AOS-W Instant 6.2.1.0-3.3.0.2

Alcatel·Lucent

Release Notes

Copyright

© 2013 Alcatel-Lucent. All rights reserved.

Specifications in this manual are subject to change without notice.

Originated in the USA.

AOS-W, Alcatel 4302, Alcatel 4304, Alcatel 4306, Alcatel 4308, Alcatel 4324, Alcatel 4504, Alcatel 4604, Alcatel 4704, Alcatel 6000, OAW-AP41, OAW-AP68, OAW-AP60/61/65, OAW-AP70, OAW-AP80, OAW-AP92/93, OAW-AP105, OAW-AP120/121, OAW-AP124/125, OAW-AP175, OAW-IAP92/93/105, OAW-RAP2, OAW-RAP5, and Omnivista 3600 Air Manager are trademarks of Alcatel-Lucent in the United States and certain other countries.

Any other trademarks appearing in this manual are the property of their respective companies. Includes software from 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.

Legal Notice

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

Alcatel·Lucent

www.alcatel-lucent.com

26801 West Agoura Road
Calabasas, CA 91301

Contents

Chapter 1

Release Overview

AOS-W Instant 6.2.1.0-3.3.0.2 is a software patch release that introduces fixes to the issues identified in the previous releases.

Contents

- "What's New in this Release" on page 7 lists the issues fixed in this release of AOS-W Instant.
- "Features Added in the Previous Release" on page 9 describes the new features introduced in AOS-W Instant 6.2.1.0-3.3.
- "Issues Fixed in Previous Releases" on page 17 lists the issues fixed in the previous releases of AOS-W Instant.
- "Known Issues from Previous Releases" on page 21 describes the known issues and limitations identified in the previous releases of AOS-W Instant.

Contacting Support

Contact Center Online	
● **Main Site**	http://www.alcatel-lucent.com/enterprise
● **Support Site**	https://service.esd.alcatel-lucent.com
● **Email**	esd.support@alcatel-lucent.com
Service & Support Contact Center Telephone	
● **North America**	1-800-995-2696
● **Latin America**	1-877-919-9526
● **Europe**	+33 (0) 38 855 6929
● **Asia Pacific**	+65 6240 8484
● **Worldwide**	1-818-878-4507

What’s New in this Release

The following issues are fixed in the current release of AOS-W Instant.

AP Regulatory Domain Updates

The following table describes regulatory domain updates included in the AOS-W Instant 6.2.1.0-3.3.0.2 release.

Table 1 *Regulatory Domain Support*

Hardware/ Device	Domain Support
OAW-RAP155/ 155P	The OAW-RAP155/155P now supports the European Union (EU) regulatory domain. Ensure that the Equivalent isotropically radiated power (EIRP) settings applicable for the EU domain are applied to the devices running in the EU domain.

Issues Fixed in this Release

Mesh Network

Table 2 *Mesh Network Fixed Issues*

Bug ID	Description
84220	**Symptom:** A Mesh OAW-IAP rebooted due to inappropriate memory allocation. Changes to the wireless driver have resolved the memory allocation issue. **Scenario:** The issue was observed in dual radio OAW-IAPs where at least one OAW-IAP functioned as a Mesh portal and the available memory was less than 2 MB. The issue was not limited to a specific OAW-IAP model or AOS-W Instant release version.
84744	**Symptom**: Wired clients could not access the network through Ethernet0 bridging port configured on an OAW-IAP. Changes in the Address Resolution Protocol (ARP) packets broadcasting process for the Ethernet0 bridging scenario have resolved this issue. **Scenario**: This issue occurred when Ethernet0 bridging was enabled for the wired clients. Due to this issue, the ARP packets were sent back to the Switch. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3 in Mesh topology.
84826	**Symptom:** In some cases, a Mesh point could not connect to the Mesh portal. Upgrading to AOS-W Instant 6.2.1.0-3.3.0.2 resolves this issue. **Scenario:** This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3.0.1 in Mesh topology.

Station Management

Table 3 *Station Management Fixed Issue*

Bug ID	Description
84827	**Symptom:** Incorrect status details were displayed for the unauthenticated clients. Changes to the code base have resolved this issue. **Scenario:** Due to this issue, the **show clients** command output displayed incorrect channel and device type parameters. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.3.

VLAN Configuration

Table 4 *VLAN Configuration Fixed Issue*

Bug ID	Description
85013	**Symptom:** Client authentication through the slave OAW-IAP failed when Dynamic RADIUS Proxy was enabled and the uplink VLAN was configured. To resolve this issue, a check is introduced to verify the uplink VLAN configuration, before sending the RADIUS packets when Dynamic RADIUS Proxy is enabled. **Scenario:** This issue occurred because RADIUS packets were tagged with an incorrect VLAN. Due to this issue, the RADIUS packets from the OAW-IAP could not reach the authentication server. This issue was found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3.

Chapter 3

Features Added in the Previous Release

This chapter provides a brief summary of the new features included in the previous version of AOS-W Instant.

For more information on the features listed in section and the related configuration procedures, see *AOS-W Instant 6.2.1.0-3.3 User Guide.*

Features and Enhancements

Configuration of OAW-IAPs Using AOS-W Instant CLI

In the current release, AOS-W Instant supports scripting through Command Line Interface (CLI). You can access the AOS-W Instant CLI through a Secure Shell (SSH).

To enable the SSH access to the AOS-W Instant CLI, go to **System** > **Show advanced options** and select **Enabled** from the **Terminal access** drop-down list.

When you make configuration changes on a master in the CLI, all associated OAW-IAPs in the cluster inherit these changes and subsequently update their configurations. The changes configured in a CLI session are saved in the CLI context. The CLI does not support the configuration data exceeding a buffer size of 4K in a CLI session; therefore, Alcatel-Lucent recommends that you configure fewer changes at a time and apply the changes at regular intervals.

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

```
(Instant Access Point)# commit apply
```

Sequence-Sensitive Commands

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

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

Table 1 *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command
`opendns <username <password>`	`no opendns`
`rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit |deny | src-nat | dst-nat {<IPaddress> <port>|<port>}}[<option1....option9>]`	`no rule <dest> <:mask> <match> <protocol> <start-port> <end-port> {permit | deny | src-nat | dst-nat}`
`mgmt-auth-server <auth-profile-name>`	`no mgmt-auth-server <auth-profile-name>`

Table 1 *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command
set-role <attribute>{{equals| not-equals| startswith| ends-with| contains} <operator> <role>| valueof}	no set-role <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator>| value-of} no set-role
set-vlan <attribute>{{equals| not-equals| startswith| ends-with| contains} <operator> <VLAN-ID>| value-of}	no set-vlan <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator>| value-of} no set-vlan
auth-server <name>	no auth-server <name>

AOS-W Instant User Interface (UI) Enhancements

In the current release, the AOS-W Instant UI is enhanced, and the menu options and configuration windows are reorganized. For more information on the new UI layout and menu categories, see *AOS-W Instant 6.2.1.0-3.3.0.1 User Guide.*

Spectrum Load Balancing

Spectrum load balancing feature helps optimize network resources by balancing client load across channels and by dividing APs in a cluster into several logical AP RF neighborhood domains, which share the same clients. When the Spectrum load balancing feature is enabled, the Virtual Controller (VC) determines the distribution of clients and balances client load across channels, regardless of whether the AP is responding to the wireless clients' probe requests.

With this feature, the client load for an AP is determined based on the value specified for the SLB threshold. When the client load on an AP reaches or exceeds the SLB threshold in comparison to its neighbors, or if a neighboring AP on another channel does not have any clients, load balancing is enabled on that AP, to allow clients to connect to an available or less loaded channel. When the client count reaches or exceeds the threshold, the APs with load balancing enabled will not send probe response or authentication response to the new client requests.

You can enable spectrum load balancing by using the AOS-W Instant UI or CLI. For more information, see *AOS-W Instant 6.2.1.0-3.3.0.1 User Guide.*

WMM Traffic Management

The Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance specification based on the IEEE 802.11e wireless Quality of Service (QoS) standard. You can allocate WMM traffic share for the voice, video, best effort, and background access categories when configuring an SSID profile.

The following parameters can be configured for a WLAN SSID profile:

- **Background WMM share** — Allocates bandwidth for background traffic such as file downloads or print jobs.
- **Best effort WMM share** —Allocates bandwidth for best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS.
- **Video WMM share** —Allocates bandwidth for video traffic generated from video streaming.
- **Voice WMM share** —Allocates bandwidth for voice traffic generated from incoming and outgoing voice communication.

In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can allocate higher values for Best effort WMM share and Voice WMM share to allocate a higher bandwidth to clients transmitting best effort and voice traffic.

You can configure WMM traffic management parameters by using AOS-W Instant UI or CLI. For more information, see *AOS-W Instant 6.2.1.0-3.3.0.1 User Guide*.

Role Derivation for Wired Clients

AOS-W Instant now supports role derivation for wired network profiles. The administrators can configure roles and access rules for the user roles, and assign user roles to determine the network privileges for wired clients. You can also assign a pre-authentication role and enforce MAC authentication only roles for wired clients.

The pre-authentication role is assigned to the users in the following scenarios:

- When the Captive portal authentication fails in a guest wired network that has only the Captive Portal authentication enabled.
- When both MAC authentication and Captive portal authentication fail in a guest network that has both Captive portal and MAC authentication enabled.
- When the 802.1X authentication fails in an employee network that has the 802.1X authentication enabled.

The MAC authentication only role is assigned to the users in the following scenarios:

- When the MAC authentication is successful in a guest wired network that has both Captive portal and MAC authentication enabled.
- When the MAC authentication is successful and if the 802.1X authentication fails in an employee network that has both 802.1X and MAC authentication enabled.

The user roles can be configured by using the AOS-W Instant UI or CLI.

Reboot After an OAW-IAP Upgrade

AOS-W Instant now allows the users to defer rebooting of the OAW-IAP after a software upgrade. The users can choose to reboot the OAW-IAP after the upgrade or at a later time by navigating to **Maintenance > Firmware** and selecting or clearing the **Reboot all APs after upgrade** check box or by using the `upgrade-image2-no-reboot <ftp/tftp/http-URL>`. By default, all OAW-IAPs reboot after an upgrade.

Configurable SSID Status

The users can now disable an SSID and enable it when required. The disabled SSID is not removed from the network and will be indicated as a disabled SSID. All SSIDs are enabled by default.

You can configure SSID status by using AOS-W Instant UI or CLI. For more information, see *AOS-W Instant 6.2.1.0-3.3.0.1 User Guide*.

Broadcasting of AOS-W Instant SSID Based on AirWave and Activate Availability

The OAW-IAPs boot with factory default configuration and will try to provision automatically. If the automatic provisioning is successful, the instant SSID will not be available. If AirWave and Activate are not reachable and the automatic provisioning fails, the instant SSID becomes available and the users can connect to a provisioning network by using the instant SSID.

Read-Only Access to the AOS-W Instant UI When AirWave is in the Management Mode

In the AirWave User Interface (UI), you can select either **Manage Read/Write** or M**onitoronly+Firmware Upgrades** as management modes. When the Management level is set to **Manage Read/Write**, the AOS-W

Instant UI is in the read-only mode. If Airwave Management Level is set to **Monitoronly+Firmware Upgrades** mode, the AOS-W Instant UI changes to the read-write mode.

IAP-VPN Enhancements

AOS-W Instant allows you to configure the DHCP address assignment modes for the branches connected to the corporate network through VPN. You can configure the range of DHCP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

You can configure Distributed, L2, Distributed, L3, Local, Local-L3 (NAT and L3 switching), and Centralized, L2 DHCP scopes and vendor-specific DHCP options for the DHCP scopes.

NOTE

The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The OAW-IAP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.

The AOS-W Instant UI is enhanced to provide a easy and flexible workflow for configuration and the `show iap table` command available on the controller now displays the branch name, ID, and subnet details. For more information on configuring DHCP scopes, see *AOS-W Instant 6.2.1.0-3.3.0.1 User Guide*.

Support for Dual Ethernet Uplinks

AOS-W Instant supports configuration of dual Ethernet uplinks for wired profiles. When the primary uplink on an existing Ethernet port fails, the OAW-IAP switches over to the uplink available on an alternate physical port. You can also set a priority for uplinks, so that the OAW-IAP can switch over to a higher priority uplink when required. By default, the Eth0 uplink is set as a high priority uplink.

Ethernet VLAN Assignment and VLAN Derivation

In the current release, the Virtual Controller can assign a guest VLAN for a wired network profile. You can also assign VLANs for wired clients based on the user roles configured wired network profile.

You can assign VLANs and configure VLAN derivation rules by using AOS-W Instant UI or CLI. For more information, see *AOS-W Instant 6.2.1.0-3.3.0.1 User Guide*.

VLAN Derivation Based on DHCP Option

You can now configure VLAN derivation rules based on a DHCP option. The **dhcp-option** is available in the list of attributes in the **New VLAN Assignment Rule** window. You can also configure VLAN derivation rules based on DHCP option for Captive portal authentication. When the Captive portal authentication is successful, the role derivation based on DHCP option assigns a new user role to the guest users, instead of the pre-authenticated role.

Protection from ARPs Attack

AOS-W Instant allows you to enable firewall settings to protect against wired attacks, such as ARP attacks or malformed DHCP packets, and notify the administrator when these attacks are detected.

Captive Portal Enhancements

Access to the Internet When the External Captive Portal Server is Not Available

This feature allows the guest users to access the Internet when the external Captive portal is not available. When the external Captive portal is not available, the guest users are redirected to the URL specified in the SSID profile.

Configurable Accounting Modes for Guest Users

This feature allows you to configure the accounting mode for guest users to determine when to start and stop accounting for a captive portal SSID. When the accounting mode is set to **Authentication**, the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the Accounting mode is set to **Association**, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.

Disable Captive Portal Authentication based on the Current Uplink Type

This feature allows you to disable redirection to the Captive portal based on the type of current uplink. The disable uplink option is available for both internal and external Captive portal splash pages.

8021X Authentication with Captive Portal Role

AOS-W Instant now supports the configuration of access rules to enforce Captive portal authentication for an SSID that has 802.1X authentication enabled. You can configure rules to provide access to external Captive portal, internal Captive portal, or none, so that some of the clients using this SSID can derive the Captive portal role.

The following conditions apply to the 802.1X and Captive portal authentication configuration:

- If a user role does not have Captive portal settings configured, the Captive portal settings configured for an SSID are applied to the client's profile.
- If the SSID does not have Captive portal settings configured, the Captive portal settings configured for a user role are applied to the client's profile.
- If Captive portal settings are configured for both SSID and user role, the Captive portal settings configured for a user role are applied to the client's profile.

You can create a Captive portal role for both **Internal-acknowledged** and **External Authentication Text** splash page types.

Automatic Whitelisting of URLs

You can now enable or disable automatic whitelisting of the URLs when setting up a guest network by using the AOS-W Instant UI or CLI. The **Automatic URL Whitelisting** check box is introduced in the **External-RADIUS Authentication** and **External Authentication Text** splash pages in the AOS-W Instant UI to allow the users to enable or disable this feature.

On selecting the check box for the external Captive portal authentication, the URLs that the unauthenticated users are allowed to access are automatically whitelisted. In the current release, the automatic URL whitelisting is disabled by default.

You can also enable or disable the automatic whitelisting of URLs by using AOS-W Instant CLI:

To disable automatic whitelisting of URLs:

```
auto-whitelist-disable
```

To re-enable automatic whitelisting of URLs:

```
no auto-whitelist-disable
```

Configurable VLAN for the Virtual Controller IP

AOS-W Instant supports assigning a VLAN for the Virtual Controller (VC). You can configure the VC IP, VLAN, Mask, and Gateway. When the VC VLAN is not configured, the VC IP is configured with the default mask. When a new VLAN, mask and gateway are assigned, the VC IP is updated with the new mask configured.

Support for 512 User Entries in the Local User Database of OAW-IAPs

The local user database of APs can support up to 512 user entries except IAP-9x. IAP-9x supports only 256 user entries. If there are already 512 users, IAP-9x will not be able to join the cluster.

Support for Configuring Hotspot Profiles

Hotspot 2.0 is a Wi-Fi Alliance specification based on the 802.11u protocol, which allows wireless clients to discover hotspots using management frames (such as beacon, association request and association response), connect to networks, and roam between networks without additional authentication. The Hotspot 2.0 provides the following services:

- Network discovery and selection— Allows the clients to discover suitable and available networks by advertising the access network type, roaming consortium, and venue information through the management frames. For network discovery and selection, Generic Advertisement Service (GAS) and Access Network Query Protocol (ANQP) are used.
- QOS Mapping— Provides a mapping between the network-layer QoS packet marking and over- the-air QoS frame marking based on user priority.This feature supports the configuration hotspot profiles for a WLAN SSID profile.

A hotspot profile contains one or several advertisement profiles. You can configure the following advertisement profiles through the AOS-W Instant CLI:

- NAI Realm profile
- Venue Name Profile
- Network Auth Profile
- Roaming Consortium Profile
- 3GPP Profile
- IP Address availability Profile
- Domain Name Profile
- Operator Friendly Name Profile
- Connection Capability Profile
- Operating Class Profile
- WAN Metrics Profile

NOTE

In the current release, AOS-W Instant supports the hotspot profile configuration only through the CLI.

You can configure a hotspot profile and associate the advertisement profiles to use for a hotspot network connection or setup. The hotspot profile can be enabled on one or more SSID profile by creating a reference in the WLAN SSID profile.

Support for Policy Based Corporate Access and Source Based Routing

You can configure a policy based corporate access for client traffic in AOS-W Instant. For example, you can configure an OAW-IAP to send all traffic on an SSID to the corporate network, while another SSID can be configured with direct access to the Internet for some services, protocols, or destinations.

You can also configure source based routing for client traffic by allowing traffic on one SSID to reach the Internet through a corporate network and another SSID to use an alternate uplink.

AirGroup Enhancements

AirGroup now enables a client to perform a location-based discovery. For example, when a client roams from one OAW-IAP cluster to another, it can discover devices available in the new cluster to which the client is currently connected.

The AirGroup users can also configure Bonjour Services in the guest VLAN. When enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN.

Support for SNMP Standard Tables

AOS-W Instant now supports the standard SNMP IF-MIB and Q-BRIDGE MIB tables, and System MIB objects. The aiRadioTable and aiAccessPointTable are also enhanced to include objects to indicate the OAW-IAP status, memory, and the radio status of an OAW-IAP. For more information on the SNMP MIB objects and AOS-W Instant MIB enhancements, see *AOS-W Instant 6.2.1.0-3.3.0.1 MIB Reference Guide*.

Issues Fixed in Previous Releases

The following issues were fixed in the previous release of AOS-W Instant.

Issues Fixed in 6.2.1.0-3.3.0.1

Adaptive Radio Management

Table 1 *Adaptive Radio Management Fixed Issue*

Bug ID	Description
83332	**Symptom:** The OAW-IAPs now show the updated EIRP values for the Europe (EU and Croatia) regulatory domains. **Scenario:** Due to a change in regulatory standards for the Europe and Croatia domains, the EIRP values were updated. The OAW-IAPs running AOS-W Instant 6.2.1.0-3.3.0.1 now display the updated EIRP values for these regulatory domains.

Authentication

Table 2 *Authentication Fixed Issue*

Bug ID	Description
81530	**Symptom:** Clients devices such as Apple MacBook and iPhone were intermittently disconnected from the network and lost connection to the Gateway and Internet, although they were connected to the OAW-IAP. Internal changes to the authentication process and performing a full authentication have fixed this issue. **Scenario:** This issue occurred because the client access role was placed in denied state randomly when the MAC authentication was enabled on the SSID. This was a rare issue and was not limited to a specific OAW-IAP model or a software version.

Captive Portal

Table 3 *Captive Portal Fixed Issue*

Bug ID	Description
77136	**Symptom:** The Captive portal page displayed incomplete information during Captive portal authentication of guest users. Changes to the OAW-IAP code have fixed this issue. **Scenario:** This issue occurred because a Fully Qualified Domain Name (FQDN) was used for HTTP redirection.This issue was found in OAW-IAPs running AOS-W Instant version 6.1.3.4-3.1.0.0 or later.

Instant UI

Table 4 *Instant UI Fixed Issue*

Bug ID	Description
80501	**Symptom:** The Japanese version of Instant UI displayed garbled and unreadable Japanese characters when launched through Google Chrome. Changes to the default character set in the Web server have fixed this issue. **Scenario:** This issue occurred when a user tried to access the Japanese version of Instant UI through Google Chrome 25 and later versions. This issue occurred because the Japanese version of 6.2.0.0-3.2.0.2 Instant UI was not compatible with Google Chrome 25 and later versions.

Syslog

Table 5 *Syslog Fixed Issue*

Bug ID	Description
83649	**Symptom:** OAW-IAPs did not provide the user ID, IP address and MAC address of the authenticated clients in a single log file. With changes in the Syslog Logging Levels configuration, the OAW-IAPs now provide a single log file that displays the User ID, IP address, and MAC address information when the authenticated clients are connected. **Scenario:** This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.3 or lower versions.

VLAN Configuration

Table 6 *VLAN Configuration Fixed Issue*

Bug ID	Description
82710 82984	**Symptom:** A WLAN client was unable to obtain an IP address from the OAW-IAP. Changes to the client VLAN assignment have fixed this issue. **Scenario:** The issue occurred when the OAW-IAP sent VLAN ID tag in frames for clients connected to an SSID. The native VLAN with a non-default value was configured for the OAW-IAP uplink. Therefore, clients connecting to the native VLAN could not obtain an IP address. The issue was not specific to any OAW-IAP model and was observed in AOS-W Instant 6.2.0.0-3.2.0.2.

Issues Fixed in 6.2.1.0-3.3

Authentication

Table 7 *Authentication Fixed Issue*

Bug ID	Description
75822	**Symptom:** The idle timeout value set on the RADIUS server could not take effect on an OAW-IAP. Changes to the control path have resolved this issue. **Scenario:** This issue occurred when different values for the idle timeout were configured on the RADIUS server and the OAW-IAP. This issue was found in OAW-IAPs running AOS-W Instant 6.2.0.0-3.2.

VPN Configuration

Table 8 *VPN Configuration Fixed Issue*

Bug ID	Description
72166	**Symptom:** The clients in the VPN NAT mode could not ping large packets of data to the corporate IP address. Changes to the code base have resolved this issue. **Scenario:** This issue was not limited to a specific OAW-IAP model or AOS-W Instant version.

Chapter 5

Known Issues from Previous Releases

The known issues and limitations identified in the previous releases of AOS-W Instant are described in the following tables.

SNMP

Table 1 *SNMP Known Issues*

Bug ID	Description
82752	**Symptom**: The value for the SNMP aiRadioPhyEvents counter is always displayed as **0**. **Scenario**: This issue is found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3. **Workaround:** None

VLAN Configuration

Table 2 *VLAN Configuration Known Issue and Limitation*

Bug ID	Description
75496	**Symptom:** A slave OAW-IAP cannot connect to the master OAW-IAP when reconnecting to the network. **Scenario:** This issue occurs when the Ethernet uplink fails and switches over to another available uplink. This issue was observed in a hierarchical network topology when the native VLAN on a wired port was set to a value that is not equal to 1. This issue is found in OAW-IAPs running AOS-W Instant version 6.2.0.0-3.2 or later. **Workaround:** None
80849	**Symptom:** In a hierarchical topology, although the clients can obtain an IP address, the Virtual Controller Gateway IP address resolution fails. **Scenario:** This issue occurs when the master OAW-IAP assigns a guest VLAN IP address to the client. As the DHCP scope configuration on the slave OAW-IAP uses a different subnet, the Virtual Controller gateway IP address cannot be resolved. This issue is found in OAW-IAPs running AOS-W Instant 6.2.1.0-3.3. **Workaround:** Manually configure the DHCP pool to ensure that the appropriate subnet is used for assigning IP addresses to the clients.