



## **Cisco DNA Service for Bonjour Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9200 Switches)**

**First Published:** 2021-06-21

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

<b>CHAPTER 1</b>	<b>Cisco DNA Service for Bonjour Solution Overview</b>	<b>1</b>
	About Cisco DNA Service for Bonjour Solution	1
	Solution Components	2
	Supported Platforms	3
	Supported Network Design	4
	Traditional Wired and Wireless Networks	4
	Wired Networks	5
	Wireless Networks	6
	Cisco SD-Access Wired and Wireless Networks	8
	Fabric-Enabled Wired and Wireless Networks	8
	Fabric-Enabled Policy Extended Node	10
	BGP EVPN Networks	11
<b>CHAPTER 2</b>	<b>Configuring Local Area Bonjour in Multicast DNS Mode for LAN and Wireless Networks</b>	<b>13</b>
	How to configure Multicast DNS Mode for LAN and Wired Networks	13
	Enabling mDNS Gateway on the Device	13
	Creating Custom Service Definition	14
	Creating Service List	15
	Creating Service Policy	16
	Associating Service Policy to an Interface	17
	How to Configure Local Area Bonjour in Multicast DNS Mode for Wireless Networks	19
	Enabling mDNS Gateway on the Device	20
	Creating Custom Service Definition	22
	Creating Service List	22
	Creating Service Policy	24
	Verifying Local Area Bonjour in Multicast DNS Mode for LAN and Wireless Networks	24

Verifying SDG-Agent Status 24

Verifying Wide Area Bonjour Controller Status 26

Verifying Local Area Bonjour Configuration for LAN and Wireless Networks 27

---

**CHAPTER 3**

**Configuring VRF-Aware Local Area Bonjour Services 29**

Prerequisites for VRF-Aware Local Area Bonjour Services 29

Restrictions for VRF-Aware Local Area Bonjour Services 30

Information about VRF-Aware Local Area Bonjour Services 30

    Gateway Modes for VRF-Aware Bonjour Services 31

Understanding VRF-Aware Wide Area Bonjour Services 32

Understanding VRF-Aware Service on Multilayered Wired and Wireless Networks 33

How to configure Intra-Virtual Network Proxy Service on Local Area Bonjour Domain 35

How to configure Inter-Virtual Network Proxy Service on Local Area Bonjour Domain 36

    Configuring Inter-Virtual Network Location-Filter 37

Verifying VRF-Aware Local Area Bonjour Services 39

---

**CHAPTER 4**

**Feature History for Cisco DNA Service for Bonjour 43**

Feature History for Cisco DNA Service for Bonjour 43



## CHAPTER 1

# Cisco DNA Service for Bonjour Solution Overview

---

- [About Cisco DNA Service for Bonjour Solution, on page 1](#)
- [Solution Components, on page 2](#)
- [Supported Platforms, on page 3](#)
- [Supported Network Design, on page 4](#)

## About Cisco DNA Service for Bonjour Solution

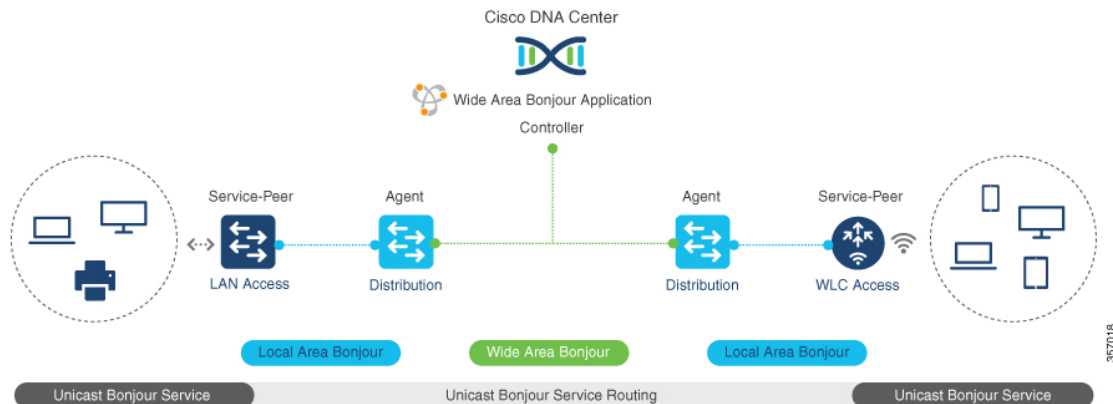
The Apple Bonjour protocol is a zero-configuration solution that simplifies network configuration and enables communication between connected devices, services, and applications. Using Bonjour, you can discover and use shared services with minimal intervention and configuration. Bonjour is designed for single Layer 2 domains that are ideal for small, flat, single-domain setups, such as home networks. The Cisco DNA Service for Bonjour solution eliminates the single Layer 2 domain constraint and expands the scope to enterprise-grade traditional wired and wireless networks, including overlay networks such as Cisco Software-Defined Access (SD-Access) and industry-standard BGP EVPN with VXLAN. The Cisco Catalyst 9000 series LAN switches and wireless LAN controllers follow the industry standard, RFC 6762-based multicast DNS (mDNS) specification to support interoperability with various compatible wired and wireless consumer products in enterprise networks.

The Cisco Wide Area Bonjour application is a software-defined, controller-based solution that enables devices to advertise and discover Bonjour services across Layer 2 domains, making these services applicable to a wide variety of wired and wireless enterprise networks. The Cisco Wide Area Bonjour application also addresses problems relating to security, policy enforcement, and services administration on a large scale. The new distributed architecture is designed to eliminate mDNS flood boundaries and transition to unicast-based service routing, providing policy enforcement points and enabling the management of Bonjour services. With the Cisco Wide Area Bonjour application, you can seamlessly introduce new services into the existing enterprise environment without modifying the existing network design or configuration.

The enhanced intuitive GUI provides you with centralized access control and monitoring capabilities, combined with the scalability and performance required for large-scale Bonjour services deployments for various supporting enterprise network types.

The following figure illustrates how the Cisco Wide Area Bonjour application operates across two integrated domain networks with end-to-end unicast-based service routing.

Figure 1: Cisco Wide Area Bonjour Solution



- Local-Area Service Discovery Gateway Domain - Multicast DNS Mode:** The classic Layer 2 multicast flood-n-learn-based deployment model. The service provider and receiver can discover and browse within the common VLAN or broadcast domain without any security and location-based policy enforcement. The Cisco Catalyst switches at the Layer 3 boundary function as the Service Discovery Gateway (SDG) to discover and distribute services between local wired or wireless VLANs based on applied policies. The inter-VLAN service routing at a single gateway is known as Local Area Bonjour.
- Local Area Service Discovery Gateway Domain - Unicast Mode:** The new enhanced Layer 2 unicast policy-based deployment model. The new mDNS service discovery and distribution using Layer 2 unicast address enables flood-free LAN and wireless networks. Cisco Catalyst switches and Cisco Catalyst 9800 series wireless LAN controllers in Layer 2 mode introduce a new service-peer role, replacing classic flood-n-learn, for new unicast-based service routing support in the network. The service-peer switch and wireless LAN controller also replace mDNS flood-n-learn with unicast-based communication with any RFC 6762 mDNS-compatible wired and wireless endpoints.
- Wide-Area Service Discovery Gateway Domain:** The Wide Area Bonjour domain is a controller-based solution. The Bonjour gateway role and responsibilities of Cisco Catalyst switches are extended from a single SDG switch to an SDG agent, enabling Wide Area Bonjour service routing beyond a single IP gateway. The network-wide distributed SDG agent devices establish a lightweight, stateful, and reliable communication channel with a centralized Cisco DNA Center controller running the Cisco Wide Area Bonjour application. Service routing between the SDG agents and the controller operates over regular IP networks using TCP port 9991. The SDG agents route locally discovered services based on the export policy.

## Solution Components

The Cisco DNA Service for Bonjour solution is an end-to-end solution that includes the following key components and system roles to enable unicast-based service routing across the local area and Wide Area Bonjour domain:

- Cisco Service peer:** A Cisco Catalyst switch and Catalyst Wireless LAN Controller (WLC) in Layer 2 access function in service peer mode to support unicast-based communication with local attached endpoints and export service information to the upstream Cisco SDG agent in the distribution layer.

- **Cisco SDG agent:** A Cisco Catalyst switch functions as an SDG agent and communicates with the Bonjour service endpoints in Layer 3 access mode. At the distribution layer, the SDG agent aggregates information from the downstream Cisco service peer switch and WLC, and exports information to the central Cisco DNA controller.
- **Cisco DNA controller:** The Cisco DNA controller builds the Wide Area Bonjour domain with network-wide and distributed trusted SDG agents using a secure communication channel for centralized services management and controlled service routing.
- **Endpoints:** A Bonjour endpoint is any device that advertises or queries Bonjour services conforming to RFC 6762. The Bonjour endpoints can be in either LANs or WLANs. The Cisco Wide Area Bonjour application is designed to integrate with RFC 6762-compliant Bonjour services, including AirPlay, Google Chrome cast, AirPrint, and so on.

## Supported Platforms

The following table lists the supported controllers, along with the supported hardware and software versions.

**Table 1: Supported Controllers with Supported Hardware and Software Versions**

Supported Controller	Hardware	Software Version
Cisco DNA Center appliance	DN2-HW-APL DN2-HW-APL-L DN2-HW-APL-XL	Cisco DNA Center, Release 2.2.3
Cisco Wide Area Bonjour application	—	2.4.264.12003

The following table lists the supported SDG agents along with their license and software requirements.

**Table 2: Supported SDG Agents with Supported License and Software Requirements**

Supported Platform	Supported Role	Local Area SDG	Wide Area SDG	Minimum Software
Cisco Catalyst 9200 Series Switches	SDG	Cisco DNA Advantage	Unsupported	Cisco IOS XE Bengaluru 17.6.1
Cisco Catalyst 9200L Series Switches	—	Unsupported	Unsupported	—
Cisco Catalyst 9300 Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.1
Cisco Catalyst 9400 Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.1
Cisco Catalyst 9500 Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.1

Supported Platform	Supported Role	Local Area SDG	Wide Area SDG	Minimum Software
Cisco Catalyst 9500 High Performance Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.1
Cisco Catalyst 9600 Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.1
Cisco Catalyst 9800 WLC	Service peer	Cisco DNA Advantage	Unsupported	Cisco IOS XE Bengaluru 17.6.1
Cisco Catalyst 9800-L WLC	Service peer	Cisco DNA Advantage	Unsupported	Cisco IOS XE Bengaluru 17.6.1

## Supported Network Design

The Cisco DNA Service for Bonjour supports a broad range of enterprise-grade networks. The end-to-end unicast-based Bonjour service routing is supported on traditional, Cisco SD-Access, and BGP EVPN-enabled wired and wireless networks.

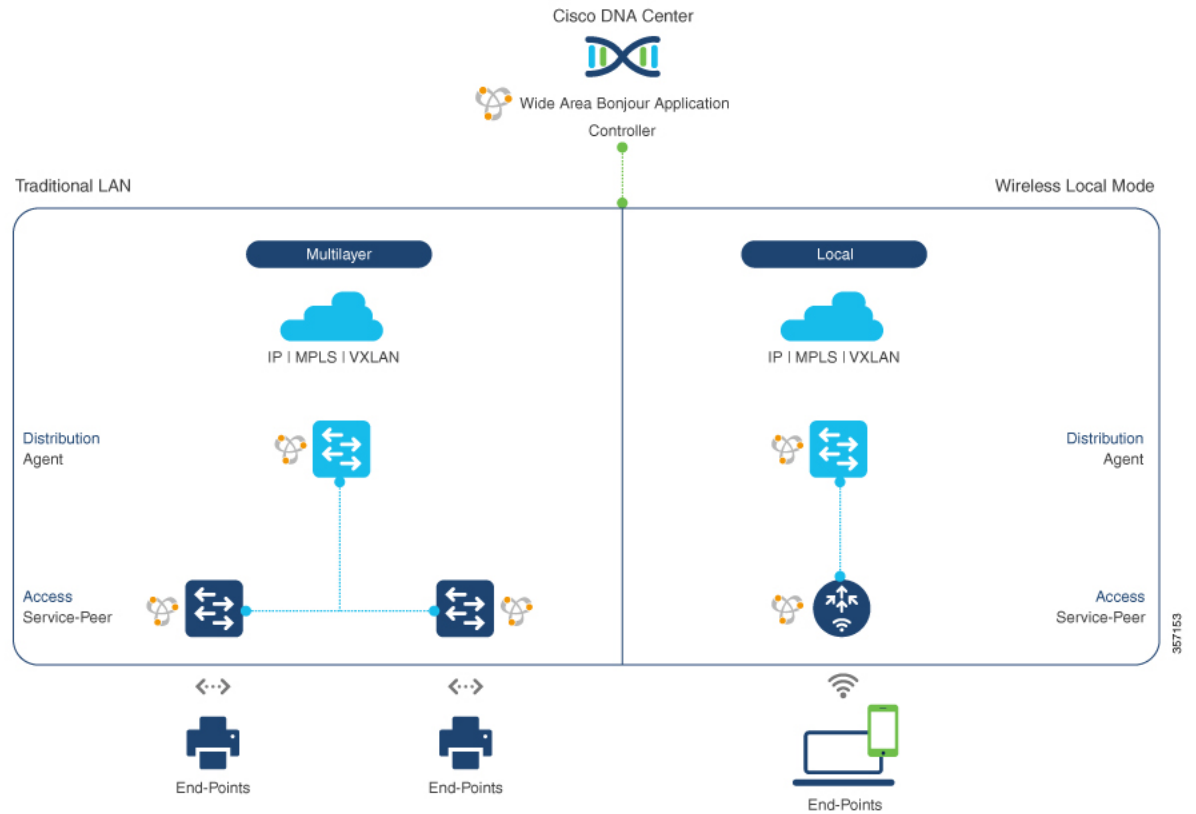
### Traditional Wired and Wireless Networks

Traditional networks are classic wired and wireless modes deployed in enterprise networks. Cisco DNA Service for Bonjour supports a broad range of network designs to enable end-to-end service routing.

The following figure illustrates traditional LAN network designs that are commonly deployed in an enterprise.



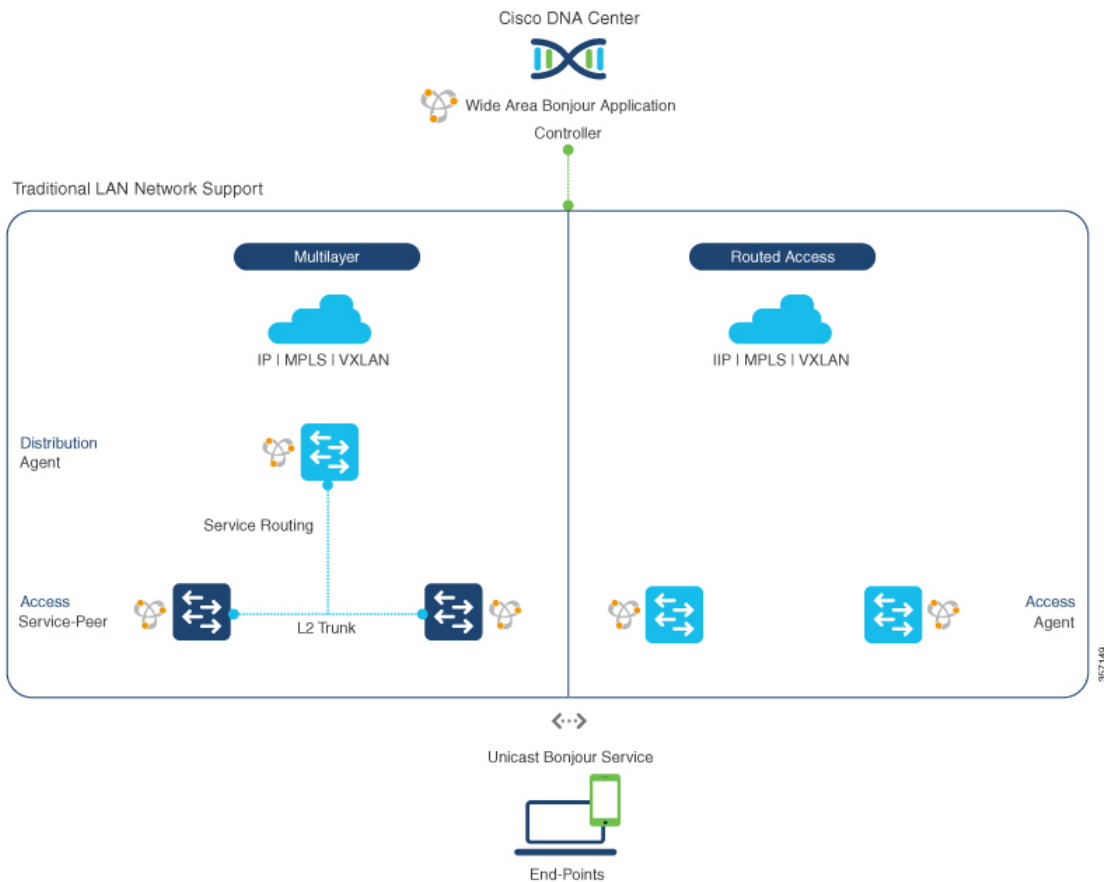
Figure 2: Enterprise Traditional LAN Network Design



## Wired Networks

The following figure shows the supported LAN network designs that are commonly deployed in an enterprise.

Figure 3: Enterprise Multilayer and Routed Access Network Design



The SDG agent that provides Bonjour gateway functions is typically an IP gateway for wired endpoints that could reside in the distribution layer in multilayer network designs, or in the access layer in routed access network designs:

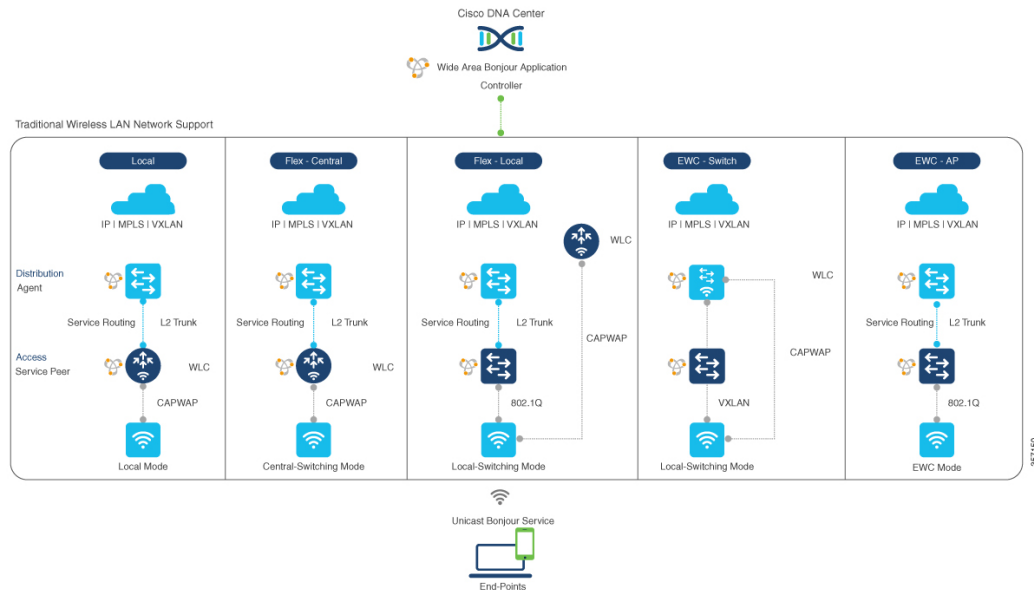
- **Multilayer LAN:** In this deployment mode, the Layer 2 access switch provides the first-hop Bonjour gateway function to locally attached wired endpoints. The Bonjour services and global discovery request are routed to the distribution layer systems that act as the IP gateway or SDG agent. There's no additional configuration or new requirement to modify the existing Layer 2 trunk settings between the access and distribution layers of the Cisco Catalyst switches. The policy-based service routing between the Layer 2 service-peer switches is performed by the SDG agent. The policy-based service routing between the SDG agents is performed by the Cisco DNA Center controller.
- **Routed Access:** In this deployment mode, the first-hop switch is an IP gateway boundary and, therefore, it must also perform the SDG agent role. The policy-based service routing between the SDG agents is performed by the Cisco DNA Center controller.

## Wireless Networks

The Cisco DNA Service for Bonjour also supports various wireless LAN network designs that are commonly deployed in an enterprise. The Cisco Catalyst 9800 Series Wireless LAN Controller (WLC) can be deployed in a service-peer role supporting the mDNS gateway and paired with an upstream gateway switch for end-to-end service routing.

The following figure shows the supported wireless LAN network designs that are commonly deployed in an enterprise.

**Figure 4: Enterprise Traditional Wireless LAN Network Design**



The Cisco DNA Service for Bonjour supports the following modes for wireless LAN networks:

- Local Mode:** In this central switching wireless deployment mode, the Bonjour traffic is encapsulated within the CAPWAP tunnel from the Cisco access points to the centrally deployed Cisco Wireless LAN Controller. The Cisco access points are configured to be in local mode (central switching also allows the access point to be configured in FlexConnect mode). With central switching, the Cisco Catalyst 9800 Series Wireless LAN Controller provides the mDNS gateway function of Bonjour services in the service-peer role. The WLC can discover and distribute services to local wireless users and perform unicast service routing over a wireless management interface to the Cisco Catalyst switch in the distribution layer, which acts as the IP gateway and the SDG agent. There's no additional configuration or requirement to modify the existing Layer 2 trunk settings between the Cisco Wireless LAN Controller and the distribution layer of the Cisco Catalyst switch. The Cisco Wireless LAN Controller must be configured with Global Multicast and AP Multicast in Multicast mode. Unless the access point joins the wireless LAN controller-announced multicast group, communication to and from Bonjour endpoints is not enabled for the wireless user group.
- FlexConnect:** In FlexConnect local switching mode, both wired and wireless users share the same gateway in the access layer. The Layer 2 access switch provides the policy-based mDNS gateway function to locally attached wired and wireless users. The Cisco Catalyst switches in the distribution layer function as SDG agents for the LAN and wireless LAN user groups.
- Embedded Wireless Controller - Switch:** The Cisco Embedded Wireless Controller solution enables the lightweight integrated wireless LAN controller function within the Cisco Catalyst 9300 series switch. The Cisco Catalyst switches in the distribution layer function as SDG agents to the LAN and wireless LAN user groups. The SDG agent in the distribution layer provides unicast service routing across all wireless access point and Layer 2 service-peer switches without any mDNS flooding. The embedded Cisco Wireless LAN Controller switch must be configured with Global Multicast and AP Multicast in Multicast mode and mDNS must be set in bridging mode.

- **Embedded Wireless Controller - Access Point:** The Cisco Embedded Wireless Controller solution enables the lightweight integrated wireless LAN controller function within the Cisco access points configured in the primary role. The wireless users share the same Bonjour gateway in the access layer as the wired endpoints. The Cisco Catalyst switches in the access layer function as service peers to the LAN and wireless LAN user groups. The SDG agent in the distribution layer provides unicast service routing across all Layer 2 service-peer switches in the Layer 2 network block without any mDNS flooding. AP multicast is required for Embedded Wireless mode AP, and mDNS must be set in bridging mode.



---

**Note** The Cisco AireOS-based WLC can be deployed as an mDNS pass-through network device between the wireless endpoints. The upstream SDG agent provides consistent Bonjour gateway functions for wireless endpoints, as for wired networks. In general, the IP gateway of wireless clients is also a Bonjour gateway. However, the placement of the SDG agent may vary depending on the wireless LAN deployment mode.

---

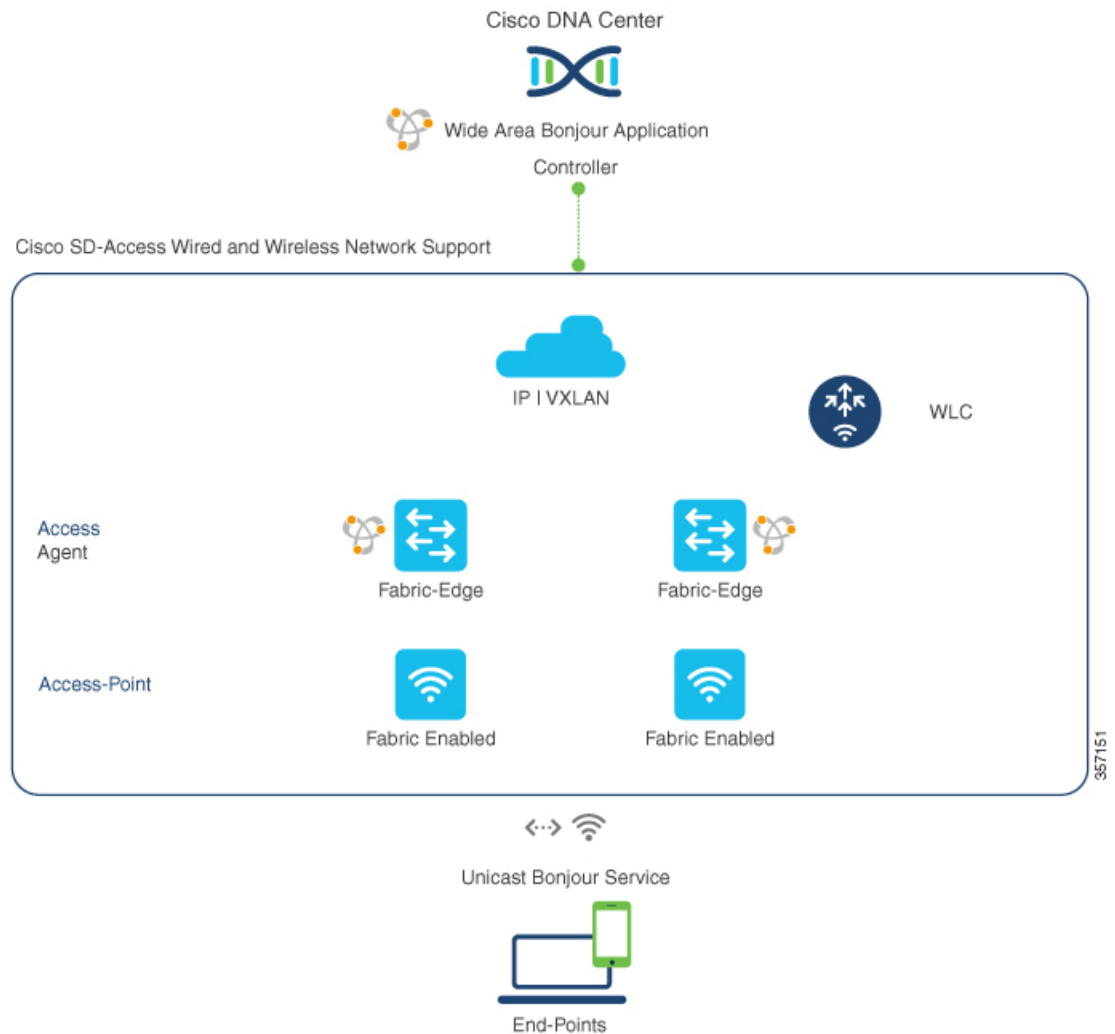
## Cisco SD-Access Wired and Wireless Networks

Cisco SD-Access-enabled wired and wireless networks support Cisco DNA Service for Bonjour. From Cisco IOS-XE Release 17.4.1, the VRF-aware Wide Area Bonjour service routing provides secure and segmented mDNS service discovery and distribution management for fabric-enabled wired and wireless networks. The VRF-aware Wide Area Bonjour service routing eliminates the need for Layer 2 flooding. The Layer 3 Fabric Edge switch in the access layer must be configured as the SDG agent and paired with the central Cisco DNA Center for end-to-end service routing. Wide Area Bonjour policies must be aligned with the SD-Access network policies for virtual networks and SGT policies, if any.

### Fabric-Enabled Wired and Wireless Networks

The following figure shows Cisco SD-Access-enabled wired and wireless networks without extending the Layer 2 network boundaries.

Figure 5: Cisco SD-Access Network Design



The Cisco DNA Service for Bonjour for SD-Access-enabled wired and wireless networks uses two logical components:

- **SDG agent:** The Layer 3 Fabric Edge switch in the access layer network is configured as the SDG agent. The VRF-aware mDNS gateway and Wide Area Bonjour service routing configuration is added only after SD-Access is configured.
- **Cisco DNA controller:** The Cisco Wide Area Bonjour application on Cisco DNA Center acts as the controller that supports policy and location-based service discovery and distribution between network-wide distributed Fabric Edge switches.

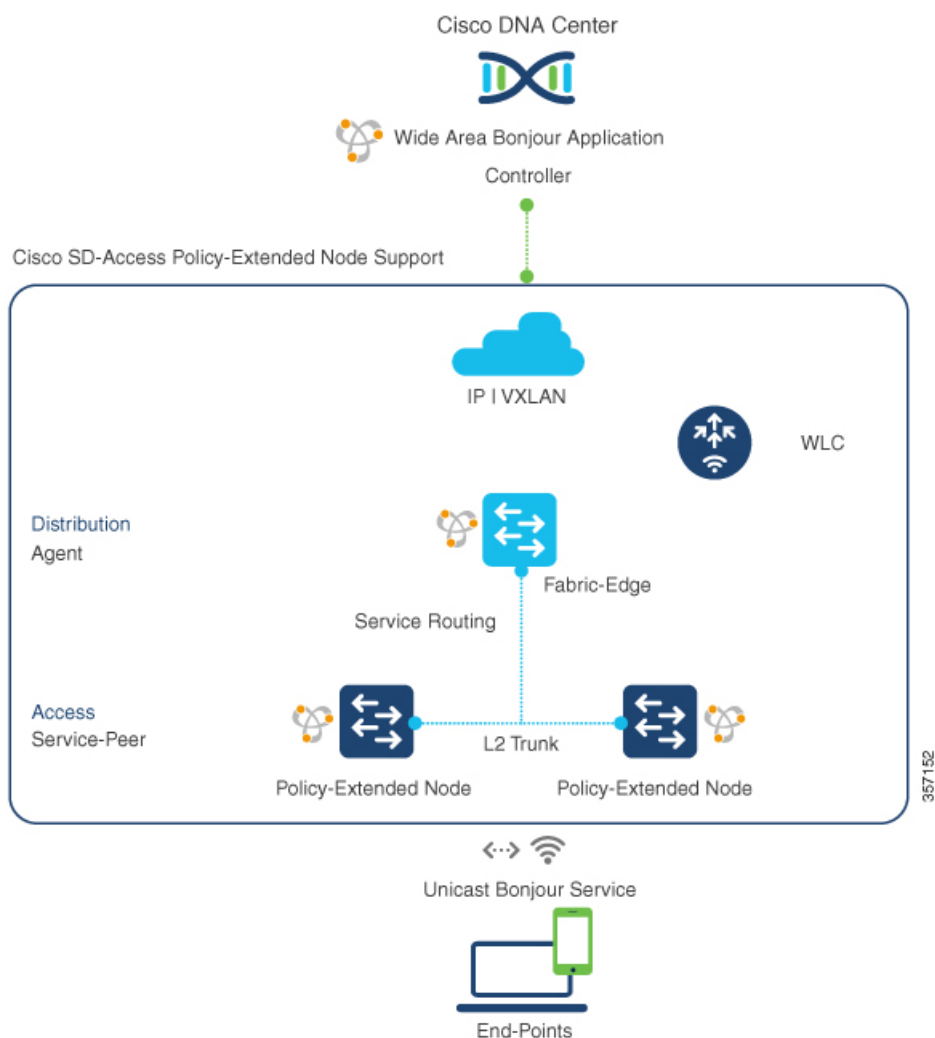
The Wide Area Bonjour communication between the SDG agent and the controller takes place through the network underlay. The SDG agent forwards the endpoint announcements or queries to the controller through the fabric underlay based on policies. After discovering a service, a Bonjour-enabled application establishes direct unicast communication between endpoints through the fabric overlay. This communication is subject to configured overlay IP routing and SGT policies, if any.

The Cisco Wireless LAN Controller must be configured with Global Multicast and AP Multicast in Multicast mode. The network administrator must enable IP Multicast in the underlay and ensure all fabric-enabled Cisco wireless access points have successfully joined the multicast group. The mDNS snooping configuration on the Cisco Wireless LAN Controller is ineffective and must remain in disabled mode.

## Fabric-Enabled Policy Extended Node

The security policy can be extended to Cisco Catalyst 9000 Series Switches at Layer 2 access with the Policy Extended Node (PEN) function in a Cisco SD-Access fabric network. The network security and mDNS service policy can be combined at the Layer 2 access PEN switch in a service-peer role combined with Fabric Edge supporting SDG agent mode in Layer 2/3 distribution layer for Wide Area Bonjour service routing with Cisco DNA Center.

**Figure 6: Fabric-Enabled Policy Extended Node**

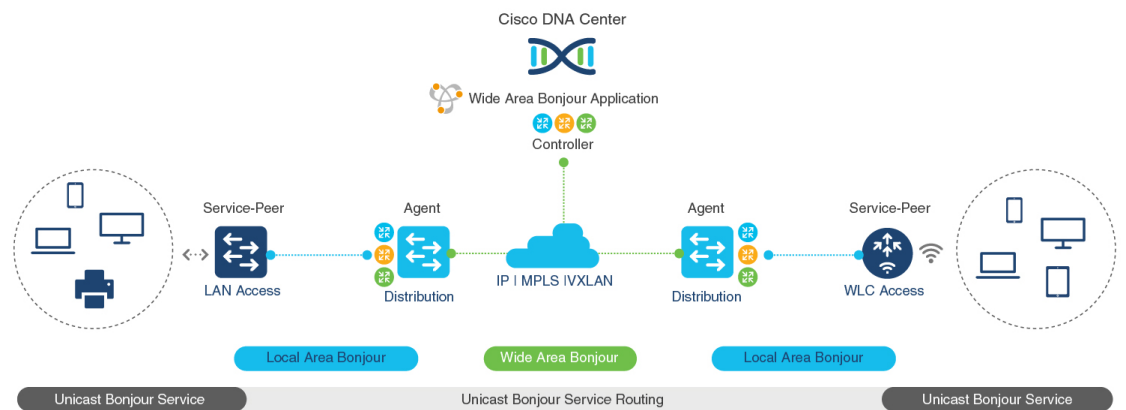


## BGP EVPN Networks

The BGP EVPN-based enterprise network provides a flexible Layer 3 segmentation and Layer 2 extension overlay network. From Cisco IOS-XE Release 17.4.1, the VRF-aware Wide Area Bonjour service routing provides secure and segmented mDNS service discovery and distribution management for all common VXLAN overlay deployment models. The VRF-aware Wide Area Bonjour service routing eliminates mDNS flooding over Layer 2 extended EVPN VXLAN networks (symmetric and asymmetric integrated routing and bridging (IRB)) and service reachability challenges for Layer 3 segmented EVPN VXLAN networks in the fabric.

The following figure shows the BGP EVPN leaf switch in Layer 3 access mode, supporting overlay Bonjour service routing for a BGP EVPN-enabled wired and wireless enterprise network over various types of Layer 2 networks and Layer 3 segmented VRF-enabled networks.

**Figure 7: Overlay Bonjour Service for a BGP EVPN-Enabled Enterprise Network**

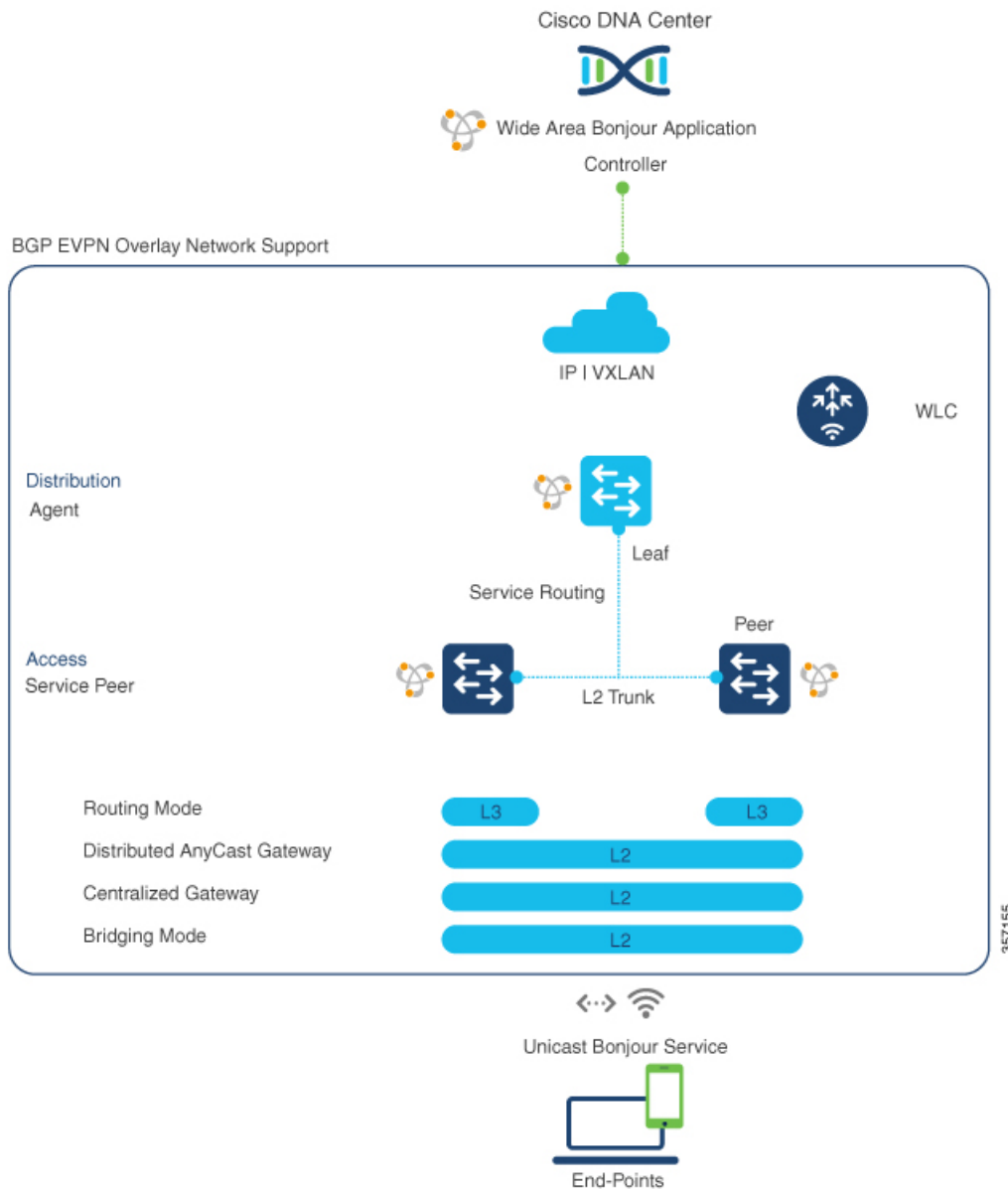


Cisco DNA Service for Bonjour supports Wide Area Bonjour service routing for BGP EVPN networks extended with Layer 2 service-peer network devices, such as a Cisco Catalyst switch or 9800 series WLC. The BGP EVPN leaf device in the distribution layer supports the SDG agent role for overlay service routing.

The Cisco DNA Service for Bonjour solution for BGP EVPN networks enables policy-based end-to-end service routing for virtual network environments. The solution helps to protect enterprise network scale and performance by eliminating the Layer 2 mDNS flood over the VXLAN across the IP core network.

The following figure shows mDNS endpoints connecting the Layer 2 access switch in service-peer mode to the upstream BGP EVPN leaf switch in the Layer 2/3 distribution layer supporting overlay Bonjour service routing for a BGP EVPN-enabled wired and wireless enterprise network over various types of Layer 2 networks and Layer 3 segmented VRF-enabled networks.

Figure 8: mDNS Endpoints Connecting an L2 Switch to an Upstream BGP EVPN Leaf Switch



For more information about BGP EVPN networks, see [Cisco DNA Service for Bonjour Configuration Guide, Cisco IOS XE Bengaluru 17.6.x \(Catalyst 9600 Switches\)](#).





## CHAPTER 2

# Configuring Local Area Bonjour in Multicast DNS Mode for LAN and Wireless Networks

- [How to configure Multicast DNS Mode for LAN and Wired Networks, on page 13](#)
- [How to Configure Local Area Bonjour in Multicast DNS Mode for Wireless Networks , on page 19](#)
- [Verifying Local Area Bonjour in Multicast DNS Mode for LAN and Wireless Networks, on page 24](#)

## How to configure Multicast DNS Mode for LAN and Wired Networks

This section provides information about how to configure Local Area Bonjour in multicast DNS mode.

### Enabling mDNS Gateway on the Device

To configure mDNS on the device, follow these steps:

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <code>enable</code>	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>mdns-sd gateway</b> <b>Example:</b> Device(config)# <code>mdns-sd gateway</code>	Enables mDNS on the device and enters mDNS gateway configuration mode. Enter the following commands in mDNS gateway configuration mode to enable the respective functionalities:

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <b>air-print-helper</b>: Enables IOS devices like iPADs to discover and use older printers that support Bonjour</li> <li>• <b>cache-memory-max</b>: Configures the percentage memory for cache</li> <li>• <b>ingress-client</b>: Configures Ingress Client Packet Tuners</li> <li>• <b>rate-limit</b>: Enables rate limiting of incoming mDNS packets</li> <li>• <b>service-announcement-count</b>: Configures maximum service advertisement count</li> <li>• <b>service-announcement-timer</b>: Configures advertisements announce timer periodicity</li> <li>• <b>service-query-count</b>: Configures maximum query count</li> <li>• <b>service-query-timer</b>: Configures query forward timer periodicity</li> </ul> <p><b>Note</b> For <b>cache-memory-max</b>, <b>ingress-client</b>, <b>rate-limit</b>, <b>service-announcement-count</b>, <b>service-announcement-timer</b>, <b>service-query-count</b>, and <b>service-query-timer</b> commands, you can retain the default value of the respective parameter for general deployments. Configure a different value, if required, for a specific deployment.</p>
<b>Step 4</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Device(config-mdns-sd)# exit</pre>	Exits mDNS gateway configuration mode.

## Creating Custom Service Definition

Service definition is a construct that provides an admin friendly name to one or more mDNS service types or PTR Resource Record Name. By default, a few built-in service definitions are already predefined and available for admin to use. In addition to built-in service definitions, admin can also define custom service definitions.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>mdns-sd service-definition</b> <i>service-definition-name</i> <b>Example:</b> Device(config)# <b>mdns-sd</b> <b>service-definition CUSTOM1</b>	Configures mDNS service definition. <b>Note</b> All the created custom service definitions are added to the primary service list. Primary service list comprises of a list of custom and built-in service definitions.
<b>Step 4</b>	<b>service-type</b> <i>string</i> <b>Example:</b> Device(config-mdns-ser-def)# <b>service-type</b> <b>_custom1._tcp.local</b>	Configures mDNS service type.
<b>Step 5</b>	Repeat step 4 to configure more than one service type in the custom service definition.	
<b>Step 6</b>	<b>exit</b> <b>Example:</b> Device(config-mdns-ser-def)# <b>exit</b>	Exit mDNS service definition configuration mode.

## Creating Service List

mDNS service list is a collection of service definitions. To create a service list, follow these steps:

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<b>mdns-sd service-list</b> <i>service-list-name</i> {in   out}  <b>Example:</b> Device(config)# <b>mdns-sd service-list</b> <b>VLAN100-list in</b>	Configures mDNS service list.
Step 4	<b>match</b> <i>service-definition-name</i> [message-type {any   announcement   query}]  <b>Example:</b> Device(config-mdns-sl-in)# <b>match</b> <b>PRINTER-IPPS message-type announcement</b>	Matches the service to the message type. Here, <i>service-definition-name</i> refers to the names of services, such as, airplay, airserver, airtunes, and so on.  <b>Note</b> To add a service, the service name must be part of the primary service list.  If the mDNS service list is set to IN, the applicable command syntax is: <b>match</b> <i>service-definition-name</i> [message-type {any   announcement   query}].  If the mDNS service list is set to OUT, the applicable command syntax is: <b>match</b> <i>service-definition-name</i> [message-type {any   announcement   query}] [location-filter <i>location-filter-name</i> ] [source-interface {mDNS-VLAN-number   mDNS-VLAN-range}].
Step 5	<b>exit</b>  <b>Example:</b> Device(config-mdns-sl-in)# <b>exit</b>	Exits mDNS service list configuration mode.

## Creating Service Policy

A Service Policy that is applied to an interface specifies the allowed Bonjour service announcements or the queries of specific service types that should be processed, in ingress direction or egress direction or both. For this, the service policy specifies two service-lists, one each for ingress and egress directions. In the Local Area Bonjour domain, the same service policy can be attached to one or more Bonjour client VLANs; however, different VLANs may have different service policies.

To configure service policy with service lists, follow these steps:

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>mdns-sd service-policy <i>service-policy-name</i></b> <b>Example:</b> Device(config)# <b>mdns-sd service-policy mdns-policy1</b>	Configures mDNS service policy.
<b>Step 4</b>	<b>service-list <i>service-list-name</i> {in   out}</b> <b>Example:</b> Device(config-mdns-ser-pol)# <b>service-list VLAN100-list in</b> Device(config-mdns-ser-pol)# <b>service-list VLAN300-list out</b>	Configures service lists for IN and OUT directions.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> Device(config-mdns-ser-pol)# <b>exit</b>	Exits mDNS service policy configuration mode.

## Associating Service Policy to an Interface

To configure mDNS on the device, follow these steps:

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-name</i></b> <b>Example:</b> Device(config)# <b>interface Vlan 601</b>	Enters interface mDNS configuration mode and enables interface configuration.

	Command or Action	Purpose
Step 4	<p><b>mdns-sd gateway</b></p> <p><b>Example:</b></p> <pre>Device(config-if)# mdns-sd gateway</pre>	<p>Configures mDNS gateway on the interface.</p> <p>Enter the following commands in the interface mDNS gateway configuration mode to enable the respective functionalities:</p> <ul style="list-style-type: none"> <li>• <b>active-query</b>: Sets the time interval for SDG agent to refresh the active status of connected Bonjour client services. The timer value ranges from 60 to 3600 seconds.</li> </ul> <p><b>Note</b> This configuration is mandatory only on VLANs whose Bonjour policy is configured to accept Bonjour service announcements from connected Bonjour clients. If the VLAN is configured to only accept Bonjour queries but not Bonjour service announcements, this configuration is optional.</p> <ul style="list-style-type: none"> <li>• <b>service-instance-suffix</b>(Optional) : Appends the service instance suffix to any announced service name that is forwarded to the controller.</li> <li>• <b>service-mdns-query [ ptr   all ]</b>: Configures mDNS query request message processing for the specified query types.</li> </ul> <p>If the <b>service-mdns-query</b> command is used without any keyword, then all Bonjour query types (PTR, SRV, and TXT) are processed by default. It is recommended to use the <b>service-mdns-query ptr</b> command.</p> <ul style="list-style-type: none"> <li>• <b>service-policy policy-name</b>: Attaches the specified service policy to the VLAN. Bonjour announcements, and queries received by and sent from the VLAN are governed by the policies configured in the service policy. This configuration is mandatory for all VLANs.</li> </ul> <p><b>Note</b> Service policies can only be attached at interface level.</p> <ul style="list-style-type: none"> <li>• <b>transport [ all   ipv4   ipv6 ]</b> (Optional): Configures BCP parameter.</li> </ul>

	Command or Action	Purpose
		It is recommended to use <b>transport ipv4</b> command, except in those networks where the Bonjour clients send only IPv6 announcements and queries.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Device(config-if-mdns-sd)# exit	Exits mDNS gateway configuration mode.

## How to Configure Local Area Bonjour in Multicast DNS Mode for Wireless Networks

The configuration of local area Bonjour on a switch that acts as the SDG Agent in a wireless network involves the same set of procedures that are used to configure local area Bonjour on a switch that acts as the SDG Agent in a wired network.

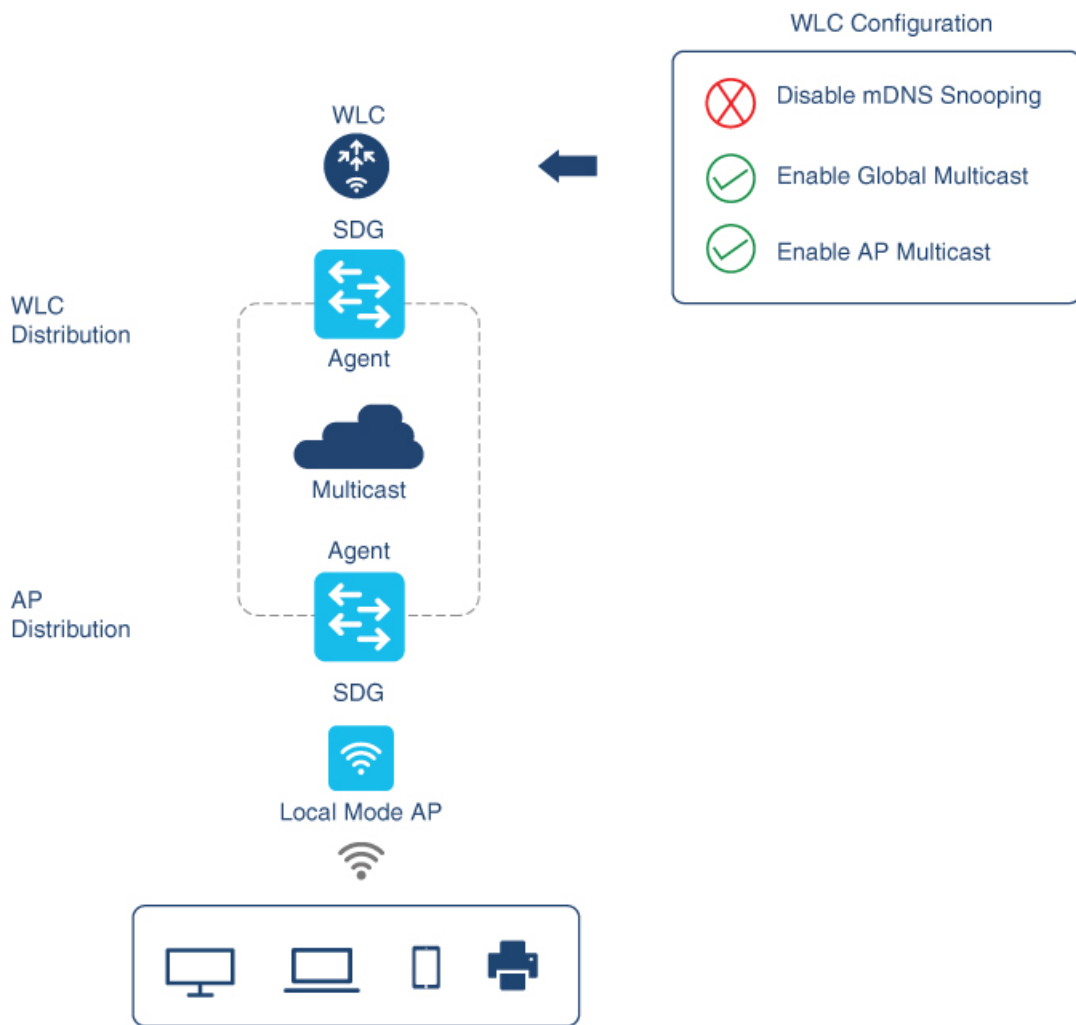
The Bonjour protocol operates on service announcements and queries. Each query or advertisement is sent to the mDNS IPv4 address 224.0.0.251 and IPv6 address FF02::FB. The mDNS messages are carried over well-known industry standard UDP port 5353, over both Layer 3 transport types.

The Layer 2 address used by the Bonjour protocol is link-local multicast address and therefore it's only forwarded to the same Layer 2 network. As multicast DNS (mDNS) is limited to a Layer 2 domain, for a client to discover a service, it has to be a part of the same Layer 2 domain. This isn't always possible in a large-scale deployment or enterprise.

To enable mDNS communication between Wireless endpoints and Cisco Catalyst switch that acts as an SDG Agent, the intermediate WLC must transparently allow the network to transmit and receive mDNS messages.

Hence, for a Multicast DNS Mode Wireless network deployment, disable the mDNS Snooping on Cisco AireOS based WLC and enable mDNS Gateway feature on Cisco Catalyst 9800 series WLC and set the AP Multicast Mode to Multicast.

Figure below illustrates a prerequisite configuration for Wireless network to enable seamless communication between SDG-Agent switches and Wireless endpoints.



The Cisco WLC and Access Points by default prevent the forwarding of Layer 2 or Layer 3 Multicast frames between Wireless and Wired network infrastructure. The forwarding is supported with stateful capabilities enabled using AP Multicast. The network administrator must globally enable Multicast and configure a unique Multicast Group to advertise in the network. This multicast group is only required for Cisco Access Points to enable Multicast over Multicast (MCMC) capabilities across the LAN network. The Bonjour solution doesn't require any Multicast requirements on Wireless Client VLAN; thus, it's optional and applicable only for other Layer 3 Multicast applications.

The core network must be configured with appropriate Multicast routing to allow the Access Points to join WLC Multicast Group. The Multicast configuration must be enabled on Cisco WLC management VLAN and on the Cisco Access Points of their respective distribution layer switch.

## Enabling mDNS Gateway on the Device

To configure mDNS on the device, follow these steps:



## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>mdns-sd gateway</b> <b>Example:</b> Device(config)# <b>mdns-sd gateway</b>	Enables mDNS on the device and enters mDNS gateway configuration mode. Enter the following commands in mDNS gateway configuration mode to enable the respective functionalities: <ul style="list-style-type: none"> <li>• <b>air-print-helper</b>: Enables IOS devices like iPads to discover and use older printers that support Bonjour</li> <li>• <b>cache-memory-max</b>: Configures the percentage memory for cache</li> <li>• <b>ingress-client</b>: Configures Ingress Client Packet Tuners</li> <li>• <b>rate-limit</b>: Enables rate limiting of incoming mDNS packets</li> <li>• <b>service-announcement-count</b>: Configures maximum service advertisement count</li> <li>• <b>service-announcement-timer</b>: Configures advertisements announce timer periodicity</li> <li>• <b>service-query-count</b>: Configures maximum query count</li> <li>• <b>service-query-timer</b>: Configures query forward timer periodicity</li> </ul> <p><b>Note</b> For <b>cache-memory-max</b>, <b>ingress-client</b>, <b>rate-limit</b>, <b>service-announcement-count</b>, <b>service-announcement-timer</b>, <b>service-query-count</b>, and <b>service-query-timer</b> commands, you can retain the default value of the respective parameter for general deployments. Configure a different value, if required, for a specific deployment.</p>

	Command or Action	Purpose
Step 4	<b>exit</b> <b>Example:</b> Device(config-mdns-sd)# exit	Exits mDNS gateway configuration mode.

## Creating Custom Service Definition

Service definition is a construct that provides an admin friendly name to one or more mDNS service types or PTR Resource Record Name. By default, a few built-in service definitions are already predefined and available for admin to use. In addition to built-in service definitions, admin can also define custom service definitions.

### Procedure

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>mdns-sd service-definition</b> <i>service-definition-name</i> <b>Example:</b> Device(config)# mdns-sd service-definition CUSTOM1	Configures mDNS service definition.  <b>Note</b> All the created custom service definitions are added to the primary service list. Primary service list comprises of a list of custom and built-in service definitions.
Step 4	<b>service-type</b> <i>string</i> <b>Example:</b> Device(config-mdns-ser-def)# service-type _custom1._tcp.local	Configures mDNS service type.
Step 5	Repeat step 4 to configure more than one service type in the custom service definition.	
Step 6	<b>exit</b> <b>Example:</b> Device(config-mdns-ser-def)# exit	Exit mDNS service definition configuration mode.

## Creating Service List

mDNS service list is a collection of service definitions. To create a service list, follow these steps:

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>mdns-sd service-list <i>service-list-name</i> {in   out}</b> <b>Example:</b> Device(config)# <b>mdns-sd service-list VLAN100-list in</b>	Configures mDNS service list.
<b>Step 4</b>	<b>match <i>service-definition-name</i> [message-type {any   announcement   query}]</b> <b>Example:</b> Device(config-mdns-sl-in)# <b>match PRINTER-IPPS message-type announcement</b>	Matches the service to the message type. Here, <i>service-definition-name</i> refers to the names of services, such as, airplay, airserver, airtunes, and so on.  <b>Note</b> To add a service, the service name must be part of the primary service list.  If the mDNS service list is set to IN, the applicable command syntax is: <b>match <i>service-definition-name</i> [message-type {any   announcement   query}]</b> .  If the mDNS service list is set to OUT, the applicable command syntax is: <b>match <i>service-definition-name</i> [message-type {any   announcement   query}] [location-filter <i>location-filter-name</i>] [source-interface {mDNS-VLAN-number   mDNS-VLAN-range}]</b> .
<b>Step 5</b>	<b>exit</b> <b>Example:</b> Device(config-mdns-sl-in)# <b>exit</b>	Exits mDNS service list configuration mode.

## Creating Service Policy

A Service Policy that is applied to an interface specifies the allowed Bonjour service announcements or the queries of specific service types that should be processed, in ingress direction or egress direction or both. For this, the service policy specifies two service-lists, one each for ingress and egress directions. In the Local Area Bonjour domain, the same service policy can be attached to one or more Bonjour client VLANs; however, different VLANs may have different service policies.

To configure service policy with service lists, follow these steps:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>mdns-sd service-policy <i>service-policy-name</i></b> <b>Example:</b> Device(config)# <b>mdns-sd service-policy mdns-policy1</b>	Configures mDNS service policy.
<b>Step 4</b>	<b>service-list <i>service-list-name</i> {in   out}</b> <b>Example:</b> Device(config-mdns-ser-pol)# <b>service-list VLAN100-list in</b> Device(config-mdns-ser-pol)# <b>service-list VLAN300-list out</b>	Configures service lists for IN and OUT directions.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> Device(config-mdns-ser-pol)# <b>exit</b>	Exits mDNS service policy configuration mode.

## Verifying Local Area Bonjour in Multicast DNS Mode for LAN and Wireless Networks

This section shows how to verify Local Area Bonjour in Multicast DNS mode for LAN and Wireless networks.

### Verifying SDG-Agent Status

The following is a sample output of the **show mdns-sd service-list *service-list-name* {in | out}** command.

```

Name                Direction  Service  Message-Type  Source
=====
VLAN100-list        In         Printer  Announcement   -
                   In         Airplay  Query           -
                   In         CUSTOM1  Any             -
VLAN300-list        Out        Printer  Announcement   V1200

```

The following is a sample output of the **show mdns-sd service-definition** *service-definition-name* **service-type** {*custom* | *built-in*} command.

```

Service              PTR                                     Type
=====
apple-tv              _airplay._tcp.local                    Built-In
                     _raop._tcp.local
apple-file-share      _afpovertcp._tcp.local                 Built-In
CUSTOM1                _custom1._tcp.local                    Custom
CUSTOM2                _customA._tcp.local                    Custom
                     _customA._tcp.local

```

The following is a sample output of the **show mdns-sd** *service-policy-name* **interface** *interface-name* command.

```

Name  Service-List-In  Service-List-Out
=====
mdns-policy-1  VLAN100-list     VLAN300-list
mdns-policy-2  VLAN400-list     VLAN400-list

```

The following is a sample output of the **show mdns-sd summary** command.

```

mDNS Gateway: Enabled
Mode: Service Peer
Service Announcement Periodicity(in seconds): 30
Service Announcement Count: 50
Service Query Periodicity(in seconds): 15
Service Query Count: 50
Active Response Timer (in seconds): Disabled
ANY Query Forward: Disabled
SDG Agent IP: 9.8.57.10
Active Query Periodicity (in minutes): 30
mDNS Query Type: PTR only
Transport Type: IPv4
mDNS AP service policy: default-mdns-service-policy

```

The following is a sample output of the **show mdns-sd sp-sdg statistics** command.

```

mDNS SP Statistics
last reset time: 07/27/21 15:36:33
Messages sent:
Query : 122
ANY query : 35
Advertisements : 12

```

```

Advertisement Withdraw : 1
Service-peer cache clear : 0
Resync response : 3
Srvc Discovery response : 0
Keep-Alive : 2043
Messages received:
Query response : 0
ANY Query response : 0
Cache-sync : 9
Get service-instance : 0
Srvc Discovery request : 0
Keep-Alive Response : 2042

```

## Verifying Wide Area Bonjour Controller Status

The following is a sample output of the **show mdns controller summary** command.

```

Device# show mdns controller summary

Controller Summary
=====
Controller Name   : DNAC-BONJOUR-CONTROLLER
Controller IP     : 10.104.52.241
State            : UP
Port             : 9991
Interface        : Loopback0
Filter List      : policy1
Dead Time        : 00:01:00

```

The following is a sample output of the **show mdns controller export-summary** command.

```

Device# show mdns controller export-summary

Controller Export Summary
=====
Controller IP     : 10.104.52.241
State            : UP
Filter List      : policy1
Count            : 100
Delay Timer      : 30 seconds
Export           : 300
Drop             : 0
Next Export      : 00:00:01

```

The following is a sample output of the **show mdns controller statistics** command.

```

Device# show mdns controller statistics

Total BCP message sent           : 47589
Total BCP message received      : 3
Interface WITHDRAW messages sent : 0
Clear cache messages sent       : 0
Total RESYNC state count        : 0
Last successful RESYNC           : Not-Applicable

```

```

Service Advertisements:
  IPv6 advertised           : 0
  IPv4 advertised           : 300
  Withdraws sent           : 0
  Advertisements Filtered  : 0
  Total service resynced   : 0

Service Queries:
  IPv6 queries sent         : 0
  IPv6 query responses received : 0
  IPv4 queries sent         : 0
  IPv4 query responses received : 0

```

The following is a sample output of the **show mdns controller detail** command.

```

Device# show mdns controller detail

Controller : DNAC-BONJOUR-CONTROLLER
  IP : 10.104.52.241, Dest Port : 9991, Src Port : 0, State : UP
  Source Interface : Loopback0, MD5 Disabled
  Hello Timer 0 sec, Dead Timer 0 sec, Next Hello 00:00:00
  Uptime 00:00:00
Service Announcement :
  Filter : policy1
  Count 100, Delay Timer 30 sec, Pending Announcement 0, Pending Withdraw
  0
  Total Export Count 300, Next Export in 00:00:16
Service Query :
  Query Suppression Disabled
  Query Count 50, Query Delay Timer 15 sec, Pending 0
  Total Query Count 0, Next Query in 00:00:01

```

## Verifying Local Area Bonjour Configuration for LAN and Wireless Networks

The following is a sample output of the **show run** command.

```

mdns-sd gateway

mdns-sd service-definition custom1
  service-type _airplay._tcp.local
  service-type _raop._tcp.local

mdns-sd service-list list1 IN
  match custom1
mdns-sd service-list list2 OUT
  match custom1

mdns-sd service-policy policy1

```

```
service-list list1 IN  
service-list list2 OUT
```

```
service-export mdns-sd controller DNAC-CONTROLLER-POLICY  
controller-address 99.99.99.10  
controller-service-policy policy1 OUT  
controller-source-interface Loopback0
```





## CHAPTER 3

# Configuring VRF-Aware Local Area Bonjour Services

---

Beginning from Cisco IOS XE Bengaluru 17.4.1, Cisco Catalyst 9000 Series switches supports Virtual Routing and Forwarding-Aware (VRF-Aware) services in Local Area Bonjour domain. VRF-Aware Local Area Bonjour services provide boundary-based service discovery for Layer 3 segmented IPv4 and IPv6 network and support policy-based (secure) routing services for Wired and Wireless networks. VRF-Aware Local Area Bonjour service is supported on enterprise-grade, traditional, and next-generation fabric-based deployment models as described in [Cisco DNA Service for Bonjour Solution Overview](#).

- [Prerequisites for VRF-Aware Local Area Bonjour Services, on page 29](#)
- [Restrictions for VRF-Aware Local Area Bonjour Services, on page 30](#)
- [Information about VRF-Aware Local Area Bonjour Services, on page 30](#)
- [Understanding VRF-Aware Wide Area Bonjour Services, on page 32](#)
- [Understanding VRF-Aware Service on Multilayered Wired and Wireless Networks, on page 33](#)
- [How to configure Intra-Virtual Network Proxy Service on Local Area Bonjour Domain, on page 35](#)
- [How to configure Inter-Virtual Network Proxy Service on Local Area Bonjour Domain, on page 36](#)
- [Verifying VRF-Aware Local Area Bonjour Services, on page 39](#)

## Prerequisites for VRF-Aware Local Area Bonjour Services

- You must understand the mDNS service segmentation capabilities to implement, manage, and troubleshoot the proxy service in Local Area Bonjour domain.
- Ensure that the Cisco Catalyst 9000 Series switch is configured in SDG-Agent mode. VRF-Aware Local Area Bonjour service is supported on first-hop IP gateway of switches configured in SDG-Agent mode in Wired and Wireless networks.
- Ensure that the software version installed on the Cisco Catalyst 9000 Series switch is Cisco IOS XE Bengaluru 17.4.1 or higher.
- Ensure that all required IP VRF with IPv4 or IPv6 address-family configurations is completed. These configurations are required to activate VRF on the switch configured in SDG-Agent mode.
- Ensure that the IP VRF configured to a local SVI interface supports IP gateway so that the mDNS Wired and Wireless endpoint can be attached directly or remotely.

- To activate mDNS gateway in Unicast mode for a VLAN, ensure that the mDNS gateway and service policy is configured after enabling the VLAN using the **vlan configuration id** command.
- Ensure that all configurations for IPv4 or IPv6-based data routing and forwarding both within the same VRF or different VRFs are complete including network requirements such as stateful firewall configuration, route-leaking configuration and so on.

## Restrictions for VRF-Aware Local Area Bonjour Services

- VRF-Aware Local Area Bonjour service is not supported on a Layer 2 Cisco Catalyst 9000 Series switch or a Layer 2 Cisco Catalyst 9800 WLC in Service-Peer mode.
- VRF-Aware Local Area Bonjour services are configured to provide mDNS service discovery information between Layer 3 segments within the same or different IP VRF, or share services from non-VRF enabled networks only. Any additional IP routing and data forwarding configurations are beyond the scope of this implementation.

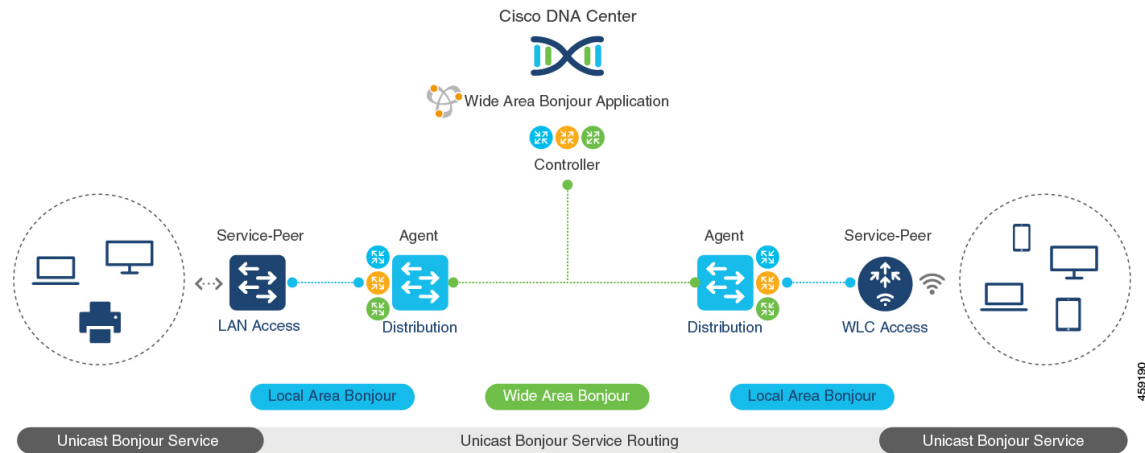
## Information about VRF-Aware Local Area Bonjour Services

The Cisco DNA Service for Bonjour solution provides end-to-end service-routing for enterprise-grade Wired and Wireless networks. The enterprise network builds secure and segmented networks that protect IT-managed infrastructure and shares services and resources among trusted and untrusted user group. The physical infrastructure can be logically virtualized into a private networking space that supports secure communication services within closed user groups and conditionally extends boundary services based on business and technical demands.

VRF-Aware Local Area Bonjour gateway services allow to dynamically discover and distribute mDNS services on the same VRF segmented Layer 3 overlay networks based on policy. You can also build an Extranet network using the mDNS location-filter policy that supports proxy services among multiple logical VRF or a global IP routing domain on a local system. The Layer 3 VRF segmented networks can also be configured to route in overlay using any next-generation overlay networks such as Cisco SD-Access, BGPEVPN VXLAN or classic technologies such as Multi-VRF, MPLS.

[Figure 9: Cisco DNA Service for Bonjour with VRF-Aware Services](#) illustrates the Cisco DNA Service for Bonjour solution configured with VRF-Aware services for enterprise-grade Wired and Wireless networks.

Figure 9: Cisco DNA Service for Bonjour with VRF-Aware Services

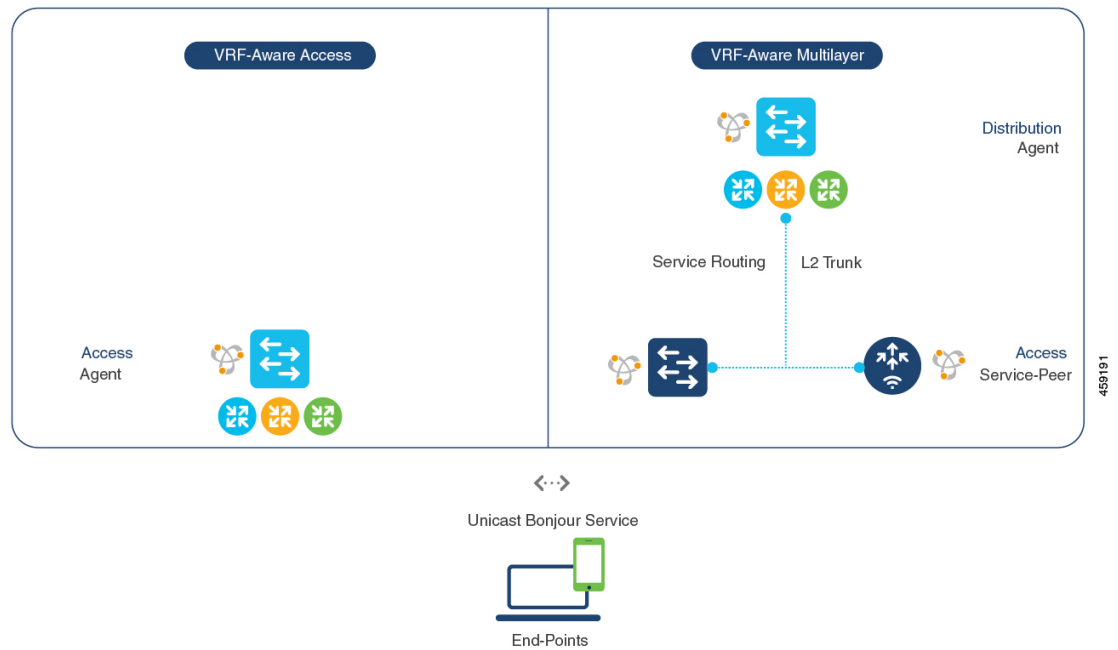


## Gateway Modes for VRF-Aware Bonjour Services

VRF is a Layer 3 specific virtual routing function and therefore it is implemented on Layer 3 Ethernet switches with first-hop IP gateways that can directly or remotely attach mDNS endpoints.

Figure 10: Gateway Modes for VRF-Aware Services illustrates the Cisco Catalyst 9000 Series switch in SDG-Agent mode supporting VRF-Aware services in Layer 3 access mode and in multi-layer network deployment mode. In multi-layer network deployment mode, the gateway to the distribution layer provides a Layer 2 or Layer 3 boundary to a downstream Layer 2 Cisco Catalyst 9000 Series switch and Cisco Catalyst 9800 WLC for local proxy service with local VLANs.

Figure 10: Gateway Modes for VRF-Aware Services



- VRF-Aware Routed Access:** The Cisco Catalyst 9000 Series switch can be deployed as an IP gateway for directly attached Wired or Wireless mDNS endpoints. The Cisco Wireless SSID can be configured as fabric-enabled or as FlexConnect with local switching that provides local termination point to a first-hop Ethernet switch that supports Layer 3 overlay networks such as Cisco SD-Access or BGP-EVPN based-fabric networks. A Cisco Catalyst 9000 Series switch configured in SDG-Agent mode provides unicast-based mDNS gateway services to directly attached Wired and Wireless endpoints within the same or different virtual routing network space or a default global IP network.
- VRF-Aware Multilayer:** The Cisco Catalyst 9000 Series Switch can be deployed as an IP gateway for remotely attached Wired or Wireless mDNS endpoints through an intermediate Layer 2 Cisco Catalyst 9000 Series switch or Cisco Catalyst 9800 Series WLC. A Cisco Catalyst 9000 Series switch, configured in SDG-Agent mode and in the distribution layer, provides VRF-Aware mDNS gateway services, while the Layer 2 Ethernet switch and Cisco WLC in Unicast mode provides local proxy services to directly attached Wired and Wireless endpoints within the same or different VLAN.

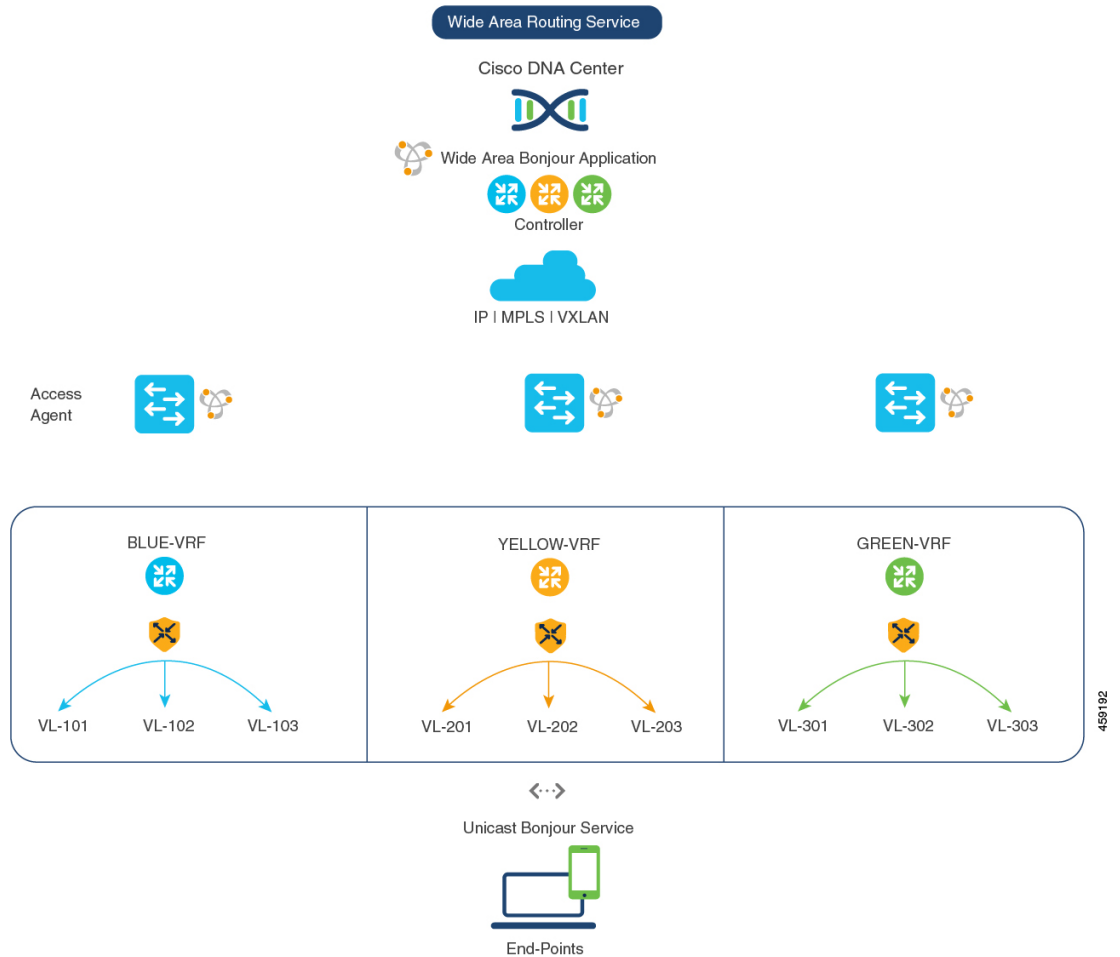
## Understanding VRF-Aware Wide Area Bonjour Services

The VRF-Aware service discovery and distribution can be implemented across multiple switches in SDG-Agent mode on an IP, MPLS, or VXLAN-enabled network with Wide Area Bonjour. The Cisco DNA-Center Wide Area Bonjour application supports granular and policy-based routing services that allow discovery and distribution of mDNS services dynamically over overlay networks. You can build a global policy combining one or more source and receiver SDG-Agents that allow distributing or advertising services from a specific IPv4 or even an IPv6 network mapped to the VRF.

The network wide and distributed switches in SDG-Agent mode transport locally discovered or requested mDNS service information over lightweight unicast routing services to a centralized Cisco DNA-Center controller in an underlay IPv4 network. These switches must be configured with a unified service-export policy for local networks mapped to one or more VRFs or to a global IP routing domain.

Figure 11: VRF-Aware Wide Area Bonjour Services illustrates VRF-Aware Wide Area Bonjour services for IP, MPLS, or VXLAN enabled overlay networks.

Figure 11: VRF-Aware Wide Area Bonjour Services



458192

## Understanding VRF-Aware Service on Multilayered Wired and Wireless Networks

The Cisco Catalyst 9000 Series switches support VRF-Aware service for multilayered Wired and central-switching Wireless-enabled networks. The Layer 2 or Layer 3 network boundary to the Cisco Catalyst 9000 Series switches is extended at the distribution layer with an intermediate Layer 2 Cisco Catalyst 9000

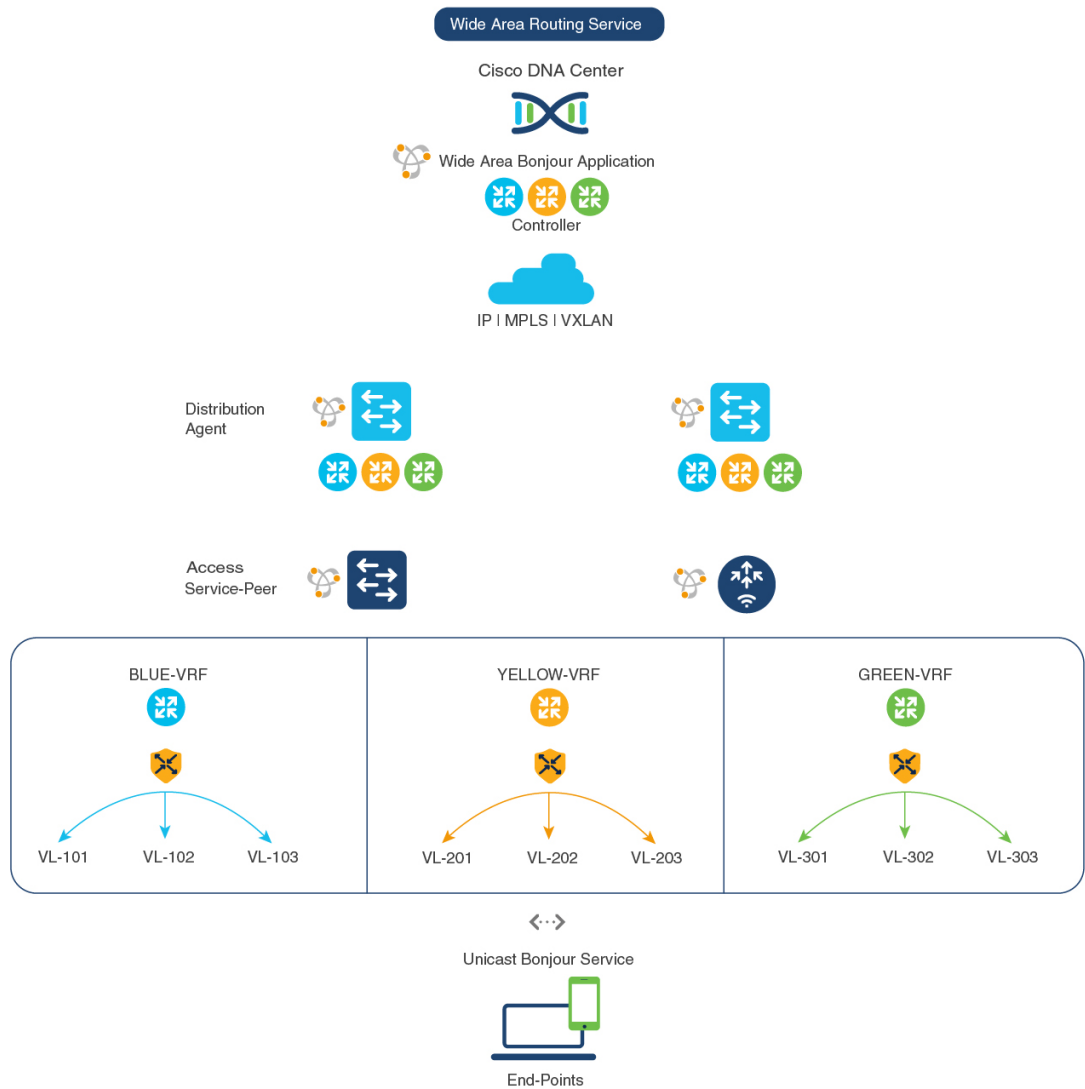
Series switch or Cisco Catalyst 9800 Series WLC and directly attached to the Wired and central-switching Wireless endpoints. As the IP gateway shifts, the Cisco Catalyst 9000 Series switches in the distribution layer must be configured in SDG-Agent mode and the downstream Layer 2 switch and WLC network devices must be configured in Service-Peer mode to support mDNS proxy services to locally attached endpoints.

The VRF-Aware service configured on a switch, in SDG-Agent mode and in the distribution layer, follows configuration and operation guidelines for Wired and central-switching Wireless as described in [Understanding VRF-Aware Wide Area Bonjour Services, on page 32](#). The Layer 2 switch and WLC network devices remains transparent to VRF-Aware services and continues to provide local proxy services to locally attached users in the same or different VLANs.

The VRF-Aware service discovery and distribution can be implemented across multiple switches in SDG-Agent mode on an IP, MPLS, or VXLAN-enabled network with Wide Area Bonjour. The Cisco DNA-Center Wide Area Bonjour application supports granular and policy-based routing services that allow discovery and distribution of mDNS services dynamically for overlay networks. You can build a global policy combining one or more source and receiver SDG-Agent that allow distributing or advertising services from a specific IPv4 or even an IPv6 network mapped to the VRF.

[Figure 12: VRF-Aware on Multilayered Wired and Wireless Network](#) illustrates end-to-end VRF-Aware on multilayered Wired and Wireless networks across Wide Area Bonjour domain with Cisco DNA-Center.

Figure 12: VRF-Aware on Multilayered Wired and Wireless Network



## How to configure Intra-Virtual Network Proxy Service on Local Area Bonjour Domain

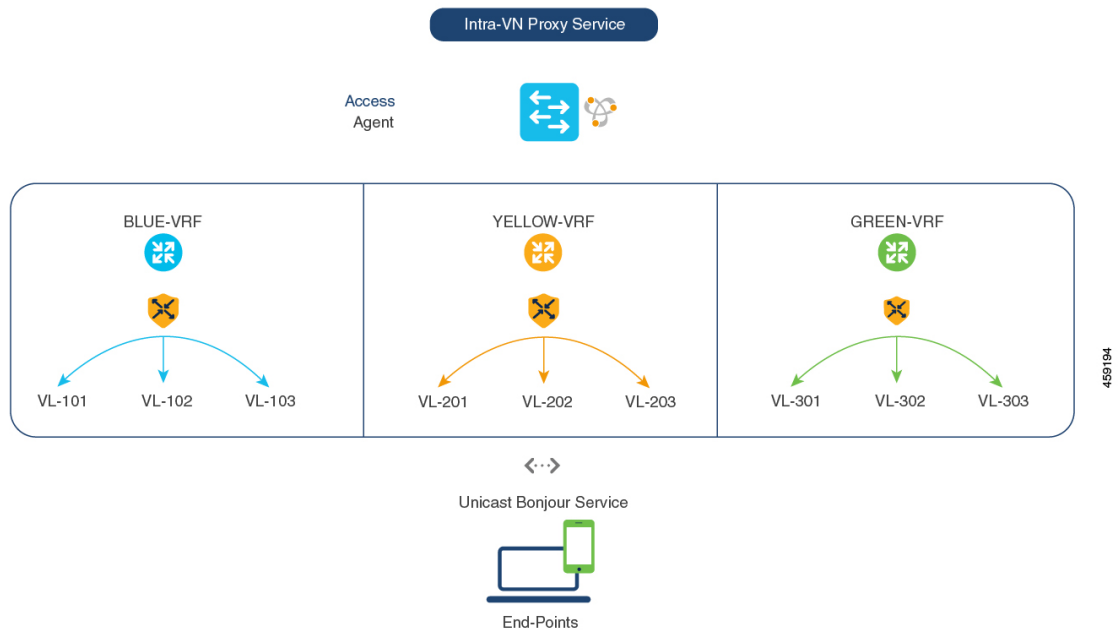
Intra-Virtual Network (Intra-VN) Proxy Service is a policy-based VRF-Aware service discovery and distribution implemented on the IP VRF of a switch in SDG-Agent mode connected to multiple IP networks.

Beginning from Cisco IOS XE Bengaluru 17.4.1, the Cisco Catalyst 9000 Series switches support mDNS gateway service as the default on each VRF. You must build a mDNS service policy that implicitly allows required mDNS service types and mapping services to endpoint facing VLANs. The Cisco Catalyst 9000 Series switch can automatically discover VRF associations to a VLAN interface without additional configurations.

The Cisco Catalyst 9000 Series switch in SDG-Agent mode dynamically discovers mDNS services from a local network and automatically builds VRF-aware service information. To enable Layer 3 segmented proxy service by default, the SDG-Agent provides limited mDNS service proxy response to endpoints in other VLANs mapped with the same VRF.

**Figure 13: Intra-VN Service Proxy** illustrates VRF-Aware enabled on an Intra-VN proxy service.

**Figure 13: Intra-VN Service Proxy**



## How to configure Inter-Virtual Network Proxy Service on Local Area Bonjour Domain

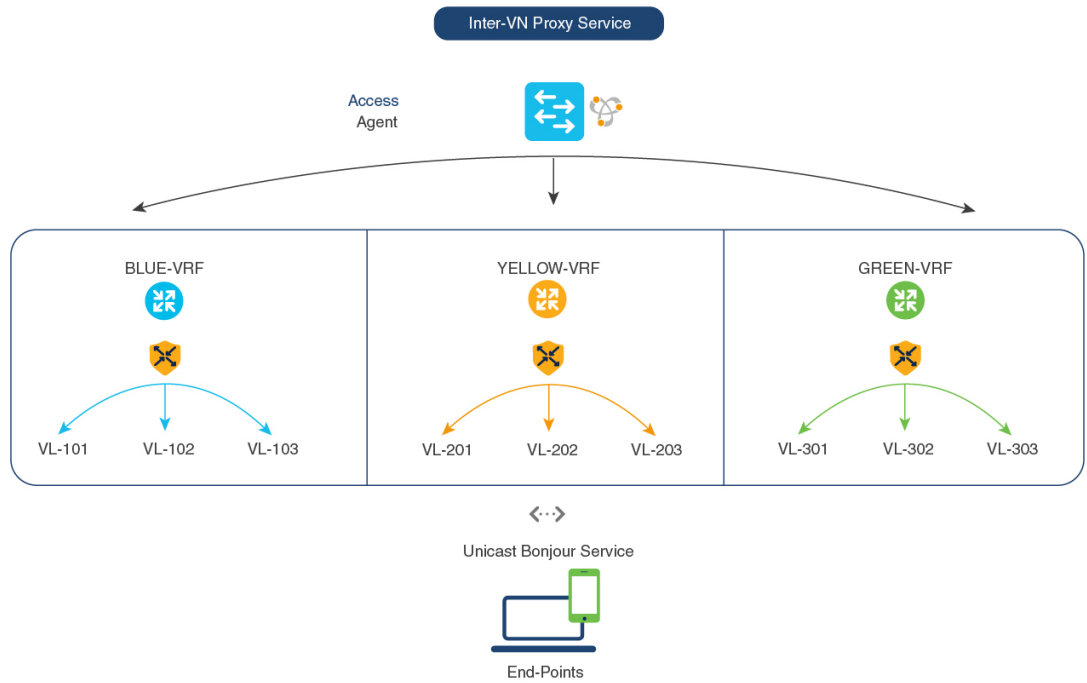
Inter-VN Proxy Service is a policy-based VRF-Aware service discovery and distribution implemented on multiple IP VRFs or on a global IP routing domain of a switch in SDG-Agent mode connected to multiple IP networks.

Beginning from Cisco IOS XE Bengaluru 17.4.1, the Cisco Catalyst 9000 Series switches support mDNS service discovery and distribution between IP VRFs or on a global routing domain based on the configured mDNS location-filter policy. The existing location-filter configuration on an SDG-Agent permits mDNS service information between configured VLANs and records discovery and distribution on the mapping table. Although configuring inter-VN provides Extranet mDNS proxy services between Wired and Wireless networks, additional methods such as stateful firewall, route-leaking and so on must also be configured to handle the data transfer between Inter-VN or VRF to global IP routing.

**Figure 14: Inter-VN Proxy Service** shows Inter-VN proxy service for Extranet network.



Figure 14: Inter-VN Proxy Service



455195

## Configuring Inter-Virtual Network Location-Filter

To enable the local service proxy on the switch to discover mDNS services between local VLANs, perform the following steps:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>vlan ID</b> <b>Example:</b> Device(config)# <b>vlan 101</b> Device(config-vlan)# <b>name BLUE-VRF</b> Device(config)# <b>vlan 201</b> Device(config-vlan)# <b>name YELLOW-VRF</b> Device(config)# <b>vlan 301</b> Device(config-vlan)# <b>name GREEN-VRF</b>	Configures a VLAN ID in local database for overlay mDNS endpoints.

	Command or Action	Purpose
<b>Step 4</b>	<b>mdns-sd location-filter</b> <i>location-filter-name</i> <b>Example:</b> Device(config)# <b>mdns-sd location-filter</b> <b>INTER-VN-LOCAL-PROXY</b>	Configures a unique location-filter.
<b>Step 5</b>	<b>match location</b> {all   default   ID} <b>vlan</b> [ID] <b>Example:</b> Device(config-mdns-loc-filter)# <b>match</b> <b>location-group default vlan 101</b> Device(config-mdns-loc-filter)# <b>match</b> <b>location-group default vlan 201</b> Device(config-mdns-loc-filter)# <b>match</b> <b>location-group default vlan 301</b>	Configures the match criteria that mutually distribute permitted services between grouped VLANs.
<b>Step 6</b>	<b>mdns-sd service-list</b> <i>service-list-name</i> {in   out} <b>Example:</b> Device(config)# <b>mdns-sd service-list</b> <b>BLUE-VRF-LIST-OUT out</b>	Configures mDNS service-list to classify one or more service-types. Unique service-list is required to process incoming mDNS message and the outbound response to the requesting end points.
<b>Step 7</b>	<b>match</b> <i>service-destination-name</i> <b>[message-type {any   announcement   query}]</b> <b>Example:</b> Device(config)# <b>mdns-sd service-list</b> <b>BLUE-VRF-LIST-OUT out</b> Device(config-mdns-sl-out)# <b>match</b> <b>APPLE-TV location-filter LOCAL-PROXY</b>	<p>Associates the location-filter to one or more service-types to enable local proxy between local VLANs. For example, the Apple-TV learned from the YELLOW-VRF VLAN 201 and the GREEN-VRF VLAN 301 will be distributed to the receiver in the BLUE-VRF VLAN 101.</p> <p>The service-list contains implicit deny at the end.</p> <p>The message-type for outbound service-list is not required.</p>
<b>Step 8</b>	<b>mdns-sd service-policy</b> <i>service-policy-name</i> <b>Example:</b> Device(config)# <b>mdns-sd service-policy</b> <b>BLUE-VRF-POLICY</b>	Creates a unique mDNS service-policy.
<b>Step 9</b>	<b>service-list</b> <i>service-list-name</i> {in   out} <b>Example:</b> Device(config)# <b>mdns-sd service-policy</b> <b>BLUE-VRF-POLICY</b> Device(config-mdns-ser-policy)# <b>service-list BLUE-VRF-LIST-OUT out</b>	Configures an mDNS service policy to associate with the service-list for each direction.
<b>Step 10</b>	<b>vlan configuration</b> <i>ID</i> <b>Example:</b> Device(config)# <b>vlan configuration</b> <b>101-103</b>	<p>Enables VLAN configuration for advanced service parameters.</p> <p>One or more VLANs can be created for the same settings. For example, the VLAN</p>

	Command or Action	Purpose
		configuration range 101-110 or 200 allows to configure consecutive and nonconsecutive VLAN IDs.
<b>Step 11</b>	<b>mdns-sd gateway</b> <b>Example:</b> Device(config-vlan)# <b>mdns-sd gateway</b>	Enables the mDNS gateway on the specified VLAN IDs.
<b>Step 12</b>	<b>service-policy BLUE-VRF-POLICY</b> <b>Example:</b> Device(config-vlan-mdns)# <b>service-policy BLUE-VRF-POLICY</b>	Associates an mDNS service-policy with the specified VLAN IDs.
<b>Step 13</b>	<b>end</b> <b>Example:</b> Device(config-vlan-mdns)# <b>end</b>	Returns to privileged EXEC mode.

## Verifying VRF-Aware Local Area Bonjour Services

The dynamically discovered VRF-Aware service information can be verified on Cisco Catalyst 9000 Series switch in SDG-Agent mode by including the **vrf** keyword on the existing **show mdns-sd** command. You can verify each VRF-service record information based on the unique VRF name.

The following is an example of the command that displays the dynamically discovered mDNS service records in the BLUE-VRF:

```
Device# show mdns-sd cache vrf BLUE-VRF
```

```

                                     mDNS CACHE
-----
[<NAME>]                               [<TYPE>]      [<TTL>/Remaining] [Vlan-Id/If-name]
[Mac Address]           [<RR Record Data>]

RTP-ATV-1._device-info._tcp.local      TXT           4500/4495         511
a018.28f2.9889          (13)'model=J33iAP'
_airplay._tcp.local                PTR           4500/4495         511
a018.28f2.9889          RTP-ATV-1._airplay._tcp.local
_raop._tcp.local                  PTR           4500/4495         511
a018.28f2.9889          A01828F29889@RTP-ATV-1._raop._tcp.local
RTP-ATV-1._airplay._tcp.local      SRV           4500/4495         511
a018.28f2.9889          0             0                 7000             RTP-ATV-3.local
A01828F29889@RTP-ATV-1._raop._tcp.local SRV           4500/4495         511
a018.28f2.9889          0             0                 7000             RTP-ATV-3.local
RTP-ATV-1.local                    AAAA          4500/4495         511
a018.28f2.9889          2001:10:153:2:C2F:9445:7062:5C3C
RTP-ATV-1.local                    A             4500/4495         511
a018.28f2.9889          10.155.1.17
RTP-ATV-1._airplay._tcp.local      TXT           4500/4495         511
a018.28f2.9889
(208)'deviceid=A0:18:28:F2:98:89''features=0x5A7FFFFF7,0x1E''flags=0x44''model=~'~
A01828F29889@RTP-ATV-1._raop._tcp.local TXT           4500/4495         511

```

```
a018.28f2.9889
(177)'cn=0,1,2,3'da=true'et=0,3,5'ft=0x5A7FFFF7,0x1E'md=0,1,2'am=AppleTV3,2'~
```

Use the following commands in privileged EXEC mode on a Cisco Catalyst 9000 Series switch configured in SDG-Agent mode to verify various Local Area Bonjour domain mDNS parameters such as service configuration, cache records, statistics, and so on.

**Table 3: Commands to Verify VRF-Aware Services**

Command	Purpose
<b>show mdns-sd cache</b> {all   interface   mac   name   service-peer   static   type   vlan   vrf}	<p>Displays all available mDNS cache record that supports multiple variables and provides granular source details. The following variables are available:</p> <ul style="list-style-type: none"> <li>• <b>all</b>: Displays all available cache records discovered from multiple source connections of a system.</li> <li>• <b>interface</b>: Displays the available cache records discovered from a specified Layer 3 interface.</li> <li>• <b>mac</b>: Displays the available cache records discovered from the specified MAC address.</li> <li>• <b>name</b>: Displays the available cache records based on service provider announced name.</li> <li>• <b>service-peer</b>: Displays available cache records discovered from the specified Layer 2 Service-Peer.</li> <li>• <b>static</b>: Displays the locally configured static mDNS cache entries.</li> <li>• <b>type</b>: Displays the available cache records based on the specific mDNS record type (PTR, SRV, TXT, A, or AAAA).</li> <li>• <b>vlan</b>: Displays the available cache records discovered from the specified Layer 2 VLAN ID in unicast mode.</li> <li>• <b>vrf</b>: Displays each VRF available cache records based on the specific mDNS record type (PTR, SRV, TXT, A, or AAAA).</li> </ul>
<b>show mdns-sd service-definition</b> {name   type}	<p>Displays the built-in and user-defined custom service definitions and provides the mapping from service name to mDNS PTR records.</p> <p>The service-definition can be filtered by name or type.</p>

Command	Purpose
<b>show mdns-sd service-list</b> { <b>direction</b>   <b>name</b> }	<p>Displays the configured inbound or outbound service-list that classifies matching service types for a service policy.</p> <p>The service lists can be filtered by name or specific direction.</p>
<b>show mdns-sd service-policy</b> { <b>interface</b>   <b>name</b> }	<p>Displays the list of mDNS service policies mapped with inbound or outbound service-lists.</p> <p>The service policies list can be filtered by the associated specified interface or by name.</p>
<b>show mdns-sd statistics</b> { <b>all</b>   <b>cache</b>   <b>debug</b>   <b>interface</b>   <b>service-list</b>   <b>service-policy</b>   <b>services</b>   <b>vlan</b> }	<p>Displays the detailed mDNS statistics processed bidirectionally by the system on each mDNS-gateway-enabled VLAN, when mDNS is configured in unicast mode.</p> <p>The keywords for the mDNS statistics provide a detail view on the interface, policy, service-list, and services.</p>
<b>show mdns-sd summary</b> { <b>interface</b>   <b>vlan</b> }	<p>Displays the brief information about mDNS gateway and the key configuration status on all VLANs and interfaces of the system.</p>





## CHAPTER 4

# Feature History for Cisco DNA Service for Bonjour

- [Feature History for Cisco DNA Service for Bonjour, on page 43](#)

## Feature History for Cisco DNA Service for Bonjour

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Release	Modification
Cisco IOS 15.2(6) E2	Cisco DNA Service for Local Area Bonjour and Wide Area Bonjour (Multicast DNS Mode only), was introduced on the following platforms: <ul style="list-style-type: none"><li>• Cisco Catalyst 2960-X Series Switches</li><li>• Cisco Catalyst 2960-XR Series Switches</li></ul>
Cisco IOS 15.5(1)SY4	Cisco DNA Service for Local Area Bonjour and Wide Area Bonjour (Multicast DNS Mode only) was introduced on Cisco Catalyst 6800 Series Switches.
Cisco IOS XE 3.11.0 E	Cisco DNA Service for Local Area Bonjour and Wide Area Bonjour (Multicast DNS Mode only) was introduced on the following platforms: <ul style="list-style-type: none"><li>• Cisco Catalyst 4500-E Series Switches</li><li>• Cisco Catalyst 4500-X Series Switches</li></ul>

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	<p>Cisco DNA Service for Local Area Bonjour and Wide Area Bonjour (Multicast DNS Mode only) was introduced on the following platforms:</p> <ul style="list-style-type: none"> <li>• Cisco Catalyst 3650 Series Switches</li> <li>• Cisco Catalyst 3850 Series Switches</li> <li>• Cisco Catalyst 9300 Series Switches</li> <li>• Cisco Catalyst 9400 Series Switches</li> <li>• Cisco Catalyst 9500 Series Switches</li> <li>• Cisco Catalyst 9500 Series Switches - High Performance</li> <li>• Cisco Catalyst 9600 Series Switches</li> <li>• Cisco Catalyst 9800 Series Wireless Controllers</li> <li>• Cisco 5500 Series Wireless Controllers</li> <li>• Cisco 8540 Wireless Controllers</li> <li>• Cisco 4000 Series Integrated Services Routers (ISR)</li> </ul>
Cisco IOS XE Amsterdam 17.1.1	Cisco DNA Service for Local Area Bonjour was introduced on Cisco Catalyst 9200 Series Switches.
Cisco IOS XE Amsterdam 17.2.1	<p>Introduced Cisco DNA Service for Bonjour support for the following:</p> <ul style="list-style-type: none"> <li>• SD-Access network</li> <li>• Unicast mode for LAN network</li> </ul>
Cisco IOS XE Amsterdam 17.3.2a	<p>Introduced Cisco DNA Service for Bonjour support for the following:</p> <ul style="list-style-type: none"> <li>• Multilayer networks</li> <li>• Location grouping in wired networks</li> <li>• mDNS AP group in wireless networks</li> </ul>



Release	Modification
Cisco IOS XE Bengaluru 17.6.1	<p>Introduced support for the following features for Local Area Bonjour in Unicast Mode for LAN networks:</p> <ul style="list-style-type: none"><li>• FHRP-based Service Peer</li><li>• mDNS SSO</li></ul> <p>The following commands have been modified:</p> <ul style="list-style-type: none"><li>• The <b>active-query timer</b> command can be configured globally in Service-Peer for multilayer network and in SDG agent for routed access networks.</li><li>• The unit of measurement for the <b>active-query timer</b> is changed to minutes from seconds.</li><li>• The <b>service-mdns-query</b> command can be configured globally under a Layer 2 switch.</li><li>• The <b>match all</b> command can be configured under a service-list to accept all mDNS service-types.</li><li>• Configuring a service policy name using the <b>service-policy</b> <i>service-policy-name</i> command is optional. If no service policy is configured, then the default is used.</li></ul>

