Configure Best Recommended Design as per Known Issues with mDNS Bonjour Services on Catalyst 9800 WLC

Contents

Introduction

This document describes the recommended design for mDNS and issue scenarios with mDNS in Cisco Catalyst 9800 Series WLC.

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- Cisco Catalyst 9800 Series Wireless LAN Controller (WLC) multicast domain name server (mDNS) concepts
- Cisco Catalyst 9800 Series WLC configuration

Components Used

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.

- Cisco Catalyst 9800 Wireless Controller Series (Catalyst 9800-CL), Cisco IOS® XE Cupertino 17.18.3
- Cisco Catalyst 3560 Series Switch, Cisco IOS® 15.2.4E10
- Cisco Catalyst Access Point CW9178

Core Architecture and Operating Modes

Before troubleshooting, verify which mode the 9800 is expected to operate in. The mDNS policy mode applied to a Policy Profile dictates how the WLC handles mDNS packets.

Gateway (Recommended)

The WLC snoops mDNS packets, builds a cache of services, and responds via unicast to client queries across different VLANs.

Within the Gateway architecture, there are two deployment models based on where the AP is located:

Central mDNS Gateway (Local Mode APs)

The Cisco Catalyst 9800 WLC itself acts as the gateway. All mDNS traffic is CAPWAP-tunneled to the WLC, where the WLC builds the cache and proxies the responses.

FlexConnect mDNS AP (Distributed Gateway)

In branch deployments, where APs are in FlexConnect Local Switching mode, sending broadcast/multicast mDNS traffic over the WAN back to the WLC is highly inefficient. By enabling **mDNS AP** in the Flex Profile, the Access Point itself runs the Gateway engine. The AP builds a local cache of printers on the local switch of the branch and responds directly to wireless clients at the branch, keeping mDNS traffic completely off the WAN link.

Bridging

The WLC simply bridges the multicast packets to the wired/wireless network. Only useful if clients and services are on the *exact same VLAN*.

Drop

All mDNS packets are dropped. (Useful for high-density networks where mDNS is not supported to save airtime).

Configuration Best Practices

Following architectural mandatory configurations need to be checked:

- **Wired-Side Traffic Validation:** The 9800 mDNS Gateway acts as a proxy. If a wireless client queries for a wired printer, the WLC must forward that query to the wired network and receive the response. You must confirm mDNS traffic is traversing the wired trunks to the WLC. If the upstream switch drops UDP 5353, the WLC cache remains empty.
- **SVI Mandate:** The mDNS Gateway module on the 9800 *requires* an active SVI (Interface VLAN) with an IP address for every VLAN it needs to snoop (both client and service VLANs). The WLC cannot route the mDNS cache between VLANs without these SVIs being up/up.
- **Broadcast/Multicast vs. Unicast Over the Air:** It is recommended to minimize airtime utilization. By using the mDNS Gateway, the WLC answers client mDNS queries via **Unicast**, protecting the RF environment from excessive multicast flooding. Do not enable global multicast routing just to fix mDNS.
- **When to use mDNS Bridging (Same VLAN):** When the wireless client, like an iPhone, and the

service provider (like an Apple TV or AirPrint printer) reside on the exact same VLAN/subnet.

Best Practices and Requirements

Wired Configuration

You must have global Multicast Routing and IGMP Snooping enabled on your wired switches so the multicast traffic can physically reach other devices on that VLAN.

- **Wireless Configuration:** On the 9800 WLC, you must enable Global Multicast and Wireless Broadcast.
- **Caveat:** Bridging is *not* recommended for very large subnets (such as /16 or /22 enterprise networks). Multicast traffic is sent at the lowest basic data rate, which consumes massive amounts of wireless airtime and CPU on the WLC. Bridging must only be used in small deployments or isolated, dedicated VLANs.

When to Use mDNS Gateway (Different VLANs / Enterprise Deployments)

When the wireless client (such as Guest or Employee VLAN) and the service provider (such as Printers VLAN, IoT VLAN) reside on different VLANs/subnets. This is the standard deployment model for enterprise networks.

SVI Requirement

The 9800 WLC *must* have an active Switched Virtual Interface (SVI) with an IP address for every VLAN it needs to snoop (for example, interface vlan 10 for clients, interface vlan 20 for printers). The WLC uses this IP to answer queries.

- **Policy Control:** You must apply an mDNS Service Policy to the Policy Profile. This allows you to define exactly which services are permitted to cross VLAN boundaries (for example, permit apple-airprint but deny apple-timecapsule).Migrate Service list properly by not using legacy AireOS concepts blindly.
- **Location Specific Services (LSS):** In a large enterprise using the Gateway, always enable LSS. This ensures that a user in Building A only sees printers physically located in Building A, rather than seeing every printer cached across the entire global network. If location is not specified in the service policy, the location is considered from the global mDNS gateway. By default, the global mDNS gateway location is defined as **lss** .
- **Active Query:** Enable mdns-sd active-query. This allows the WLC to periodically poll the network for services rather than strictly waiting for a device to announce itself.
- **Same-VLAN Branch Deployments (Rely on L2 Bridging)**

Design Recommendation

If your deployment utilizes FlexConnect Local Switching, and both the wireless clients and the wired services (like printers, Apple TVs) reside in the exact same VLAN (Broadcast Domain)

- Bypass the AP-based mDNS Gateway features entirely. Allow native Layer 2 bridging on the FlexConnect AP.
- Ensure that standard IGMP Snooping and multicast forwarding are enabled on the local branch switch.

Ensure Multicast config Configured across Network

To ensure multicast forwarding and Bonjour/mDNS advertisements work across the required VLANs, verify these areas end-to-end:

1. Enable mDNS Gateway globally on the WLC.
2. Create and apply an mDNS policy under the WLAN Policy Profile.
3. Add the required service definitions (for example Google Chromecast, AirPlay, printers, and more) to the policy.
4. Ensure the client VLANs participating in mDNS have reachable SVIs/interfaces in the network.
5. Verify multicast routing/PIM configuration if the traffic traverses Layer 3 boundaries.
6. Enable IGMP snooping on all switching infrastructure carrying the wireless VLANs.
7. Confirm multicast is not blocked by ACLs, firewall rules, or security policies.
8. Make sure WLAN peer/client isolation settings do not block the required service discovery traffic.
9. Verify AP switchports and trunk links allow the required VLANs.
10. Confirm querier functionality exists in the VLAN if required by the switching design.

Common Scenarios and Field Remediations

Scenario A: Cross-VLAN Service Discovery Fails (AirPrint / AirPlay)

Symptom

Clients on VAN 10 cannot see Printers (AirPrint) on VLAN 20.

Root Cause Analysis

- **Missing SVIs:** As noted above, the WLC lacks an SVI for VLAN 10 or VLAN 20.
- **Policy Misconfiguration:** The mDNS policy applied to the client-side Policy Profile only allows IN (learning) but not OUT (querying).

Remediation

1. Ensure interface vlan X exists on the WLC with a valid IP and is up/up.
2. Verify the mDNS Policy has both IN and OUT directions permitted for the required services (apple-airplay, apple-airprint).

Scenario B: FlexConnect Local Switching mDNS Failures

Symptom

APs in FlexConnect mode dropping mDNS traffic or failing to apply Location Specific Services (LSS).

Remediation

1. Navigate to **Configuration > Tags and Profiles > Flex**.
2. Under the Flex profile, ensure the **mDNS** tab is configured to enable mDNS AP (if doing distributed gateway).
3. *Note on LSS:* If Location Specific Services (LSS) is enabled, the WLC filters services based on the physical location (MAC/Site tag) of the AP. If a printer is on a wired switch far from the AP, LSS can filter it out. Try temporarily disabling LSS in the mDNS profile to isolate the issue.

Scenario C: High CPU, MSG_Queue Full, or Network Degradation

Symptom

WLC logs show MSG_Queue gets full, high CPU on datapath processes, or complete loss of mDNS capabilities periodically.

Remediation and Isolation (Blocking mDNS)

If a multicast loop or excessive Bonjour chatter is bringing down the WLC, you could need to temporarily block mDNS for stability:

To block mDNS centrally, create an IPv4 ACL denying UDP 5353 and apply it to the wireless client-side Policy Profile, or disable mDNS entirely under **Configuration > Services > mDNS**.

1. **Disable mDNS Bridging:** Disable global **mDNS Bridging** and **Wireless Broadcast** on large subnets. Rely strictly on the **mDNS Gateway**.
2. Audit wired switches to ensure IGMP Snooping is enabled to prevent mDNS flooding on the wired trunks connected to the WLC.

Scenario Chromecast Discovered via mDNS but Casting Fails ("No Internet

Connection")

Symptom

Google Chromecast devices could successfully join the WLAN and be discovered by clients via mDNS. However, when users attempted to actually cast media, the casting failed with the error message: “You have no internet connection, please check your connection to internet.”

Remediation

Enable P2P Blocking: Enabled WLAN Peer-to-Peer (P2P) blocking (often set to *Forward-UpStream* to force client-to-client traffic through the gateway rather than dropping it at the AP).

Scenario E: Choppy Audio on Vocera Broadcasts / Multicast Traffic Dropping

Symptom

Vocera badges experience choppy audio during broadcast calls, or IPTV streams pixelate heavily.

Root Cause

If Multicast-Direct is enabled globally but the specific multicast stream (such as Vocera 239.x.x.x address) is not explicitly permitted under the media-stream configuration, or if the AP radio is configured to drop streams when bandwidth is full (Admission Control).

Remediation

1. **Admission control:** Check the 5GHz/2.4GHz radio configurations for Media Stream. If you see violation drop, the WLC drops the multicast stream if the RF channel utilization is too high.
    - Change the violation to **fallback: ap dot11 5ghz media-stream multicast-direct admission-besteffort** (this allows it to fall back to standard multicast if unicast conversion bandwidth is not available).
2. **Stream Configuration:** Explicitly define the multicast IP range that needs conversion: **wireless media-stream group <Stream_Name> <Start_IP> <End_IP>**

Comprehensive Logging and Diagnostic Steps

When troubleshooting, follow this order of operations to isolate where the break occurs (**Client -> AP -> WLC -> Server**).

Phase 1: CLI Verification Checks

Is mDNS globally enabled?

show mdns-sd summary

Has the WLC learned the service? (Look for the Printer/TV MAC or IP)

show mdns-sd cache

show mdns-sd cache detail

Are queries hitting the WLC and being dropped?

show mdns-sd statistics

#Is multicast control plane between WLC and AP established?

show ap multicast mom

Verify the policy applied to the client

show wireless profile policy all | inc mDNS

Phase 2: Trace and Debug Mechanisms

Radioactive Trace (always start here): Run an RA trace against the MAC address of the Client AND the Service Provider.

- **debug wireless mac <Client_MAC> internal**
- **debug wireless mac <Printer_MAC> internal** (This shows if the WLC datapath is intentionally dropping the UDP 5353 packet due to policy or LSS filtering).
- Set platform software **trace wncd <0-7> chassis active R0 mdns debug**

To get the logs, show the log:

show platform software trace message wncd <0-7> chassis active R0

Phase 3: Embedded Packet Capture (EPC)

To prove definitively if the packets are reaching the WLC from the wired side or leaving the WLC over the air:

1. Navigate to **Troubleshooting > Packet Capture** in the 9800 GUI.
2. Set up an EPC on the WLC uplink (Te0/0/0 or Port-Channel) to validate the **wired infrastructure**.
3. Set up an EPC on the specific SVIs to validate **wireless routing**.
4. Create an IPv4 ACL targeting UDP Port 5353.
5. Export the PCAP to Wireshark and filter by udp.port == 5353 || mdns.

Analysis

Verify that the WLC receives the query from the client, routes it, and sends a Unicast response back to the client containing the Printer/Apple TV details.

Reference Information and Official Documentation

- Understand mDNS on Catalyst 9800 WLC