Verify Hardware Failures and Gather Data Before RMA

Contents

Introduction

This document provides a checklist of data for bulk failures of Access Points which is beneficial for TAC to troubleshoot further and perform RMA.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Cisco Wave1, Cisco Wave2 and/or 11AX APs
- Good understating of the AP join process with the catalyst 9800 WLC.
- Indoor and Outdoor AP Installation Best Practices.

Components Used

This document is not restricted to specific software and hardware versions of access points and is applicable to all Cisco Access Points.

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.

Background information

This article provides good understanding of the data that needs to be gathered before performing a hardware replacement in situations of bulk failure or replacement of APs. It also provides steps to gather the trigger and data for future failures.. The data gathered is beneficial for TAC to validate, troubleshoot further and perform RMA or hardware replacement as needed.

Information to Collect for Wireless AP RMAs

It is recommended to gather this information and provide to TAC via Service Request:

- The total number of units that have failed in a specific environment. Percentage of failure provides good clarity on how many units failed out of how man
- Device Part Number (PID) or Model(s) and Serial Number(s) of units.

- Software version that was running on the device when it failed.

- If a hardware or software upgrade was performed recently or any changes to uplink switch, verify if device(s) are failing in same site always or Random or All sites? If many sites are impacted, please share the relevant information from all the sites:

    ◦ If devices are failing always in a specific site, identify if there is any dependency and trigger in terms of: Physical Location
    ◦ Environment
    ◦ Weather
    ◦ Powering Option(POE or Injector or Adapter)
    ◦ Client load

- Verify if device(s) are failing in same site always or Random or All sites? If many sites are impacted, please share the relevant information from all the sites.

    ◦ If devices are failing always in a specific site, identify if there is any dependency and trigger in terms of : Physical Location, Environment, Weather, Powering Option(POE or Injector or Adapter), Load of clients, if an Hardware Upgrade or Software Upgrade was performed recently or any changes to uplink switch.

- Verify if devices failed immediately after installation or soon after powering up or if they came dead on arrival.

- If devices did not fail immediately after installation, gather the data on number of days or months the devices were up before failing . If part did not fail immediately, retrieve a copy of most recent configuration available.

- If AP is powering up, verify LED status. Check the installation guide, section - Access Point LED status. A sample link : Checking Access Point LEDs

- If console or SSH to AP is available, gather these logs :
    ◦ **show logging**
    ◦ **show tech**
    ◦ **dir flash:** Check for any crash or core files)
    ◦ **more flash:<filename>**
    ◦ AP crashe files can also be obtained from 9800 WLC using the procedure : AP Crashes

This helps verify if there if there are any issues at software level like crashes.

- If AP is failing to power, please validate whether the device is getting enough power via UPOE or POE+. In case the switch is providing the power, try swapping with a known working cable, switchport, switch, power injector, or power adapter one at a time to identify the source of failure.
- For outdoor deployments, verify whether there is proper grounding. If yes, please collect pictures and provide the pertinent information in the TAC case description.
    ◦ If grounding is not done for APs, please refer to the outdoor installation best practices video

series in the "Related Information" section of this article.
- If indoor AP is deployed in an outdoor environment, ensure there is a NEMA enclosure. Verify if there is any water leakage, corrosion or physical damage. It is recommended you use industrial grade, rugged equipment for harsh environments.
- Stockpiling and bulk replacement requests are to be avoided. It is suggested to replace on failure.
- In cases where there are repeated failures at the same site and failure is higher, please have TAC file an EFA for Failure Analysis. With this process, the failure part could be shipped to the site where the hardware team can perform advanced analysis and share the failure report.
- Please keep an eye out for field notices Field Notice Search and SN validator tools available within FN. Refer to AP boot failure FN for a sample field notice on image corruption post upgrade. This is a software issue and the hardware does not need to be replaced or swapped since there are recovery procedures.

Conclusion

Leveraging the checklist and isolating the trigger helps in cases of bulk failures thus saving time for customers and partners by using the right methodical step to troubleshoot, identify and replace the failed units.

Related Information

If Grounding is not done for APs, please refer to outdoor installation best practice guide and videos :

Video Series: Best Practices for Installing Outdoor Wireless Access Points

YouTube Video Links:

- Best Practices for Installing Outdoor Wireless Access Points: An Overview
- Best Practices for Installing Outdoor Wireless Access Points: Antenna
- Best Practices for Installing Outdoor Wireless Access Points: Power Supply
- Best Practices for Outdoor Wireless Access Points: Mounting Accessories
- Best Practices for Installing Outdoor Wireless Access Points: Grounding
- Best Practices for Outdoor Access Points - Lightning Protection
- Best Practices for Installing Outdoor Wireless Access Points: Water Intrusion Protection
- Best Practices for Outdoor Wireless Access Points: Cable and Connector Wraps
- Best Practices for Outdoor Wireless Access Points: Electronic or Cabinet Enclosure
- Outdoor And Industrial Wireless APs