Troubleshoot AireOS Wireless LAN Controllers

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Controller Component Issues
IDS Signatures
NAC
OEAP
Rule-based Rogue Classification
Rogue Containment
IDS Signature
RLDP
Diagnostic Channel
Inter Controller Mobility
Honeypot AP
AirMagnet Integration
Local Authentication
Controller Debug
General AAA Authentication
TACACS+
LDAP
Client Management Frame Protection (MFP)
Mobility
Report Problems
FIPS Related Issues
Wireless Client Uses Local Authenticator with EAP-TLS, EAP-FAST and PEAP
512 WLANs/AP Groups
ACLs, Pre Auth ACLs and CPU ACLs
DHCP
Guest Access Related Issues
WLC High Availability Issues
Controller H-REAP Related Issues
Media-Stream
Location Related Issues
System Memory, Out of Memory Issues
Mesh Related Issues
Issues with NTP Client and Time Configuration on the Controller
RF Component Issues for the WLCs
Introduction

This document describes how to use the `debug` and `show` commands to troubleshoot wireless LAN controllers (WLCs).

Prerequisites

Requirements

There are no specific requirements for this document.
Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Controller Component Issues

IDS Signatures

- debug wips sig enable

NAC

- debug nac events enable
- debug nac packets enable

OEAP

Controller Show Commands

- show ap join stats detail <ap mac add>
- show h-reap summary
- show h-reap latency
- show ap link-encryption
- show ap data-plane

AP Side Show/Debugs

- show logging
- show lwapp/capwap client rcb
- show lwapp/capwap client config
- test lwapp/capwap iapp-data-echo
- debug lwapp/capwap iapp-data-echo
- show lwapp/capwap reap
- show controller

Rule-based Rogue Classification

Debugs to Collect
• debug dot11 rogue rule enable

Captures to Take
Not applicable.

Config and Show Output to Collect

• show rogue rule summary
• show rogue rule detailed <rule>
• show rogue ap detailed <rogue-mac> (if a particular rogue is wrongly classified)

Rogue Containment

Ensure there is a DHCP server configured on the network for the Rogue Access Point (AP) to use if static IP addressing is used.

Debugs to Collect

• debug dot11 rogue enable

Captures to Take
Airopeek trace on the rogue channel.

Note: Watch out for disassociated frames.

Config and Show Output to Collect

• show rogue ap detailed <contained rogue-mac>
• show ap config 802.11b/a <ap-name from the earlier command>

IDS Signature

Make sure there is a DHCP server configured on the network for the Rogue AP to use if static IP addressing is used.

Debugs to Collect

• debug wips sig enable

Captures to Take
Airopeek capture on the channel signature detected.

Debug and Show Output to Collect

In software before 5.2, LWAPP can be used in place of CAPWAP for these commands:

• show capwap ids sig dump - Dumps Signatures and Signature Detection Hit Counts that
include the MAC address with the largest hits. Also includes current status of the IDS packet trace.

- **show capwap ids rogue containment <slot#> chan**- Displays the current list of Rogue Containment requests at this AP. Containment requests are grouped by channel.

- **show capwap ids rogue containment <slot#> rad**- Displays the current list of Rogue Containment requests at this AP. This list corresponds to the list of requests as received from the controller.

- **debug capwap ids sig**- Turns on debugs for IDS Signature and Containment Detection.

- **test capwap ids trace match <message type-name>**- Traces all packets received by the IDS Signature Detection Module of message type=<message type-name>; <message type-name> = FF to trace all message types. Signature Debugs in section 8.2.1 need to be turned on to have the traced packets displayed.

- **test capwap ids trace rcv <type-name>**- Traces for all packets that match any currently installed signatures for the IDS Signature Detection Module of message type=<message type-name>; <message type-name> = FF to trace all message types that match a signature. Signature Debugs in section 8.2.1 need to be turned on to have the traced packets displayed.

**RLDP**

**Debugs to Collect**

On the WLC:

- debug dot11 rldp enable

On the AP:

- debug lwapp client mgmt

**Captures to Take**

Airopeek capture on the rogue channel.

**Config and Show Output to Collect**

- config rogue ap rldp initiate <rogue-mac>

**Diagnostic Channel**

**Debugs to Collect**

- debug client <client mac>
- debug ccxdiag all enable

**Captures to Take**

Airopeek capture on the channel from which the AP is set. It is recommended to avoid filtering because beacon and probe req/resp packets can be missed.
Config and Show Output to Collect

- `show sysinfo`
- `show wlan x`
- `show run-config`
- `show tech-support`
- `show debug`
- `show msglog`
- `show client summary`
- `show client detail <client mac>`

Client Details

- Client hardware
- Supplicant software details such as software version, software name (for example, Aironet Desktop Utility [ADU] or Odyssey), and driver version in case of ADU
- Client OS

Inter Controller Mobility

Debugs to Collect

- `debug client <client mac>` on both WLCs
- `debug mobility handoff` enables on both WLCs (Remember the order and always enable the `debug client` first.)
- Debug pem state enable

- If mobility control path or data up is down, then turn on `debug mobility keepalive enable` on both switches (remember the software version on both controllers).
- If Address Resolution Protocol (ARP) does not work, turn on `debug arp all enable` on both switches.
- If DHCP does not work, turn on `debug dhcp message enable` and `debug dhcp packet enable` on both switches.
- If IPSec is involved: debug pm sa-export enable, debug pm sa-import enable.
- If the client connects after a while, show how long it took.

Captures to Take

Capture by the roaming type, such as CCKM, PMKID or TGR.

Config and Show Output to Collect

Same as Client connection issue and also these:

- `show pmk-cache <client mac>` (on the target controller)
- `show client details <client mac>` (when client is connected on old AP)
- `show mobility summary` (on both WLCs)
Same as particular roaming type, such as CCKM, PMKID or TGR.

**Honeypot AP**

**Debugs to Collect**

Not applicable.

**Captures to Take**

Capture Airopeek trace on the channel the trap is received in order to confirm that the rogue uses the Cisco SSID.

**Config and Show Output to Collect**

- `show traplog`

**AirMagnet Integration**

**Debugs to Collect**

On the WLC for NMSP-related issues:

- `debug wips nmsp enable`
- `debug wips event enable`
- `debug wips error enable`

For CAPWAP-related issues:

- `debug wips event enable`
- `debug wips error enable`
- `debug iapp error enable`
- `debug iapp event enable`

For corrupted alarm/device report information:

- `debug wips all enable`

On the AP:

- `debug capwap am event`
- `debug capwap am error`

**Captures to Take**

- Airopeek capture of the attack
- Ethereal capture of the reports (sent as data packet)

**Config and Show Output to Collect**

On the AP:

- `show capwap am stats`
- `show capwap am buffer [run it few times]`
- show capwap am policy [alarm-id]
- show capwap am alarm [alarm-id]

**Local Authentication**

**Things to Check Before You Log a Bug**

Ensure the client can associate to the WLAN. If the client cannot, then the problem is at the dot1x level. If certificates are used, ensure there are devices and CA certificates installed on the WLC. Also, ensure you have selected the correct certificate issuer in the local-auth config in order to select the correct set of certificates on the WLC.

If the local database is used for user credentials, check that the username exists in the database. If the Lightweight Directory Access Protocol (LDAP) is used, see the debugging LDAP section for more debugging information.

**Debugs to Collect**

**WLC:**

- debug aaa local-auth eap framework errors enable
- debug aaa local-auth eap method errors enable
- debug aaa local-auth eap method events enable
- debug aaa local-auth eap method sm enable
- debug aaa local-auth db enable
- debug aaa local-auth shim enable

**Config and Show Output to Collect**

- show local-auth config
- show local-auth statistics
- show local-auth certificates (when an Extensible Authentication Protocol [EAP] method with certificates is used)

**Client Details**

The type of client, plus the EAP configuration details that show which method is selected and what parameters are set for that method on the client. Also, the text of any error message seen at the client.

**Controller Debug**

- debug pm pki enable—Details on certificate validation.
- debug aaa events enable—This helps if there are any authorization list related issues.
- show certificate lsc summary—for any LSC-related summary.

**General AAA Authentication**

These debugs are helpful for debugging RADIUS authentication, authorization, or account issues.

**Debugs to Collect**
- debug client <client mac>—Gives information on how reauth related attributes, such as session-timeout and action-type, are applied.
- debug aaa events enable—Helps to troubleshoot how different AAA servers are used for authentication, authorization and account.
- debug aaa packet enable—Helps to troubleshoot what different AAA attributes are received and applied.

Captures to Take

A wired capture can be collected between the controller and RADIUS server if the earlier debugs do not indicate the issue.

Config and Show Output to Collect

Same as [Client connection issue](#) and also this:

- show radius summary

Client Details

Same as [Client connection issue](#).

TACACS+

Debugs to Collect

- debug aaa tacacs enable (at WLC collect the log at the ACS/RADIUS server for account)
- debug aaa events
- debug aaa detail
- debug dot11 mobile
- debug dot11 state
- debug pem events
- debug pem state

Captures to Take

- A wired capture can be collected between the controller and RADIUS server if the earlier debugs do not indicate the issue.

Config and Show Output to Collect

- show tacacs summary
- Change of Authorization (CoA) and Packet of Disconnect (PD) issue - RFC 3576
- show radius summary

LDAP

Things to Check Before You Log a Bug

Make sure the LDAP server is pingable from the WLC.

If you use the Active Directory and local EAP authentication, these EAP methods are not
supported:

- LEAP
- EAP-FAST MSCHAPv2
- PEAP MSCHAPv2

This is because the Active Directory is not able to return a clear text password that can be used for the MSCHAPv2 authentication.

**Debugs to Collect**

- `debug aaa ldap enable`

If the problem occurs when you use LDAP with local authentication, see the [Local Authentication](#) section for more debugs.

**Config and Show Output to Collect**

- `show ldap summary`
- `show ldap <server no.>`
- `show ldap statistics`
- `show local-auth statistics` (if the problem occurs when used with LDAP with local EAP authentication)

**Client Management Frame Protection (MFP)**

**For All Problems**

- `debug wps mfp client`
- `show wps mfp summary`

**Config and Show Output to Collect**

- `show wps mfp statistics`

**Configuration Problems**

**Controller debugs:**

- `debug wps mfp lwapp`
- `debug lwapp mfp` (on Aironet APs)

**Client Does not Associate**

**Controller debugs:**

- `debug wps mfp client`
- `debug wps mfp detail`
- `debug pem state`
- `debug pem events`
- `debug dot1x events`

**Config and Show Output to Collect:**

- `show msglog`
• show client detail

**Additional 1130/1240 AP Debugs when Client Does not Associate**

- debug dot11 mgmt msg
- debug dot11 aaa manager all (for H-REAP standalone mode)

**Aironet AP Debugs when Client Does not Associate in H-REAP Standalone Mode**

- debug dot11 mfp client
- debug dot11 mgmt msg
- debug dot11 mgmt interface
- debug dot11 mgmt station
- debug dot11 supp-sm-dot1x
- debug dot11 aaa manager all
- debug dot11 wpa-cckm-km-dot1x

**Mobility**

**Controller Debugs**

- debug wps mfp mm enable
- debug mobility directory

**Config and Show Output to Collect**

- show mobility summary
- show mobility statistics

**Report Problems**

**Controller Debugs**

- debug wps mfp report

**Config and Show Output to Collect**

- show wps mfp statistics

  **Note:** This must be invoked immediately after errors are generated.

**FIPS Related Issues**

When the controller is placed in Federal Information Processing Standard (FIPS) mode, only approved cryptographic functions can be used. As a result, you must lock the SSL down to use TLS_RSA authentication algorithm with AES cipher.

**Cannot Break into Boot Menu**

This is a feature for FIPS. The feature is enabled with this command:

- config switchconfig boot-break disable
Cannot Download New Image

- This is a feature for FIPS. Transfer is disabled when boot-break is disabled.

Wireless Client Uses Local Authenticator with EAP-TLS, EAP-FAST and PEAP

Debugs to Collect

Based on the communication in trouble, these debugs can be enabled:

- debug wps cids enable
- debug locp event enable
- debug emweb server enable
- debug aaa.local-auth eap method events enable

Captures to Take

Sniffer trace between the WLC and the device with the issue.

**Note:** The WLC can start communication as soon as the relevant service starts. It is recommended to start sniffer before the WLC powers up.

Config and Show Output to Collect

- show switchconfig

512 WLANs/AP Groups

512 WLANs

A 512 WLANs bug is if the client can connect to a 'default-group' AP but cannot connect to an AP set to a custom AP group.

Show Output to Collect on the Controller:

- show sysinfo
- show running-config
- show wlan summary
- show wlan apgroup
- show msglog

Show Output to Collect on the AP:

- show controller
- show capwap client mn
- show log

Debugs to Collect:

- debug group enable
• debug capwap event

**Note**: These debugs or any other debug must be switched ON after the `debug client<client mac>` command is used. This command causes all earlier debugs to be disabled.

**Trace to Collect:**

• wireless trace

**AP Groups**

Any problems related the addition or deletion of the AP group, or to the addition of an interface to the AP group.

**Show Output to Collect:**

• show sysinfo
• show running-config
• show wlan summary
• show wlan apgroup
• show msglog

**Debugs to Collect:**

• debug group enable

**ACLs, Pre Auth ACLs and CPU ACLs**

```bash
>show acl ?
summary  Display a summary of the Access Control Lists.
detailed Display detailed Access Control List information.
cpu      Display CPU Acl Information
```

**DHCP**

**Debug DHCP In-Band**

• debug dhcp message enable
• debug dhcp packet enable

**Debug DHCP for the Service-Port Enable**

• debug dhcp service-port enable

**Guest Access Related Issues**

**Guest WLAN**

• debug mobility handoff enable
• debug pem events enable
• debug pem state enable

**For DHCP Problems:**
- debug dhcp packet enable
- debug dhcp message enable

For Mobile Connection Problems:

- debug dot11 events enable
- debug dot11 mobile enable

For RADIUS/AAA Problems:

- debug dot1x aaa enable

WLC High Availability Issues

AP Failover

Configuration Issue

Collect and examine these configurations files:

- All related WLC configuration files—show run-config and show running-config.
- Is AP failover priority configured?
- Per AP primary WLC ("Primary Cisco Switch [Name | IP Address]" field under "AP Config")
- Per AP secondary WLC ("Secondary Cisco Switch [Name | IP Address]" field under "AP Config")
- Per AP tertiary WLC ("Tertiary Cisco Switch [Name | IP Address]" field under "AP Config")
- The corresponding AP configuration parameters in WLC—show ap config <AP name>.
- The only supported AP mode for fast-heartbeat are local and h-reap ("AP Mode" field).
- The corresponding AP configuration parameters in AP—show capwap client config.

Failover to Unexpected WLC

- show sysinfo—The maximum number of APs supported by the expected WLC.
- show ap summary—APs that have joined the expected WLC.
- show capwap client ha—If fast-heartbeat is enabled, examine the backup list in the AP.

Transport Issue

If DHCP is enabled for AP Ethernet interface, has it fetched an IP address? Use show interface FastEthernet0.

- ping <IP address>—Decides whether the AP and WLC can ping each other.

CAPWAP Protocols

Common WLC and AP debug commands:

- Debug CAPWAP events and state—debug capwap events enable/disable
- Debug CAPWAP errors—debug capwap errors enable/disable
- Debug CAPWAP details—debug capwap detail enable/disable
- Debug CAPWAP info—debug capwap info message enable/disable
- Debug CAPWAP payload—debug capwap payload enable/disable
- Debug CAPWAP hexdump—debug capwap hexdump enable/disable

AP fast-heartbeat specific debug command:
• Debug fast-heartbeat—show capwap client ha

  **Note:** Sometimes you need the network analyzer (such as wireshark) output.

**AP Priority**

• Decide whether the AP priority is enabled—show run-conf ("AP Join Priority" field under "Network Information")
• Decide the maximum number of APs supported by the WLC—show sysinfo ("Maximum number of AP supported")
• Decide how many APs have joined the WLC—show ap summary
• Examine the join priority of each AP—show ap summary (last column)

**Transporter and CAPWAP Issues**

See the corresponding sessions in the [AP Failover](#) section.

• show tech-support
• show run-config
• show running-config
• show ap config general <AP name>
• show capwap client config

**Controller H-REAP Related Issues**

**H-REAP**

Controller Debugs:

• debug client <mac>

**AP Debugs:**

• debug lwapp reap mgmt
• debug dot11 mgmt msg
• debug dot11 mgmt int

**H-REAP CCKM Issues**

Controller Debugs:

• debug cckm
• debug hreap cckm

**AP Show/Debugs:**

• debug lwapp reap mgmt
• debug dot11 aaa manager key
• debug lwapp reap cckm
• debug dot11 mgmt msg
• show lwapp reap cckm

**H-REAP Local RADIUS**
Controller Debugs:

- debug hreap group
- debug hreap aaa

AP/Show Debugs:

- debug lwapp reap
- debug lwapp client config
- show run

Media-Stream

- debug media-stream
- Admission—Client admission debugs that are useful when debugging client denial/delist issues.
- Event—Dumps IGMP / Media direct client updates.
- RRC—RRC state machine updates.

ddebug bcast

- igmp—Client IGMP join request/report messages.

Location Related Issues

>show location ?

  ap-detect        Display devices detected by specified AP
  detail           Display detailed location information.
  plm              Display Location's Path Loss Measurement(CCX S60) Configuration
  statistics       Display Location Based System statistics.
  summary          Display Location Based System summary information.

System Memory, Out of Memory Issues

Config and Show Output to Collect

- show memory stat
- show buffers
- show process memory

  Note: If the "config memory monitor errors" flag is set to "disable", the memory corruption details can be uploaded with these commands:

- transfer upload datatype errorlog
- transfer upload filename memerrors.txt
- transfer upload start

Mesh Related Issues

There are multiple points of failure (or bug presence):
Controller
Mesh APs
GUI/WLC

**General Guidelines**

- Find the point of failure and isolate the failing component.
- Correlate traces from the controller, Mesh APs, and also visual output on the CLI/GUI/WLC to find the failure point.
- In case of packet related issues, collect Airopeek or ethereal traces to confirm preliminary analysis.
- Analyze the reason for the failure and how the problem can be reproduced.

**Configuration**

- Trigger action

**Overall Guidelines**

This section is intended to provide enough pointers to debug a mesh bug and collect relevant information to help the DEs understand the bug more efficiently. Given that it can be impossible to pin-point a bug at first glance, this document is a set of suggestions for the DT not a rule-book. The DT uses discretion to attach relevant debugs in order to help study efficiently and resolve the bug as quickly as possible.

**Suspect Packets Go Missing**

Collect Ethereal and Airopeek traces.

**Debug Command Sets**

This is a set of generic `debug` commands that can be used to obtain information about the system.

**General Show CLI:**

- `show version`
- `show capwap client rcb`
- `show mesh status`
- `show mesh module adjacency`
- `show mesh channel [current]`

**Test Mesh CLI:**

- `test mesh adjacency`—for Mesh adjacency test commands
- `test mesh astools`—for MESH Anti-strand tools
- `test mesh awpp`—for Mesh AWPP test commands
- `test mesh disable`—to disable a feature
- `test mesh enable`—to enable a feature
- `test mesh forwarding`—for Mesh forwarding test commands
- `test mesh linktest`—for test for mesh link test
- `test mesh mperf`—for MESH BW test tool

**Specific Issues**
- any link connection issue
- debug mesh link
- show mesh adjacency (child/parent/all)

**Radio:**

- show controller d0, d1, ... (for all Radio-related issues)
- Traces from the air (between the affected nodes)

**Interface (Data Traffic related) issues:**

- show int d0, d1, G0, G1, ...

**Ethernet Traces between controller and Roof-top Access Point (RAP)**

**Forwarding:**

- show mesh forwarding table
- debug mesh forwarding [table/packet]
- show mesh forwarding links
- show mesh forwarding port-state
- debug mesh forwarding port-filter

**IP Address/DHCP:**

- debug ip address
- show ip int bri
- show int bvi1
- show run int bvi 1
- show mesh forwarding port-state
- test mesh disables port-filter, and pings router

**IP Traffic and DHCP:**

- debug ip udp
- debug ip icmp
- debug dhcp [detail]

**Exclusion Listing:**

- debug mesh adjacency exclusion—Watch events that exclude parents.
- test mesh adjacency exclusion clear—Clear out the current exclusion listing counters and start fresh.

**Adjacency State Machine:**

- debug mesh adjacency event
- debug mesh adjacency state
- debug mesh adjacency timer

**Adjacency Communication:**

- debug mesh adjacency packet
- debug mesh adjacency message

**Adjacency Link Issues:**
• debug mesh adjacency channel
• debug mesh adjacency neighbor
• debug mesh adjacency parent

**Signal-to-noise Ratio (SNR) Changes:**

• debug mesh adjacency snr

**Dynamic Frequency Selection (DFS):**

• debug mesh adjacency dfs

**Workgroup Bridge (WGB) Does Not Associate:**

• Collect client debugs on the controller and the AP.
• Collect Airopeek sniffer traces between the WGB and parent Mesh AP.
• Wired Client behind the WGB cannot pass traffic.
• Get state of the parent WGB on the controller.
• Collect debugs on the controller, Mesh AP and WGB.
• Collect Ethereal traces between the parent Mesh AP and controller.

**AP Cannot Be JOINED:**

• Collect Debug Message on the Controller:
  • debug capwap errors enable
  • debug capwap events enable

**Collect Debug Message on the AP:**

• debug capwap client event
• debug capwap client error

**For more information, use these additional debugs:**

**Controller Debugs:**

• debug capwap detail enable
• debug capwap info enable
• debug capwap payload enable
• debug capwap hexdump enable

**AP Debugs:**

• debug capwap client config
• debug capwap client detail
• debug capwap client fwd
• debug capwap client hexdump
• debug capwap client info
• debug capwap client payload
• debug capwap client reassembly

**ShowCommands:**

• show capwap client rcb—shows radio control block configuration
• show capwap client config—shows radio configuration from nvram

**Test Commands:**
• test mesh lwapp restart
• test mesh mode bridge/local
• test mesh role rap/map
• test mesh bgn xxxx
• test lwapp console cli
• test lwapp controller ip

Anti-Stranding Tools:

AP Commands

debg mesh astools
  event -- Event debugs
  level -- Level of detail in debugs
  packet -- packet related debugs
  timer -- timer debugs

Controller

• debug mesh astools troubleshoot <MAC addr>—The b/g radio MAC address of the stranded AP.

Show Commands

• show mesh astools config—current configuration
• show mesh astools stranded-ap-list—print list of detected stranded APs - No Beacons are Heard

• Ensure there is at least one adjacent AP that has joined the controller and can listen to the stranded AP.
• Show cont d0 to determine the current channel of 11b radios that operates.
• Collect all possible debugs that are relevant.

Mperf bandwidth measurement tool:

• Show Commands
  show mesh mperf ?
  globals --- Print configuration used to spawn objects
  print [all/id] --- Print active connections

• Debug Commands
  debug mesh mperf ?
  bwreport -- Bandwidth output reports
  fds -- Multiple connection state machine multiplexing
  general -- All general debugs
  jitter -- Jitter calculations
  sockdata -- Socket data RX and TX
  timer -- Timer related

Issues with NTP Client and Time Configuration on the Controller

• debug ntp packet enable
• debug ntp low enable
• debug ntp detail enable
• show time
• Ethereal capture on controller management port

## RF Component Issues for the WLCs

```plaintext
>debug airewave-director ?

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Configures debug of all Airewave Director logs</td>
</tr>
<tr>
<td>channel</td>
<td>Configures debug of Airewave Director channel assignment protocol</td>
</tr>
<tr>
<td>error</td>
<td>Configures debug of Airewave Director error logs</td>
</tr>
<tr>
<td>detail</td>
<td>Configures debug of Airewave Director detail logs</td>
</tr>
<tr>
<td>group</td>
<td>Configures debug of Airewave Director grouping protocol</td>
</tr>
<tr>
<td>manager</td>
<td>Configures debug of Airewave Director manager</td>
</tr>
<tr>
<td>message</td>
<td>Configures debug of Airewave Director messages</td>
</tr>
<tr>
<td>packet</td>
<td>Configures debug of Airewave Director packets</td>
</tr>
<tr>
<td>power</td>
<td>Configures debug of Airewave Director power assignment protocol</td>
</tr>
<tr>
<td>radar</td>
<td>Configures debug of Airewave Director radar detection/avoidance protocol</td>
</tr>
<tr>
<td>plm</td>
<td>Configures debug of CCX S60 Power Measurement Loss messages</td>
</tr>
<tr>
<td>rf-change</td>
<td>Configures logging of Airewave Director rf changes</td>
</tr>
<tr>
<td>profile</td>
<td>Configures logging of Airewave Director profile events</td>
</tr>
</tbody>
</table>
```

### SNMP Component for WLCs

```plaintext
>debug snmp ?

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Configures debug of all SNMP messages.</td>
</tr>
<tr>
<td>agent</td>
<td>Configures debug of SNMP agent.</td>
</tr>
<tr>
<td>mib</td>
<td>Configures debug of SNMP MIB.</td>
</tr>
<tr>
<td>trap</td>
<td>Configures debug of SNMP traps.</td>
</tr>
<tr>
<td>engine</td>
<td>Configures debug of SNMP engine.</td>
</tr>
</tbody>
</table>
```

- Attach the Simple Network Management Protocol (SNMP) command which failed.
- If the WCS indicates that SNMP failed, then try to run the SNMP set/get command either from MG-soft or any other SNMP manager.
- Check to see if it works from the Controller UI or CLI.
- Attach a screenshot of the CLI/Controller UI.
- If there are memory leaks or CPU issues, mention how long the system has been up.
- Look at the SNMP debugs to see if anything is evident. `debug snmp mibs enable` `debug snmp agent enable` `debug snmp traps enable`.
- Attach out of the earlier debugs.

## Issues with TFTP Upload/Download That Include Upgrade/Downgrade

```plaintext
>debug transfer tftp ?

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables debug.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables debug.</td>
</tr>
</tbody>
</table>
```

### Web GUI Component for WLCs

- Mention which browser issue is seen.
• Check if any java script issue is present. If Firefox is used, check the error console. Attach a screenshot of the java script error. Internet Explorer displays a popup window. For Firefox, attach the error console window.
• If the configuration fails, check with the CLI. Attach the CLI output.
• Attach the screenshot to the bug.
• Mention the controller and AP platform.
• If there is a crash in emweb task, then look at the crash stack trace. If the stack trace indicates CLI, then do not use this component.

Webauth Config and Authentication Issues

• debug pm ssh-appgw enable
• debug pm ssh-tcp enable

WLC-Webauth-Template

Basic Information

Determine the topology of the network at the time webauth was performed.

• Is it a guest setup or normal association at a single WLC, or after roam webauth was done?
• What kind of webauth is configured (internal, external, customized or web-passthru)?
• What is the login page used?
• Download the webauth bundle and provide that.
• Have you enabled secure-web? If yes, disable and see if webauth works.

Show Commands:

• show client details <mac>
• show wlan <wlanid>
• show rules show custom-web

Debug

• debug emweb server enable
• debug pm ssh-tcp enable
• debug pm ssh-engine enable packet <>
• debug pm ssh-appgw enable
debug client <mac>

Note: Issue this debug if the page is not displayed. Make sure to collect this debug separately.

• debug mobility handoff enable

Note: Issue this debug if webauth does not work after roaming.

Sniffers

• WLC DS port—This is helpful for a RADIUS authentication problem.WLC AP port—if http
packets are dropped between the WLC and APOver the air—if the AP drops packets

Controller XML Config Related Issues and Enhancements

XML Validation

- XML Validation Error messages, such as Validation for node ptr_apfCfgData.apfVAPIDDData.apfVapSecurity.<any configuration data>, are observed while system boots.
- the whole XML validation error message
- the CLI or GUI procedure to configure the WLANs prior to system boot
- the CLI or XML config file that is generated and saved to TFTP prior to system boot
- show invalid-config

Diagnostic Channel

- debug client <client mac>
- debug ccxdiag all enable

Dynamic Channel Allocation

- debug airwave-director channel enable
- debug airwave-director radar enable

TACACS+

- debug aaa tacacs enable
- show tacacs summary

WLC-Multicast-Guide

Basic Information

- Topology of the network
- Make sure the multicast stream address is not the IANA reserved address for the application that is in use.
- Multicast addresses used
- The multicast stream rate and packet size
- Make sure the configured AP group multicast address is not the same as the multicast stream address.
- The WLC model (2106, 4404, 4402, WiSM...)
- The AP model (1131, 1232, 1242, 1250...)
- Radio used by the client
- MAC address of the client

WLC Information (All Flavors)

Dumps of:
- show interface summary
debbug bcast * enable
- show network summary
- show network multicast mgid summary
- show network multicast mgid detail <mgid>
- For G release and later: show wlan apgroups
- For TALWAR/2106 with new FP code:
  If IGMP snooping is enabled, debug fastpath cfgtool --mcast4db.dump
debbug fastpath cfgtool --mcast2db.dump
  If IGMP Snooping is disabled, debug fastpath cfgtool --mcast2db.dump
  If Multicast-Unicast is enabled, debug fastpath cfgtool --mcastrgdb.dump

AP Information (All Flavors)

Dumps of:

- show lwapp mcast
  show lwapp mcast mgid all
  show lwapp mcast mgid id <mgid>
  show lwapp client traffic-four times with 1 minute interval

Radio Debugs:

1. The Ethernet overrun rate
2. The radio transmit rate
3. The radio discard rate
4. The power-save mode of the basic service set (BSS)
5. The total Ethernet RX rate
6. The Ethernet multicast RX rate

For #1, run the show int g0 | inc overrun command periodically.

For #2, #3 and #4, run the show cont d0 | beg queues command periodically. Look at the send/discard counts for each queue.

Also, for #3, run the show int d0 | inc output drop command periodically.

For #5, run the show cont g0 | inc RX count command periodically.

For #6, run the show cont g0 | inc multicast command periodically. The first line shows the RX multicast/broadcast.

In order to get the packet rates, run a command every 10 seconds and divide the difference by 10. If a lot of packets are sent on the Mcast queue (for a BSS), then the BSS is in power-save mode. The maximum multicast packet rate for a power-save BSS is relatively low. This is a well-known issue.

Switch Information

Check the switch version with the show version command. The switch can have the "advance ip base" version (for example, Cisco IOS Software, C3750 Software [C3750-ADVIPSERVICESK9-M], Version 12.2(40)SE, RELEASE SOFTWARE (fc3). [image: c3750-advipservicesk9-mz.122-40.SE.bin]). The "ip base" version has an issue in routing inter-VLAN multicast traffic.

Some debugs:

- Check if multicast routing is enabled. ("show run" can include "ip multicast-routing distributed"
Check if "ip pim sparse-dense-mode" config is added to the VLAN configured.

show ip igmp group

**Sniffer Captures**

- DS interface of the WLAN
- Mgmt interface of the WLC
- Ap-Mgr to which the AP is connected (only required when mcast src is wireless)
- Eth interface of the AP
- On the air

**Analysis of Sniffer Captures**

**Multicast Source is Wired Side**

- Check if the packets reach the WLC on the DS interface.
- Check if the LWAPP encapsulated multicast packet is sent on the mgmt interface. The packet must have: outer ip dst addr = configured ap group multicast address udp dst port = 12224
- Check if the packet seen in 'b' is seen at the eth intf of the AP.
- Check if the mcast stream packet is seen on the air.

**Multicast Source is Wireless Side**

- Check if the LWAPP encapsulated packets are received at ap-mgr intf. Here, LWAPP is unicast.
- Check if a multicast packet is sent from the DS intf.
- Check if the LWAPP encapsulated multicast packet is sent on the mgmt interface. The packet must have: outer ip dst addr = configured ap group multicast address udp dst port = 12224
- Check if the packet seen in 'b' is seen at the eth intf of AP.
- Check if the mcast stream packet is seen on the air.

**Switch Configuration Check for WiSM**

- When you use a Wireless Services Module (WiSM), check if you get the same issue mentioned in the section after this one.
- Cisco bug ID **CSCsj48453** — CAT6k does not forward multicast traffic to WISM in L3 mode.
- Symptom—Multicast traffic does not flow from a wired host to a wireless host through the WiSM card in L3 mode, for example, when both the hosts are in different VLANs. Only the first packet reaches successfully. Thereafter, the traffic stops.
- Conditions—The traffic stops only when the multicast replication mode is egress.
- Workaround—A workaround is to change the multicast replication mode to ingress with the **mls ip multicast replication-mode ingress** command. The traffic flows properly in the ingress mode. Verify it uses the same **show mls ip multicast capability** command.

Further Problem Description—The problem is seen with CAT6k and a WiSM. The multicast traffic flows from the wireless host to the wired host works fine, even in L3. Also, the multicast traffic flows from the wired host to the wireless host through the WiSM card works fine in L2 mode.

**WLC-QoS-Guide**

**Minimum Debugs**
• Get the ‘show run-config’ from all switches in the mobility group.
• When the problem occurs, capture these debugs: debug aaa all enabled
debug pem state enabled
debug pem events enabled
debug mobility handoff enabled
debug dot11 mobile enabled
debug dot11 state enable
• Get an Airopeek or AirMagnet trace near the problematic AP/phone/handset.
• Get an Ethereal or Etherpeek capture of the switch DS port, the AP upstream switch, and the SpectraLink Voice Priorities (SVPs).

**CallControl (SIP Classification) Debug**

**Questions**

• Is it a Session Initiation Protocol (SIP) client?
• What IP PBX\sip server is used?
• Does it show that it is registered on that given SIP server?
• Does the 7921 work as expected, and only the SIP clients have an issue?

**WLC Information**

• show wlan summary [wlan #]
• Debug call-control all
• Debug call-control events
• Show call-control errors
• Show call-control calls

**AP Information**

• Debug dot11 cc details
• Debug dot11 cc errors
• Debug dot11 cc events
• Show lwapp client call-info mac (MAC address of client in question)

**Load Based Admission Control and Voice Metrics**

**Questions to Answer**

• Does it happen with both radios ‘a’ and ‘b’?
• What is the Channel Utilization value when the call is rejected?
• Is this with 7921 phones only, or with other phones as well? If yes, what are the phones? If not, can this be tried on another TSPEC phone?
• Is this with 11n or regular APs?
• Do you use the inter-controller mobility?
• Is the TSPEC phone capable?
• Does it do the UAPSD?
• Is this reproducible in 2006 or 4100 platforms?
• Is it a shielded room environment?
• Was there a special condition for which the call was rejected?

**Debug and Show Commands on WLC for LBCAC**

• debug cac all enable
- show 802.11a/b/g
- show wlan <wlan id>
- show ap stats 802.11a/b/g <ap-name>
- show ap auto-rf 802.11a/b/g <ap-name>

**Debug the AP for LBCAC**

- debug dot11 cac unit
- debug dot11 cac metrics
- debug dot11 cac events

**Voice Metrics**

- Over the air and wire sniffer captures
- Check to see if UP6 traffic generates continuously.
- Make sure the WLAN has the right QoS profile and the Wi-Fi Multimedia (WMM) policy.
- Most of the questions asked for LBCAC are applicable for voice metrics.

**Debugs and show commands on the WLC for voice metrics:**

- show 802.11a/b/g o show wlan <wlan id>
- show ap stats 802.11a/b/g <ap-name>
- show ap stats 802.11a/b/g <ap-name> tsm
- show client tsm 802.11a/b/g <client-mac> <AP mac>
- debug iapp packet enable o debug iapp error enable
- debug iapp all enable o debug client <client mac>

**Debugs on the AP for voice metrics:**

- debug dot11 tsm
- debug lwapp client voice-metrics

**WLC-License-Guide**

**Debugs to Collect on Controller**

- Console output
- msglog

**ARP Issues**

**Debugs to Collect on Controller**

- debug arp all enable

**Network Issues**

**Debugs to Collect on Controller**

- debug packet logging enable
- dump-low-level-debugs
Others

Debugs to Collect on Controller

- dump-low-level-debugs
- msglog

Access Point Issues

IAPP

- show wgb summary
- show wgb detail <wgb mac>

WGB Association Issues

- debug dot11 mobile enable
- debug dot11 state enable
- debug pem events enable
- debug pem state enable
- debug iapp all enable

WGB or Wired Client Does not Get DHCP Address

- debug dhcp packet enable
- debug dhcp message enable

WGB or Wired Client Uses Static IP Address but IP Address Does not Appear on Controller

- debug dot11 mobile enable
- debug dot11 state enable

AP Username Password

Debugs to Collect on AP

- debug lwapp client config

Captures to Take

- Not applicable.

Config and Show Output to Collect

- config ap mgmtuser

Client Connection Issues
Client Debug

- debug client xx.xx.xx.xx.xx.xx

Controller Does not Like the Association Request

Packet Capture

- Airopeek capture on the channel from which the AP is set. It is recommended to avoid filtering because the beacon and probe req/resp packets can be missed. Make sure to capture the event when the connection is ended.
- In case the client does not connect, capture the whole event from prob request until the session is ended (for example, deauth is sent and association response with status-code as non 0).
- Provide the client and AP MAC addresses.

  Note: The AP MAC is base Radio MAC + WLAN-ID.

Config and Show Output to Collect on the Controller

- show sysinfo—WLC’s version details
- show wlan x—on WLC for the affected WLAN
- show run-config—of WLC
- show debug
- show msglog
- show tech-support—of WLC (good to have, but not necessary)

Client Details

- Client hardware—Supplicant software details such as version and software name (for example, ADU or Odyssey)
- Client OS—If it is Windows, provide the client system configuration, go to Programs > Accessories > System Tools > System Information.

RADIUS Server Details

Provide the RADIUS server type (SBR, Cisco ACS, Linux, and so on) and configuration if applicable.

Client Does Not Respond to EAP Requests

See the Controller Does not Like the Association Request section.

EAP Authentication Does Not Go Through

See the Controller Does not Like the Association Request section.

DHCP Request from Client Fails

See the Controller Does not Like the Association Request section.
EAPOL Exchange Does Not Go Through

See the Controller Does not Like the Association Request section.

CCKM Roaming Fails

Debugs to Collect

Most of the debugs are the same as the earlier section, Client connection issue. However, these new debugs help more in CCKM debugging. This debug command is available from 5.0 and later:

- debug cckm enable
- show pmk-cache <client mac>—on the target controller
- show client details <client mac>—when client is connected on the old AP
- debug cckm enable

Note: These debugs or any other debug must be switched ON after you issue debug client<client mac>. This is because the debug client<mac> command causes all earlier debugs to be disabled.

Captures to Take

Make sure you capture on the channel where the target AP is. For example, you want to capture all management packets between the client and the target AP. See the Controller Does not Like the Association Request section for more information.

Config and Show Output to Collect on Controller

See the Controller Does not Like the Association Request section and issue these commands:

- show pmk-cache <client mac>—on the target controller
- show client details <client mac>—when client is connected on the old AP

Client Details

See the Controller Does not Like the Association Request section.

PMKID Caching Fails

Check if the client supports opportunistic key cache (OKC).

Note: OKC is not the same as proactive key cache (PKC) as specified in 802.11I. The WLC only supports OKC.

Debugs to Collect

See the Controller Does not Like the Association Request section.

Captures to Take

Make sure you capture on the channel where the target AP is. For example, you want to capture
all management packets between the client and the target AP.

See the [Controller Does not Like the Association Request](#) section.

### Config and Show Output to Collect on Controller

See the [Controller Does not Like the Association Request](#) section and issue these commands:

- show pmk-cache <client mac>—on the target controller
- show client details <client mac>—when client is connected on the old AP

### Client Details

See the [Controller Does not Like the Association Request](#) section.

### Reauth Issues

### Debugs to Collect

See the [Controller Does not Like the Association Request](#) section.

### Captures to Take

Not applicable.

### Config and Show Output to Collect on Controller

See the [Controller Does not Like the Association Request](#) section and issue these commands:

- show radius summary
- show client details <client mac>
- show pmk-cache <client mac>

### Client Details

See the [Controller Does not Like the Association Request](#) section.

### 802.11R (Fast Transition) Roaming Does Not Work

### Debugs to Collect

- debug client <client mac>
- debug ft events enable
- debug ft keys enable

**Note:** These debugs or any other debug must be switched ON after you issue `debug client <client mac>`. This is because the `debug client <mac>` command causes all earlier debugs to be disabled.

### Captures to Take

When you roam over the air, collect Airopeek capture on the channel where the target AP is. For
example, you want to capture all 802.11 auth FT req/resp frames and reassociation req/resp.

When you roam over the DS, collect Airopeek capture on the channel where the source AP is. For example, if you want to capture reassociation req/resp frames. You also want to capture Action frame’s FT req/resp on the source AP’s channel.

**Note:** It is recommended to keep the source and destination APs in the same channel in order to debug the 802.11R roaming issue. This allows you to capture FT req/resp and reassociation req/resp in a single capture file.

### Config and Show Output to Collect on Controller

See the Controller Does not Like the Association Request section and issue these commands:

- `show pmk-cache <client mac>`—on the target and source controller
- `show client details <client mac>`—when client is connected on the old AP
- `show mobility summary`—to get the mobility domain ID

### Client Details

Currently, only the WGB is the known 802.11R client. See the Controller Does not Like the Association Request section for more information.

### Inter Controller Mobility

### Debugs to Collect

- `debug client <client mac>`—on both WLCs
- `debug mobility handoff enable`—on both WLCs (Remember the order: always enable debug client first.)
- `Debug pem state enable`
- `Eping <ip>`
- `Mping <ip>`

If mobility control path or data up is down, then turn on ‘debug mobility keepalive enable’ on both switches (make a note of the software version on both controllers).

If ARP does not work, turn on ‘debug arp all enable’ on both switches.

If DHCP does not work, turn on ‘debug dhcp message enable’ and ‘debug dhcp packet enable’ on both switches.

If IPSec is involved: `debug pm sa-export enable`, `debug pm sa-import enable`.

If the client connects after a while, show how long it took.

### Captures to Take

Capture by the roaming type, such as CCKM, PMKID or TGR.

### Config and Show Output to Collect
See the **Controller Does not Like the Association Request** section and issue these commands:

- `show pmk-cache <client mac>`—on the target controller
- `show client details <client mac>`—when client is connected on the old AP
- `show mobility summary`—on both WLCs

**Client Details**

See particular roaming type, such as CCKM, PMKID or TGR.

**Disable Debugs**

In order to disable all debug messages, use the `debug disable-all` command.

Alternatively, you can disable specific debugs with the `debug` command and the `disable` keyword:

```
ddebug capwap events disable
```

**Related Information**

- [Technical Support & Documentation](#)
- [Understand Wireless Debugs and Log Collection on Catalyst 9800 Wireless LAN Controllers](#)