This issue was observed when more than 50 user roles were configured on a controller running ArubaOS 6.2.1.3.
90180	**Symptom**: Re-authentication of the management users was not triggered upon password change. The users are now getting **Password changed, please re-authenticate** message on the console, forcing the user to login again with the new password. **Scenario**: The issue was observed when users were already connected, and the password for these users was changed. The re-authentication message for these users was not shown. This issue was not limited to any specific controller model or ArubaOS version.
90209	**Symptom:** A controller rebooted unexpectedly. The log files for the event listed the reason as **datapath timeout**. **Scenario:** The timeout occurred due to a VIA client sending an SSL fallback packet, where the third SSL record encapsulating the IPSec packet had an invalid IP header. This issue was not limited to a specific controller model and was observed in ArubaOS 6.2.1.2.
90233	**Symptom:** Clients with a logon user role did not age out from the user-table after the logonlifetime AAA timer expired. Users are mpw aged out with the logon user role if the User Derivation Rule (UDR) is configured in the AAA profile. **Scenario**: This issue was observed when UDR was configured in the AAA profile with the logon defined as the default user role. This issue was observed on controllers running ArubaOS 6.2.1.x.
90454	**Symptom**: A remote AP unexpectedly rebooted because it failed to receive heartbeat responses from the controller. Changes to the order in which new IPsec SAs are added and older IPsec SAs are removed resolved this issue. **Scenario**: This issue occurred after a random IPsec rekey, and was triggered when the outbound IPsec SA was deleted before the inbound IPsec SA was added. This removed the route cache for the inner IP, causing the session entry to incorrectly point to the default gateway, and preventing heartbeat responses from reaching the AP.
90904 92079	**Symptom:** In the ArubaOS Dashboard, under **Clients > IP address**, the IP addresses, Role Names, and names of clients connected to a RAP in split tunnel mode were not displayed. **Scenario:** The client information was not being sent correctly to through the controller and, therefore, not being displayed in the dashboard.
91548	**Symptom**: The error message **User licensed count error** appeared in the error log. However, the system functionality was not affected. **Scenario:** This issue occurred on controllers running ArubaOS 6.2.1.3 and later. This occurred when the VIA client connected to a RAP in split-tunnel or bridge-mode and the RAP was connected to the same controller from behind NAT.

Table 206: *Base OS Security Fixed Issues*

Bug ID	Description
92674	**Symptom:** Class attribute was missing in the Accounting STOP packet. This issue is resolved by not resetting the counters when an IPv6 user entry is deleted. **Scenario:** This issue occurred when the counters were reset during an IPv6 user entry aged out. This issue was not limited to any specific controller or ArubaOS version.
92817	**Symptom:** Wireless clients were blacklisted even when the rate of the IP Session did not exceed the threshold value set. This issue is resolved by increasing the storage of the threshold to 16 bits. **Scenario:** This issue was observed if the threshold of the IP Session rate was set to a value greater than 255. This issue was observed in controllers running ArubaOS 6.x.
93066 93868	**Symptom:** The MAPC module on the controller crashed unexpectedly. The log files for the event listed the reason for the crash as **mapc segmentation fault**. Internal code changes in the MAPC module of the controller fixed this issue. **Scenario:** This issue was observed when IF-MAP was configured on the controller to communicate with ClearPass Policy Manager (CPPM). This issue was observed on 7200 Series controllers running ArubaOS 6.3 or later versions.
93130	**Symptom:** A controller reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. This issue is resolved by adding SSL implementation to validate a packet before processing it. **Scenario**: This issue was observed when VIA was used to establish a tunnel with the controller, using SSL fallback. This issue was not limited to any specific controller model or ArubaOS version.
93237	**Symptom:** An internal module (Authentication) crashed on the controller. Ignoring the usage of the **equivalentToMe** attribute, which was not used by the master controller resolved this issue. **Scenario**: This issue was observed when the Novell Directory System (NDS) pushed the bulk of user data as the value for the attribute to the master controller. This issue was not limited to any specific controller model or ArubaOS version.
95367	**Symptom:** Issuing **show rules <role-name>** command from the command-line interface of a controller resulted in an internal module (Authentication) crash. Ensuring that Access Control Lists (ACLs) are not configured with spaces in the code resolved the issue. **Scenario:** This issue was observed when a large number of ACL was configured with spaces in their names. This was not limited to any specific controller model or ArubaOS version.

Configuration

Table 207: *Configuration Fixed Issues*

Bug ID	Description
73459 85136 86427 90081	**Symptom:** The output of the **show acl hits** CLI command and the **Firewall Hits** information on the **UI Monitoring** page of the controller WebUI showed inconsistent information. This issue is resolved by displaying consistent information. **Scenario:** This issue occurred because the formatting of the XML response from the controller to the WebUI was incorrect, when the output was beyond the specified limit. This issue was not limited to a specific controller model or release version.
88120	**Symptom**: The **Configuration > Wireless > AP Installation > AP provisioning > Status** tab of the controller WebUI and the output of the commands **show ap database long status up start 0 sort-by status sort-direction ascending** and **show ap database long status up start 0 sort-by status sort-direction descending** do not correctly sort the AP entries in ascending or descending order by up time. Improvements to how the controller sorts APs by status and up time resolve this issue. **Scenario**: This issue was identified in controllers running ArubaOS 6.2.1.2
91903 93462 93631	**Symptom:** The controller's fpcli process crashed when executing the command **show ap tech-support ap-name <ap name>** with a non-existing or incorrect AP name. Now, when this command is executed with a non-existent AP, the CLI returns AP with name "X" not found. **Scenario:** This issue was observed on an M3 controller running ArubaOS 6.1.3.10 but was not limited to a specific controller model.

Captive Portal

Table 208: *Captive Portal Fixed Issues*

Bug ID	Description
87294 87589 92575	**Symptom:** Captive Portal (CP) whitelist that was mapped to the user-role did not get synchronized with the standby controller. Checks in the CP whitelist database fixed this issue. **Scenario:** This issue was observed when a net-destination was created and added to the CP profile whitelist that mapped to the user-role in the master controller. This issue was observed in ArubaOS 6.2.1.2 and was not limited to any specific controller model.
88001	**Symptom:** The domain name whitelist could not be configured using wild card characters in the Captive Portal profile. The fix ensures that the wild card characters are supported while configuring the domain name whitelist. **Scenario:** This issue was not limited to any specific controller model or release version.
88116	**Symptom:** Captive Portal user was incorrectly redirected to the **User Authenticated** page even when the user provided a wrong username or password. The user now gets an **Invalid username or password** error message when providing wrong credentials. **Scenario:** This issue was observed if MSCHAPv2 was used for Captive Portal authentication. This issue was not limited to a specific controller model or release version.
88283	**Symptom:** The captive portal profile used https by default. For authentication, the user was redirected to the https://securelogin.example.com. But if this URL was manually changed to http://securelogin.example.com, then connection remained insecure from that point onwards. The controller now sends a redirect URL using the protocol configured on the controller. **Scenario:** This issue was observed when there was a mismatch between the protocol configured on the AAA profile and the protocol from the browser, This issue was not limited to a specific controller model or release version.

Table 208: *Captive Portal Fixed Issues*

Bug ID	Description
88405	**Symptom**: After successfully authenticating a client using Captive Portal, the browser did not automatically redirect the client to the original URL. **Scenario**: This issue was observed in the 7200 Series controller running ArubaOS 6.3.0.0.
91442	**Symptom:** In the master controller's command line interface **Login** page, the question mark symbol was neither getting pushed nor getting added to the local controller. This issue is resolved by ensuring that the master controller's command line interface accepts the question mark symbol. **Scenario:** This issue was observed while synchronizing the configuration from the master controller to the local controller.
92170	**Symptom:** In Captive Portal, a custom welcome page did not redirect to the original Web page after successful client authentication. Changes in the Captive Portal code to send "url" cookie to the Web browser fixed this issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.0.0 or later versions.
93674	**Symptom**: Clients were unable to access an external captive portal page after the controller reset. Changes in how ArubaOS manages captive portal authentication profiles resolved this issue. **Scenario**: This issue occurred in ArubaOS 6.1.3.x when the controller failed to use the correct ACL entry for a pre-authentication captive portal role.
94167	**Symptom:** When client traffic was moving through an L3 GRE tunnel between a switch and a controller, the controller did not provide the captive portal page to the client. **Scenario:** This issue was observed after an M3 was upgraded to ArubaOS 6.1.3.10. This issue was caused because the controller was unable to find the correct role for the client traffic and, therefore, did to provide the captive portal page.

Controller-Datapath

Table 209: *Controller-Datapath Fixed Issues*

Bug ID	Description
82770	**Symptom:** Using ADP, access points did not discover the master controller after enabling Broadcast/Multicast (BC/MC) rate optimization. With this new fix, enabling BC/MC rate optimization does not block ADP packets. **Scenario:** When BC/MC rate optimization was enabled on the VLAN, the controller dropped ADP packets from access points. This issue was not limited to a specific controller model or release version.
82824	**Symptom**: In some cases, when there was a large number of users on the network (more than 16k), and the **Enforce DHCP** parameter was enabled in the AP group's AAA profile, a user was flagged as an IP spoofed user. Changes to how ArubaOS manages route cache entries with the 'DHCP snooped' flag resolves this issue. **Scenario**: This issue was observed in controllers running ArubaOS 6.3.
83422 85600 87794 88311 88360 88505 88683 88740 88833 88985 89004 89303 89910 90450 90457 90482 90609 90836 91170 91363 91695 92161 92177 92811 93064 93572 93985 94025 94514	**Symptom:** A 7200 Series controller unexpectedly rebooted. The controller log files listed the reason for the event as a **datapath timeout**. Improvements in creating tunnels in the internal controller datapath resolved this issue. **Scenario:** This issue was observed in 7200 Series controllers running ArubaOS 6.2.1.x.
85398 85627	**Symptom:** A controller responded to the Domain Name System (DNS) queries even when the IP domain lookup was disabled. This issue is resolved by ensuring that the DNS service is completely stopped if the IP domain lookup is disabled. **Scenario:** This issue occurred when the controller responded to DNS requests with its own IP. This issue was observed in controllers running ArubaOS 6.1.3.6.

Table 209: *Controller-Datapath Fixed Issues*

Bug ID	Description
85685 85543 87406	**Symptom:** M3 controller running ArubaOS 6.1.3.8 stopped responding and rebooted. The log files for the event listed the reason for the crash as **fpapps: Segmentation fault**. Changes to the process that handles the VLAN interfaces fixed the issue. **Scenario:** This issue was observed when the VLAN interface on the controller constantly switched between an UP and DOWN state, resulting in VRRP status change. This issue was not limited to a specific controller model or ArubaOS release version.
85796 88233 88731 90350 91310 93153 93183	**Symptom:** A controller crash was observed due to a session table entry corruption. This issue is resolved by modifying the method by which the IGMP query is handled over a port channel. **Scenario:** This issue occurred when an IGMP query was triggered on the port channel. This issue was observed in 3000 Series controllers, 7200 Series controllers, and M3 controllers running ArubaOS 6.2.x.
85843	**Symptom**: A controller unexpectedly rebooted. Log files for the event listed the reason for the reboot as **datapath exception**. Memory improvements resolve this issue in ArubaOS 6.4. **Scenario**: This issue was observed in a 7200 Series controller running ArubaOS 6.2.1.1.
87295	**Symptom:** A crash was observed in a controller when it received certain types of DNS packets. This issue is fixed by modifying the internal code to handle the DNS packets correctly. **Scenario:** This issue was observed when the **firewall-visibility** feature was enabled on a controller running ArubaOS 6.2 or later.
88325	**Symptom**: Enabling support for jumbo frames on an uplink interface caused pings larger than 1472 bytes to fail. This issue is resolved by changes that ensure ArubaOS uses the correct default MTU size when jumbo frames are disabled globally, while still enabled on a port. **Scenario**: This issue was observed in ArubaOS 6.3.1.0, on a controller with jumbo frames disabled globally, but enabled on a port.
88469 90779	**Symptom:** A controller denied any FTP download that used Extended Passive mode over IPv4. Modifying the FTP ALG to handle Extended Passive mode correctly resolved this issue. **Scenario:** This issue was observed when an IPv4 FTP client used Extended Passive mode. In such a case, the FTP ALG on the controller detected it as a Bounce Attack and denied the session. This issue was not limited to a specific controller model or release version.

Table 209: *Controller-Datapath Fixed Issues*

Bug ID	Description
87417 87846 87949 88039 88226 88445 89433 89539 89641 90024 90458 90469 90746 90896 91853 92284 92464 92466 92827 92828 92829 92830 92832 94007 95012	**Symptom:** A master controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. Enhancements to the AP driver of the access point fixed this issue. **Scenario:** This issue was observed in 7240 controller running ArubaOS 6.3.1.1 in a master-local topology.
87949 88039 88226 88445 89433 89539 89641 90024 90458 90469 90746 90896 91853 92294 92464 92466 92827 92828 92829 92830 92832 92988 93555	**Symptom:** A controller stopped responding to network traffic and rebooted. The log file for the event listed the reason for the reboot as **datapath timeout**. This fix ensures that the CPU livelock does not recur. **Scenario:** This issue occurred on 7200 Series controllers running ArubaOS 6.3.0.1 and 6.2.x.x.

Table 209: *Controller-Datapath Fixed Issues*

Bug ID	Description
89906 92248 93423 94010 94682 94989 95215 95958	**Symptom:** A controller unexpectedly rebooted and the log file listed the reason for the reboot as **datapath timeout**. This issue is fixed by increasing the stack memory size in the data plane. **Scenario:** This issue was observed when clients using SSL VPN connected to RAP and the controller tried to decompress these packets. This issue is not limited to any specific controller model or ArubaOS release version.
93874	**Symptom:** With Multiple TID Traffic to Temptrak device with AES Encryption, the device drops packets from AP. **Scenario:** This issue was observed on ArubaOS 6.3.1.1 and is specific to 7200 Series controllers. This issue occurred because the controller was using multiple replay counters, which the device did not support.
93466	**Symptom**: The 7200 Series controllers rebooted and the log files for the event displayed the reason for the reboot as **datapath timeout**. This issue is fixed by not forwarding the mirrored packets to monitor port when the monitor port status is down. **Scenario**: This issue was observed when the port monitor was enabled on the controller and then a Small Form-factor Pluggable (SFP) was plugged in the monitor port. This issue was observed in 7200 Series controllers and was not limited to a specific ArubaOS version.
95927	**Symptom:** Winphone devices were unable to pass traffic as the ARP requests from the devices were considered as ARP spoofs . This issue is resolved by using DHCP binding to verify if the IP address acquired by the device was already used by an old user in the controller and avoid incorrect determination of a valid ARP request as spoof. **Scenario:** This issue was observed when the devices acquired an IP address that was used by an old user earlier on the controller. This issue is not limited to any specific controller model or release version.
95588	**Symptom:** GRE tunnel groups sessions initiated by remote clients failed. This issue is resolved by redirecting the traffic initiated only by local clients. **Scenario:** This issue was observed when traffic from remote clients was redirected. This issue was observed in controllers running ArubaOS 6.3 or later.

Controller-Platform

Table 210: *Controller-Platform Fixed Issues*

Bug ID	Description
70068 85684 87008	**Symptom**: An internal controller module stops responding when a user attempts to add or delete a large number of VRRP instances. This issue is resolved by internal work flow enhancements that prevent this issue from occurring. **Scenario**: This error can be triggered by a VRRP state change, enabling or disabling an interface, or adding or deleting a tunnel.
82402 84212 86636 87552 89437 90466 91280 93591 94721 94727 95074 95624 95643 95644	**Symptom:** A controller unexpectedly stopped responding and rebooted. The log files for the event listed the reason for the crash as **httpd_wrap process died**. Verifying the Process Application Programming Interface (PAPI) packet before processing it resolved the issue. **Scenario:** This issue was observed when the PAPI library used by all applications did not filter the broadcast traffic correctly prior to PAPI inspection that caused the applications to crash. This issue occurred in 3400 controllers running ArubaOS 6.2.1.0.
82736 82875 83329 83762 84022 85355 85370 85628 86005 86029 86031 86572 86589 87410 87505 87587 88005 88332 88351 88434 88921 89636 89818 90909 91269 91308 91370 91517 92823 93294 93770 95946	**Symptom:** A controller rebooted unexpectedly. Changes in the watchdog implementation on the controller resolved the issue. **Scenario:** Log files for the event indicated the reasons for the reboot were **soft watchdog reset** or user pushed reset. This issue was identified in ArubaOS 6.1.x.x, and is not limited to any specific controller model.

Table 210: *Controller-Platform Fixed Issues*

Bug ID	Description
83502 83762 85355 85370 86029 86031 88005 89636 92823	**Symptom**: A controller rebooted unexpectedly. Changes in the watchdog implementation on the controller resolved the issue. **Scenario**: Log files for the event indicated the reason for the reboot as **user pushed reset** This issue was identified in ArubaOS 6.1.3.x, and is not limited to a specific controller model.
86107 93279	**Symptom**: The controller stopped processing radius packets every three hours and then resumed after one minute. This issue was resolved by setting **aaa profile <aaa-profile-name>** to **no devtype-classification** for all aaa profiles in use. Then execute the **clear aaa device-id-cache all** command. **Scenario:** An internal process took a backup of the database every three hours, and during this time authentication tried to access information from the database and waited there until backup was complete. Authentication resumed after that. This issue was observed on controllers running ArubaOS 6.2 or earlier.
86216 85566 87090 87635 88321 88387 88699 89436 89727 89839 89911 90162 90338 90481 91193 91387 91941 92139 92187 92516 92808 93630 93693 93931 94308	**Symptom:** During a kernel panic or crash, the panic dump generated by the controller was empty. New infrastructure has been added to improve the collection of crash dumps. **Scenario:** This issue impacts 3000 Series, 600 Series, and M3 controllers and was observed on ArubaOS 6.1.3.7.
86266	**Symptom**: In rare cases, issuing commands through a telnet shell caused an internal controller process to stop responding, triggering an unexpected controller reboot. This issue is resolved by changes that prevent ArubaOS from referencing null pointers within the software. **Scenario**: This issue was triggered by varying sequences of commands issued via the telnet shell, and is not specific to a controller model or release version.
87498	**Symptom**: An internal process (FPAPPS) failed unexpectedly. **Scenario:** This issue occurred on a 3200 controller running ArubaOS 6.3.0.1 when the PPOE/PPP connection was established.

Table 210: *Controller-Platform Fixed Issues*

Bug ID	Description
89155	**Symptom**: 600 Series controllers experienced high levels of CPU usage while booting, triggering the warning messages **Resource 'Controlpath CPU' has exceeded 30% threshold.** This issue is resolved by changes to internal CPU thresholds that better reflect expected CPU usage levels. **Scenario**: This issue was observed in controllers running ArubaOS 6.1.2.3.
90751 90633 90863 91154 91138 91474 91656	**Symptom:** Controllers continuously stopped responding and rebooted. Enhancements to memory allocation resolved this issue. **Scenario:** The issue occurred when an internal module (FPCLI) crashed due to memory corruption. This issue was observed in M3 controllers and is not limited to a specific ArubaOS version.
90619 92250	**Symptom:** The controller WebUI stopped responding indefinitely. The fix ensures that the AirWave query fails if there is no firewall visibility. **Scenario:** This issue occurred when AirWave queried for firewall visibility details from a controller on which the firewall visibility feature was disabled. This issue was observed in controllers running ArubaOS 6.2 or later.
91383	**Symptom:** Executing a **show** command causes the controller command-line interface to display an error: **Module Configuration Manager is busy. Please try later.** Improvements to how the controller manages HTTP session keys resolved this issue. **Scenario:** This issue occurred when issuing **show** commands from the command-line interface of a 3000 Series standby controller, and is triggered when the database synchronization process attempts to simultaneously replace and add an HTTP session key in the user database.
91778	**Symptom**: A controller unexpectedly reboots, displaying the error message **Mobility Processor update**. **Scenario**: This issue was observed in a local M3 controller module running ArubaOS 6.3.x.x in a master-local topology.
93990	**Symptom:** A few **Not Found** error messages appeared in the controller's console while performing initial configuration while booting. Modifying the make subsystem, and packaging the binary resolved this issue. **Scenario:** A certain binary was not built correctly due to changes in make or packaging script. This issue was observed in 600 Series controllers running ArubaOS 6.1.x.x or later.
94013 94045 95079	**Symptom:** A controller rebooted due to low memory. Changes in the internal code of the controller software fixed this issue. **Scenario:** This issue occurred when there was continuous high traffic terminating on the control plane. This resulted in an internal component of the ArubaOS software to take up high memory. This issue was observed in 600 Series, 3000 Series, and M3 controllers running ArubaOS 6.1 or later versions.
95044	**Symptom:** All access points went down when the controller to which they were connected rebooted and an error was displayed - **Ancillary image stored on flash is not for this release**. This issue is resolved by writing the boot partition information to the secondary bank of the NVRAM. **Scenario:** This issue occurred when the controller rebooted due to a watchdog reset. This issue is observed only in 7200 Series controllers.

Control Plane Security

Table 211: *Control Plane Security Fixed Issues*

Bug ID	Description
85402	**Symptom:** When sending the RAP whitelist information to CPPM, ArubaOS did not fill the Calling-Station-Id correctly. **Scenario:** The controller returned a Calling-Station-Id value of 000000000000 instead of the actual value. This issue was caused by a malfunction in an internal controller process (auth) and was observed on a controller running ArubaOS 6.3.0.

DHCP

Table 212: *DHCP Fixed Issues*

Bug ID	Description
90611	**Symptom:** The Dynamic Host Configuration Protocol (DHCP) module crashed on a controller and users were not able to perform a new DHCP configuration. The updates to the DHCP wrapper fixed this issue in ArubaOS 6.4. **Scenario:** This issue was triggered by a race condition that caused the DHCP wrapper process to crash with continuous restarts. This issue was not limited to a specific controller model or release version.
92438	**Symptom:** Dynamic Host Configuration Protocol (DHCP) logs were displayed even when the DHCP debug logs were not configured. The fix ensures that the DHCP logs are printed only when the debug log is configured. This issue is resolved by changing the DHCP debug log configuration. **Scenario:** This issue was observed on controllers running ArubaOS 6.2 or later.

Generic Routing Encapsulation

Table 213: *Generic Routing Encapsulation Fixed Issues*

Bug ID	Description
89832	**Symptom:** Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel between L2 connected controllers dropped because of keepalive failures. This issue is fixed by bridging the packets before routing in the forwarding pipeline. **Scenario:** This issue occurred when the GRE tunnel keep alive was enabled and the **Configuration > Network > IP > IP Interface > Edit VLAN (1) > Enable Inter-VLAN Routing** option was disabled. This issue was observed in controllers running ArubaOS 6.3 configured with L2 GRE tunnel between L2 connected switches.

GSM

Table 214: *GSM Fixed Issues*

Bug ID	Description
91870	**Symptom:** The output of the **show ap database** command indicated that a RAP-5 was inactive and that the RAP-5 would not come up. This issue is resolved by increasing the allocation for AP wired ports to 16x. **Scenario:** This issue was observed with RAP-5 APs when all four wired AP ports were enabled in ArubaOS 6.3. ArubaOS 6.3 introduced GSM where space was pre-allocated for the AP wired ports based on the maximum number of APs times the maximum number of wired ports, because RAP-5 has four wired ports and the controller allowed four times the campus APs. As a result, the number of GSM slots was insufficient.

Guest Provisioning

Table 215: *Guest Provisioning Fixed Issues*

Bug ID	Description
87091	**Symptom:** The **Guest Provisioning** page of the WebUI showed incorrect alignment when it was printed from the Internet Explorer 8 or the Internet Explorer 9 Web browser. Improvements in the HTML styles resolved this issue. **Scenario:** This issue was first identified in ArubaOS 5.0.4.0. This issue was not observed when users viewed the controller WebUI using older versions of Internet Explorer (version 6 and 7).

HA-Lite

Table 216: *HA-Lite Fixed Issues*

Bug ID	Description
80206	**Symptom:** The high availability: fast failover feature introduced in ArubaOS 6.3 did not support VRRP-based LMS redundancy in a deployment with master-master redundancy. This topology is supported in ArubaOS 6.4. **Scenario:** This issue occurred because the high availability: fast failover feature does not allow the APs to form standby tunnels to the standby master controller.

Hardware Management

Table 217: *Hardware Management Fixed Issues*

Bug ID	Description
87481	**Symptom:** 7200 Series controller returned an invalid value when an SNMP query was performed on the internal temperature details (OID .1.3.6.1.4.1.14823.2.2.1.2.1.10). The fix ensures that the SNMP attribute is set correctly for the temperature details. **Scenario:** This issue was limited to 7200 Series controllers running ArubaOS 6.3 or later versions.

IGMP Snooping

Table 218: *IGMP Snooping Fixed Issues*

Bug ID	Description
93737	**Symptom:** The **ERROR: IGMP configuration failed** error message was displayed when the **IGMP** proxy was configured using the WebUI. This issue is resolved by ensuring that only one of the following radio buttons - **Enable IGMP**, **Snooping**, or **Proxy** under the **Configuration** > **Network** > **IP** > **IP Interface** > **Edit VLAN** page of the WebUI is enabled. **Scenario:** This issue was not limited to any specific controller model or ArubaOS version.

IPv6

Table 219: *IPv6 Fixed Issues*

Bug ID	Description
88814	**Symptom:** When clients connected to a controller, they received IPV6 router advertisements from VLANs with which they were not associated. This issue is resolved by updating the datapath with the router advertisements conversion flag, so that datapath converts multicast router advertisements to unicast. **Scenario:** This issue was observed in IPv6 networks with derived VLANs and was not limited to a specific controller model or release version.

Licensing

Table 220: *Licensing Fixed Issues*

Bug ID	Description
87424	**Symptom:** The licenses were lost on a standby master controller due to which the configuration on the local controller was also lost. Caching the master controller's license limits on the standby controller for a maximum of 30 days resolved this issue. **Scenario:** This issue occurred when the standby comes up before the master after a reboot. This occurred in all master scenarios when running ArubaOS 6.3 or later.
89294	**Symptom:** RAPs were unable to come up on a standby controller if the AP licenses were installed only on the master controller. **Scenario:** This issue occurred when centralized licensing was enabled and all AP licenses were installed on the master controller and the RAP feature was disabled on the standby controller. This issue was observed in controllers running ArubaOS 6.3.

Local Database

Table 221: *Local Database Fixed Issues*

Bug ID	Description
88019	**Symptom:** A warning message **WARNING: This controller has RAP whitelist data stored in pre-6.3 format, which is consuming .....running the command 'local-userdb-ap del all** appeared when a user logged into the controller. This issue is fixed by deleting the warning file when all the old entries are deleted. **Scenario:** This issue occurred when a controller was upgraded from a previous version of ArubaOS to 6.3 or later version. This issue was not limited to any specific controller model or release version.

Master-Redundancy

Table 222: *Master-Redundancy Fixed Issues*

Bug ID	Description
80041 87032 87946 88067	**Symptom:** The show **database synchronize** command displayed a FAILED message and the standby controller was out of sync with the Master. Additionally, if there is a switchover at this time, the system is in an inconsistent state. This issue is resolved by ignoring any aborted database's synchronization sequence number on the master controller, so that the subsequent database synchronization can proceed without waiting for a response from the standby controller for previous aborted database synchronization. **Scenario:** This issue occurred when a controller was upgraded from a previous version of ArubaOS to 6.3 or later version. This issue was not limited to any specific controller model or release version.

Mesh

Table 223: *Mesh Fixed Issues*

Bug ID	Description
89458 91343 92614	**Symptom:** A Mesh Point rebooted frequently as it could not connect to a Mesh Portal. This issue is resolved by allowing Mesh Point to use the configured power for transmitting probe requests instead of reduced power. **Scenario:** This issue occurred when the transmission power on the Mesh Point was very low compared to the configured power. This issue was observed in AP-105 and AP-175 with controllers running ArubaOS 6.1.x and later versions.

Mobility

Table 224: *Mobility Fixed Issues*

Bug ID	Description
88281	**Symptom:** IP mobility entries were not cleared even when the client leaves the controller and user entries aged out. Additionally, the command **clear ip mobile host <mac-address>** did not clear the stale entry. **Scenario:** This issue was caused by a message loss between the controller's Mobile IP and authentication internal processes. Due to the message loss, the affected clients were blocked. This issue was observed in controllers running ArubaOS 6.3.x, 6.2.x, and 6.1.x.

PPPoE

Table 225: *PPPoE Fixed Issues*

Bug ID	Description
86681	**Symptom**: A controller was not able to connect to the Internet. This issue is fixed by modifying the way Point-to-Point Protocol over Ethernet (PPPoE) handles user name that contains special characters. **Scenario:** The PPPoE connection was not established with an internet service provider (ISP) server when a PPPoE user name contained special characters (for example: #0001@t-online.de). This issue was observed on controllers running ArubaOS 6.1.3.7 or later.
94356	**Symptom:** PPPoE connection did not work with 'ip nat inside' configuration. Changes to the logic that prevented NAT to occur in datapath fixed this issue. **Scenario:** This issue was observed on controllers with uplink as a PPPoE interface, and the client VLAN has 'ip nat inside' enabled.

Remote AP

Table 226: *Remote AP Fixed Issues*

Bug ID	Description
82015	**Symptom:** An AP associated with a controller did not age out as expected when you changed the heartbeat threshold and interval parameters. Changes in the internal code fixed this issue. **Scenario:** This issue occurred when you changed the heartbeat threshold and interval parameters in the AP's system profile while the AP's status is UP in the controller. This issue was not limited to any specific controller, AP model, or ArubaOS release version.
85249	**Symptom:** A degradation of Transmission Control Protocol (TCP) throughput by 9 to 11 Mbps was observed on a RAP. This issue is resolved by optimizing driver code. **Scenario:** This issue occurred in RAPs with any forwarding mode and not specific to any AP model.
85970	**Symptom:** RAPs were rebooting or crashing with a reboot reason as **Kernel page fault at virtual address**. This issue is resolved by adding a check while processing packets with no session entry. **Scenario:** This issue was observed when the RAPs received some packets with no session entries from the IPSec tunnel. This issue was observed only in RAPs running ArubaOS 6.2.x.
86650	**Symptom**: A controller sent continuous RADIUS requests for the clients connected behind the wired port of a remote AP (RAP). This issue is resolved by ArubaOS enhancements that prevent memory corruption. **Scenario**: This issue was observed when a RAP used a PPPoE uplink and operated as a wired AP in split-tunnel or bridge mode. This issue occurred on ArubaOS running 6.1.3.6, and was not limited to any specific controller model.
86934	**Symptom:** The AP failed during boot up when the Huawei® modem E1371 was used. Clearing an empty device descriptor of the modem fixed the issue. **Scenario:** This issue was caused by an internal code error when using this modem. This issue was observed in RAP-108 and RAP-109 running ArubaOS 6.3.
88193	**Symptom:** BOSE WiFi products were not able to acquire an IP address through the internal built-in DHCP server in a RAP-5WN. **Scenario:** This issue occurred on controllers running ArubaOS 6.1.3.9 and later. The DHCP client did not receive an DHCP offer or acknowledgment from the DHCP server.
90355	**Symptom:** AP-70 and RAP-108 access points connecting to the network using a cellular uplink were not able to achieve a 3G connection. This issue is resolved by improvements to the AP boot process, and changes that allow cellular modems to support multiple ports on the AP. **Scenario:** This issue was observed in 6.3.x.x nd 6.2.x.x, when AP-70 and RAP-108 access points connected to a Huawei® E220 Modem.
91106	**Symptom:** When a Remote Access Point (RAP) was rebooted from the controller using the **apboot** command, the system did not generate a log message. Changes to the internal code for handling log messages fix this issue. **Scenario:** This issue was observed in Remote Access Points running ArubaOS 6.1.x.x.
91292	**Symptom:** A Remote AP (RAP) failed over from backup LMS to primary and did not shutdown wired port. This issue is fixed by ensuring that the wired port is shut down initially when a failover occurs from backup LMS to primary LMS and then reconnects to primary LMS. This ensures that the wired port is enabled and the DHCP process is initiated. **Scenario:** This issue occurred when wired clients retained the old IP address retrieved from backup LMS and connected to primary LMS with LMS pre-emption enabled. This issue was observed in RAPs running ArubaOS 6.3.1.0.

Table 226: *Remote AP Fixed Issues*

Bug ID	Description
93707	**Symptom:** The RAP rebootstraps every 6 minutes if the RAP's local gateway IP is 192.168.11.1. **Scenario:** This issue occurred on controllers running ArubaOS6.2.1.4 and 6.3.1.1. It was caused by the DHCP server net assignment conflicting with the RAP's local networks.
94140	**Symptom:** IAP whitelist database on the controller did not allow multiple APs in same branch to share a common remote IP. **Scenario:** Starting with ArubaOS 6.4, this option is now supported. This issue was caused by a typecasting error that prevented smaller IP addresses from being allowed.
94703	**Symptom:** IAP-VPN connection disconnected intermittently. This issue is resolved by not allowing IAP database to store more than six subnets per branch. **Scenario:** This issue was observed when IAP database had more than six subnets-per-branch although a maximum of six subnets-per-branch is allowed. IAP-VPN branch with six subnets went down for more than idle timeout and came up with different DHCP profiles which led to more than six subnet entries for the branch in the IAP database.

Role/VLAN Derivation

Table 227: *Role/VLAN Derivation Fixed Issues*

Bug ID	Description
88508	**Symptom:** User derived roles were not considered for DHCP options. This issue is resolved by removing the ceiling limit set on the packet length. **Scenario:** This issue was observed when the DHCP packet length was greater than 1000 bytes in controllers running ArubaOS versions 6.3.x or earlier versions.

SNMP

Table 228: *SNMP Fixed Issues*

Bug ID	Description
85119	**Symptom:** The **wlsxNLowMemory** trap could not be triggered when the free memory of a controller was low. This issue is fixed by allowing a controller to send the **wlsxNLowMemory** trap, when the free memory of a controller reaches a threshold of 50 Mb. When the free memory of a controller reaches more than 50 Mb, the controller sends the **wlsxMemoryUsageOK** trap. **Scenario:** This issue occurred because the **wlsxNLowMemory** trap was not implemented. This issue was observed in controllers running ArubaOS 6.x.
83948 85146 87842	**Symptom:** The Simple Network Management Protocol (SNMP) module crashed when the management interface was deactivated while an SNMP query was running. A build option was modified to avoid generating code that may access invalid memory. **Scenario:** This issue was observed when SNMP was enabled and AirWave was used to monitor 620 and 3600 controllers running ArubaOS 6.3.0.0.
90453	**Symptom:** The **wlsxStackTopologyChangeTrap** SNMP trap was seen on AirWave from the controller AirWave doesn't support. This issues is resolved by updating to the latest ArubaOS MIBs on AirWave**.** **Scenario:** This issue was observed on controllers running AirWave 7.7.4 and ArubaOS 6.3.0.1.
94205	**Symptom:** The **sysExtFanSTatus** MIB could not be queried**.** This issue is resolved by initializing the value of the fanCount. **Scenario:** This issue was triggered when the **hwMon** process did not return the proper value for fanStatus SNMP queries. This issue occurred in 7200 Series controllers running ArubaOS 6.3.1.1.

Station Management

Table 229: *Station Management Fixed Issues*

Bug ID	Description
85662 84880 88009 88319 89321 89321 91963 92164 93243 93388 93389 93984	**Symptom:** The state of APs were displayed as **down** on the master controller even if these APs were connected and UP. Internal code changes resolved this issue. **Scenario**: This issue was observed when AP's system profile had a local controller as the primary Local Management Switch (Primary-LMS) and master controller was configured as a backup Local Management Switch (Backup-LMS). This issue was not limited to any specific controller model and occurred in ArubaOS 6.3 or later.
86357	**Symptom:** Station Down messages were not logged in the syslog messages. Changes to syslog messaging resolved this issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.3.x.x.
88938 88999	**Symptom:** A controller's internal station management module stopped responding, causing the AP-125 access points associated to that controller to rebootstrap. Improvements to the process that updates internal tables for the client match feature resolve this issue. **Scenario:** This issue occurred on controllers running ArubaOS 6.3.0.1 and using the client match feature.

TACACS

Table 230: *TACACS Fixed Issues*

Bug ID	Description
89676	**Symptom:** Users were not able to authenticate against a TACACS server. **Scenario:** This issue was observed in controllers running ArubaOS 6.1.3.7 and later. This was triggered when non-blocking sockets for TCP connect() were not polled long enough (at least 2-3 seconds are required) before closing the tcp socket.

VLAN

Table 231: *VLAN Fixed Issues*

Bug ID	Description
95622	**Symptom:** The even VLAN distribution did not work correctly as the VLAN assignment number and the AP VLAN usage number did not match. The fix ensures that the VLAN assignment and AP VLAN usage numbers match. **Scenario**: This issue was observed in clients that were frequently roaming when even VLAN distribution was enabled. This issue was observed in controllers running ArubaOS 6.3.1.2.

Voice

Table 232: *Voice Fixed Issues*

Bug ID	Description
77716 88996 90000	**Symptom:** Incompatibility issues observed between a 3600 controller and a Cisco CUCM using SCCP version 20. Users were able to make and receive calls using a Cisco phone but there was no audio. This issue is resolved by changes that allow the controller to handle Open Receive Channel Acknowledge (ORCA) messages for SCCP Version 20. **Scenario:** The Cisco CUCM was compatible with the Skinny Client Control Protocol (SCCP) version 20, while the 3600 controller supported only up to version 17 of the SCCP. This incompatibility issue resulted in media traffic not passing through the 3600 controller as the controller was not able to parse the SCCP signaling packets. This issue was observed in a 3600 controller running ArubaOS 6.0 or later.
86224	**Symptom:** Calls dropped after 30 seconds when performing a blindly transferred SIP call. Ignoring the mid call re-invite message (by SIP ALG state machine) handling process resolves the issue. **Scenario:** This issue was observed on the M3 controller module running ArubaOS version 6.2.1. It occurred when Ascom phones sent a DELTS request upon receiving either an "invite" message from the SIP server or after sending a "180 Ringing" message back to the server.
86683	**Symptom:** The **show voice call-cdrs** and **show voice client-status** command outputs did not display the call details for Lync wired clients with media classification configured on session ACL. This issue is resolved by ensuring to handle the message appropriately for wired clients. **Scenario**: This issue was observed when Lync clients were identified as voice clients via media classification. This issue occurred on ArubaOS running 6.2 and 6.3 versions, and not limited to any specific controller version.
93517	**Symptom:** Access point rebooted unexpectedly resulting in wireless clients losing network connectivity. Releasing CDR events for AP statistics and AP event in the CDR buffer resolved the issue. **Scenario:** This issue was observed in a VoIP deployment when the Station Management (STM) process that handles AP management and user association crashed on the controller. This issue was observed in controllers running ArubaOS 6.1 or later versions.

WebUI

Table 233: *WebUI Fixed Issues*

Bug ID	Description
73459	**Symptom:** The output of the **show acl hits** command and the firewall hits information on the **Monitoring** page of the controller WebUI shows inconsistent information. The issue is resolved by displaying consistent information in the CLI and WebUI. **Scenario:** This issue occurred because the formatting of the XML response from the controller to the WebUI was incorrect, when the output exceeded the specified limit. This issue was not limited to a specific controller model or release version.
76439	**Symptom**: The Spectrum Analysis section of the WebUI fails to respond when a connected spectrum monitor is in a DOWN state. Changes to how ArubaOS manages popup error messages resolve this issue. **Scenario**: This issue occurred in ArubaOS 6.2.0.0, when an AP-105 access point in hybrid AP mode failed to appear as a connected spectrum monitor in the controller WebUI.
85225	**Symptom:** The following two issues were observed when adding an SNMPv3 user under the **Configuration** > **Management** > **SNMP** page of the WebUI: **1. User Name** field was not editable. **2. Privacy Protocol** value changed to null, when the **Authentication Protocol** was edited in SNMPv3 user entry. The first issue is an expected behavior for SNMPV3 users and the button caption is changed to **DONE** in the **Edit** mode. The second issue is fixed by avoiding the **Privacy Protocol** value changing to null. **Scenario:** This issue was not limited to any specific controller model or release version.
87457	**Symptom:** The **PKCS#12 Passphrase** field was incorrectly enabled while provisioning a regular remote AP in the WebUI (under the **Configuration** > **Wireless** > **AP Installation** > **Provision** page). The **PKCS#12 Passphrase** field is now enabled in the WebUI only for provisioning a certificate based remote AP. **Scenario:** This issue was not limited to a specific controller model or software version.
87078	**Symptom:** While accessing **AP Configuration** or **Authentication** options, the system displayed **show aaa authentication mgmt: data null** error. This issue is resolved by restarting an internal process in the controller. **Scenario:** This issue was observed in 3200 Series controllers running ArubaOS 6.1.3.5.
87720	**Symptom:** The **Reset** button on the **Monitoring** page was not functioning correctly. The **Reset** button now resets all Air Monitors correctly. **Scenario:** This issue was not limited to a specific controller model or release version.
88066	**Symptom:** Users were unable to generate Certificate Signing Request (CSR) with a comma in the **Organization** field in the WebUI and displayed a message **Invalid Character(s) Input for Organization**. This issue is fixed by GUI updates to allow comma in the **Organization** field. **Scenario:** This issue occurred only in the WebUI and there was no impact in the Command Line Interface (CLI). This issue was not limited to any specific controller model or release version.
88398	**Symptom:** Network administrators were unable to manually contain or reclassify a group of detected rogue APs in the **Dashboard** > **Security** page of the WebUI. This issue is fixed by adding support to select multiple rouge APs . **Scenario:** This issue occurred when multiple rogue APs were selected in the **Dashboard** > **Security** page. This issue was observed in controllers running ArubaOS 6.2.1.3.
88802 91141	**Symptom:** When the client tried to access the **Air Group** option from the WebUI, the system did not respond. To resolve this issue the **Air Group** option is now removed from the WebUI for 600 Series controllers. **Scenario:** This issue was observed only in 600 Series controllers running ArubaOS 6.3.x.

Table 233: *WebUI Fixed Issues*

Bug ID	Description
89092	**Symptom:** When an administrator added bulk VLANs under **Configuration > Network > VLAN > VLAN ID**, the controller did not add the bulk VLANs and the web page displayed a JavaScript error. Correction in the formatting of the XML response from the controller to the WebUI fixed this issue. **Scenario:** This issue was observed in controllers running ArubaOS 6.4.
90110	**Symptom:** The ArubaOS Campus WLAN Wizard was not accessible. This issue is resolved by changing the LDAP server filter to include an ampersand (&). **Scenario:** The Campus WLAN wizard was not accessible due to the presence of an ampersand (&) in the LDAP server filter. This issue was observed in a 650 controller running ArubaOS 6.2.1.3, but could impact any controller model.
90264	**Symptom:** Layer 2 Tunneling Protocol (L2TP) pool was not displayed when the user-role was configured in the WebUI of a controller without an AP license. This issue is fixed by removing the WLAN_REMOTE_AP license validation while configuring L2TP pool. **Scenario:** This issue was triggered by Policy Enforcement Firewall (PEF) license with WLAN_REMOTE_AP validation while configuring L2TP pool on a controller. This issue was not limited to any specific controller model or release version.
92340 92649	**Symptom:** The WebUI of a controller failed to load in Internet Explorer 11 with the error message **can't create XMLHttpRequest object: Object doesn't support property or method 'creatXMLHttpRequest**. The ArubaOS WebUI is updated to be compatible with the new standards in Internet Explorer 11. **Scenario:** This issue was caused by changes in Internet Explorer 11 from Internet Explorer 10. This issue was observed in Internet Explorer 11 and not limited to any specific controller model or release version.
92620	**Symptom:** When TPM Initialization failed, the following error message was displayed: **TPM Initialization or Certificate Initialization failed. For debug information see /tmp/deviceCertLib.log**. The fix ensures that the error message points to the **show tpm errorlog** command. **Scenario:** This issue was observed when the Trusted Platform Module (TPM) Initialization or Certificate Initialization failed. This issue was not limited to a specific controller model.
93606	**Symptom:** Clients were not displayed in the **Monitoring** > **Controller** > **Clients** page of the WebUI when filtered with AP Name. This issue is fixed by changing the **show user-table location <ap-name>** command to **show user-table ap-name <ap-name>**. **Scenario:** This issue was triggered by changes to CLI commands. This issue was observed in controllers running ArubaOS 6.2 and 6.3.

WLAN Management System

Table 234: *WLAN Management System Fixed Issues*

Bug ID	Description
84146	**Symptom:** WLAN Management System (WMS) slowed down with redundant database queries in a controller. This issue is fixed by ignoring queries to the database that determine if there are more Virtual APs (VAPs) present on the probe. Now, the information on VAP presence can be retrieved from the in-memory data structures. **Scenario:** This issue occurred when many APs rebooted, WMS marked them as down. This caused the WMS to slow down by generating redundant database queries. This issue was not limited to any specific controller model or release version.

XML API

Table 235: *XML API Fixed Issues*

Bug ID	Description
84801	**Symptom:** Clients connected to the local controller were unable to access the Captive Portal (CP) page from an external server. This issue is resolved by configuring the **default-xml-api** parameter in the AAA profile. **Scenario:** This issue was observed when the **default-xml-api** was not configured. This issue was not limited to any specific controller or AP model.

This chapter describes the known and outstanding issues identified in ArubaOS 6.4.x release versions.

Known Issues and Limitations in ArubaOS 6.4.3.1

The following are the known issues and limitations found in ArubaOS 6.4.3.1. Applicable Bug IDs and workarounds are included.

AP-Platform

Table 236: *AP-Platform Known Issues*

Bug ID	Description
109921	**Symptom:** When a Pre-Shared Key (PSK) in the SSID profile is configured it cannot contain single quotes, double quotes, or blank spaces in the same passphrase. **Scenario:** This issue is observed in 7210 controllers running ArubaOS 6.3.1.10. **Platform:** 7210 controllers. **Reported Version:** ArubaOS 6.3.1.10. **Workaround:** None.
114495	**Symptom:** An AP transmits DHCPv6 solicit messages even when the **M** flag in Router Advertisement (RA) is set to 0 and the **O** flag is set to 1. **Scenario:** This issue is observed in an IPv6 network in 600 Series controllers running ArubaOS 6.4.2.3. This issue is caused when an AP sends a solicit message instead of a DHCPv6 information request. **Platform:** 600 Series controllers. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.
115075	**Symptom:** The monitoring tab in the WebUI does not display the information about an access point when the client count is more than 75. **Scenario:** This issue occurs in AP-225 access points connected to standalone master controllers running ArubaOS 6.4.2.4. **Platform:** AP-225 access points. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.
115303	**Symptom:** The status of an AP is displayed as inactive after it is consecutively UP for many days. **Scenario:** This issue is observed in 7240 controllers running ArubaOS 6.4.0.3, with VRRP enabled. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.0.3. **Workaround:** None.
115418	**Symptom:** When the users in the bridge forwarding mode age out, multiple RAPs crash unexpectedly. **Scenario:** This issue is observed in 7220 controllers running ArubaOS 6.4.2.2. **Platform:** AP-93 and AP-103 access points. **Reported Version:** ArubaOS 6.4.2.2. **Workaround:** None.

Table 236: *AP-Platform Known Issues*

Bug ID	Description
115477	**Symptom:** Random AP's reset to factory default settings by themselves and come up on the default group. **Scenario:** This issue is observed in AP-105 access points connected to 3600 controllers running ArubaOS 6.4.2.5. **Platform:** AP-105 access points. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** Re-provision the access point.
116348	**Symptom:** Clients cannot connect to AP-224/AP-225 access points and display **[reason_code Denied: AP Ageout]** error message. **Scenario:** This issue occurs in AP-224/AP-225 access points connected to controllers running ArubaOS 6.4.2.5. **Platform:** AP-224/AP-225 access points. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.
116349	**Symptom:** Randomly, clients cannot associate with a local controller. However, if the access point is rebooted, the clients associate successfully. **Scenario:** This issue is observed in AP-103H, AP-105, and AP-225 access points connected to 7240 controllers running ArubaOS 6.4.2.3. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.

AP-Wireless

Table 237: *AP-Wireless Known Issues*

Bug ID	Description
109745	**Symptom:** Wireless clients are unable to check the Basic Service Set Identifier (BSSID) of the access point, due to a rapid increase in the **Tx Failed Beacons** messages. **Scenario:** This issue is observed in AP-103 access points connected to 7240 controllers running ArubaOS 6.4.2.0. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.0. **Workaround:** Reboot the AP.
113971	**Symptom:** An AP-103H access point reboots randomly without reboot information. **Scenario:** This issue is observed in a master-local topology where the AP-103H access point is connected to wired clients. **Platform:** AP-103H access points. **Reported Version:** ArubaOS 6.4.2.0. **Workaround:** None.
115161	**Symptom:** An AP-225 access point crashes unexpectedly when multiple clients are connected to it. **Scenario:** This issue is observed when Control Plane Security (CPSec) is enabled in the controller. This issue is observed in controllers running ArubaOS 6.4.3 in a master-local topology. **Platform:** AP-225 access points. **Reported Version:** ArubaOS 6.4.3.0. **Workaround:** None.

Table 237: *AP-Wireless Known Issues*

Bug ID	Description
115865	**Symptom:** Clients experience connectivity issues on the G radios of AP-105 and AP-225 access points. **Scenario:** This issue is observed in AP-105 and AP-225 access points connected to 7240 controllers running ArubaOS 6.4.2.5. when striping-ip is configured in ap-lacp-striping-ip. **Platform:** AP-105 and AP-225 access points. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** Remove the striping-ip in the ap-lacp-striping-ip.
116158	**Symptom:** AP-224/AP-225 access points reboot with cause **Reboot caused by kernel panic: Fatal exception**. **Scenario:** This issue occurs in AP-224/AP-225 access points connected to controllers running ArubaOS 6.4.2.5. **Platform:** AP-224/AP-225 access points. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.

ARM

Table 238: *ARM Known Issues*

Bug ID	Description
115215	**Symptom:** The **show ap radio-summary** command displays Co-Channel Interference (CCI) instead of non-Wi-Fi interference. **Scenario:** This issue is observed in AP-225 access points running any version of ArubaOS **Platform:** AP-225 access points. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.

Base OS Security

Table 239: *Base OS Security Known Issues*

Bug ID	Description
108906 112128	**Symptom:** A tunnel fails due to SSL fallback. The log files for the event list the reason for the failure as **SSL tunneling could not be turned on**. **Scenario:** This issue is observed in controllers running ArubaOS 6.4.2.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2. **Workaround:** Reboot the controller.
112845	**Symptom:** The **no netdestinatination <name>** command fails even when there are no net destinations in use. **Scenario:** Net destinations that are not in use could not be deleted. This issue is observed in 7210 controllers running ArubaOS 6.4.2.3. **Platform:** 7210 controllers. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** Restart the authentication process by issuing the **process restart auth** command in the controller CLI.

Captive Portal

Table 240: *Captive Portal Known Issues*

Bug ID	Description
109303	**Symptom:** The controller displays the following error logs frequently for applications like Skype and QQ messenger: • AH01264: script not found or unable to stat: /mswitch/apache/cgi-bin/micromsg-bin, referer • AH00574: ap_content_length_filter: apr_bucket_read() failed, referer • AH00135: Invalid method in request "\xbe(\xaf8\x817\xe8\xe4G\xeaO\xff, referer **Scenario:** This issue is observed when applications use port 443 for a secure connection and applications like Skype send encrypted requests to port 80. This issue is not specific to any controller model or ArubaOS version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.0. **Workaround:** Change the httpd logging level to **critical** by issuing the command, **logging level critical system process httpd**.
116073	**Symptom:** Clients do not get an IP address unless the old user entry is deleted from the controller. **Scenario:** This issue is observed in AP-105 and AP-225 access points connected to 7220 controllers running ArubaOS 6.4.2.5. **Platform:** 7220 controllers. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.

Controller-Datapath

Table 241: *Controller-Datapath Known Issues*

Bug ID	Description
92955	**Symptom:** When sending small-sized data packets at a high speed data rate through an IPsec tunnel, the controller crashes due to a datapath timeout. **Scenario:** This issue is observed when the controller sends IPsec traffic at 400 Mbps with a 64-byte packet size. This causes the controller's ingress queue to run out of buffer. This issue is not limited to a specific controller model or software release version. **Platform:** All platform. **Reported Version:** ArubaOS 6.4.0.0. **Workaround:** None.
93327	**Symptom:** World of Warcraft® online game sessions are not getting classified correctly. **Scenario**: This issue occurs on 7200 Series controllers running ArubaOS 6.4 when AppRF is enabled on the controller. **Platform:** 7200 Series controllers. **Reported Version:** ArubaOS 6.4.0.0. **Workaround:** None.
107982 109009 109489 109891 109929 109981 109985 111795 112598 112715 113655 113928 114634 115296	**Symptom:** The datapath process crashes when Deep Packet Inspection (DPI) is enabled in the **Configuration > Advanced Services > Stateful Firewall > Global Settings** option of the controller WebUI. **Scenario:** This issue is observed in 7210 controllers running ArubaOS 6.4.2.0. **Platform:** 7210 controllers. **Reported Version:** ArubaOS 6.4.2.0. **Workaround:** None.
110159 111832	**Symptom:** A 7240 controller stops responding and reboots unexpectedly. The log files for the event list the reason as **Reboot cause: Datapath timeout**. **Scenario:** This issue is observed when Networking Acceleration Engine (NAE) traffic stalls on the 7240 controller running ArubaOS 6.4.2.1. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.1. **Workaround:** None.
110810	**Symptom:** An M3 controller reboots unexpectedly. The log files for the event list the reason as **datapath crash**. **Scenario:** This issue is observed in M3 controllers running ArubaOS 6.4.x. **Platform:** All platforms **Reported Version:** ArubaOS 6.4.1.0. **Workaround:** None.
112527	**Symptom:** A controller reboots unexpectedly. The log files for the event list the reason for the reboot as **datapath exception**. **Scenario:** This issue is observed in M3 controllers running ArubaOS 6.4.2.3. This issue occurs when the kernel does not send heartbeat messages to the SOS module and SOS in turn does not send heartbeat messages to the control plane. If more than 40 heartbeat messages are not transmitted from SOS to the control plane, the controller reboots. **Platform:** M3 controllers. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.

Table 241: *Controller-Datapath Known Issues*

Bug ID	Description
112651	**Symptom:** The Datapath module crashes, resulting in a controller rebooting unexpectedly. The log files for the event list the reason for the reboot as **datapath exception**. **Scenario:** This issue is observed in 7210 controllers running ArubaOS 6.4.2.0. **Platform:** 7210 controllers. **Reported Version:** ArubaOS 6.4.2.0. **Workaround:** None.
114217	**Symptom:** A controller stops responding and reboots. The log files for the event list the reason as **datapath exception**. **Scenario:** This issue is observed when issuing the **tar log tech-support** command while IPv6 MLD snooping is enabled in the controller. This issue is observed in a 7240 controller running ArubaOS 6.4.2.5. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.
114684	**Symptom:** A controller stops responding and reboots. The log files for the event list the reason as **datapath timeout**. **Scenario:** This issue is observed in 7200 Series controllers where the Aggregate MAC Service Data Unit (AMSDU) feature is enabled. This issue is observed when the crypto engine is interrupted. **Platform:** 7200 Series controllers. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.
115868	**Symptom:** A 7240 controller reboots because of datapath timeout. **Scenario:** This issue is observed in 7240 controllers running ArubaOS 6.4.2.5. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.
116324	**Symptom:** A controller reboots with **Reboot Cause: Datapath timeout (intent:cause:register:56:86:2)** error message. **Scenario:** This issue is observed in 7240 controllers running ArubaOS 6.4.2.4. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.

Controller-Platform

Table 242: *Controller-Platform Known Issues*

Bug ID	Description
114607	**Symptom:** The **httpd** process crashes and results in a controller reboot. **Scenario:** This issue is observed in controllers running ArubaOS 6.4.2.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2. **Workaround:** None.
114603	**Symptom:** The SNMP query to retrieve an **ifAlias** entry returns incorrect value. **Scenario:** This issue is observed when a query to retrieve an **ifAlias** entry is executed after the SNMP server is configured. This issue is observed in 7010 and 3200 controllers running ArubaOS 6.3.1.9 and 6.4.2.5. **Platform:** 7010 and 3200 controllers. **Reported Version:** ArubaOS 6.3.1.9 and 6.4.2.5. **Workaround:** None.
115433	**Symptom:** Users are unable to log in through SSH and a lot of kernel messages are displayed in the controller system logs. **Scenario:** This issue is observed in a 7010 controller running ArubaOS 6.4.2.5 with a Netgear modem. **Platform:** 7010 controllers. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.
115591	**Symptom:** A controller crashes because of memory leak in nanny, aaa, syslogd, and cfgm modules. **Scenario:** This issue is observed in 7240 controllers running ArubaOS 6.4.2.4. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.
115984	**Symptom:** The WMS, STM, and authentication modules crash in a local controller. **Scenario:** This issue is observed in 3600 controllers running ArubaOS 6.4.1.0 in master-local-local topology. **Platform:** 3600 controllers. **Reported Version:** ArubaOS 6.4.1.0. **Workaround:** None.
116085	**Symptom:** A controller reboots unexpectedly with **Kernel panic** error message. **Scenario:** This issue is observed in 3600 controllers running ArubaOS 6.4.2.5. **Platform:** 3600 controllers. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.
116086	**Symptom:** A controller reboots unexpectedly with **Kernel panic** error message. **Scenario:** This issue is observed in 3600 controllers running ArubaOS 6.4.2.5. **Platform:** 3600 controllers. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.

Table 242: *Controller-Platform Known Issues*

Bug ID	Description
116154	**Symptom:** A controller does not save the configuration. **Scenario:** This issue is observed in 7010 controllers running ArubaOS 6.4.2.5. **Platform:** 7010 controllers. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.
116174	**Symptom:** The HTTPD process crashes when running captive portal. **Scenario:** This issue is observed in 7024 controllers running ArubaOS 6.4.3.1. **Platform:** 7024 controllers. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.
116341	**Symptom:** The kernel module of a 7220 controller crashes.. **Scenario:** This issue is observed in 7220 controllers running ArubaOS 6.4.2.4.. **Platform:** 7220 controllers. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.

DDS

Table 243: *DDS Known Issues*

Bug ID	Description
113121	**Symptom:** The controller reports very high Distributed Data Store (DDS) CPU utilization. **Scenario:** This issue is observed when user roaming is high. This issue is specific to 7240 controllers running ArubaOS 6.4.2.3. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** Minimizing user roaming can reduce DDS CPU utilization.

HA-Lite

Table 244: *HA-Lite Known Issues*

Bug ID	Description
115921	**Symptom:** The AP tunnel is not formed on the standby controller. **Scenario:** This issue is observed in AP-224/AP-225 access points connected to 3600 controllers running ArubaOS 6.4.2.5 in master-standby HA configuration. **Platform:** AP-224/AP-225 access points. **Reported Version:** ArubaOS 6.4.2.5. **Workaround:** None.

Licensing

Table 245: *Licensing Known Issues*

Bug ID	Description
112069	**Symptom:** The local controller displays the following warning message: **Licenses sent by the server will expire in 29 days**. This count decreases every day. **Scenario:** An initial investigation suggests that the local controller sends the license heartbeat request but the master controller (where the license server exists) fails to respond. This issue is observed in a master-local topology where the controllers are running ArubaOS 6.4.2.3. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.

Master-Local

Table 246: *Master-Local Known Issues*

Bug ID	Description

110421	**Symptom:** A Pre-Shared Key (PSK) with a double quote (") symbol fails to synchronize with the local controller.
	Scenario: This issue is observed when a PSK is configured with a (") symbol on the master controller. This issue occurs in a master-local topology.
	Platform: All platforms.
	Reported Version: ArubaOS 6.4.2.2.
	Workaround: On the master controller, change the master-local synchronization type to **complete**.
	`(host)(config) #cfgm set sync-type complete`
	`(host)(config) #write config`
	OR
	On adding a PSK in the master controller with the (") symbol, issue the **clear master-local-session <local switch IP address>** command. This induces a full configuration synchronization. Use this option if you do not want a full configuration synchronization every time.

Voice

Table 247: *Voice Known Issues*

Bug ID	Description
87316	**Symptom:** The Call Detailed Record (CDR) for a VoIP client goes into the **ABORTED** state due to a session age-out. **Scenario:** This issue is observed in an L3 mobility deployment if the Real-time Transport Protocol (RTP) packets do not get tunneled to the Home Agent (HA) when a client that has roamed to the Foreign Agent (FA) initiates a Lync call. This issue is observed in controllers running ArubaOS 6.3 or later. **Platform:** All platforms. **Reported Version:** ArubaOS 6.3.1.0. **Workaround:** None.

WebUI

Table 248: *WebUI Known Issues*

Bug ID	Description
114923	**Symptom:** The initialization process is halted if the **no masterip** command is executed after loading a controller. This prevents the execution of the **write-mem** command. **Scenario:** The processes hang if the **no masterip** command is executed before the controller initializes, as the processes cannot find the master IP address. This issue is not specific to any controller or release version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.3.0. **Workaround:** Execute the **no masterip** command after the processes are initialized. If the **no masterip** command is executed before initialization is complete, reload the controller without saving the configuration.

Known Issues and Limitations in ArubaOS 6.4.3.0

The following are the known issues and limitations found in ArubaOS 6.4.3.0. Applicable Bug IDs and workarounds are included.

AP-Wireless

Table 249: *AP-Wireless Known Issues*

Bug ID	Description
109200	**Symptom:** An AP-225 crashes randomly after upgrading to ArubaOS 6.3.1.12. **Scenario:** This issue is observed when the clients connect and send traffic. This issue is observed in 7240 controllers running ArubaOS 6.3.1.12. **Platform:** AP-220 Series. **Reported Version:** ArubaOS 6.3.1.12. **Workaround:** Disable Airtime fairness.
111952	**Symptom:** Clients are unable to pass traffic after waking up from sleep mode. **Scenario:** This issue is observed in an AP-135 running ArubaOS 6.4.2.3. **Platform:** AP-135 access points. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.

Base OS Security

Table 250: *Base OS Security Known Issues*

Bug ID	Description
111127	**Symptom:** An HP Officejet Pro 8500 A910® printer with b/g/n radios are unable to obtain an IP address. **Scenario:** This issue is observed during wpa-psk-aes authentication in controllers running ArubaOS versions 6.4.2.3 and later. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.

Configuration

Table 251: *Configuration Known Issues*

Bug ID	Description
108743 108744 108746 108747	**Symptom:** The configuration process crashes. **Scenario:** This issue is observed in 620 controllers running ArubaOS 6.4.2.2. **Platform:** 620 controllers. **Reported Version:** ArubaOS 6.4.2.2 **Workaround:** None.

Controller-Datapath

Table 252: *Controller-Datapath Known Issues*

Bug ID	Description
88629	**Symptom:** ACL enforcement for Microsoft® Skype doesn't work consistently. **Scenario:** This issue occurs on 7200 Series controllers running ArubaOS 6.4 when Deep Packet Inspection (DPI) is enabled on the controller. **Platform:** 7200 Series controllers. **Reported Version:** ArubaOS 6.4.0.0. **Workaround:** None.
107826	**Symptom:** A local controller reboots and the log files for the event display the reason for the reboot as **datapath timeout**. **Scenario:** A Security Acceleration Engine (SAE) delay occurs due to heavy traffic and this slows down the packet forwarding process. This issue is observed in 7240 controllers running ArubaOS 6.4.1.0. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.1.0. **Workaround:** Reboot the controller.
110159 111832	**Symptom:** A 7240 controller stops responding and reboots unexpectedly. The log files for the event list the reason as **Reboot cause: Datapath timeout**. **Scenario:** This issue is observed when Networking Acceleration Engine (NAE) traffic stalled on the 7240 controller running ArubaOS 6.4.2.1. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.0. **Workaround:** None.

Controller-Platform

Table 253: *Controller-Platform Known Issues*

Bug ID	Description
108832	**Symptom:** The **show global-user-table list** command does not show user output. **Scenario:** This issue is observed in controllers running ArubaOS 6.4.1.0. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.1.0. **Workaround:** Use **show user-table** command.
110879	**Symptom:** A controller crashes and reboots unexpectedly. The log file for the event lists the reason as **Kernel Panic**. **Scenario:** This issue is observed in 7010 controllers running ArubaOS 6.4.2.2. **Platform:** 7010 controllers. **Reported Version:** ArubaOS 6.4.2.2. **Workaround:** None.
111882 111891	**Symptom:** The **MD5 Secret** parameter in the **Configuration>Management > Clock** page of the WebUI does not accept the dollar ($) character. **Scenario:** This issue is not specific to any controller or release version. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.
112162	**Symptom:** The STM SNMP logging process cannot be disabled under a high load. **Scenario:** This issue is observed in 7220 controllers running ArubaOS 6.4.2.2. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.2. **Workaround:** Restart syslogd and stm process.

HA-Lite

Table 254: *HA-Lite Known Issues*

Bug ID	Description
108534	**Symptom:** Access Points frequently fail over to the standby controller. **Scenario:** This issue is observed when high availability intercontroller heartbeat is enabled. This issue is observed in controllers running ArubaOS 6.4.2.2. **Platform:** All platforms **Reported Version:** ArubaOS 6.4.2.2. **Workaround:** None.

Licensing

Table 255: *Licensing Known Issues*

Bug ID	Description
111984	**Symptom:** When the controller reboots, the controller license is lost. **Scenario:** This issue is observed when the controller reboots due to power outage. This issue is observed in 7240 controllers running ArubaOS 6.4.2.3. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3 **Workaround:** None.

Monitoring

Table 256: *Monitoring Known Issues*

Bug ID	Description
110044	**Symptom:** A 7200 controller crashes because of a memory leak. **Scenario:** This issue occurs in a 7200 master controller running ArubaOS 6.4.1.0. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.1.0. **Workaround:** None.

Radius

Table 257: *Radius Known Issues*

Bug ID	Description
112071	**Symptom:** The **ExpAuthTM** parameter displays large values when the **show aaa authentication-server radius statistics** command is executing and this results in less load distribution to the servers. **Scenario:** This issue is observed when the authorization server load-balancing is enabled. As the **ExpAuthTM** calculation sometimes returns the time in the past, negative values are stored as unsigned integers which result in large numbers. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3 **Workaround:** Decrease the authorization server dead time or run the **aaa inserver <server-group> <server-name>** command.

VRRP

Table 258: *VRRP Known Issues*

Bug ID	Description
109312	**Symptom:** After upgrading to a later version of ArubaOS, a VRRP backup controller takes over as the master controller. **Scenario:** This issue occurs after upgrading a 7220 controller from ArubaOS 6.3.1.8 to ArubaOS 6.4.2.2. **Platform:** 7220 controllers. **Reported Version:** ArubaOS 6.4.2.2. **Workaround:** None.

Known Issues and Limitations in ArubaOS 6.4.2.5

The following are the known issues and limitations found in ArubaOS 6.4.2.5. Applicable Bug IDs and workarounds are included.

AP-Datapath

Table 259: *AP-Datapath Known Issues*

Bug ID	Description
113076	**Symptom:** Wireless clients fail to get an IP address when associating to a bridge mode SSID. **Scenario:** This issue is seen after the controller is upgraded from ArubaOS 6.3.1.5 to ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.
113248	**Symptom:** After upgrading a controller to ArubaOS 6.4.2.4, clients in bridge mode cannot send/receive traffic. **Scenario:** This issue occurs after 3600 controllers in master-local topology is upgraded from ArubaOS 6.3.1.5 to ArubaOS 6.4.2.4 **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.

AP-Platform

Table 260: *AP-Platform Known Issues*

Bug ID	Description
112019	**Symptom:** A crash is observed on a DFS channel supported by an AP-115. The log files list the reason for the crash as **<4>ath data bus error: cause 0xc080841c** . **Scenario:** This issue is observed in AP-115 access points connected to controllers running ArubaOS 6.4.2.3. **Platform:** AP-115 access points. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** Avoid visiting radio register when radio chipset is reset or in the sleep mode.
112196	**Symptom:** The **Dashboard** on the local controller is not updated with the client usage. **Scenario:** The AP does not deliver AP Radio and Client Stats Updates to the local controller.This issue is observed in AP-225 access points connected to 7240 controllers running ArubaOS 6.4.2.3. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.
113103	**Symptom:** An AP-103H access point reboots randomly without displaying the reboot cause in the event logs. **Scenario:** This issue is observed only after executing the **show ap blacklist-clients** command, which causes memory overflow, and reboots the AP. **Platform:** AP-103H access points. **Reported Version:** ArubaOS 6.4.2.0. **Workaround:** None.

AP-Wireless

Table 261: *AP-Wireless Known Issues*

Bug ID	Description
112212	**Symptom:** An SCP or Windows File transfer failure is observed when the traffic is high. **Scenario:** This issue is observed in AP-225 access points connected to 7210 controllers running ArubaOS 6.3.1.8. **Platform:** AP-225 access points. **Reported Version:** ArubaOS 6.3.1.8. **Workaround:** None.
112516	**Symptom:** A Google Chromecast device disconnects from the wireless network frequently. **Scenario:** A Google Chromecast device associates, authenticates, and displays in the user-table of the controller. However, after 2-3 minutes, it disconnects from the wireless network. This issue is seen on a master-standby topology with AP-135 running ArubaOS 6.4.2.3. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.
112640	**Symptom:** A client experiences loss of multicast and unicast data. **Scenario:** This issue is observed with AP-125 access points connected to controllers running ArubaOS 6.4.2.3. **Platform:** AP-125 access points. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.

Base OS Security

Table 262: *Base OS Security Known Issues*

Bug ID	Description
112521	**Symptom:** Wireless clients fail to connect to a 802.1X SSID. **Scenario:** This issue is seen when a high number of wireless clients connect to the SSID and the authentication process consumes high CPU utilization. This issue is observed on a local controller running ArubaOS 6.4.2.4. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.
113328	**Symptom:** The station table displays duplicate entries. **Scenario:** This issue is observed in APs connected to 7240 controllers running ArubaOS 6.4.2.3. **Platform:** 7240 controllers. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** None.

Captive Portal

Table 263: *Captive Portal Known Issues*

Bug ID	Description
111838	**Symptom:** The captive portal page intermittently times out after a user enters the login credentials. **Scenario:** This issue is observed in 7240 controllers running ArubaOS 6.4.2.3 in a master-local topology. **Platform:** All platforms. **Reported Version:**ArubaOS 6.4.2.3. **Workaround:** None.

Controller-Platform

Table 264: *Controller-Platform Known Issues*

Bug ID	Description
112230	**Symptom:** The kernel in a master controller crashes and WebUI SSH does not work. **Scenario:** The issue occurs in 7210 controller running ArubaOS 6.4.2.2. **Platform:** 7210 controllers. **Reported Version:** ArubaOS 6.4.2.2. **Workaround:** None.
113043	**Symptom:** The kernel in a controller, which is sending/receiving UDP traffic, detects an error from which it cannot properly recover during a failover to a cellular uplink. **Scenario:** This issue occurs in 7005 controllers running ArubaOS 6.4.2.3. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** Reduce the bandwidth to 4 kbps for control plane traffic from the trusted port in the controller.
113462	**Symptom:** A modem does not complete the dialing process. **Scenario:** This issue occurs when: • a controller has a subnet in the 192.168.1.x range assigned to a VLAN. This subnet is the default NAT pool on the modem. • a modem uses NAT mode instead of IPT mode. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.3. **Workaround:** To avoid this issue: • Do not use the modem in NAT mode. Use IPT mode and assign a public IP to the controller. • If you want to use NAT mode in the modem, configure the modem to use another subnet for the NAT pool. • If you do not want to configure the modem to use another subnet for the NAT pool, change the subnet on the controller.
113665	**Symptom:** The WLAN Management System (WMS) crashes frequently. **Scenario:** This issue is observed in 650 controllers running ArubaOS 6.4.2.4. **Platform:** 650 controllers. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.

LLDP

Table 265: *LLDP Known Issues*

Bug ID	Description
94647	**Symptom:** In a rare instance, the controller generated the following error message: **lldp GSM PORT_INFO Lookup failed at Function: sm_handle_lldp_info_events**. **Scenario:** This issue occurs when the script to shut or open the Ethernet interface is executed multiple times. This issue is not limited to any specific controller model and occurs in ArubaOS 6.4.x. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.0.0. **Workaround:** None.

Voice

Table 266: *Voice Known Issues*

Bug ID	Description
113505	**Symptom:** Alcatel-Lucent OmniTouch WLAN clients connected to AP-205 access points display the **Network busy** error message when initiating a call. **Scenario:** This issue occurs in AP-205 access points connected to 3600 controllers running ArubaOS 6.4.2.3. **Platform:** All platforms. **Reported Version:** ArubaOS 6.4.2.4. **Workaround:** None.

Known Issues and Limitations in ArubaOS 6.4.2.4

The following are the known issues and limitations found in ArubaOS 6.4.2.4. Applicable Bug IDs and workarounds are included.

No Support for Mesh in AP-200 Series

Wireless mesh is not supported in AP-200 Series, AP-210 Series, AP-220 Series, and AP-270 Series 802.11ac access points.

AP-Datapath

Table 267: *AP-Datapath Known Issues*

Bug ID	Description
108838	**Symptom:** After upgrading the ArubaOS version on a controller, the clients connected in bridge mode cannot send traffic. **Scenario:** This issue is observed after upgrading a 7210 controller from ArubaOS 6.3.1.4 to ArubaOS 6.4.2.2. **Workaround:** None.

AP-Platform

Table 268: *AP-Platform Known Issues*

Bug ID	Description
110157	**Symptom:** The **show ap radio-database** command does not display the values for 802.11ac channel bonding. **Scenario:** This issue is observed on controllers running ArubaOS 6.3.x and 6.4.x. **Workaround:** Issue the **show ap active** command to display the correct flag.
111400	**Symptom:** When the primary controller fails, the users connected to a RAP cannot associate with the backup controller. **Scenario:** This issue is observed in a master-local topology where the master controller is the backup controller and the local controller is the primary controller. This issue is not limited to a specific controller model. This issue is observed in controllers running ArubaOS 6.4.2.2. **Workaround:** None.

AP-Wireless

Table 269: *AP-Wireless Known Issues*

Bug ID	Description
108371	**Symptom:** A delay in acknowledgment is observed when scanning a barcode using a handheld scanner. **Scenario:** This issue is observed when the handheld scanner associates with an AP-103 access point on a 2.4 GHz radio connected to a 3400 controller running ArubaOS 6.4.2.0. **Workaround:** None.
108810	**Symptom:** Multicast rate optimization cannot be enabled on an individual virtual AP. **Scenario:** This issue is observed in AP-200 Series access points connected to controllers running ArubaOS 6.3. With multiple VAPs, the multicast rate is selected non-deterministically if the parameter **BC/MC Rate Optimization** is enabled. This may lead to unintended issues when multicast traffic is used. **Workaround:** None.
109856	**Symptom:** Clients connected in bridge forwarding mode are randomly unable to send traffic. **Scenario:** This issue is observed in AP-135 access points connected to 650 controllers running ArubaOS 6.4.2.2. **Workaround:** Use tunnel forwarding mode.

Base OS Security

Table 270: *Base OS Security Known Issues*

Bug ID	Description
110693	**Symptom:** The internal controller module that handles authorization crashes due to invalid memory access. **Scenario:** This issue is observed when processing a DELETE station channel event from STM. This issue is not specific to any controller model or ArubaOS version. **Workaround:** None.

Controller-Datapath

Table 271: *Controller-Datapath Known Issues*

Bug ID	Description
110918	**Symptom:** An AP-103H access point frequently fails over to another controller when AP Fast Failover is enabled. **Scenario:** This issue is observed in AP-103H connected to 7240 controllers running ArubaOS 6.4.2.1. **Workaround:** None.
111084	**Symptom:** A controller reboots unexpectedly. The log files for the event list the reason for the reboot as **datapath exception**. **Scenario:** This issue is caused by a network flood and is observed in 7000 Series controllers running ArubaOS 6.4.2.3. **Workaround:** None.

Controller-Platform

Table 272: *Controller-Platform Known Issues*

Bug ID	Description
108220	**Symptom:** The controller stops responding and reboots. The log files for the event list the reason as **Nanny rebooted machine - fpapps process died**. **Scenario:** This issue is seen on a master-local topology where the local controller reboots. Initial investigation suggests an Out Of Memory issue. This issue is observed on controllers running ArubaOS 6.4.0.2-HDMS. **Workaround:** None.
110988	**Symptom:** A backup controller loses connectivity with the master controller and crashes. **Scenario:** This issue is observed in a standby 7210 controller running ArubaOS 6.4.2.2 in a master-standby topology. **Workaround:** None.

Known Issues and Limitations in ArubaOS 6.4.2.3

The following are the known issues and limitations found in ArubaOS 6.4.2.3. Applicable Bug IDs and workarounds are included.

Base OS Security

Table 273: *Base OS Security Known Issues*

Bug ID	Description
108745	**Symptom:** The **authentication** process crashes. **Scenario:** This issue occurs when authenticating users with MAC authentication and Captive Portal authentication. This issue is observed in 7220 controllers deployed in a master-local topology and running ArubaOS 6.4.2.0. **Workaround:** None.

Controller-Datapath

Table 274: *Controller-Datapath Known Issues*

Bug ID	Description
89722	**Symptom:** Facebook® application traffic fails to classify correctly. **Scenario:** This issue occurs on 7200 Series controllers running ArubaOS 6.4 when DPI is enabled on the controller. **Workaround:** None.
109010	**Symptom:** The 7220 controller reboots unexpectedly. The log files for the event list the reason for the reboot as **datapath timeout**. **Scenario:** This issue is observed in 7220 controllers running ArubaOS 6.4.2.0. **Workaround:** None.

Controller-Platform

Table 275: *Controller-Platform Known Issues*

Bug ID	Description
108797	**Symptom:** A 7220 controller crashes and reboots due to kernel panic. **Scenario:** This issue is observed on 7220 controllers running ArubaOS 6.4.2.2. **Workaround:** None.

HA-Lite

Table 276: *HA-Lite Known Issues*

Bug ID	Description
109076	**Symptom:** High availability failover occurs due to missed heartbeats. **Scenario:** This issue is observed when high availability inter-controller heartbeat is enabled. This issue is observed in controllers running ArubaOS 6.4.2.2. **Workaround:** None.

Port-Channel

Table 277: *Port-Channel Known Issues*

Bug ID	Description
111376	**Symptom:** The controller loses connectivity, when port monitoring is enabled to monitor a Port-Channel. **Scenario:** When port monitoring is enabled for a Port-Channel, the ports associated to the Port-Channel are blocked. This issue is observed in controllers running ArubaOS 6.4.2.3. **Workaround:** Enabling and disabling the **spanning-tree** parameter clears the blocked state of the ports.

Remote AP

Table 278: *Remote AP Known Issues*

Bug ID	Description
108824	**Symptom:** RAP fails to boot with the Huawei® E3276 USB modem. **Scenario:** This issue occurs with Huawei® E3276 USB modem running the new firmware. This issue is observed in controllers running ArubaOS 6.4.2.1. **Workaround:** None.

Voice

Table 279: *Voice Known Issues*

Bug ID	Description
111023	**Symptom:** An access point may send an unnecessary deauthorization message to an iOS client during fast transition roaming (802.11r). **Scenario:** This issue can occur if the iOS client sends multiple 802.11 authorization messages with different supplicant nonce values, prompting the AP to send a deauthorization message due to a nonce mismatch within the Fast Transition Information Element (FTIE). This issue is observed in ArubaOS 6.4.2.3, when the AP is operating in in tunnel forwarding mode when 802.11r is enabled. **Workaround**: None

Known Issues and Limitations in ArubaOS 6.4.2.1

The following are the known issues and limitations found in ArubaOS 6.4.2.1. Applicable Bug IDs and workarounds are included.

AP Wireless

Table 280: *AP Wireless Known Issues*

Bug ID	Description
102639	**Symptom:** Windows Surface RT tablets do not connect to 802.11w capable SSID with 802.1x authentication AES encryption. **Scenario:** This issue occurs when **Enable 802.11w Management Frame Protection** is set to **Capable** or **Required**. **Workaround:** Disable MFP capability.

HA-Lite

Table 281: *HA-Lite Known Issues*

Bug ID	Description
106070	**Symptom:** An AP fails to create a standby tunnel with the standby controller. **Scenario:** This issue occurs when AP rebootstraps because of a missed heartbeat with the active controller and the IP address of BLMS and IP address of standby controller is the same. **Workaround:** Do not configure BLMS in **ap system-profile**.

Local Database

Table 282: *Local Database Known Issues*

Bug ID	Description
105626	**Symptom:** A timeout occurs when authenticating a client on a local controller against the local database on a master controller. **Scenario:** This issue is observed in master-local configuration with clients on the local controller authenticating against the local database on a master controller running ArubaOS 6.4.1.0. **Workaround:** Use the local database on the local controller by configuring the **use local switch internal-db** command on the local controller.

Remote AP

Table 283: *Remote AP Known Issues*

Bug ID	Description
105794	**Symptom:** The output of the **show iap table** command displays the status of an IAP as DOWN on the controller although the VPN status shows that the IAP is UP. **Scenario:** This issue is observed because the MAC address of the IAP is missing in the trusted database of the controller running ArubaOS 6.4. **Workaround:** None.

Known Issues and Limitations in ArubaOS 6.4.2.0

The following are the known issues and limitations found in ArubaOS 6.4.2.0. Applicable Bug IDs and workarounds are included.

AP Wireless

Table 284: *AP Wireless Known Issues*

Bug ID	Description
103810 104199	**Symptom:** Following a successful association users are deauthenticated with reason **Denied; Internal Erro**r. This issue is seen intermittently after the controller is upgraded from ArubaOS 6.4.0.3 to 6.4.1.0. **Scenario:** This issue occurs on 7220 controllers running ArubaOS 6.4.1.0. **Workaround:** None.

AP Platform

Table 285: *AP Platform Known Issues*

Bug ID	Description
104218 101794	**Symptom:** An sapd process crashes while running Microsoft Request For Information (RFI) tests. **Scenario:** This issue is observed in AP-225 access points running ArubaOS 6.4.0.3. The crash is caused by zero length Fast Fourier Transforms (FFTs). **Workaround:** This issue is resolved by disabling spectrum-monitoring in the AP mode or disabling spectrum-mode.

Controller-Datapath

Table 286: *Controller-Datapath Known Issues*

Bug ID	Description
95706 100817 102229 103914 104137	**Symptom:** A 7200 Series controller unexpectedly stops passing network traffic. **Scenario:** This issue is triggered by a hardware error on a 7200 Series controller using auto negotiated Ethernet speeds. **Workaround:** Manually define ethernet speeds for each port on the 7200 Series controller.

Known Issues and Limitations in ArubaOS 6.4.1.0

The following are the known issues and limitations found in ArubaOS 6.4.1.0. Applicable Bug IDs and workarounds are included.

AP Regulatory

Table 287: *AP Regulatory Known Issues*

Bug ID	Description
99290	**Symptom:** 80 MHz channels in the Hong Kong regulatory domain are disabled on the AP-220 Series. **Scenario:** 80 MHz channels are not supported on the AP-220 Series within the Hong Kong regulatory domain. **Workaround:** Download and activate the latest regulatory file from the Aruba support site.
102555	**Symptom:** The Puerto Rico regulatory domain is disabled on the AP-270 Series. **Scenario:** The AP-270 Series is not currently supported in the Puerto Rico regulatory domain. **Workaround:** Enable the US regulatory domain or download and activate the latest regulatory file from the Aruba support site.

Controller-Datapath

Table 288: *Controller-Datapath Known Issues*

Bug ID	Description
100359	**Symptom:** Clients using phones connected to wired ports of RAPs experience poor call quality. **Scenario:** This issue is observed with RAP-2WG, RAP-3WN, and RAP-5WN running ArubaOS 6.3.1.0. **Workaround:** None.
101010	**Symptom:** When both DMO and broadcast-filter-all is enabled and port-channel is used for uplink port, incoming known multicast traffic from uplink is dropped in the controller. **Scenario:** This issue occurs in controllers running ArubaOS 6.3.x.0 and 6.4.x.0. **Workaround**: None.

Remote AP

Table 289: *Remote AP Known Issues*

Bug ID	Description
101962	**Symptom:** Remote AP (RAP) shows the status as down on the controller when custom certificate is configured on the RAP. **Scenario:** A USB containing a pfx file is connected to the RAP. During boot up, the RAP searches for the pfx file and loads the key/certificates from the pfx file. The key/certificates are used in IKEv2 tunnel establishment. When the USB has more than one pfx file in different directories having a same file name such as **<mac-address>.p12**, the RAP fails to upload the pfx files and hence cannot establish an IKEv2 tunnel. This issue is not specific to any controller model or ArubaOS release version. **Workaround:** On the USB connected to the RAP, delete any duplicate pfx file. Only one pfx file must be present with the RAP MAC address i.e., **<mac-address>.p12**.

WebUI

Table 290: *WebUI Known Issues*

Bug ID	Description
97710	**Symptom:** The WebUI displays the error, **can't do cli:SID validation failed** when a client logs in after upgrading the controller using the WebUI. **Scenario:** This issue is not limited to any specific controller model. **Workaround:** Clear the browser cache after the image is upgraded.

Known Issues and Limitations in ArubaOS 6.4.0.2

The following are the known issues and limitations in ArubaOS 6.4.0.2. Applicable Bug IDs and workarounds are included.

AP-Wireless

Table 291: *AP-Wireless Known Issues*

Bug ID	Description
88940	**Symptom:** A crash is observed on APs when the status of the channel is set inappropriately by the process handling the AP management. **Scenario:** This issue is observed when a standard RAP or CAP is configured at the Dynamic Frequency Selection (DFS) channel. This issue is observed in AP-70 connected to controllers running ArubaOS 6.3.1.2. **Workaround:** Set the AP channel to No DFS before rebooting the AP.
97333	**Symptom:** All clients associated with an AP disassociates when more than 48 users start FTP downloads. **Scenario:** This issue is observed on controllers running ArubaOS 6.4.0.1. **Workaround:** None.

Controller-Platform

Table 292: *Controller-Platform Known Issues*

Bug ID	Description
94615	**Symptom:** The controller may get into an **OutOfMemory** or **kernel panic** state during an ArubaOS image upgrade. **Scenario:** This issue is seen when you issue the **tar logs tech-support** command repetitively on the controller. This depletes the kernel **LowFree** memory. This issue is observed in 600 Series controller running ArubaOS 6.4 or later versions. **Workaround:** Do not issue the **tar logs tech-support** command repetitively before upgrading an ArubaOS software image.

LLDP

Table 293: *LLDP Known Issues*

Bug ID	Description
94302	**Symptom:** In rare cases, issuing some of the LLDP show commands display the **<ERRS> |lldp| Invalid Physical Port 0 passed at Function: li_get_handle** error message in the log. This issue does not impact any functionality. **Scenario:** This issue is not specific to any controller model and occurs on ArubaOS running 6.4. **Workaround:** None.

Startup Wizard

Table 294: *Startup Wizard Known Issues*

Bug ID	Description
98110	**Symptom:** Mobility Controller **Setup Wizard** page gets stuck with Java script error when you click **Next** on the **VLANs and IP Interfaces** tab of the controller's WebUI. **Scenario:** This issue is not limited to any specific controller model and is observed in ArubaOS 6.4.0.2. **Workaround:** Use Mozilla® Firefox browser to access the **VLANs and IP Interfaces** tab of the **Setup Wizard** page.
98159	**Symptom: Campus WLAN Wizard** page gets stuck in **Role Assignment** step when you click **Next** on the **Authentication Server** step of the controller's WebUI using Microsoft® Internet Explorer 10 or Internet Explorer 11. **Scenario:** This issue is not limited to any specific controller model and is observed in ArubaOS 6.4.0.2. **Workaround:** Use any browser other than Internet Explorer 10 and Internet Explorer 11 to access the **Role Assignment** tab under the **Setup Wizard** page.

Known Issues and Limitations in ArubaOS 6.4.0.0

The following are known issues and limitations in ArubaOS 6.4.0.0. Applicable Bug IDs and workarounds are included.

AirGroup

Table 295: *AirGroup Known Issues*

Bug ID	Description
94208	**Symptom:** Wireless Clients such as iPad and iPhone running the SONOS® Controller application do not discover the SONOS music system. **Scenario:** This issue is observed when AirGroup is enabled on a controller with the SONOS music system connected. **Workaround:** None.

AP-Platform

Table 296: *AP-Platform Known Issues*

Bug ID	Description
95764	**Symptom:** AP-125 device crashes and reboots, the log files for the event list the reason for the crash as **Kernel unaligned instruction access**. **Scenario:** This issue occurs in AP-125 access points connected to controllers running ArubaOS 6.3.1.2. **Workaround:** None.

AP-Wireless

Table 297: *AP-Wireless Known Issues*

Bug ID	Description
93511 93953	**Symptom:** The user gets error **Could not read cached limits** and **License number mismatch in cached limits** messages in a controller with master-local topology. **Scenario:** This issue is not limited to any specific controller model and is observed in controllers running ArubaOS 6.3 or later. **Workaround**: None.
95113 95086 95088 95111 95114 95115 95116 95117 95123 95124	**Symptom**: An iPad connected in tunnel mode using CCMP encryption becomes unreachable from the network once Airplay mirroring is initiated from iPad to Apple TV. **Scenario**: This issue occurs when an iPad is connected to a wireless network in forward-mode: Tunnel and opmodes: wpa2-aes/wpa2-psk-aes. This issue is observed in controllers and APs running ArubaOS 6.3.x.x or 6.4.x.x. **Workaround**: Disable **Multiple Tx Replay Counters** parameter under SSID profile.

Configuration

Table 298: *Configuration Known Issues*

Bug ID	Description
93922	**Symptom:** A custom banner with the **#** delimiter gets added as part of the **show running-config** command output. **Scenario:** The issue is observed when an administrator configures the banner using the **banner motd** command in the controller with the **#** delimiter. This issue is not limited to a specific controller model and is observed in ArubaOS 6.3.1.1 or later versions. **Workaround:** None.

Controller-Datapath

Table 299: *Controller-Datapath Known Issues*

Bug ID	Description
91085	**Symptom:** Google hangout sessions are classified as Google when AppRFv2 is enabled. **Scenario:** This issue occurs on 7200 Series controllers running ArubaOS 6.4. **Workaround:** None.
93285	**Symptom:** M3 controller reboots unexpectedly. The log files for the event listed the reason as **datapath timeout**. **Scenario**: This issue occurs in M3 controllers running ArubaOS 6.3.X.X. **Workaround:** None.
93582	**Symptom:** A 7210 controller crashes. The logs for this error listed the reason for the crash as **datapath timeout**. **Scenario:** This issue is observed in 7210 controllers running ArubaOS 6.3.1.0. **Workaround:** None.
93817	**Symptom:** The master controller throws an internal error while provisioning APs that belong to a specific local controller. **Scenario:** This issue occurs on 3200 controllers running ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.
94143	**Symptom:** A 3200 controller reboots unexpectedly. The log files for the event listed the reason as **datapath timeout**. **Scenario:** This issue is observed on a 3200 controller running ArubaOS 6.3.1.1. **Workaround:** None.
93203 94200	**Symptom:** A local controller reboots unexpectedly. The log files for the event listed the reason for the reboot as **datapath exception**. **Scenario:** This issue is observed in 7220 controller running ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.
94267	**Symptom**: After an upgrade to ArubaOS 6.3.1.x, clients unexpectedly disconnected from the network, or were unable to pass traffic for 2-3 minutes after roaming between APs. **Scenario**: This issue is observed in Psion Omni handheld scanners roaming between AP-175 and AP-120 Series access points running ArubaOS 6.3.1.1. **Workaround**: None.
94636	**Symptom:** A crash occurs on a local controller and the log files for the event listed the reason for the crash as **datapath timeout**. **Scenario:** The trigger of this issue is not known and this issue is observed in 7210 controllers running ArubaOS 6.3.0.1. **Workaround:** None.
95286	**Symptom:** A master controller crashes with log message **datapath timeout**. **Scenario:** The trigger of this issue is unknown and is observed in 7220 controllers running ArubaOS 6.3.1.1. **Workaround:** None.

Controller-Platform

Table 300: *Controller-Platform Known Issues*

Bug ID	Description
80200 81225 81752 81930 84672 85422 87079 89014 89243 89726	**Symptom:** The 600 Series and 3000 Series controllers reboots with kernel panic. **Scenario:** This issue is observed because of high traffic in control plane for a sustained period. This issue occurs on 600 Series and 3000 Series controllers running ArubaOS 6.3.0.0 or later. **Workaround:** Configure bandwidth contracts depending on the incoming traffic.
92968	**Symptom:** Generating the **tech-support.log** file from the WebUI of the controller gets truncated at times. **Scenario:** This issue is not limited to a specific controller model and is observed in ArubaOS 6.2.1.3, ArubaOS 6.3.1.0 or later versions. **Workaround:** Issue the **tar logs tech-support** command from the CLI to download the **tech-support.log** file.
93465	**Symptom:** A local controller reboots unexpectedly. The log files for the event listed the reason for the reboot as **Control Processor Kernel Panic**. **Scenario:** This issue occurs when the controller releases the memory of corrupted data packets. This issue is observed in 3000 Series and M3 controllers running ArubaOS 6.3.1.1 in a master-local topology. **Workaround:** None.
94862	**Symptom:** The master controller reboots unexpectedly with the message: "user reboot (shell)." **Scenario:** This issue occurs on the 7200 Series controllers with AP-225 APs following an upgrade to ArubaOS 6.4. **Workaround:** None.

DHCP

Table 301: *DHCP Known Issues*

Bug ID	Description
94345	**Symptom:** The Symbol N410 and Android devices do not receive an IP address from the internal DHCP Server. **Scenario:** This issue is observed on controllers running ArubaOS 6.3.1.1 and occurs when the controller's internal DHCP is configured to serve IP addresses for these devices. **Workaround:** Use an external DHCP server.
95166	**Symptom:** When a controller is configured as a DHCP server,by default it attempts Dynamic DNS updates and the following log message appears: "dhcpd: if CU-iPad-2-64-GB.aspect.com IN A rrset doesn't exist add CU-iPad-2-64-GB.aspect.com 10800 IN A 169.136.135.108: destination address required." **Scenario:** This issue is observed on controllers running ArubaOS 6.3 and later. It is caused when the DHPCD server issues a DHCP address and then attempts a DDNS update. **Workaround:** None.

Hardware-Management

Table 302: *Hardware-Management Known Issues*

Bug ID	Description
87191 87808	**Symptom:** A controller unexpectedly stops responding and reboots. **Scenario:** This issue is observed when a module (hwMon) crashes on the controller. This issue occurs on M3 series controllers running ArubaOS 6.3.0.1 or later. **Workaround:** None.

IPSec

Table 303: *IPSec Known Issues*

Bug ID	Description
80460	**Symptom:** Remote client and Site-to-Site VPN performance is low and does not scale to the controller limit when IKEv2 with GCM256-EC384 encryption algorithm configured. **Scenario:** This issue is observed on 600 Series, 3000 Series, and M3 controllers and occurs when the IKE session is established to a standby unit in a failover deployment. **Workaround:** None.
95634	**Symptom:** Site-to-Site IPsec VPN tunnels randomly lose connectivity on a 7210 controller. **Scenario:** This issue is observed where there are 500 or more remote sites terminating IPsec VPN tunnels on a 7210 controller. This issue is observed on a 7210 controller running ArubaOS 6.3.1.2. **Workaround:** None.

Local Database

Table 304: *Local Database Known Issues*

Bug ID	Description
95277	**Symptom:** The Remote AP whitelist on a master controller is not correctly synchronizing entries to local controllers. **Scenario:** This issue occurs in ArubaOS 6.3.x.x when the description field of a remote whitelist entry contains an apostrophe ('). **Workaround:** Remove the apostrophe from the whitelist entry description.

LLDP

Table 305: *LLDP Known Issues*

Bug ID	Description
92998	**Symptom:** The remote interface name appears as **Not received** while issuing the **show lldp neighbor** command. **Scenario**: This issue occurs when Link Layer Discovery Protocol (LLDP) is enabled on the controller and if the neighbor is a third-party device such as Arista or Alcatel. This issue is not specific to any controller model and occurs on ArubaOS running 6.4. **Workaround:** None.

Master-Local

Table 306: *Master-Local Known Issues*

Bug ID	Description
88430	**Symptom:** User-role configuration is lost after upgrading master, standby, and local controllers to ArubaOS 6.3.1 or later versions. **Scenario:** This issue is observed on a 7200 Series controller running ArubaOS 6.3.1 or later versions. **Workaround:** Disabling the configuration snapshot by executing the **cfgm set sync-type complete** command on master and standby controllers prevents partial configuration loss. Wait at least five (5) minutes after the upgraded master and standby have rebooted before reloading the upgraded local controller.
88919	**Symptom:** Global configuration like user-role on the master controller does not synchronize with the local controller after issuing the **write memory** command. **Scenario:** This issue is observed in a master-local topology. This issue is observed in 7200 Series controller running ArubaOS 6.3.0.0 or later versions. **Workaround:** On the master controller, issue the **cfgm set sync-type complete** command, followed by the **write memory** command to send the complete configuration file to the local controller.

RADIUS

Table 307: *RADIUS Known Issues*

Bug ID	Description
94081	**Symptom:** Multiple authentication failures are observed in the controllers. **Scenario:** This issue is observed when external LDAP server is used for authentication. This issue is not limited to a specific controller models and occurs in ArubaOS running 6.3.x versions. **Workaround:** Reduce LDAP timeout parameter value to 3 seconds for LDAP servers.

Remote AP

Table 308: *Remote AP Known Issues*

Bug ID	Description
95658	**Symptom:** Cisco® Unified IP Phone 7945G reboots randomly during an active voice call. **Scenario:** This issue is observed when a Cisco Unified IP Phone 7945G is connected to a Power over Ethernet (PoE) port of a RAP-3WNP remote AP. This issues is observed in ArubaOS 6.3.0.1. **Workaround:** None.

Station Management

Table 309: *Station Management Known Issues*

Bug ID	Description
85662 84880 88009 88319 89321 92164 93243 93388 93389 93984	**Symptom:** The state of APs are displayed as **down** on the master controller even if these APs are connected and UP. **Scenario**: This issue is observed when AP's system profile has a local controller as the primary Local Management Switch (Primary-LMS) and master controller is configured as a backup Local Management Switch (Backup-LMS). This issue is not limited to any specific controller model and occurs in ArubaOS running 6.3 or later. **Workaround:** Remove master controller as backup LMS during initial phase.
91758	**Symptom**: Stationary Apple® MacBook laptops unexpectedly disassociated from APs, and were temporarily unable to pass traffic for 3-5 minutes during a period when many users on the network were roaming between APs. **Scenario**: This issue occurs on a network with a controller running ArubaOS 6.3.1.1 with ARM channel assignment and scanning features enabled. **Workaround**: Disable ARM channel assignment and scanning features.

WebUI

Table 310: *WebUI Known Issues*

Bug ID	Description
90026	**Symptom:** When a user attempts to access the controller WebUI, the WebUI returns the **Session Invalid** error message. **Scenario:** The user is forced to attempt to access the WebUI two to three times before successfully logging in. Each failed attempt returns the **Session Invalid** error message. This error occurs on controllers running ArubaOS 6.3.0.1. **Workaround:** None.
93454	**Symptom:** The **Dashboard** > **Spectrum** page of the WebUI is not loading and re-subscription fails frequently. **Scenario:** This issue is observed in AP-105 access points associated to controllers running ArubaOS 6.3.0.1. **Workaround:** Use the **ap spectrum clear-webui-view-settings** command to avoid this issue.

Issues Under Investigation

The following issues have been reported in ArubaOS 6.4.x and are being investigated.

AP-Wireless

Table 311: *AP-Wireless Issues Under Investigation*

Bug ID	Description
110556	**Symptom:** The 2.4 GHz radio in access point reset frequently and caused the clients to experience intermittent connectivity issues for a very short duration. Note: This issue has not been observed after ArubaOS 6.4.2.2.
110683	**Symptom:** AP-103H and AP-115 access points stopped responding and rebooted. The log files for the event listed the reason as **data bus error**. This issue is observed on APs running ArubaOS 6.4.2.0.

Controller–Datapath

Table 312: *Controller –Datapath Issues Under Investigation*

Bug ID	Description
95532	**Symptom:** A 7210 controller running ArubaOS 6.3.1.1 stopped responding and rebooted. The log files for the event listed the reason as **datapath timeout**.
111953	**Symptom:** AppRF fails to block Facebook, YouTube, WhatsApp, and other applications when launched as an application from mobile devices.
114200	**Symptom:** A 7240 controller running ArubaOS 6.4.2.4 stopped responding and rebooted. The log files for the event listed the reason as **datapath timeout**.
114928	**Symptom:** Existing per-user upstream and downstream bandwidth contracts are not getting applied to the per-user traffic after upgrading the controller from ArubaOS 6.3.1.12 to 6.4.2.5.

Chapter 6
Upgrade Procedure

This chapter details software upgrade procedures. Aruba best practices recommend that you schedule a maintenance window for upgrading your controllers.

CAUTION

Read all the information in this chapter before upgrading your controller.

Topics in this chapter include:

- Upgrade Caveats on page 239
- Peer Controller Upgrade Requirement on page 240
- Installing the FIPS Version of ArubaOS 6.4.3.1 on page 240
- Important Points to Remember and Best Practices on page 240
- Memory Requirements on page 241
- Backing up Critical Data on page 242
- Upgrading in a Multi-Controller Network on page 243
- Upgrading to ArubaOS 6.4.3.1 on page 243
- Downgrading on page 247
- Before You Call Technical Support on page 249

Upgrade Caveats

Before upgrading to this version of ArubaOS, take note of these known upgrade caveats.

- AP LLDP profile is not supported on AP-120 Series in ArubaOS 6.4.x.
- Starting with ArubaOS 6.3.1.0, the local file upgrade option in the 620 and 650 controller WebUI has been disabled.
- ArubaOS 6.4.x does not allow you to create redundant firewall rules in a single ACL. ArubaOS will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
  - source IP/alias
  - destination IP/alias
  - proto-port/service

  If you are upgrading from ArubaOS 6.1 or earlier and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

  For example, in the below ACL, both ACE entries could not be configured in ArubaOS 6.4.x. Once the second ACE entry is added, the first would be overwritten.

```
(host) (config) #ip access-list session allowall-laptop
(host) (config-sess-allowall-laptop)# any any any  permit time-range test_range
(host) (config-sess-allowall-laptop)# any any any  deny
(host) (config-sess-allowall-laptop)#end
(host) #show ip access-list allowall-laptop

ip access-list session allowall-laptop
allowall-laptop
---------------
Priority  Source  Destination  Service  Action  TimeRange
--------  ------  -----------  -------  ------  ---------
1         any     any          any      deny
```

- ArubaOS 6.4.x is supported only on the newer MIPS controllers (7200 Series, 7000 Series, M3, 3200XM, 3400, 3600, and 600 Series). Legacy PPC controllers (200, 800, 2400, SC1/SC2) and 3200 controllers are not supported. Do not upgrade to ArubaOS 6.4.x if your deployment contains a mix of MIPS and PPC controllers in a master-local setup.
- When upgrading the software in a multi-controller network (one that uses two or more Aruba controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence. (See Upgrading in a Multi-Controller Network on page 243.)

Peer Controller Upgrade Requirement

If you are running an L2 and L3 GRE tunnel between two or more Aruba controllers with **keepalive** enabled, all peer controllers must be upgraded to ArubaOS 6.4.1.0. This is not a requirement if **keepalive** is disabled on the peer controllers.

NOTE

During the upgrade procedure, if one controller is upgraded and the other end point controller is yet to be upgraded, the GRE tunnel goes down. It is recommended to schedule a maintenance window to upgrade the peer controllers.

Important Points to Remember

- ArubaOS 6.4.1.0 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between end point devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Installing the FIPS Version of ArubaOS 6.4.3.1

Download the FIPS version of the software from https://support.arubanetworks.com.

Before Installing FIPS Software

Before you install a FIPS version of software on a controller that is currently running a non-FIPS version of the software, you must reset the configuration to the factory default or you will not be able to log in to the CLI or WebUI. Do this by running the **write erase** command just prior to rebooting the controller. This is the only supported method of moving from non-FIPS software to FIPS software.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions listed below. You should save this list for future use.

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network during the upgrade, such as configuration changes, hardware upgrades, or changes to the rest of the network. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions.
  - How many APs are assigned to each controller? Verify this information by navigating to the **Monitoring > Network All Access Points** section of the WebUI, or by issuing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the controller (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS is currently on the controller?
  - Are all controllers in a master-local cluster running the same version of software?
  - Which services are used on the controllers (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the controller. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the user guide.

Memory Requirements

All Aruba controllers store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the controller. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. To maintain the reliability of your WLAN network, the following compact memory best practices is recommended:

- Issue the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI, or at least 60 MB of free memory available for an upgrade using the WebUI. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up, upgrade immediately.
- Issue the **show storage** command to confirm that there is at least 60 MB of flash available for an upgrade using the CLI, or at least 75 MB of flash available for an upgrade using the WebUI.

CAUTION

In certain situations, a reboot or a shutdown could cause the controller to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you issue the **halt** command before power cycling.

If the output of the **show storage** command indicates that insufficient flash memory space is available, you must free up additional memory. Any controller logs, crash data, or flash backups should be copied to a location off the controller, then deleted from the controller to free up flash space. You can delete the following files from the controller to free memory before upgrading:

- **Crash Data:** Issue the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in Backing up Critical Data on page 242 to copy the **crash.tar** file to an external server, then issue the command **tar clean crash** to delete the file from the controller.
- **Flash Backups:** Use the procedures described in Backing up Critical Data on page 242 to back up the flash directory to a file named **flash.tar.gz**, then issue the command **tar clean flash** to delete the file from the controller.

- **Log files:** Issue the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in Backing up Critical Data on page 242 to copy the **logs.tar** file to an external server, then issue the command **tar clean logs** to delete the file from the controller.

Backing up Critical Data

It is important to frequently backup all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Custom captive portal pages
- x.509 certificates
- Controller Logs

Backup and Restore Compact Flash in the WebUI

The WebUI provides the easiest way to backup and restore the entire compact flash file system. The following steps describe how to backup and restore the compact flash file system using the WebUI on the controller:

1. Click on the **Configuration** tab.
2. Click **Save Configuration** at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to backup the contents of the compact flash file system to the **flashbackup.tar.gz** file.
5. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Backup and Restore Compact Flash in the CLI

The following steps describe the backup and restore procedure for the entire compact flash file system using the controller's command line:

1. Enter **enable** mode in the CLI on the controller, and enter the following command:

   ```
   (host) # write memory
   ```
2. Use the backup command to backup the contents of the Compact Flash file system to the **flashbackup.tar.gz** file.

   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```
3. Use the copy command to transfer the backup flash file to an external server or storage device:

```
(host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
<remote directory>
(host) copy flash: flashbackup.tar.gz usb: partition <partition-number>
```

You can later transfer the backup flash file from the external server or storage device to the Compact Flash file system with the copy command:

```
(host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
(host) # copy usb: partition <partition-number> <filename> flash: flashbackup.tar.gz
```

4. Use the restore command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system:

```
(host) # restore flash
```

Upgrading in a Multi-Controller Network

In a multi-controller network (a network with two or more Aruba controllers), special care must be taken to upgrade all controllers based on the controller type (master or local). Be sure to back up all controllers being upgraded, as described in Backing up Critical Data on page 242.

NOTE

For proper operation, all controllers in the network must be upgraded with the same version of ArubaOS software. For redundant (VRRP) environments, the controllers should be the same model.

To upgrade an existing multi-controller system to this version of ArubaOS:

1. Load the software image onto all controllers (including redundant master controllers).
2. If all the controllers cannot be upgraded with the same software image and rebooted simultaneously, use the following guidelines:
   a. Upgrade the software image on all the controllers. Reboot the master controller. Once the master controller completes rebooting, you can reboot the local controllers simultaneously.
   b. Verify that the master and all local controllers are upgraded properly.

Upgrading to ArubaOS 6.4.3.1

Install Using the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash available for an upgrade using the WebUI. For details, see Memory Requirements on page 241.

NOTE

When you navigate to the **Configuration** tab of the controller's WebUI, the controller may display an error message **Error getting information: command is not supported on this platform**. This error occurs when you upgrade the controller from the WebUI and navigate to the **Configuration** tab as soon as the controller completes rebooting. This error is expected and disappears after clearing the Web browser cache.

Upgrading From an Older version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.4.3.1.

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS 3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download and install the latest version of ArubaOS 5.0.4.x.
- For ArubaOS 6.0.0.0 or 6.0.0.1 versions, download and install the latest version of ArubaOS 6.0.1.x.

Follow step 2 to step 11 of the procedure described in Upgrading From a Recent version of ArubaOS on page 244 to install the interim version of ArubaOS, then repeat steps 1 through 11 of the procedure to download and install ArubaOS 6.4.3.1.

Upgrading From a Recent version of ArubaOS

The following steps describe the procedure to upgrade from one of these recent versions of ArubaOS:

- 3.4.4.1 or later
- 5.0.3.1 or later 5.0.x
- 6.0.1.0 or later 6.x

Install the ArubaOS software image from a PC or workstation using the Web User Interface (WebUI) on the controller. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Download ArubaOS 6.4.3.1 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
   a. Download the file **Aruba.sha256** from the download directory.
   b. To verify the image, load the image onto a Linux system and execute the command **sha256sum <filename>** or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
   c. Verify that the output produced by this command matches the hash value found on the support site.

NOTE

The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates pre-loaded on the controller at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the controller will not load a corrupted image.

4. Log in to the ArubaOS WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
   a. Select the **Upload Local File** option.
   b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. In the **partition to upgrade** field, select the non-boot partition.
8. In the **Reboot Controller After Upgrade** field, best practices is to select **Yes** to automatically reboot after upgrading. If you do not want the controller to reboot immediately, select **No**.

NOTE

Note that the upgrade will not take effect until you reboot the controller.

9. In the **Save Current Configuration Before Reboot** field, select **Yes**.
10. Click **Upgrade**.

    When the software image is uploaded to the controller, a popup window displays the message **Changes were written to flash successfully**.
11. Click **OK**.

    If you chose to automatically reboot the controller in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).
12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade.

When your upgrade is complete, perform the following steps to verify that the controller is behaving as expected.

1. Log in to the WebUI to verify all your controllers are up after the reboot.
2. Navigate to **Monitoring > Network Summary** to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a back up of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 242 for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses. The RAP-5/RAP-5WN reboots to complete the provisioning image upgrade.

Install Using the CLI

CAUTION

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash available for an upgrade using the CLI. For details, see Memory Requirements on page 241.

Upgrading From an Older Version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.4.3.1.

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS RN-3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
- For ArubaOS 6.0.0.0 or 6.0.0.1 versions, download the latest version of ArubaOS 6.0.1.x.

Follow steps 2 through 7 of the procedure described in Upgrading From a Recent Version of ArubaOS on page 245 to install the interim version of ArubaOS, and then repeat steps 1 through 7 of the procedure to download and install ArubaOS 6.4.3.1.

Upgrading From a Recent Version of ArubaOS

The following steps describe the procedure to upgrade from one of these recent versions of ArubaOS:

- 3.4.4.1 or later
- 5.0.3.1 or later 5.0.x
- 6.0.1.0 or later 6.x

To install the ArubaOS software image from a PC or workstation using the Command-Line Interface (CLI) on the controller:

1. Download ArubaOS 6.4.3.1 from the customer support site.
2. Open a Secure Shell session (SSH) on your master (and local) controllers.
3. Execute the **ping** command to verify the network connection from the target controller to the SCP/FTP/TFTP server:

   ```
   (hostname)# ping <ftphost>
   ```

   or

   ```
   (hostname)# ping <tftphost>
   ```

   or

   ```
   (hostname)# ping <scphost>
   ```

4. Use the **show image version** command to check the ArubaOS images loaded on the controller's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

```
(hostname) #show image version
----------------------------------
Partition               : 0:0 (/dev/ha1)
Software Version        : ArubaOS 6.1.1.0 (Digitally Signed - Production Build)
Build number            : 28288
Label                   : 28288
Built on                : Thu Apr 21 12:09:15 PDT 2012
----------------------------------
Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
Build number            : 38319
Label                   : 38319
Built on                : Fri June 07 00:03:14 2013
```

5. Use the **copy** command to load the new image onto the non-boot partition:

```
(hostname)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```

NOTE

The USB option is available on the 7010, 7030, and 7200 Series controllers.

6. Issue the **show image version** command to verify the new image is loaded:

```
(hostname)# show image version

----------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : ArubaOS 6.4.3.1 (Digitally Signed - Beta Build)
Build number            : 49734
Label                   : 49734
Built on                : Tue Apr 21 15:06:01 PDT 2015
----------------------------------
Partition               : 0:1 (/dev/hda2)
Software Version        : ArubaOS 6.4.3.0 (Digitally Signed - Production Build)
Build number            : 49296
Label                   : 49296
Built on                : Sun Mar 15 01:15:24 PDT 2015
```

7. Reboot the controller:

```
(hostname)# reload
```

8. Execute the **show version** command to verify the upgrade is complete.

```
(hostname)# show version
```

Once your upgrade is complete, perform the following steps to verify that the controller is behaving as expected.

1. Log in to the command-line interface to verify all your controllers are up after the reboot.
2. Issue the **show ap active** command to determine if your APs are up and ready to accept clients.

3. Issue the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See Backing up Critical Data on page 242 for information on creating a backup.

Downgrading

If necessary, you can return to your previous version of ArubaOS.

WARNING

If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.4.3.1 are lost after the downgrade (this warning does not apply to upgrades from 3.4.x to 6.1).

CAUTION

If you do not downgrade to a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.4.3.1 to 5.0.3.2, changes made to WIPS in 6.x prevent the new predefined IDS profile assigned to an AP group from being recognized by the older version of ArubaOS. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

These new IDS profiles begin with *ids-transitional* while older IDS profiles do not include *transitional*. If you have encountered this issue, use the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with AP Group.

CAUTION

When reverting the controller software, whenever possible, use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Before You Begin

Before you reboot the controller with the pre-upgrade software version, you must perform the following steps:

1. Back up your controller. For details, see Backing up Critical Data on page 242.
2. Verify that control plane security is disabled.
3. Set the controller to boot with the previously-saved pre-ArubaOS 6.4.3.1 configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message is displayed if system boot parameters are set for incompatible image and configuration files.
5. After downgrading the software on the controller:
   - Restore pre-ArubaOS 6.4.3.1 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.4.3.1 flash backup file.
   - You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.4.3.1, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.4.3.1, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading Using the WebUI

The following sections describe how to use the WebUI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the pre-upgrade configuration file.
   b. For **Destination Selection**, enter a filename (other than default.cfg) for Flash File System.
2. Set the controller to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the Configuration File menu.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition):
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

The following sections describe how to use the CLI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:

   ```
   (host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
   ```

   or

   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```

2. Set the controller to boot with your pre-upgrade configuration file.

   ```
   (host) # boot config-file <backup configuration filename>
   ```

3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).

   In the following example, partition 1, the backup system partition, contains the backup release ArubaOS 6.1.3.2. Partition 0, the default boot partition, contains the ArubaOS 6.4.3.1 image:

   ```
   #show image version
   ----------------------------------
   Partition                : 0:0 (/dev/hda1) **Default boot**
   Software Version         : ArubaOS 6.4.3.1 (Digitally Signed - Beta Build)
   Build number             : 49734
   Label                    : 49734
   Built on                 : Tue Apr 21 15:06:01 PDT 2015
   ----------------------------------
   Partition                : 0:1 (/dev/hda2)
   Software Version         : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
   Build number             : 38319
   Label                    : 38319
   ```

```
Built on                : Fri June 07 00:03:14 2013
```

4. Set the backup system partition as the new boot partition:

   ```
   (host) # boot system partition 1
   ```

5. Reboot the controller:

   ```
   (host) # reload
   ```

6. When the boot process is complete, verify that the controller is using the correct software:

   ```
   (host) # show image version
   ```

Before You Call Technical Support

Before you place a call to Technical Support, follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba controller with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file of the controller at the time of the problem. Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture logs from the controller.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Aruba controller) or any recent changes to your controller and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred. If the problem is reproducible, list the exact steps taken to recreate the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the controller site access information, if possible.