

Configure el mejor diseño recomendado según los problemas conocidos con los servicios mDNS Bonjour en el WLC Catalyst 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Arquitectura principal y modos operativos](#)

[Gateway \(recomendado\)](#)

[Gateway mDNS central \(puntos de acceso de modo local\)](#)

[AP mDNS de FlexConnect \(gateway distribuido\)](#)

[Conexión en puente](#)

[Abandonar](#)

[Prácticas recomendadas de configuración](#)

[Prácticas recomendadas y requisitos](#)

[Configuración por cable](#)

[Cuándo Utilizar el Gateway mDNS \(Diferentes VLAN / Implementaciones Empresariales\)](#)

[Requisito de SVI](#)

[Recomendación de diseño](#)

[Garantía de configuración de multidifusión configurada en toda la red](#)

[Escenarios comunes y remediaciones de campo](#)

[Escenario A: Fallos en el descubrimiento del servicio de VLAN cruzada \(AirPrint / AirPlay\)](#)

[Síntoma](#)

[Análisis de causa raíz](#)

[Corrección](#)

[Situación B: Fallos de mDNS de switching local de FlexConnect](#)

[Síntoma](#)

[Corrección](#)

[Situación C: CPU alta, MSG Queue lleno o degradación de la red](#)

[Síntoma](#)

[Solución y aislamiento \(bloqueo de mDNS\)](#)

[Chromecast de escenario detectado mediante mDNS pero fallo de conversión \("sin conexión a Internet"\)](#)

[Síntoma](#)

[Corrección](#)

[Situación E: Audio entrecortado en transmisiones de voz / tráfico multidifusión descartado](#)

[Síntoma](#)

[Causa raíz](#)

[Corrección](#)

[Completo pasos de registro y diagnóstico](#)

[Fase 1: Comprobaciones de verificación de CLI](#)

Introducción

Este documento describe el diseño recomendado para mDNS y los escenarios de problemas con mDNS en Cisco Catalyst 9800 Series WLC.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- Conceptos de servidor de nombres de dominio multidifusión (mDNS) del controlador de LAN inalámbrica (WLC) Cisco Catalyst serie 9800
- Configuración del WLC de Cisco Catalyst serie 9800

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

- Controlador inalámbrico Cisco Catalyst serie 9800 (Catalyst 9800-CL), Cisco IOS® XE Cupertino 17.18.3
- Switch Catalyst de Cisco serie 3560, Cisco IOS® 15.2.4E10
- Punto de acceso Cisco Catalyst CW9178

Arquitectura principal y modos operativos

Antes de iniciar la localización de averías, compruebe en qué modo se espera que funcione el 9800. El modo de la política mDNS aplicado a un perfil de la política dicta cómo el WLC maneja

los paquetes mDNS.

Gateway (recomendado)

El WLC detecta los paquetes mDNS, construye una memoria caché de los servicios, y responde vía unicast a las consultas del cliente a través de las diversas VLAN.

Dentro de la arquitectura de gateway, hay dos modelos de implementación basados en la ubicación del AP:

Gateway mDNS central (puntos de acceso de modo local)

El WLC del Cisco Catalyst 9800 actúa como el gateway. Todo el tráfico mDNS se tuneliza CAPWAP al WLC, donde el WLC construye la memoria caché y hace proxy las respuestas.

AP mDNS de FlexConnect (gateway distribuido)

En las implementaciones de sucursales, donde los AP están en el modo de switching local de FlexConnect, el envío de tráfico mDNS de difusión/multidifusión a través de la WAN de vuelta al WLC es muy ineficiente. Al habilitar mDNS AP en Flex Profile, el punto de acceso ejecuta el motor de la puerta de enlace. El AP crea una memoria caché local de impresoras en el switch local de la sucursal y responde directamente a los clientes inalámbricos en la sucursal, manteniendo el tráfico mDNS completamente fuera del link WAN.

Conexión en puente

El WLC simplemente une los paquetes multicast a la red por cable/inalámbrica. Sólo es útil si los clientes y los servicios están en la misma VLAN.

Abandonar

Se descartan todos los paquetes mDNS. (Útil para redes de alta densidad en las que no se admite mDNS para ahorrar tiempo de transmisión).

Prácticas recomendadas de configuración

Es necesario comprobar las siguientes configuraciones obligatorias de la arquitectura:

- Validación del tráfico en el lado cableado: la puerta de enlace mDNS 9800 actúa como proxy. Si un cliente inalámbrico solicita una impresora cableada, el WLC debe reenviar esa consulta a la red cableada y recibir la respuesta. Debe confirmar que el tráfico mDNS está atravesando los trunks cableados al WLC. Si el switch ascendente descarta UDP 5353, la memoria caché del WLC permanece vacía.
- Mandato SVI: el módulo de gateway mDNS en el 9800 requiere una SVI (VLAN de interfaz) activa con una dirección IP para cada VLAN que necesita buscar (VLAN de cliente y de servicio). El WLC no puede rutear la memoria caché mDNS entre las VLANs sin que estas SVIs estén up/up.
- Difusión/multidifusión frente a unidifusión en directo: se recomienda minimizar la utilización del tiempo de transmisión. Mediante el uso de la puerta de enlace mDNS, el WLC responde a las consultas mDNS del cliente a través de Unicast, protegiendo el entorno de RF de la inundación excesiva de la multidifusión. No habilite el ruteo multicast global sólo para arreglar mDNS.
- Cuándo utilizar mDNS Bridging (Misma VLAN): Cuando el cliente inalámbrico, como un iPhone, y el proveedor de servicios (como un Apple TV o una impresora AirPrint) residen exactamente en la misma VLAN/subred.

Prácticas recomendadas y requisitos

Configuración por cable

Debe tener habilitado el routing multidifusión global y la detección IGMP en los switches por cable para que el tráfico multidifusión pueda llegar físicamente a otros dispositivos en esa VLAN.

- Configuración inalámbrica: en el WLC 9800, debe habilitar la multidifusión global y la difusión inalámbrica.
- Advertencia: El puente no se recomienda para subredes muy grandes (como redes empresariales /16 o /22). El tráfico de multidifusión se envía a la velocidad de datos básica más baja, que consume cantidades masivas de tiempo de conexión inalámbrica y CPU en el WLC. La conexión en puente sólo se debe utilizar en implementaciones pequeñas o en VLAN dedicadas aisladas.

Cuándo Utilizar el Gateway mDNS (Diferentes VLAN / Implementaciones Empresariales)

Cuando el cliente inalámbrico (como la VLAN de invitado o de empleado) y el proveedor de servicios (como la VLAN de impresoras o la VLAN de IoT) residen en distintas VLAN o subredes. Este es el modelo de implementación estándar para redes empresariales.

Requisito de SVI

El WLC 9800 debe tener una interfaz virtual conmutada (SVI) activa con una dirección IP para cada VLAN que necesita para indagar (por ejemplo, la interfaz vlan 10 para clientes, la interfaz vlan 20 para impresoras). El WLC utiliza esta IP para responder las consultas.

- Control de políticas: debe aplicar una política de servicio mDNS al perfil de políticas. Esto le permite definir exactamente qué servicios están permitidos para cruzar los límites de VLAN (por ejemplo, permitir Apple Airprint pero denegar Apple Time Capsula). Migrar la lista de servicios correctamente al no utilizar los conceptos de AireOS heredados ciegamente.
- Servicios específicos de ubicación (LSS): en una empresa grande que utilice la puerta de enlace, active siempre LSS. Esto garantiza que un usuario del edificio A solo ve las impresoras ubicadas físicamente en el edificio A, en lugar de ver todas las impresoras almacenadas en caché en toda la red global. Si la ubicación no se especifica en la directiva de servicio, se considera desde el gateway mDNS global. De forma predeterminada, la ubicación global del gateway mDNS se define como menos .
- Consulta activa: Habilite mdns-sd active-query. Esto permite que el WLC sondee periódicamente la red para los servicios en lugar de esperar estrictamente a que un dispositivo se anuncie.
- Implementaciones de sucursales con la misma VLAN (dependen del puente L2)

Recomendación de diseño

Si su implementación utiliza FlexConnect Local Switching y tanto los clientes inalámbricos como los servicios por cable (como impresoras o Apple TV) residen exactamente en la misma VLAN (dominio de difusión)

- Omitir por completo las funciones de la puerta de enlace mDNS basada en AP. Permita la conexión en puente de capa 2 nativa en el AP FlexConnect.
- Asegúrese de que la detección IGMP estándar y el reenvío multidifusión estén habilitados en el switch de sucursal local.

Garantía de configuración de multidifusión configurada en toda la red

Para garantizar que el reenvío de multidifusión y los anuncios de Bonjour/mDNS funcionen en las VLAN necesarias, verifique estas áreas de extremo a extremo:

1. Habilite mDNS Gateway globalmente en el WLC.
2. Cree y aplique una política mDNS en el perfil de política WLAN.
3. Agregue las definiciones de servicio necesarias (por ejemplo, Google Chromecast, AirPlay, impresoras, etc.) a la directiva.

4. Asegúrese de que las VLAN del cliente que participan en mDNS tengan interfaces o SVI alcanzables en la red.
5. Verifique el ruteo multicast/configuración PIM si el tráfico atraviesa los límites de la Capa 3.
6. Habilite la indagación IGMP en toda la infraestructura de switching que transporta las VLAN inalámbricas.
7. Confirme que la multidifusión no está bloqueada por las ACL, las reglas de firewall o las políticas de seguridad.
8. Asegúrese de que la configuración de aislamiento del cliente/par WLAN no bloquee el tráfico de detección de servicios requerido.
9. Verifique que los puertos de switch AP y los links troncales permitan las VLAN requeridas.
10. Confirme que la funcionalidad del solicitante existe en la VLAN si lo requiere el diseño de conmutación.

Escenarios comunes y remediaciones de campo

Escenario A: Fallos en el descubrimiento del servicio de VLAN cruzada (AirPrint / AirPlay)

Síntoma

Los clientes de la VLAN 10 no pueden ver las impresoras (AirPrint) en la VLAN 20.

Análisis de causa raíz

- Faltan SVIs: Como se mencionó anteriormente, el WLC carece de una SVI para VLAN 10 o VLAN 20.
- Configuración incorrecta de la política: la política mDNS aplicada al perfil de política del cliente solo permite la entrada (aprendizaje) pero no la salida (consulta).

Corrección

1. Asegúrese de que la interfaz vlan X exista en el WLC con una IP válida y que esté activa/activa.
2. Verifique que la política mDNS tenga permitidas las direcciones IN y OUT para los servicios requeridos (apple-airplay, apple-airprint).

Situación B: Fallos de mDNS de switching local de FlexConnect

Síntoma

Los AP en modo FlexConnect descartan el tráfico mDNS o no aplican los servicios específicos de ubicación (LSS).

Corrección

1. Vaya a Configuration > Tags and Profiles > Flex.
2. En el perfil Flex, asegúrese de que la ficha mDNS esté configurada para habilitar el AP mDNS (si se realiza una gateway distribuida).
3. Nota en LSS: Si se habilita Location Specific Services (LSS), el WLC filtra los servicios en función de la ubicación física (etiqueta MAC/Site) del AP. Si una impresora está en un switch con cable lejos del AP, LSS puede filtrarlo. Intente deshabilitar temporalmente LSS en el perfil mDNS para aislar el problema.

Situación C: CPU alta, MSG_Queue lleno o degradación de la red

Síntoma

Los registros de WLC muestran que MSG_Queue se llena, CPU alta en los procesos de ruta de datos, o pérdida completa de las capacidades mDNS periódicamente.

Solución y aislamiento (bloqueo de mDNS)

Si un loop multicast o una charla excesiva de Bonjour está derribando el WLC, usted podría necesitar bloquear temporalmente mDNS para la estabilidad:

Para bloquear mDNS de forma centralizada, cree una ACL IPv4 que rechace UDP 5353 y aplíquelo al perfil de política inalámbrica del lado del cliente, o inhabilite mDNS completamente en Configuration > Services > mDNS.

1. Desactivar el puente mDNS: Desactivar el puente mDNS global y la difusión inalámbrica en subredes grandes. Confíe estrictamente en la puerta de enlace mDNS.
2. Audite los switches cableados para asegurarse de que la indagación IGMP esté habilitada para evitar la inundación mDNS en los trunks cableados conectados al WLC.

Situación Chromecast detectado a través de mDNS pero falló la conversión ("sin conexión a Internet")

Síntoma

Los dispositivos Chromecast de Google podrían unirse con éxito a la WLAN y ser descubiertos por los clientes a través de mDNS. Sin embargo, cuando los usuarios intentaron convertir medios, la conversión falló con el mensaje de error: "No tiene conexión a Internet, compruebe la conexión a Internet."

Corrección

Activar bloqueo P2P: Activación del bloqueo P2P (punto a punto) de WLAN (a menudo configurado como Forward-UpStream para forzar el tráfico cliente a cliente a través del gateway en lugar de descartarlo en el AP).

Situación E: Audio entrecortado en transmisiones de voz / tráfico multidifusión descartado

Síntoma

Las insignias de Vocera experimentan audio entrecortado durante las llamadas de difusión, o las transmisiones IPTV se pixelan fuertemente.

Causa raíz

Si Multicast-Direct está habilitado globalmente pero el flujo multicast específico (como la dirección Vocera 239.x.x.x) no está permitido explícitamente bajo la configuración de flujo de medios, o si la radio AP está configurada para descartar flujos cuando el ancho de banda está lleno (Control de admisión).

Corrección

1. Control de admisión: compruebe las configuraciones de radio de 5 GHz y 2,4 GHz para ver si hay transmisión multimedia. Si observa una caída de violación, el WLC descarta el flujo multicast si la utilización del canal RF es demasiado alta.
 - Cambie la violación a fallback: `ap dot11 5ghz media-stream multicast-direct admission-besteffort` (esto le permite volver a multicast estándar si el ancho de banda de conversión de unidifusión no está disponible).
2. Configuración de flujo: defina explícitamente el rango de IP multicast que necesita conversión: `wireless media-stream group <Stream_Name> <Start_IP> <End_IP>`

Completos pasos de registro y diagnóstico

Al resolver problemas, siga este orden de operaciones para aislar dónde se produce la interrupción (Cliente -> AP -> WLC -> Servidor).

Fase 1: Comprobaciones de verificación de CLI

¿Se habilita mDNS globalmente?

```
show mdns-sd summary
```

¿El WLC ha aprendido el servicio? (Busque la impresora/TV MAC o IP)

```
show mdns-sd cache
```

```
show mdns-sd cache detail
```

¿Las consultas están golpeando el WLC y siendo descartadas?

```
show mdns-sd statistics
```

¿Se estableció el plano de control de multidifusión #ls entre el WLC y el AP?

```
show ap multicast Mom
```

Verificar la política aplicada al cliente

```
show wireless profile policy all | inc mDNS
```

Fase 2: Mecanismos de seguimiento y depuración

Seguimiento radioactivo (comience siempre aquí): Ejecute un seguimiento de RA contra la dirección MAC del cliente Y el proveedor de servicios.

- debug wireless mac <Client_MAC> internal
- debug wireless mac <Printer_MAC> internal (muestra si la ruta de datos WLC está

descartando intencionadamente el paquete UDP 5353 debido a una política o a un filtrado LSS).

- Set platform software trace wncd <0-7> chassis active R0 mdns debug

Para obtener los registros, muestre el registro:

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

Fase 3: Captura de paquetes integrada (EPC)

Para probar definitivamente si los paquetes están alcanzando el WLC del lado cableado o están dejando el WLC sobre el aire:

1. Vaya a Troubleshooting > Packet Capture en la GUI del 9800.
2. Configure un EPC en el link ascendente WLC (Te0/0/0 o Port-Channel) para validar la infraestructura cableada.
3. Configure un EPC en las SVI específicas para validar el routing inalámbrico.
4. Cree una ACL IPv4 dirigida al puerto UDP 5353.
5. Exportar el PCAP a Wireshark y filtrar por udp.port == 5353 | mdns.

Análisis

Verifique que el WLC reciba la consulta del cliente, la rutee y envíe una respuesta Unicast al cliente que contenga los detalles de la impresora/Apple TV.

Información de referencia y documentación oficial

- [Comprensión de mDNS en Catalyst 9800 WLC](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).