AOS-W Instant AP

Alcatel·Lucent Enterprise

Troubleshooting Guide

Contents

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

About this Guide

The AOS-W Instant AP Troubleshooting Guide contains information on how to troubleshoot the common errors encountered in AOS-W Instant APs. This guide contains information on the symptom of the issue, procedures to identify the cause, and steps to resolve them. The errors described in this guide are largely configuration issues that can be resolved with basic troubleshooting. If the solution described in the guide does not resolve the issue contact Alcatel-Lucent Technical Support.

Intended Audience

This guide is intended for administrators who configure and use OAW-IAPs.

Related Documents

In addition to this document, the OAW-IAP product documentation includes the following:

- Alcatel-Lucent AP Software Quick Start Guide
- AOS-W Instant Access Point Installation Guides
- AOS-W Instant CLI Reference Guide
- AOS-W Instant Release Notes
- AOS-W Instant REST API Guide
- AOS-W Instant Syslog Messages Reference Guide
- AOS-W Instant User Guide

Conventions

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

Table 2: *Typographical Conventions*

Style Type	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: ■ Sample screen output ■ System prompts ■ Filenames, software devices, and specific commands when mentioned in the text.
`Commands`	In the command examples, this style depicts the keywords that must be typed exactly as shown.

Table 2: *Typographical Conventions*

Style Type	Description
<Arguments>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: `# `**`send`**` <text message>` In this example, you would type "send" at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
`[Optional]`	Command examples enclosed in square brackets are optional. Do not type the square brackets.
`{Item A | Item B}`	In the command examples, items within curly brackets and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the curly brackets or bars.

The following informational icons are used throughout this guide:

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

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

Indicates a risk of personal injury or death.

Contacting Support

Table 3: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal2.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

The following are common issues observed during the provisioning process of an AP:

- AP Fails to Receive Provisioning Rule from Activate
- AP Fails to Receive Provisioning Rule from DHCP Server
- The SetMeUp SSID for AP Provisioning is Not Broadcasted
- Slave AP Fails to Provision in an AOS-W Instant Cluster

AP Fails to Receive Provisioning Rule from Activate

The APs after receiving its IP address, netmask, and gateway IP address from the DHCP server will establish a connection with the Activate server to retrieve the provisioning rule. In some cases, the AP might fail to receive the provisioning rule and remain in the factory default state.

The following procedure describes how to troubleshoot issues, if the AP fails to receive the provisioning rule from Activate:

1. Check the Uplink of the AP
2. Check the Status of Activate Connection
3. Check if Access to Activate Server is Allowed in the Network Firewall

Check the Uplink of the AP

Ensure that the AP has an active uplink connection to reach the Activate server.

Run the **show uplink status** command to the view the state of uplink connections of the AP. If the state of the active uplink connection is **DOWN**, resolve the issue with the AP uplink.

The sample below displays information of the uplink connection of the AP, generated by the **show uplink status** command:

```
(Instant AP)# show uplink status

Uplink preemption             :enable
Uplink preemption interval    :600
Uplink enforce                :none
Ethernet uplink eth0          :DHCP
Uplink Table
------------
Type       State   Priority   In Use
----       -----   --------   ------
eth0       DOWN    0          Yes
Wifi-sta   INIT    6          No
3G/4G      INIT    7          No
Internet failover                     :disable
Max allowed test packet loss          :10
Secs between test packets             :30
VPN failover timeout (secs)           :180
Internet check timeout (secs)         :10
ICMP pkt sent        :0
```

```
ICMP pkt lost         :0
Continuous pkt lost   :0
VPN down time         :0
AP1X type:NONE
Certification type:NONE
Validate server:NONE
```

Check the Status of Activate Connection

Run the **show activate status** command to view the status of Activate connection. The output of this command will display the reason for failure, if the AP fails to connect to Activate.

The following are possible states of the Activate connection:

Activate Status	Inference
success	The AP is connected to Activate and received a provisioning rule.
connection_failed	The AP failed to connect to Activate. The reason for connection failure is displayed in the Activate fail reason line.
connecting	The AP is able to reach Activate but the provisioning rule is not defined.
fail-prov-no-rule	
fail-TCP-error	There in an uplink error in the TCP port of the AP.

The sample below displays the Activate connection information of the AP, generated by the **show activate status** command:

```
(Instant AP)# show activate status
IAP MAC Address           :90:4c:81:c3:28:1e
IAP Serial Number         :USGHK514D1
Cloud Activation Key      :
Activate Server           :device.arubanetworks.com
Activate Status           :connection-failed
Activate fail reason      :dns error
Provision interval        :5 minutes
```

Check if Access to Activate Server is Allowed in the Network Firewall

Check the network firewall and ensure that traffic to **device.arubanetworks.com** is allowed.

AP Fails to Receive Provisioning Rule from DHCP Server

After initial boot up all APs connect to the DHCP server to receive IP address, netmask, and gateway IP address. APs can be configured to receive the provisioning rule through the DHCP server by configuring DHCP options- **option 60** and **option 43**.

The following procedure describes how to troubleshoot issues, if the AP fails to receive provisioning rule from DHCP server:

1. Check the Configuration of DHCP Options
2. Check if the AP has OmniVista 3600 Air Manager IP Configured

Check the Configuration of DHCP Options

Run the **show dhcpc-opts** command to view DHCP options received from the DHCP server. If the DHCP options, option 43 and option 60, are not displayed in the output, configure the options again in the DHCP server and retry provisioning. Ensure to use the correct syntax when configuring the DHCP options.

The following is the syntax to configure the DHCP options:

DHCP Option	Syntax	Example
Option 060	ArubaInstantAP — for OAW-IAP deployments	ArubaInstantAP
Option 043	<Organization name>, <OmniVista 3600 Air Manager IP>, <OmniVista 3600 Air Manager Shared key>	Aruba, 192.0.2.20, 12344567
	<Organization name>, <OmniVista 3600 Air Manager domain**>**	Aruba, aruba.support.com

The sample below displays the DHCP options received by the AP, generated by the **show dhcp-opts** command:

```
[Instant AP]# show dhcpc-opts


------------------DHCP option43 -------------------
Not available
```

Check if the AP has OmniVista 3600 Air Manager IP Configured

APs will not use DHCP options for provisioning if OmniVista 3600 Air Manager IP is configured. OmniVista 3600 Air Manager IP takes precedence over DHCP options.

Run the **show summary** command to view the configuration summary of the AP. In the configuration summary, check the OmniVista 3600 Air Manager server line to determine if the OmniVista 3600 Air Manager IP is configured. If OmniVista 3600 Air Manager IP is confiigured, clear all configurations and reboot the AP to provision using the DHCP options.

The sample below displays the summary of AP configuration, generated by the **show summary** command:

```
[Instant AP]# show summary


Name                  :SetMeUp-CF:77:34
System Location       :
Domain                :
VC IP Address         :0.0.0.0
VC IPv6 Address       :::
AP1X                  :NONE
VC VLAN               :0
VC Mask               :0.0.0.0
VC Gateway            :0.0.0.0
VC DNS                :0.0.0.0
IP Mode               :v4-only
Cluster-Security DTLS:disable
Content Filtering     :disable
Terminal Access       :enable
```

```
Telnet Server       :disable
Activate Disable    :disable
Organization        :
Disable ciphers     :
Airwave Server      :
Airwave Backup Server:
Airwave Prov Backup :
Number of VC transition  :0
Airwave Shared Key  :
Airwave Config Via  :DHCP
Airwave             :Not Set Up
Managed Via         :Local
```

The SetMeUp SSID for AP Provisioning is Not Broadcasted

During the initial boot of a factory default AP, a SetMeUp SSID is broadcasted by the AP on the 2.4 GHz band. The provisioning rule for the AP can be defined using the AOS-W Instant WebUI by logging into the SetMeUp SSID. In certain cases, the SetMeUp SSID may not be broadcasted or the client may be fail to connect to the SSID.

The following procedure describes how to troubleshoot issues, if the AP fails to broadcast the Set Me Up SSID:

1. Check if the AP Received a Provisioning Rule
2. Check the Uplink of the AP
3. Connect to the SSID Using a Different Client Device

Check if the AP Received a Provisioning Rule

The Set Me Up SSID is configured to disable automatically when the AP receives a provisioning rule from Activate, OmniVista 3600 Air Manager, or DHCP server.

Run **show summary** command to view the configuration summary of the AP. Check if the AP has any provisioning rule from Activate, OmniVista 3600 Air Manager or the DHCP server. If the AP has a provisioning rule, clear all configurations, reboot the AP, and retry provisioning.

The sample below displays the summary of AP configuration, generated by the **show summary** command:

```
[Instant AP]# show summary

Name                :SetMeUp-CF:77:34
System Location     :
Domain              :IN
VC IP Address       :0.0.0.0
VC IPv6 Address     :::
AP1X                :NONE
VC VLAN             :0
VC Mask             :0.0.0.0
VC Gateway          :0.0.0.0
VC DNS              :0.0.0.0
IP Mode             :v4-only
Cluster-Security DTLS:disable
Content Filtering   :disable
Terminal Access     :enable
Telnet Server       :disable
Activate Disable    :disable
Organization        :
Disable ciphers     :
Airwave Server      :
```

```
Airwave Backup Server:
Airwave Prov Backup  :
Number of VC transition  :0
Airwave Shared Key   :
Airwave Config Via   :DHCP
Airwave              :Not Set Up
Managed Via          :Local
```

Check the Uplink of the AP

The broadcast of SetMeUp SSID will be disabled if the AP does not have an active uplink connection.

Run the **show uplink status** command to the view the state of uplink connections of the AP. If the state of the active uplink connection is **DOWN**, resolve the issue with the AP uplink.

The sample below displays information of the uplink connection of the AP, generated by the **show uplink status** command:

```
(Instant AP)# show uplink status

Uplink preemption            :enable
Uplink preemption interval   :600
Uplink enforce               :none
Ethernet uplink eth0         :DHCP
Uplink Table
------------
Type       State  Priority  In Use
----       -----  --------  ------
eth0       DOWN   0         Yes
Wifi-sta   INIT   6         No
3G/4G      INIT   7         No
Internet failover                   :disable
Max allowed test packet loss        :10
Secs between test packets           :30
VPN failover timeout (secs)         :180
Internet check timeout (secs)       :10
ICMP pkt sent        :0
ICMP pkt lost        :0
Continuous pkt lost  :0
VPN down time        :0
AP1X type:NONE
Certification type:NONE
Validate server:NONE
```

Connect to the SSID Using a Different Client Device

In certain scenarios, the Windows client is unable to access **instant.arubanetworks.com** despite the AP getting the IP address, netmask, and gateway IP address from the DHCP server. This is a limitation identified with certain versions of Windows. In such a scenario, connect to the SetMeUp SSID using a client running macOS or a different version of Windows.

Slave AP Fails to Provision in an AOS-W Instant Cluster

When an OAW-IAP is plugged into a network with an existing AOS-W Instant cluster, the AP should associate itself as a slave to the master AP and join the cluster. However in certain scenarios the AP might fail to associate with the master AP and remain unprovisioned.

The following procedure describes how to troubleshoot issues, if the slave AP fails to join the cluster:

Check if Auto Join is Enabled on the Master AP

Either of following conditions has to be met for the new AP to join the cluster:

- Auto join mode must be enabled on the cluster.
- The MAC address of the new AP must be added to the AP Whitelist table.

The AP cannot join the cluster if neither of these conditions are met.

Run the **show allowed-aps** command on the master AP to view the auto join setting and AP whitelist table of the AOS-W Instant cluster. If **Allow New APs** is set to **disable**, do any of the following:

- Enable Auto join mode in the **Configuration > System > Advanced Options** page of the AOS-W Instant webUI.
- Add the MAC address of the new AP to the AP whitelist table using the **allowed-ap <MAC address>** command.

The sample below displays the auto join setting of the cluster, generated by the **show allowed-aps** command:

```
(Master AP)# show allowed-aps

Allow New APs  :disable

AP Whitelist
-----------
MAC Address
-----------
90:4c:81:c3:28:1e
90:4c:81:cf:77:34
```

Check if the AOS-W Instant Cluster is DTLS Enabled

A DTLS-enabled AOS-W Instant cluster can only allow DTLS-enabled slave APs to join the cluster. However if Auto join mode is enabled on the cluster or the MAC address of the new AP is added to the AP Whitelist table, the AOS-W Instant cluster will accept a non-DTLS slave AP.

Run the **show cluster-security** command on the master AP to view the cluster security profile of the AOS-W Instant network. If **Non-DTLS Slaves** is set to **Deny**, do any of the following:

- Set **Non-DTLS Slaves** to allow in the **Configuration > System > Advanced Options** page of the AOS-W Instant webUI
- Enable **Auto join mode** in the **Configuration > System > Advanced Options** page of the AOS-W Instant webUI.
- Add the MAC address of the new AP to the AP whitelist table using the **allowed-ap <MAC address>** command.

The sample below displays the security settings of the cluster, generated by the **show cluster-security** command:

```
(Master AP)# show cluster-security

Cluster Security Profile
------------------------
Parameter            Value
---------            -----
DTLS config          Enabled
DTLS state           Enabled
Low assurance devices  Deny
Non-DTLS Slaves      Deny
Reboot required      No
```

Check if the Slave AP Received an IP address

Failure to receive or retain an IP address will cause the AP to reboot and go into a degraded state. The radio lights of the AP turns amber when the AP is in degraded state. An AP may fail to receive or retain an IP address if:

- DHCP server is not working.
- DHCP scope is exhausted.
- Lease period of the IP assigned is expired and the AP fails to renew it.
- Master AP is configured with a static IP.
- The default IP, Automatic Private IP Addressing (APIPA), is not allowed in the network.

Perform the following actions based on the network configuration to ensure that the AP receives a valid IP address:

Network Configuration	Action
Networks with a DHCP server	Ensure that the DHCP server has enough IP addresses for new APs.
	Check the lease period of the IP addresses.
Master AP defined with a static IP	Assign a static IP for slave AP in the same sub network as the master AP.

Check if the Slave AP and Master AP are in Different Sub Networks

The slave AP must be in the same subnet as the master AP to join the cluster.

Run the **show summary | include IP** command on the slave AP to view the IP address configurations on the slave AP. If the master AP and the slave AP have IP addresses in different sub networks, move the slave to the sub network of the master AP.

The sample below displays the summary of AP configuration, generated by the **show summary | include IP** command:

```
(Slave AP)# show summary | include IP
VC IP Address          :0.0.0.0
VC IPv6 Address        :::
IP Mode                :v4-only
Master IP Address      :10.16.21.2
IP Address             :10.19.29.8
IPv6 Address           :--
SLAAC IP Address       :--
Link Local IP Address:--
```

Check if the Slave AP is Supported in the AOS-W Instant Cluster

The master AP will reject the association request of the slave AP if its configuration is not supported by the cluster. A slave AP will be deemed incompatible with the cluster if there is a image class mismatch, regulatory domain mismatch, or OEM mismatch between the slave AP and the master AP.

Run the **show swarm state** command in the CLI of the slave AP to view the swarm details. Check the **AP swarm state** to see if the slave AP is allowed in the network. The AP swarm state will display **swarm_not_ allowed** if the slave AP is not supported in the cluster. Use the **show log system** command to get additional information about the cause for mismatch.

The sample below displays the swarm status of the slave AP, generated by the **show swarm state** command:

```
(Slave AP)# show swarm state
AP Swarm State            :swarm_not_allowed
mesh auto eth0 bridging  :no
Config in flash        :yes
factory SSID in flash :yes
extended-ssid configured :yes
extended-ssid active      :yes
advanced-zone configured :no
Factory default status   :no
Source of system time    :Image file
Config load cnt        :1
VC Channel index       :1
IDS Client Gateway Detect :yes
Config Init success cnt for heartbeat   :0
Config Init success cnt for register    :0
Config Init skipping cnt for heartbeat  :0
Config Init skipping cnt for register   :0
Config Init last success reason   :N/A
Config Init last success time     :N/A
```

The following are probable causes for slave-cluster incompatibility:

Type of Mismatch	Cause	Log Event
Image class mismatch	Slave AP and the APs in the cluster belong to different image classes	`AP class not match, Master-X, slave -Y`
Regulatory domain Mismatch	Slave AP and the APs in the cluster are of different regulatory domains	`AP regulatory domains don't match Master-X, slave-Y`
OEM Mismatch	slave AP and the APs in the cluster are of different OEMs	`AP regulatory domains don't match Master-X, slave-Y`

NOTE: In the event of a image class mismatch, image download can be facilitated through Activate, or OmniVista 3600 Air Manager platform. If either of these management platforms are configured in the cluster, the slave AP will install the appropriate image file from the cloud platform, reboot, and join the cluster.

NOTE: In the event of a regulatory domain mismatch or OEM mismatch, the slave AP cannot be provisioned in a cluster.

The following are common issues observed in OAW-IAPs managed by OmniVista 3600 Air Manager:

- AP Fails to Connect to OmniVista 3600 Air Manager
- AP Fails to Receive Configurations From OmniVista 3600 Air Manager
- AP Fails to Download Software Image From OmniVista 3600 Air Manager
- AP Fails to Download Certificates from OmniVista 3600 Air Manager

AP Fails to Connect to OmniVista 3600 Air Manager

The following procedure describes how to troubleshoot issues, if the AP fails to connect to OmniVista 3600 Air Manager:

1. Check OmniVista 3600 Air Manager Credentials
2. Check if the AP is Connected to OmniVista 3600 Air Manager
3. Ensure that the AP is Added to a Device Group
4. Check the Authentication Settings for OAW-IAPs in OmniVista 3600 Air Manager

Check OmniVista 3600 Air Manager Credentials

Ensure that the OmniVista 3600 Air Manager credentials — Organization String, Shared Key, and the IP address of the OmniVista 3600 Air Manager server are entered correctly on the AP.

Check if the AP is Connected to OmniVista 3600 Air Manager

Run the **show ap debug airwave** command in the CLI of the AP to view details of OmniVista 3600 Air Manager server. Check the **Status** column to identify the state of OmniVista 3600 Air Manager connection.

The sample below displays details of the OmniVista 3600 Air Manager server, generated by the **show ap debug airwave** command:

```
Airwave Server List
-------------------
Domain/IP Address Type      Mode      Config-only      Rapids-mode      Status
----------------- ----      ----      -----------      -----------      ------
1.1.1.1           Primary  -         -                No               Not connected
----------------- ----      ----      -----------      -----------      ------
```

The following are possible connection states of OmniVista 3600 Air Manager:

OmniVista 3600 Air Manager Status	Inference
Connected	The AP is connected to OmniVista 3600 Air Manager but is not authenticated.

OmniVista 3600 Air Manager Status	Inference
Login-done	The AP is successfully connected to OmniVista 3600 Air Manager.
Not Connected	The AP failed to establish a TCP connection with the OmniVista 3600 Air Manager server.

Ensure that the AP is Added to a Device Group

The AP must be manually authenticated and assigned to a Device group in the **Devices > New** page in OmniVista 3600 Air Manager. Ensure that shared key entered on the AP and the shared key of the AP group are the same. If the shared key of the AP group and the AP are different, the AP will remain unprovisioned.

Check the Authentication Settings for OAW-IAPs in OmniVista 3600 Air Manager

Ensure that OmniVista 3600 Air Manager is configured with the appropriate authentication method. The authentication settings of OmniVista 3600 Air Manager are available in the OmniVista 3600 Air Manager **Setup > General** page under **Alcatel-Lucent Instant Options**.

AP Fails to Receive Configurations From OmniVista 3600 Air Manager

The following procedure describes how to troubleshoot issues, if the AP fails to receive configurations from OmniVista 3600 Air Manager:

1. Check OmniVista 3600 Air Manager Operation Mode
2. Check the Configurations Received from OmniVista 3600 Air Manager

Check OmniVista 3600 Air Manager Operation Mode

Ensure that OmniVista 3600 Air Manager management mode for the AP is **Manage Read/Write**.

Run the **show ap debug airwave** command in the CLI of the AP to view details of OmniVista 3600 Air Manager server. Check the **Mode** column to identify the management mode of OmniVista 3600 Air Manager.

The sample below displays details of the OmniVista 3600 Air Manager server, generated by the **show ap debug airwave** command:

```
Airwave Server List
-------------------
Domain/IP Address Type      Mode      Config-only     Rapids-mode     Status
----------------  ----      ----      -----------     -----------     ------
1.1.1.1           Primary   Manage    -               No              Not connected
----------------  ----      ----      -----------     -----------     ------
```

The AP cannot receive configurations from OmniVista 3600 Air Manager if the management mode is set to **Monitor-only+Firmware Upgrades**. The following procedure describes how to change the management mode of OmniVista 3600 Air Manager:

1. Navigate to the **Devices > List** page in the OmniVista 3600 Air Manager UI.
2. Right-click on the device and select **Manage** to open the **Manage** page.

3. Under **General**, select **Manage Read/Write.**
4. Click **Save & Apply**.

Check the Configurations Received from OmniVista 3600 Air Manager

Run the **show ap debug airwave-config-received** command in the CLI of the AP to view configurations received from OmniVista 3600 Air Manager. Verify if the output includes the latest configurations made in OmniVista 3600 Air Manager.

The sample below displays the configurations received by the AP from OmniVista 3600 Air Manager, generated by the **show ap debug airwave-config-received** command:

```
(Instant AP) show ap debug airwave-config-received
wlan access-rule "IHG_App001": OK
rule any any match app yahoo permit log: OK
rule any any match app yahoo-answers permit log: OK
rule any any match app yahoo-buy permit log: OK
rule any any match any any any permit: OK
exit: OK
wlan ssid-profile "IHG_App001": OK
auth-server InternalServer: OK
broadcast-filter arp: OK
captive-portal disable: OK
dmo-channel-utilization-threshold 90: OK
dtim-period 1: OK
enable: OK
essid "IHG_App001": OK
inactivity-timeout 1000: OK
local-probe-req-thresh 0: OK
max-authentication-failures 0: OK
max-clients-threshold 64: OK
opmode wpa2-psk-aes: OK
rf-band all: OK
type employee: OK
wpa-passphrase de64afc987f0b466abc88ac3239330dd79a089bfe1a359cd: OK
exit: OK
```

AP Fails to Download Software Image From OmniVista 3600 Air Manager

The following procedure describes how to troubleshoot issues, if the AP fails to connect to OmniVista 3600 Air Manager:

1. Ensure that the Software Image is Uploaded in OmniVista 3600 Air Manager
2. Check the Status of Software Download
3. Check if the AP can Download the Image File from OmniVista 3600 Air Manager

Ensure that the Software Image is Uploaded in OmniVista 3600 Air Manager

Ensure that the software image for the AP is uploaded to OmniVista 3600 Air Manager in the **Device Setup > Upload Firmware & Files** page of the OmniVista 3600 Air Manager webUI.

The OmniVista 3600 Air Manager operation mode for the AP must be **Manage** mode or **Allow firmware upgrades in monitor-only mode** must be enabled in the **AMP Setup > General** page of OmniVista 3600 Air Manager UI for **Monitor only** mode.

Check the Status of Software Download

Check the status of the software download to ensure that the AP has initiated the download process.

Run the **show upgrade** command in the CLI of the AP to view the status of software upgrade. If the AP fails to initiate the download, there is an error between the AP and the OmniVista 3600 Air Manager server.

The sample below displays the image upgrade status, generated by the **show upgrade** command:

```
(Instant AP)# show upgrade
Image Upgrade Progress
--------------------
Mac                IP Address      AP Class   Status      Image Info
                                                          Error Detail
---                ---------       --------   ------      ---------
                                                          -----------
Instant AP         192.168.1.101  Hercules   downloading
http://https://10.65.20.131/flash/AlcatelInstant_Pegasus_6_4_3_1_4_2_0_0_50105_0.bin
none
Auto reboot        :enable
Use external URL   :enable
```

The **show log upgrade** command can also be used to view the status of software download.

Check if the AP can Download the Image File from OmniVista 3600 Air Manager

Run the **debug-download <url>** command to check whether the AP can access the image file. If the connection to the download url fails, ensure that there are no issues in the network connectivity. The URL for the download file uses the following syntax: **https://<OmniVista 3600 Air Manager IP>/flash/<Image file name>**.

The following is an example of the **debug-download** command:

```
Instant AP)# debug-download https://106.120.89.90/flash/AlcatelInstant_Cassiopeia_6_
4_2_0_4_1_1_2_47823_0.bin
```

AP Fails to Download Certificates from OmniVista 3600 Air Manager

The following procedure describes how to troubleshoot issues, if the AP fails to download certificates from OmniVista 3600 Air Manager:

1. Check OmniVista 3600 Air Manager Operation Mode
2. Check the Certificates Installed on the AP

Check OmniVista 3600 Air Manager Operation Mode

Ensure that OmniVista 3600 Air Manager management mode for the AP is **Manage Read/Write**.

Run the **show ap debug airwave** command in the CLI of the AP to view details of OmniVista 3600 Air Manager server. Check the **Mode** column to identify the management mode of OmniVista 3600 Air Manager.

The sample below displays details of the OmniVista 3600 Air Manager server, generated by the **show ap debug airwave** command:

```
Airwave Server List
------------------
Domain/IP Address Type      Mode       Config-only   Rapids-mode   Status
---------------- ----      ----       -----------   -----------   ------
1.1.1.1          Primary   Manage     -             No            Not connected
---------------- ----      ----       -----------   -----------   ------
```

The AP cannot download certificates from OmniVista 3600 Air Manager if the management mode is set to **Monitor-only+Firmware Upgrades**. The following procedure describes how to change the management mode of OmniVista 3600 Air Manager:

1. Navigate to the **Devices > List** page in the OmniVista 3600 Air Manager UI.
2. Right-click on the device and select **Manage** to open the **Manage** page.
3. Under **General**, select **Manage Read/Write.**
4. Click **Save & Apply**.

Check the Certificates Installed on the AP

Run the **show cert all** command in the CLI of the AP to view certificates installed on the AP. Check if the AP received new certificates from OmniVista 3600 Air Manager.

The sample below displays certificate details of the AP, generated by the **show cert all** command:

```
(Instant AP) # show cert all
Current Server Certificate:
Version :2
Serial Number :ECD686866B183D17
Issuer :/C=CN/ST=Beijing/O=Aruba Networks/O=an HP company/OU=Aruba Instant/CN=Feng
Ding
Subject :/C=CN/ST=Beijing/O=Aruba Networks/O=an HP company/OU=Aruba Instant
(Server)/CN=www.fding.com
Issued On :Jun 12 07:04:18 2018 GMT
Expires On :Jun 9 07:04:18 2028 GMT
RSA Key size :2048 bits
Signed Using :RSA-SHA1
Default CP Server Certificate:
Version :2
Serial Number :3D
Issuer :/CN=Aruba345-CNFDK5143Q/ST=California/O=Aruba Networks/OU=Instant/C=US
Subject :/CN=securelogin.arubanetworks.com/L=Sunnyvale/ST=California/O=Aruba
Networks/OU=Instant/C=US
Issued On :Nov 20 08:29:52 2019 GMT
Expires On :Nov 17 08:29:55 2029 GMT
RSA Key size :2048 bits
Signed Using :RSA-SHA256
```

The following are common issues observed with wireless client connections:

- Wireless Client Unable to Connect to AP
- Wireless Client Unable to Get an IP Address
- Wireless Client Unable to Pass Traffic
- Wireless Client Fails 802.1X Authentication
- Wireless Client Fails MAC Authentication
- Wireless Client Fails to Reach Captive Portal Authentication Page
- Wireless Client Fails Captive Portal Authentication

Wireless Client Unable to Connect to AP

The following procedure describes how to troubleshoot issues, if the client fails to connect to AP:

1. Check the SSID Configuration of the Wireless Network
2. Verify if the SSID is Broadcast by the AP
3. Check the Quality of RF Environment
4. Check the Channel Change Behavior of the Broadcasting Radio
5. Check the Authentication Message Exchange Between the AP and Client

Check the SSID Configuration of the Wireless Network

The SSID settings must be defined to support the desired clients. The following are SSID configuration that impact a client's ability to discover and connect to the network:

- **SSID settings** — The SSID must be enabled and visible for clients to join the network. Ensure that **Hide** and **Disable** options are disabled in the SSID settings.
- **Operating radio bands** — The SSID must be broadcasted on the RF bands supported by the client. Ensure that the SSID is operating on the RF band supported by the client.
- **Minimum and maximum transmit rates of the radios** — The minimum and maximum transmit rates of the radio must include the transmit rates supported by the client. Use the following table as reference when configuring transmission rates for the network:

IEEE Standard of the Client	Supported Bands	Supported Transmit Rates
Legacy 802.11	2.4 GHz	1 to 2 Mbps
802.11a	5 GHz	Up to 54 Mbps
802.11b	2.4 GHz	Up to 11 Mbps

IEEE Standard of the Client	Supported Bands	Supported Transmit Rates
802.11g	2.4 GHz	Up to 54 Mbps
802.11n	2.4 GHz / 5 GHz	Up to 600 Mbps
802.11ac	5 GHz	Up to 866.7 Mbps (Wave 1) Up to 1.73 Gbps (Wave 2)
802.11ax	2.4 GHz / 5 GHz	Up to 2.4 Gbps

The WLAN configurations of a network can be modified by selecting the network and clicking on ✏ icon in the **Configuration > Networks** page of the AOS-W Instant WebUI.

Alternatively, the configuration can be modified through the CLI using the **wlan ssid-profile <profile name>** command.

Verify if the SSID is Broadcast by the AP

Run the **show ap bss-table** command to view the AP BSS table. Ensure that the SSID is broadcast as expected without any radio resets. The **tot-t** column in the **Alcatel-Lucent AP BSS Table** logs the total up-time of the SSID. Errors in the SSID broadcast can be inferred from the total up-time data.

```
90:4c:81:c3:28:1e# show ap bss-table
Alcatel-Lucent AP BSS Table
------------------
bss              ess    port  ip          phy   type  ch/EIRP/max-EIRP  cur-cl  ap
name             in-t(s)  tot-t   flags
---              ---    ----  --          ---   ----  ----------------  ------  ---
----             -------  -----   -----
90:4c:81:b2:81:e1  test  ?/?   10.16.21.2  g-HT  ap    11/10.2/26.2      0
90:4c:81:c3:28:1e  0        20m:20s
Channel followed by "*" indicates channel selected due to unsupported configured
channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.
Num APs:1
Num Associations:0
Flags:
K = 802.11K Enabled; W = 802.11W Enabled; r = 802.11r Enabled; 3 = WPA3 BSS; O =
Enhanced-open BSS with transition mode;
o = Enhanced-open transition mode open BSS; M = WPA3-SAE mixed mode BSS; E =
Enhanced-open BSS without transition mode; m = Agile Multiband (MBO) BSS;
c = MBO Cellular Data Capable BSS; I = Imminent VAP Down; T = Individual TWT
Enabled; t = Broadcast TWT Enabled; d = Deferred Delete Pending;
a = Airslice policy; A = Airslice app monitoring;
```

Check the Quality of RF Environment

Run the **show ap arm rf-summary** command to view the RF environment report of the AP. Clients may fail to connect if there is lot of interference from neighboring devices in the channels operated by the AP.

Check the Channel Change Behavior of the Broadcasting Radio

Run the **show ap arm history** command in the CLI of the AP to view the channel change history of the radios. Frequent channel changes by the AP radio may affect the ability of client devices to discover and connect to the SSID. This is commonly observed in clients with a limited channel range.

Check the Authentication Message Exchange Between the AP and Client

Check the authentication logs in the AP to identify any association issues between the client and the AP.

Run the **show ap debug mgmt-frames <MAC address>** command to view authentication messages exchanged between the client and the AP. Use the client MAC address in the MAC address parameter to filter management frames specific to the client. Any authentication errors in the client association process will be displayed in the output.

Wireless Client Unable to Get an IP Address

The following procedure describes how to troubleshoot issues, if the client fails to get an IP address:

1. Check the VLAN Settings of the Network
2. Debug the DHCP Packets of the Client

Before troubleshooting, ensure that the client is connected to the AP.

Check the VLAN Settings of the Network

Incorrect VLAN settings can stop the client from getting an IP address. Perform the following checks depending on the VLAN configuration of your network:

VLAN Assignment Type	Action
Virtual Controller Managed	Ensure that the custom DHCP scope defined is valid and supported in the subnet.
Network Managed	Ensure that the VLAN defined is allowed in the wired port profile. For trunked VLANs, ensure that the VLAN is allowed in the uplink switch.
	Ensure that a DHCP server is available in the uplink switch to supply IP addresses to clients.

Debug the DHCP Packets of the Client

Run the **debug pkt match mac <mac address> type dhcp** in the CLI to view the dhcp packets exchanged between the client and the AP for more information. Use the MAC address of the client in the **match** parameter to filter packets specific to a client.

The following command syntax is used to view the dhcp packets specific to a client:

```
(Instant AP)#debug pkt match <MAC address> type dhcp
(Instant AP)#debug pkt dump
```

Wireless Client Unable to Pass Traffic

The following procedure describes how to troubleshoot issues, if the client is unable to pass traffic in the network:

1. Check the Role Assigned to Client
2. Check if Client Can Reach the Gateway IP
3. Check the Firewall Rules of the User Role

Check the Role Assigned to Client

Run the **show clients** command to view clients connected to the AP and verify if the client has inherited the desired role. For SSIDs with a captive portal, ensure that the client has completed authentication and is assigned a post auth role.

Check if Client Can Reach the Gateway IP

Routing errors may prevent the client from passing traffic in the network. Ping the default gateway IP address from the client and check the ping information. If the ping to the default gateway IP address fails, check the routing profile of the AP.

Check the Firewall Rules of the User Role

Check if the firewall rules of the user role allow the user to pass the desired traffic.

The following procedure describes how to check firewall rules for a user role:

1. Run the **show datapath user** command to view the datapath information of clients connected to the access point.
2. Identify the ACL number assigned to the client from the **ACLs** column of the **Datapath User Table Entries** table.
3. Check the access control entries in the ACL using the **show datapath acl <acl number>** command.
4. Verify if the ACL rules are configured to allow the desired traffic.

Wireless Client Fails 802.1X Authentication

The following procedure describes how to troubleshoot issues, if the wireless client fails 802.1X authentication:

1. Check Authentication Process Logs on the AP
2. Check the Status of the RADIUS Server
3. Debug the RADIUS Packets of the Client

Check Authentication Process Logs on the AP

Check the authentication logs to view and identify errors in the authentication process between the client and the AP and the radius server.

Run the **show ap debug auth-trace-buff <MAC address>** command to view the authentication process logs between the client and the AP. Use the MAC address of the client to filter packets specific to a client. Any error in the authentication process will be displayed in the output.

Check the Status of the RADIUS Server

Ping the RADIUS server from the AP or run an authentication server test for the RADIUS server.

Run the **aaa test-server** command to the test the authentication server. The following command syntax is used to test the RADIUS server:

```
(Instant AP)#aaa test-server <servername> username <username> password <passwd>
auth-type <type>
```

Debug the RADIUS Packets of the Client

Run the **debug pkt match <MAC address> type radius** command and check the RADIUS packets exchanged between the client and the AP for more information. Use the MAC address of the client in the **match** parameter to filter packets specific to a client.

The following command syntax is used to view the radius packets specific to a client:

```
(Instant AP)#debug pkt match <MAC address> type radius
(Instant AP)#debug pkt dump
```

Wireless Client Fails MAC Authentication

Clients must pass MAC authentication to connect to the AP if MAC authentication is enabled. However clients can connect to the AP despite MAC authentication failure, if MAC authentication is used in combination with:

- 802.1X authentication and **MAC authentication fail-thru** is enabled.
- Captive portal authentication and **MAC authentication fail-thru** is enabled.

The following procedure describes how to troubleshoot issues, if the client fails MAC authentication:

Check Authentication Process Logs on the AP

Check the authentication logs to view and identify errors in the authentication process between the client and the AP.

Run the **show ap debug auth-trace-buff <MAC address>** command to view the authentication process logs between the client and the AP. Use the MAC address of the client to filter packets specific to a client. Any error in the authentication process will be displayed in the output.

Wireless Client Fails to Reach Captive Portal Authentication Page

The following procedure describes how to troubleshoot issues, if the client fails to reach the captive portal authentication page:

1. Identify the Captive Portal Mode of the SSID
2. Debug ECP Mode Behavior on Client PC

Identify the Captive Portal Mode of the SSID

There are two modes of captive portal authentication provided by the AP:

- **ECP tiny proxy mode** — the captive portal page is provided by the AP and the AP mediates authentication between the client and the captive portal server.
- **ECP redirect mode** — the AP redirects the client to the captive portal server for authentication.

Run the **show external-captive-portal** command in the CLI to view the captive portal mode of the SSID.

```
(Instant AP0# show external-captive-portal
External Captive Portal
----------------------
Name           Server       Port  Url                 Auth Text  Redirect Url  Server
Fail Through   Disable Auto Whitelist   Use HTTPs    In Use   Redirect Mode
----           ------       ----  ---                 ---------  ------------  --------
```

```
-----------  ---------------------  ---------  ------  -------------
default      10.64.18.200  80    /guest/bmrpl.php                         Disable
             Enable              No          No     Yes
bwang1       10.64.18.200  80    /guest/bmrpl.php                         Disable
             Enable              No          Yes    Yes
"a a a a a"  10.64.18.200  80    /guest/bmrpl.php                         Disable
             Disable             No          Yes    No
amigoport    10.64.17.246  80    /aruba.php                               Disable
             Enable              No          No     Yes
bwang2       10.64.18.200  80    /                                        Disable
             Enable              No          No     Yes
bwang3       10.64.18.200  80    /                                        Disable
             Enable              No          No     Yes
```

Networks using ECP redirect mode are marked **Yes** in the **Redirect Mode** column and networks using ECP tinyproxy mode are marked **No**.

Debug ECP Mode Behavior on Client PC

Check if the client is redirected to the expected URL as defined by the captive portal ECP mode using developer tools provided by the browser.

The following procedure describes how to debug captive portal communication between the client and the webserver on the client browser:

1. Open **Developer Tools** in your browser and navigate to **Network Monitor**.
2. Input a URL in the address bar and press **Enter**.
3. Click on the URL entry in the **Network Monitor** and check the header messages exchanged between the web server and the client. Depending on the ECP mode of the captive portal, you should get the following responses:

Captive Portal ECP Mode	Expected Header Response
ECP tinyproxy mode	**Status Code: 200 OK** Location in Header Response — Alcatel-Lucent AP captive portal URL (securelogin.arubanetworks.com)
ECP redirect mode	**Status Code: 302 OK** Location in Header Response — Captive portal server URL

If the client browser fails to resolve DNS, open command prompt on the client PC and run **nslookup** to check the status of DNS server.

Wireless Client Fails Captive Portal Authentication

Captive portal authentication on ECP tinyproxy mode is mediated by the AP and can be troubleshooted on the AP. Whereas captive portal authentication on ECP redirect mode has no AP mediation and can be troubleshooted only using a packet capture software.

The following procedure describes how to troubleshoot issues, if the client fails captive portal authentication on ECP tinyproxy mode:

Check Authentication Process Logs on the AP

Run the **show ap debug auth-trace-buff<MAC address>** command to view the authentication process logs between the client and the AP. Use the MAC address of the client to filter packets specific to a client. Any error in the authentication process will be displayed in the output.

The following are common issues observed with the AP Radios:

- Wireless Client Unable to Find SSID
- AP Does Not Operate on Certain Channels
- AP Changes Radio Channel Frequently

Wireless Client Unable to Find SSID

The following procedure describes how to troubleshoot issues, if the wireless client is unable to find the SSID:

1. Check the SSID Configuration of the Wireless Network
2. Check the Uplink of the AP

Check the SSID Configuration of the Wireless Network

The SSID settings must be defined to support the desired clients. The following are SSID settings that impact a client's ability to discover and connect to the network:

- **SSID settings** — The SSID must be enabled and visible for clients to join the network. Ensure that **Hide** and **Disable** options are disabled in the SSID settings.
- **Operating radio bands** — The SSID must be broadcasted on the RF bands supported by the client. Ensure that the SSID is operating on the RF band supported by the client.
- **Minimum and maximum transmit rates of the radios** — The minimum and maximum transmit rates of the radio set must include the transmit rates supported by the client. Use the following table as reference when configuring transmission rates for the network:

IEEE Standard of the Client	Supported Bands	Supported Transmit Rates
Legacy 802.11	2.4 GHz	1 to 2 Mbps
802.11a	5 GHz	Up to 54 Mbps
802.11b	2.4 GHz	Up to 11 Mbps
802.11g	2.4 GHz	Up to 54 Mbps
802.11n	2.4 GHz / 5 GHz	Up to 600 Mbps
802.11ac	5 GHz	Up to 866.7 Mbps (Wave 1) Up to 1.73 Gbps (Wave 2)
802.11ax	2.4 GHz / 5 GHz	Up to 2.4 Gbps

The SSID configurations of a network can be modified by selecting the network and clicking on ✎ in the **Configuration > Networks** page of the AOS-W Instant WebUI.

Alternatively, the SSID configuration can be modified through the CLI using the **wlan ssid-profile <profile name>** command.

Check the Uplink of the AP

SSIDs can be configured to disable automatically when the uplink connection of the AP is down. This behavior is controlled by the **Out of Service** option in the SSID settings of the network. If **Out of Service**, is configured, the AP will stop the broadcast of the SSID when the configured condition is met. To review the **Out of Service** settings of the SSID, navigate to the **Configuration > Networks > (Select SSID profile) > Basic > Advanced Options** page in the AOS-W Instant webUI.

Run the **show uplink status** command to the view the status of uplink connections of the AP. If the status of active uplink connection of the AP is **DOWN**, resolve the issue with the AP uplink before continuing the troubleshooting process.

The sample below displays information of the uplink connection of the AP, generated by the **show uplink status** command:

```
(Instant AP)# show uplink status

Uplink preemption              :enable
Uplink preemption interval     :600
Uplink enforce                 :none
Ethernet uplink eth0       :DHCP
Uplink Table
------------
Type       State   Priority   In Use
----       -----   --------   ------
eth0       DOWN    0          Yes
Wifi-sta   INIT    6          No
3G/4G      INIT    7          No
Internet failover                  :disable
Max allowed test packet loss       :10
Secs between test packets          :30
VPN failover timeout (secs)        :180
Internet check timeout (secs)      :10
ICMP pkt sent        :0
ICMP pkt lost        :0
Continuous pkt lost  :0
VPN down time        :0
AP1X type:NONE
Certification type:NONE
Validate server:NONE
```

AP Does Not Operate on Certain Channels

The following procedure describes how to troubleshoot issues, if the AP fails to broadcast on certain channels:

1. Check if ARM is Configured for the AP Radio
2. Check RF Settings of the AP

Check if ARM is Configured for the AP Radio

The AP will not participate in ARM functions if a static channel is configured.

The channel assignment settings is configured in **Configuration > Access Point > (Select Access Point) > Radio** settings of the AP. Ensure that the radio is set to **Adaptive radio management assigned** for the AP to dynamically change the broadcasting channel with respect to channel quality metrics.

Check RF Settings of the AP

The RF settings of the AP control the channel and transmission capabilities of the radio. Ensure that the required capabilities are enabled on the AP.

The RF settings of the AP is configured by selecting **Show Advanced Options** in the **Configuration > RF** page in the AOS-W Instant WebUI. The following table lists AP behaviors and the prescribed action to resolve them:

AP Behavior	Action
AP does not operate in the 80 MHz channel	Check if **80 MHz support** is enabled in **Access Point Control** settings.
AP does not operate on 40 MHz channels	Check if **Wide Channel Bands** is enabled on the radio in **Access Point Control** settings.
AP does not work on HT mode	Check if **legacy only** is enabled on the radio. This option is available in the radio profile.

AP Changes Radio Channel Frequently

The following procedure describes how to troubleshoot issues, if the AP changes radio channel frequently:

1. Check if Client Aware is Enabled
2. Check the ARM Channel Change Logs to Identify the Reason for Channel Change

Check if Client Aware is Enabled

The client aware feature stops the AP from changing channels when a client is connected to the AP. Client aware stops channel change only when clients are connected to the AP. If no client is connected, the AP will continue to change channels to identify clients.

Navigate to **Configuration > RF** page in the AOS-W Instant WebUI and ensure that **Client Aware** is enabled on the AP.

Check the ARM Channel Change Logs to Identify the Reason for Channel Change

Run the **show ap arm history** command to view ARM channel change events on the AP. Use the output of this command to identify the cause for channel change.

The sample below displays the list of allowed channels for the AP, generated by the **show ap allowed channels** command:

```
(Instant AP)# show ap arm history

Interface :wifi0
ARM History
-----------
Time of Change        Old Channel   New Channel   Old Power   New Power   Reason   Result
--------------        -----------   -----------   ---------   ---------   ------   ------
```

```
2020-04-29 01:50:33  100E        132E        18          18          I
Configured
2020-04-29 01:44:00  52E         100E        18          18          M
Configured
2020-04-29 01:38:41  116E        52E         18          18          I
Configured
2020-04-29 01:36:16  116E        116E        Max         18          P-
Configured
Interface :wifi1
ARM History
---------
Time of Change       Old Channel  New Channel  Old Power  New Power  Reason  Result
--------------       -----------  -----------  ---------  ---------  ------  ------
2020-05-17 18:49:57  1            6            9          9          I
Configured
2020-05-17 18:43:35  11           1            9          9          I
Configured
2020-05-17 18:16:22  6            11           9          9          I
Configured
2020-05-17 18:08:18  1            6            9          9          I
Configured
2020-05-17 18:00:42  11           1            9          9          I
Configured
2020-05-17 17:43:20  6            11           9          9          I
Configured
2020-05-17 17:35:58  1            6            9          9          I
Configured
2020-05-17 17:21:45  11           1            9          9          I
Configured
2020-05-17 17:09:41  6            11           9          9          I
Configured
2020-05-17 16:57:20  1            6            9          9          I
Configured
2020-05-17 16:52:22  11           52           9          9          I
Configured
2020-05-17 16:25:34  52           11           9          9          R
Configured
2020-05-17 16:17:56  6            1            9          9          I
Configured
2020-05-17 15:51:59  1            6            9          9          I
Configured
2020-05-17 15:44:20  11           1            9          9          I
Configured
2020-05-17 15:28:43  6            11           9          9          I
Configured
2020-05-17 15:22:59  1            6            9          9          I
Configured
2020-05-17 15:08:01  11           1            9          9          I
Configured
2020-05-17 14:59:42  6            100          9          9          I
Configured
2020-05-17 14:45:54  100          140          9          9          R
Configured
2020-05-17 14:35:28  140          1            9          9          R
Configured
2020-05-17 14:21:52  6            11           9          9          I
Configured
2020-05-17 14:09:06  1            6            9          9          I
Configured

I: Interference, R: Radar detection, N: Noise exceeded, Q: Bad Channel Quality E:
Error threshold exceeded, INV: Invalid Channel, G: Rogue AP Containment, M: Empty
```

```
Channel, P+: Increase Power, P-: Decrease Power, 40INT: 40MHZ intol detected on
2.4G, NO40INT: 40MHz intol cleared on 2.4G, OFF(R): Turn off Radio due to Radar, OFF
(MA): Turn off Radio due to Mode Aware, ON: Turn on Radio, D: Dynamic Bandwidth
Switch, AIRMATCH: AirMatch Event, I*: CCA Interference, C: Radar cleared, NC: Noise
Cleared, Random: Random Channel, RMC: Radio Mode Change
```

If channel change occurs due to radar detection (**R**), identify the DFS channels pertaining to the AP country code and configure valid channels in the ARM profile accordingly.

Use the **show ap allowed channels** command to view the list of allowed channels and identify the DFS channels of the AP. Remove those channels from the list of **Valid 5 GHz channels** and **Valid 2.4 GHz channels** in **ARM Advanced options** in the **Configuration > RF** page of the AOS-W Instant WebUI.

The sample below displays the list of allowed channels for the AP, generated by the **show ap allowed channels** command:

```
(Instant AP)# show ap allowed-channels
Allowed Channels for AP Type 345 Country Code IN
------------------------------------------------
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 64 100 104 108 112 116 120 124 128
132 136 140 144 149 153 157 161 165
802.11g (outdoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)        36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128
132 136 140 144 149 153 157 161 165
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 60-64 100-104 108-112 116-120 124-128
132-136 140-144 149-153 157-161
802.11g 40MHz (outdoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)  36-40 44-48 52-56 60-64 100-104 108-112 116-120 124-128
132-136 140-144 149-153 157-161
802.11a 80MHz (indoor)   36-48 52-64 100-112 116-128 132-144 149-161
802.11a 80MHz (outdoor)  36-48 52-64 100-112 116-128 132-144 149-161
802.11a 160MHz (indoor)  36-64 100-128
802.11a 160MHz (outdoor) 36-64 100-128
802.11a (DFS)            52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
144
```

The following are common issues observed in mesh networks:

- APs are Unable to Establish a Mesh Link

APs are Unable to Establish a Mesh Link

The following procedure describes how to troubleshoot issues, if APs fail to establish a mesh link:

1. Check Mesh Cluster Name and Mesh Cluster Key of the APs
2. Check the Extended SSID Settings of the APs
3. Check if a 5 GHz SSID is Configured on the Network
4. Check the Uplink Connection of the Mesh Point AP
5. Check the RF Environment of the Mesh APs

Check Mesh Cluster Name and Mesh Cluster Key of the APs

APs must have the same mesh cluster name and mesh cluster key to form a cluster. The mesh cluster name and the mesh cluster key is configured using the **mesh-cluster** command.

Run the **show mesh cluster configuration** command in the CLI to view mesh cluster information of the AP. Check the cluster details on mesh APs to verify if they have the same mesh cluster name and mesh cluster key.

The sample below displays the mesh cluster details, generated by the **show mesh cluster configuration** command:

```
(Instant AP)# show mesh cluster configuration
Mesh cluster name :mesh_clusterl
Mesh cluster key :Manual
```

Check the Extended SSID Settings of the APs

Ensure that **Extended SSID** is disabled in the AP. APs will fail to establish a mesh link, if extended SSID is enabled. The extended SSID setting is available in **General > Advanced options** in **Configuration > System** page of the Instant WebUI.

Check if a 5 GHz SSID is Configured on the Network

Th 5 GHz radio of the AP is used to handle the mesh-backhaul traffic. Instant APs automatically disable the 5 GHz radio if there are no active networks in the 5 GHz band. Therefore, it is necessary to have an SSID operating on the 5GHz band to keep alive the 5 GHz radio of the AP.

Run the **show network** command to view the list of networks enabled on the AP. Check the network list for 5 GHz networks. If there are no 5 GHz networks, configure an SSID to operate in the 5 GHz band.

Check the Uplink Connection of the Mesh Point AP

In mesh networks, the AP with the Ethernet uplink connection will function as the mesh portal AP and there can be only one mesh portal in a mesh cluster. If two APs in a mesh network have Ethernet uplink, both the

APs will assume the role of mesh portal and the mesh link will be broken. Therefore, ensure that only the mesh portal AP has an Ethernet uplink connection.

Check the RF Environment of the Mesh APs

APs in a mesh cluster must have overlapping RF environments to establish mesh links.

Run the **show ap mesh neighbor** command to view the list of neighboring mesh APs. Ensure that the mesh point AP has the mesh portal AP entry in the neighboring APs list.