Troubleshoot Catalyst 9800 AP Join or Disconnection Issues Flow

Contents

Introduction

Prerequisites

Topology

Generic Outputs to Collect from WLC

Specific Outputs from WLC for Concrete AP

Advanced Logs from WLC and AP for Concrete AP

Logs from WLC

- Logs from AP

List of All Commands

- List of All Commands from WLC
- List of All Commands from AP

Introduction

This document describes a systematic approach and list of commands to collect for troubleshooting 9800 AP join or disconnection issues.

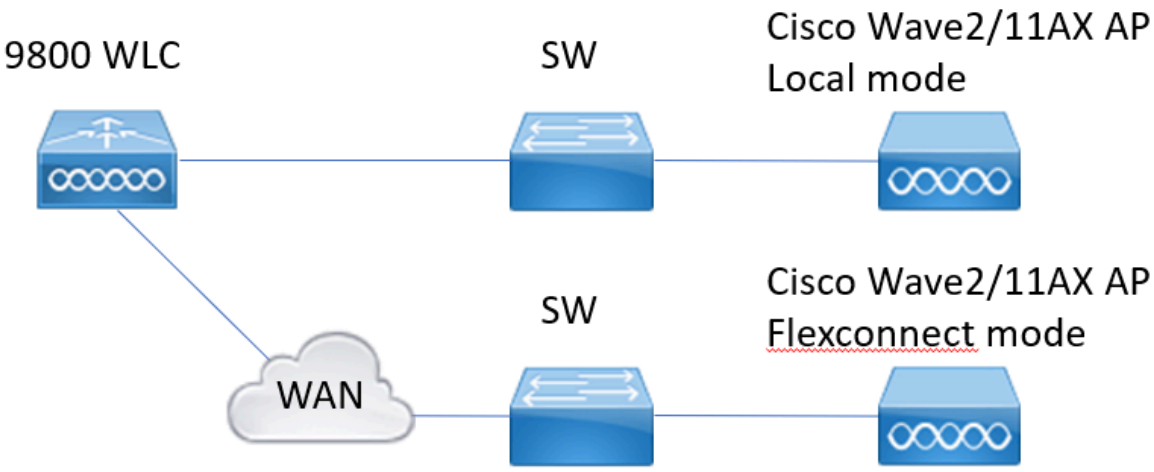
Prerequisites

Cisco recommends that you have knowledge of these topics:

Basic knowledge of Cisco WLC 9800
Basic knowledge of Cisco Wave2 and/or 11AX APs

Topology

This troubleshooting flow is applicable for APs connected in local mode or APs connected in flexconnect mode in a branch site.



Generic Outputs to Collect from WLC

1. You can start to verify that the number of APs matches the expected number of APs connnected to WLC. And reviewing WLC logs for AP disconnections.
Identify if you are missing any APs and if in the logs you observe APs disconnecting at the same time or always same APs connecting/disconnecting:

sh ap image summary | i Number of APs !!Check if number of APs matches with number we expect sh log | i AP Event: !!Check if APs are disconnecting at same time, or exist any pattern for APs connecting/disconnecting.

2. You can get list of all the APs and check for missing APs. Identify APs with lower Up Time and lower Assoc Uptime, that helps to identify if there are APs reloading or reconnecting to capwap. If APs are reloading, you can check for APs with similar uptime and check if those APs were in same switch. If you are seeing APs with high Up time and lower Association time you need to check if there were changes done to those APs that could cause capwap restart or if there are capwap flaps due to retransmissions. You can also check if there are any AP crashes.

show ap uptime !! Check Up Time vs Assoc Up Time. Check for patterns show ap cdp nei !! Identify if all APs with similar Up Time were in same switch. show ap crash !! Check if there are any AP crashes. dir all | i crash !! Find AP crashes stored in WLC.

3. You can check for all AP connect/disconnect historical events, and disconnect reasons. You can find out if disconnect reason is similar to all the APs and in which phase of the connection did disconnection happen.
Identify top disconnection reasons and if there is any time pattern for those disconnections.

show wireless stats ap history !! Find connect/disconnect events, time for those events, disconnect reason and count. show wireless stats ap discovery !! Find discovery requests been received by WLC and time for those discovery requests show wireless stats ap join summary !! Find status of the AP, last disconnection reason and in which phase disconnection occurred.

4. In case the errors are seen in the DTLS phase we can check which type of certificate and ciphers are used for AP DTLS handshake.

show wireless certification config !! Check DTLS version and cipher suite show wireless management trustpoint !! Type of certificate used show wireless dtls connections !! Show if DTLS is established for capwap control/data ports used

Specific Outputs from WLC for Concrete AP

5. Now you can focus on some concrete AP that is having issues. First you need to find the ethernet mac and radio mac for that AP. Check history for that AP and always-on-tracing
Use the show commands to have a summary of events with time reference, different phases of AP association and in which you could observe failures, reason for reboot or disconnect.
You can find out if WLC rebooted the AP due to image upgrade. Or if AP disconnected due to keepalive failure.
Then use **always-on-tracing** to have more details about what occurred to the AP showing sequence of events. With show command time reference you can focus on the events occurring around that time.

Collecting show tech wireless for concrete AP provides us config details, tag assigment, info about model, radios channels... show wireless stats ap history mac-address Ethernet_MAC@ !!Check type of event and time for the event and disconnect reason and count for specific AP. show wireless stats ap mac Radio_MAC@ discovery detailed !!Check number of discovery request/responses, discovery failures and type for last working discovery and non working discovery. show wireless stats ap mac Radio_MAC@ join detailed !!Counters for different phases discovery, dtls, join, config, data dtls. Also shows last reboot type and reason. Disconnect type and reason. show logging profile wireless start last X days filter mac <radio-or-ethernet-AP-mac> !!Always-on-tracing for this AP shows more detailed events errors stored in the WLC trace database. Config changes, radio events, association/disassociation events. show tech wireless ap name <ap-name> !! Config details, tag, radio info channels/txpower, SSIDs, ...

6. If you are observing that multiple APs that are not in same switch are disconnecting around the same time, then you can confirm if all disconnecting APs are in the same wncd.
If that is the case then you can check wncd CPU utilization to see if disconnections could be due to high wncd CPU utilization and WLC not been able to process packets received from APs.

show wireless loadbalance ap affinity mac Ethernet_MAC@ !!Check wncd assigned to concrete AP mac address, we can also get wncd for concrete site-tag show wireless loadbalance ap affinity wncd <0-7> !!Other option is to check all APs assigned to a concrete wncd. sh proc cpu platform | i wncd !! Check CPU utilization per wncd

Advanced Logs from WLC and AP for Concrete AP

7. If with previous information you are not able to identify reason for AP joins, then you need to **capture ra-traces** and packet captures and AP debugs in case you can access the AP for next event. This provides packet captures from AP and verbose level traces to identify reasons for the AP disconnections. Need to enable traces and captures before the next event to capture the data.
In case AP is accessible through SSH you can enable debugs in the AP that provides point of view of the AP about disconnections. Collecting packet capture in WLC and AP switchport could be helpful to identify if disconnections are due to some packet drops in the network.

Logs from WLC

!! Enable ra-trace for AP using default monitor-time is 1800s increse it to max in case you do not know when AP disconnection occurs. debug wireless mac <AP_Radio_MAC> internal monitor-time 2085978494 !!Using AP radio mac to capture traces with verbose level from WLC. Setting time allows us to enable traces for up to 24 days !!Or debug wireless ip <AP_IP> internal monitor-time 2085978494 !!Using AP ip address to capture traces with verbose level from WLC. Setting time allows us to enable traces for up to 24 days !!Reproduce no debug wireless mac <AP_Radio_MAC|AP_IP> internal monitor-time 2085978494 !!WLC generates an ra_trace file with AP_info, command to check for ra_trace file generated. dir bootflash: | i ra_trace !!Embedded Captures filtered by AP IP address ACL.

Filter packet captures for AP ip address in both directions and have a circular buffer to ensure that we get latest captures in case buffer exceeds 100M !!Create ACL ip access-list extended CAP-FILTER permit ip host <AP_IP> any permit ip any host <AP_IP> !!Create packet capture monitor capture MYCAP clear monitor capture MYCAP interface Po1 both monitor capture MYCAP buffer circular size 100 monitor capture MYCAP match any monitor capture MYCAP access-list CAP-FILTER monitor capture MYCAP start !!Reproduce monitor capture MYCAP stop monitor capture export flash:|tftp:|http:.../filename.pcap

Logs from AP

show tech !! Collect show tech to have all config details and radio stats for the AP. show dtls connection !! Check certificates, ports and ciphers, versions for DTLS term mon !!Basic debug capwap client events debug capwap client error !! Advanced debug capwap client pmtu debug capwap client keepalive debug capwap client payload debug capwap client details

List of All Commands

List of All Commands from WLC

show ap summary | i Number of APs
sh log | i AP Event:
show ap uptime
show ap cdp nei
show ap crash
dir all | i crash
show wireless stats ap history
show wireless stats ap discovery
show wireless stats ap join summary
show wireless certification config
show wireless management trustpoint
show wireless dtls connections
show wireless stats ap history mac-address Ethernet_MAC@
show wireless stats ap mac Radio_MAC@ discovery detailed
show wireless stats ap mac Radio_MAC@ join detailed
show logging profile wireless start last X days filter mac <radio-or-ethernet-AP-mac>
show tech wireless ap name <ap-name>
show wireless loadbalance ap affinity mac Ethernet_MAC@
show wireless loadbalance ap affinity wncd <0-7>
sh proc cpu platform | i wncd
debug wireless mac <AP_Radio_MAC> internal monitor-time 2085978494

List of All Commands from AP

show tech show dtls connection term mon debug capwap client events debug capwap client error debug capwap client pmtu debug capwap client keepalive debug capwap client payload debug capwap client details debug capwap client info