



## **Cisco DNA Service for Bonjour Configuration Guide, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9200 Switches)**

**First Published:** 2020-11-27

### **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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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)

© 2020 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### **Cisco DNA Service for Bonjour Solution Overview 1**

- Solution Components 2
- Supported Platforms 3
- Cisco Wide Area Bonjour Supported Network Design 4
  - Traditional Wired and Wireless Networks 4
    - Wired Networks 5
    - Wireless Networks 7
  - 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

---

### CHAPTER 2

#### **Configuring Local Area Bonjour in Multicast DNS Mode for LAN and Wireless Networks 13**

- Configuring Local Area Bonjour Domain for 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
- Configuring Local Area Bonjour Domain for Wireless Networks 19
  - Enabling mDNS Gateway on the Device 20
  - Creating Custom Service Definition 22
  - Creating Service List 23
  - Creating Service Policy 24
- Verifying Local and Wide Area Bonjour Domains 25
  - Verifying Service Discovery Gateway 25

Verifying Controller 26

Verifying Local Area Bonjour for Wired and Wireless Networks 27

---

**CHAPTER 3**

**Feature History for Cisco DNA Service for Bonjour 29**

Feature History for DNA Service for Bonjour 29



## CHAPTER 1

# Cisco DNA Service for Bonjour Solution Overview

---

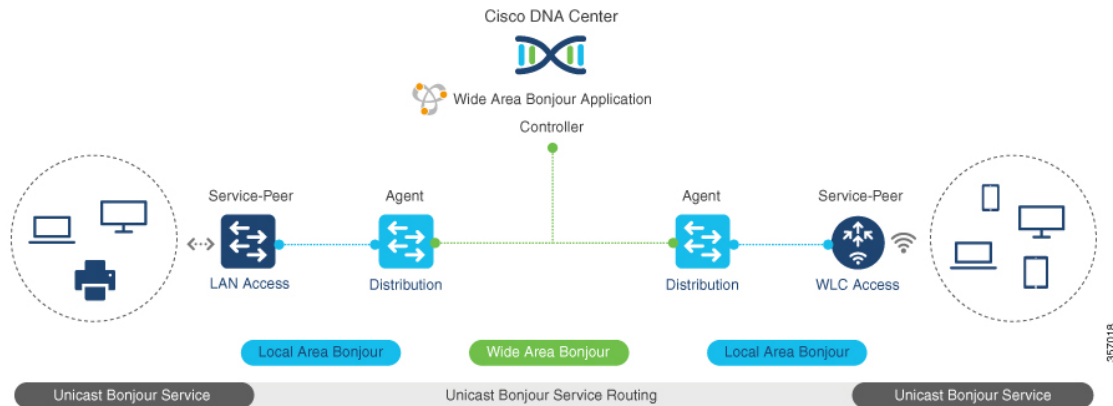
The Apple Bonjour protocol is a zero-configuration solution that simplifies network configuration and enables communication between connected devices, services, and applications. Using Bonjour, you can discover and use shared services with minimal intervention and configuration. Bonjour is designed for single Layer 2 domains that are ideal for small, flat, single-domain setups, such as home networks. The Cisco Wide Area 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 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 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 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 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, on page 2](#)
- [Supported Platforms, on page 3](#)
- [Cisco Wide Area Bonjour Supported Network Design, on page 4](#)

## 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 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 supporting 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 2.1.2
Cisco Wide Area Bonjour application	—	2.4.264.12003

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

**Table 2: Supported SDG Agents with Supported Licenses 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 Amsterdam 17.3.2a
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 Amsterdam 17.3.2a
Cisco Catalyst 9400 Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9500 Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Amsterdam 17.3.2a

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 Amsterdam 17.3.2a
Cisco Catalyst 9600 Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800 WLC	Service peer	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800-L WLC	Service peer	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Amsterdam 17.3.2a

## Cisco Wide Area Bonjour 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.

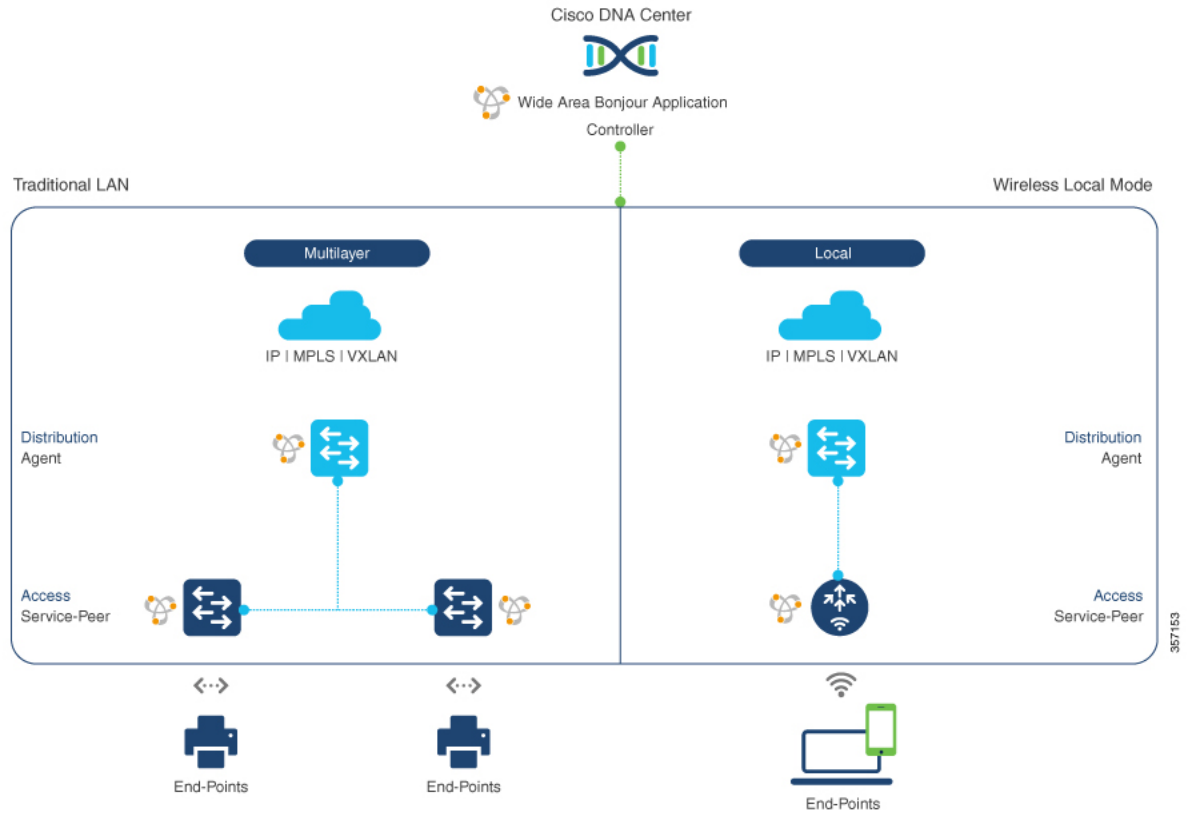
### Traditional Wired and Wireless Networks

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.



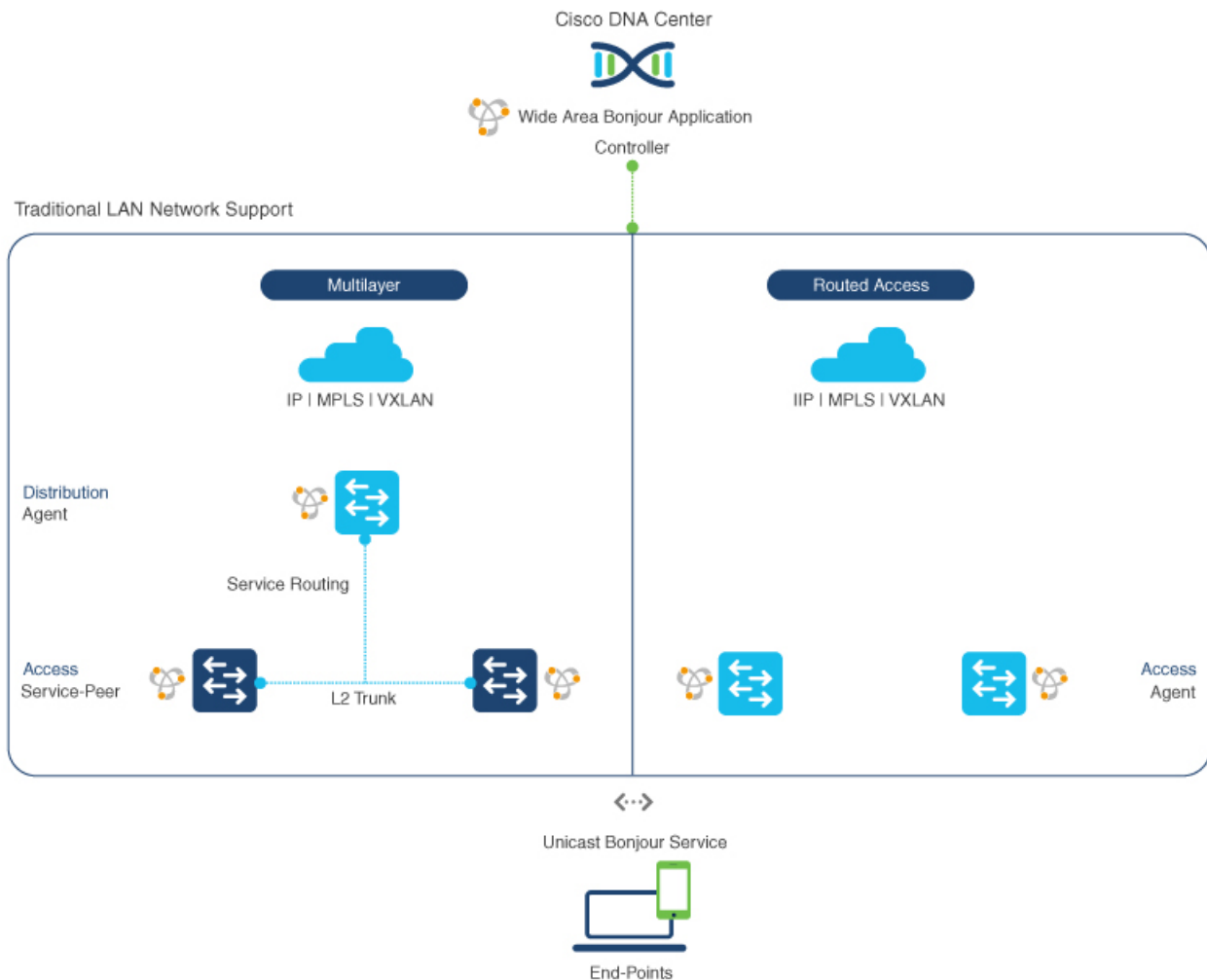
Figure 2: Enterprise Traditional LAN Network Design



## 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.

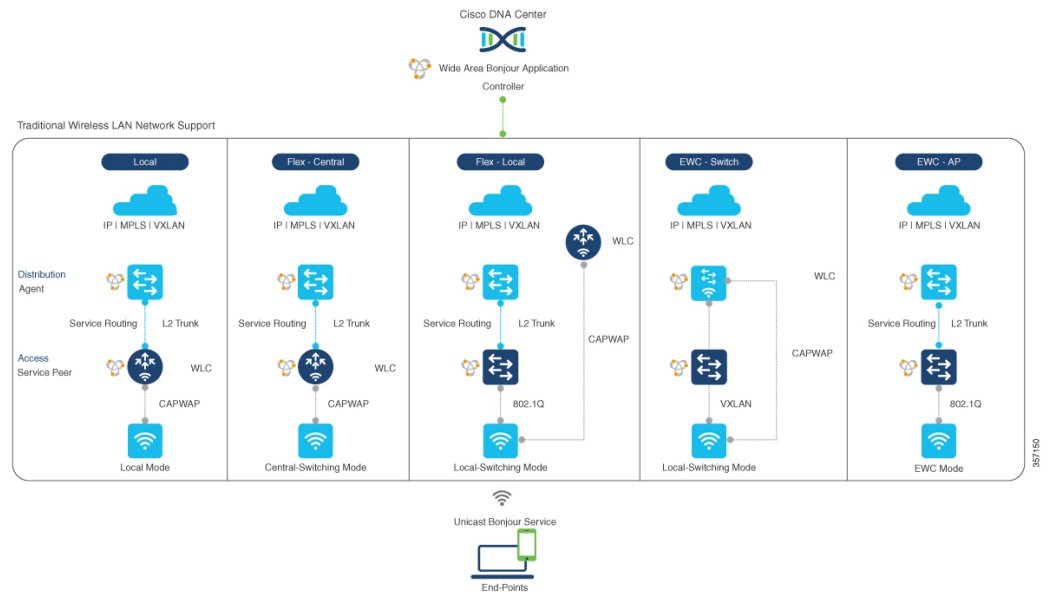
- **Multilayer LAN:** In this deployment mode, the Layer 2 access switch provides the first-hop Bonjour gateway function to locally attached wired endpoints. The Bonjour services and global discovery request are routed to the distribution layer systems that act as the IP gateway or SDG agent. There's 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**



- 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.

---

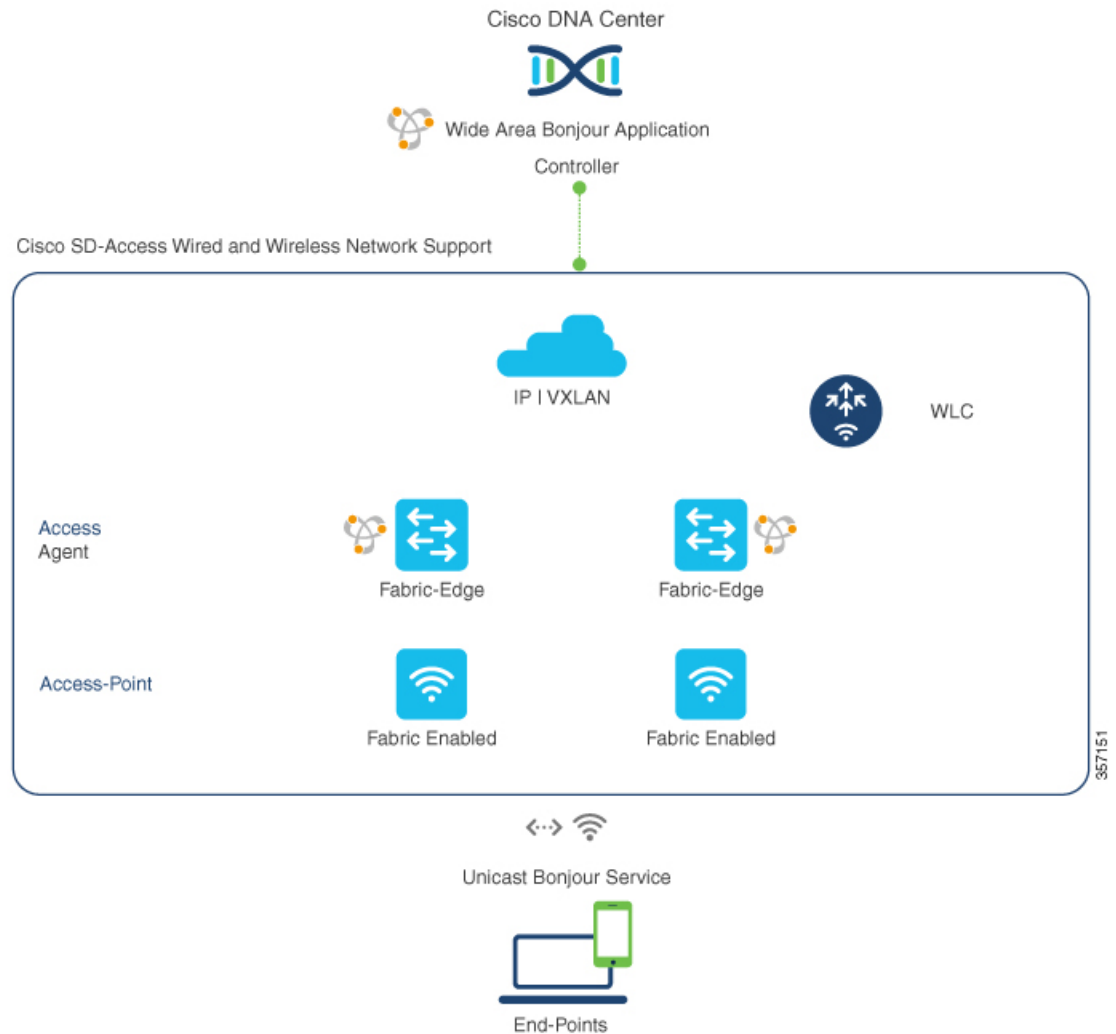
## Cisco SD-Access Wired and Wireless Networks

Cisco DNA Service for Bonjour is supported for Cisco SD-Access-enabled wired and wireless networks. The Cisco Wide Area Bonjour service routing for fabric-enabled wired and wireless networks 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 with respect to 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:

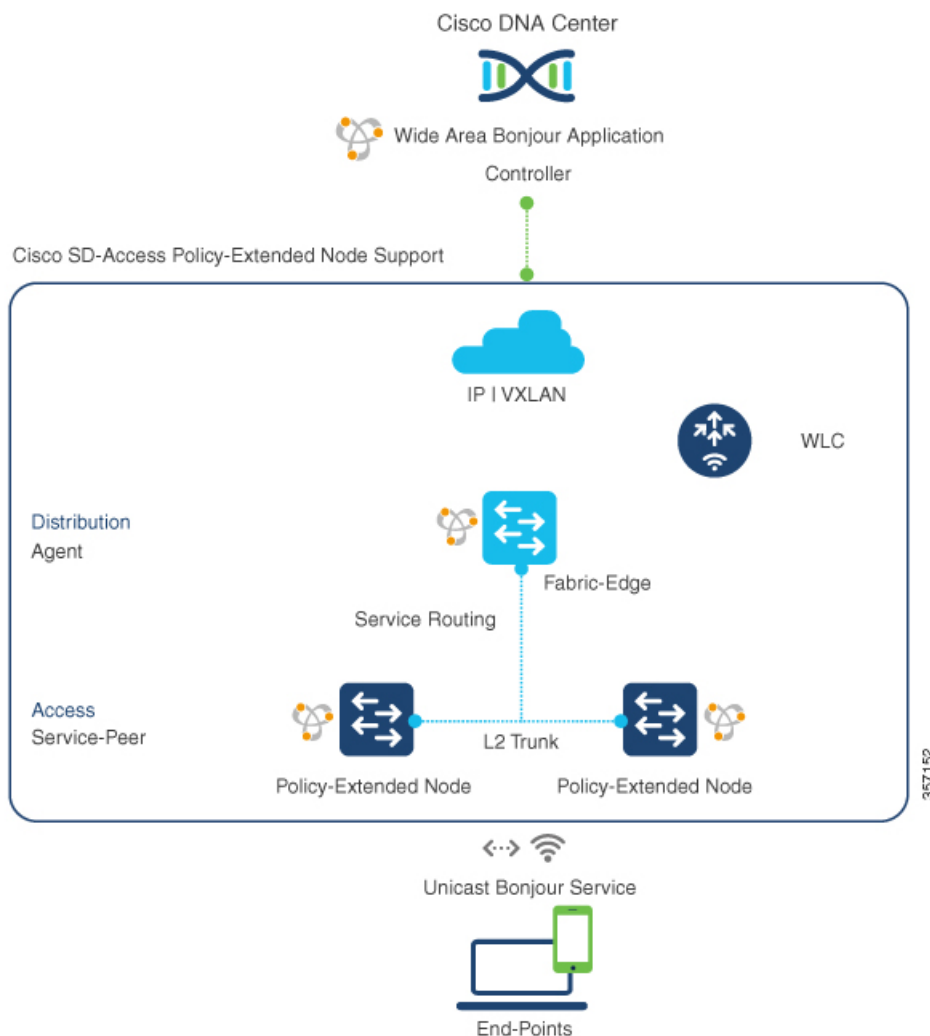
- **SDG agent:** The Layer 3 Fabric Edge switch in the access layer network is configured as the SDG agent. The mDNS gateway and Wide Area Bonjour service routing configuration is added only after SD-Access is configured.
- **Cisco DNA controller:** The Wide Area Bonjour application on Cisco DNA Center acts as the controller supporting 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

Figure 6: Fabric-Enabled Policy Extended Node



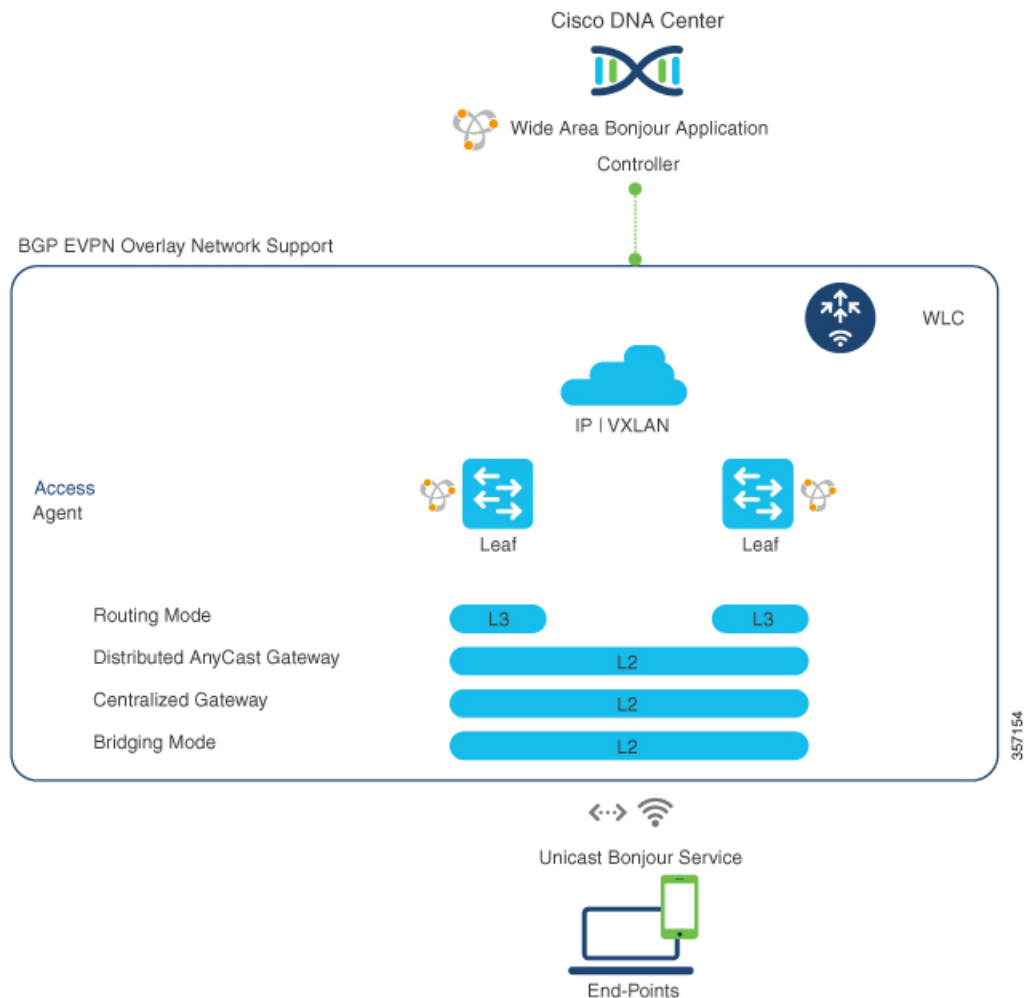
The security policy can be extended to Cisco Catalyst 9000 Series Switches at Layer 2 access with the Policy Extended Node (PEN) function in a Cisco SD-Access fabric network. The network security and mDNS service policy can be combined at the Layer 2 access PEN switch in a service-peer role combined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

## BGP EVPN Networks

The BGP EVPN-based enterprise network provides a flexible Layer 3 segmentation and Layer 2 extension overlay network. Cisco DNA Service for Bonjour supports end-to-end service routing over all common deployment models, eliminating mDNS flooding over Layer 2 extended EVPN VXLAN networks (symmetric and asymmetric 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**

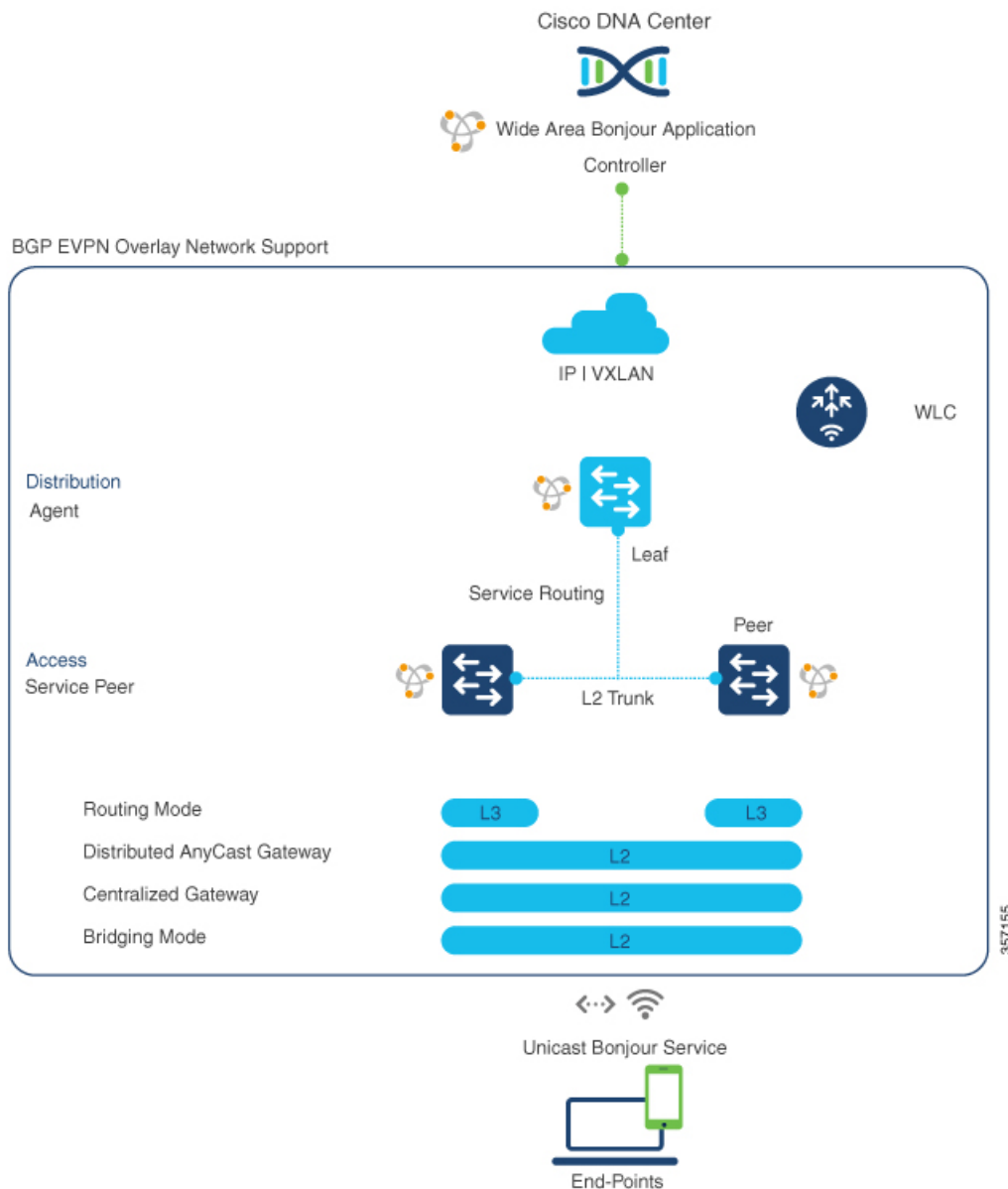


Cisco DNA Service for Bonjour supports Wide Area Bonjour service routing for BGP EVPN networks extended with Layer 2 service-peer network devices, such as a Cisco Catalyst switch or 9800 series WLC. The BGP EVPN leaf device in the distribution layer supports the SDG agent role for overlay service routing.

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 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 the Upstream BGP EVPN Leaf Switch**



For more information about BGP EVPN networks, see the [BGP EVPN VXLAN Configuration Guide, Cisco IOS XE Amsterdam 17.2.x \(Catalyst 9600 Switches\)](#).





## CHAPTER 2

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

- [Configuring Local Area Bonjour Domain for Wired Networks](#), on page 13
- [Configuring Local Area Bonjour Domain for Wireless Networks](#), on page 19
- [Verifying Local and Wide Area Bonjour Domains](#), on page 25

## Configuring Local Area Bonjour Domain for Wired Networks

### 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></ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <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 advertisements</li> <li>• <b>service-announcement-timer</b>: Configures advertisements announce timer periodicity</li> <li>• <b>service-query-count</b>: Configures maximum queries</li> <li>• <b>service-query-timer</b>: Configures query forward timer periodicity</li> <li>• <b>service-type-enumeration</b>: Configures service enumeration</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>, <b>service-query-timer</b>, and <b>service-type-enumeration</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, 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
<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**

	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.

	Command or Action	Purpose
<b>Step 3</b>	<b>mdns-sd service-list</b> <i>service-list-name</i> {in   out} <b>Example:</b> Device(config)# <b>mdns-sd service-list VLAN100-list in</b>	Configures mDNS service list.
<b>Step 4</b>	<b>match</b> <i>service-definition-name</i> [message-type {any   announcement   query}] <b>Example:</b> Device(config-mdns-sl-in)# <b>match PRINTER message-type announcement</b>	Matches the service to the message type. Here, service-definition-name 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 OFF, the applicable command syntax is: <b>match</b> <i>service-definition-name</i> .
<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>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
<b>Step 3</b>	<b>mdns-sd service-policy</b> <i>service-policy-name</i> <b>Example:</b> Device(config)# <code>mdns-sd service-policy mdns-policy1</code>	Configures mDNS service policy.
<b>Step 4</b>	<b>service-list</b> <i>service-list-name</i> { <b>in</b>   <b>out</b> } <b>Example:</b> Device(config-mdns-ser-pol)# <code>service-list VLAN100-list in</code> Device(config-mdns-ser-pol)# <code>service-list VLAN300-list out</code>	Configures service lists for IN and OUT directions.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> Device(config-mdns-ser-pol)# <code>exit</code>	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> <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>interface</b> <i>interface-name</i> <b>Example:</b> Device(config)# <code>interface Vlan 601</code>	Enters interface mDNS configuration mode and enables interface configuration.
<b>Step 4</b>	<b>mdns-sd gateway</b> <b>Example:</b> Device(config-if)# <code>mdns-sd gateway</code>	Configures mDNS gateway on the interface. Enter the following commands in the interface mDNS gateway configuration mode to enable the respective functionalities: <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 120 seconds.</li> </ul>

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

# Configuring Local Area Bonjour Domain 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.

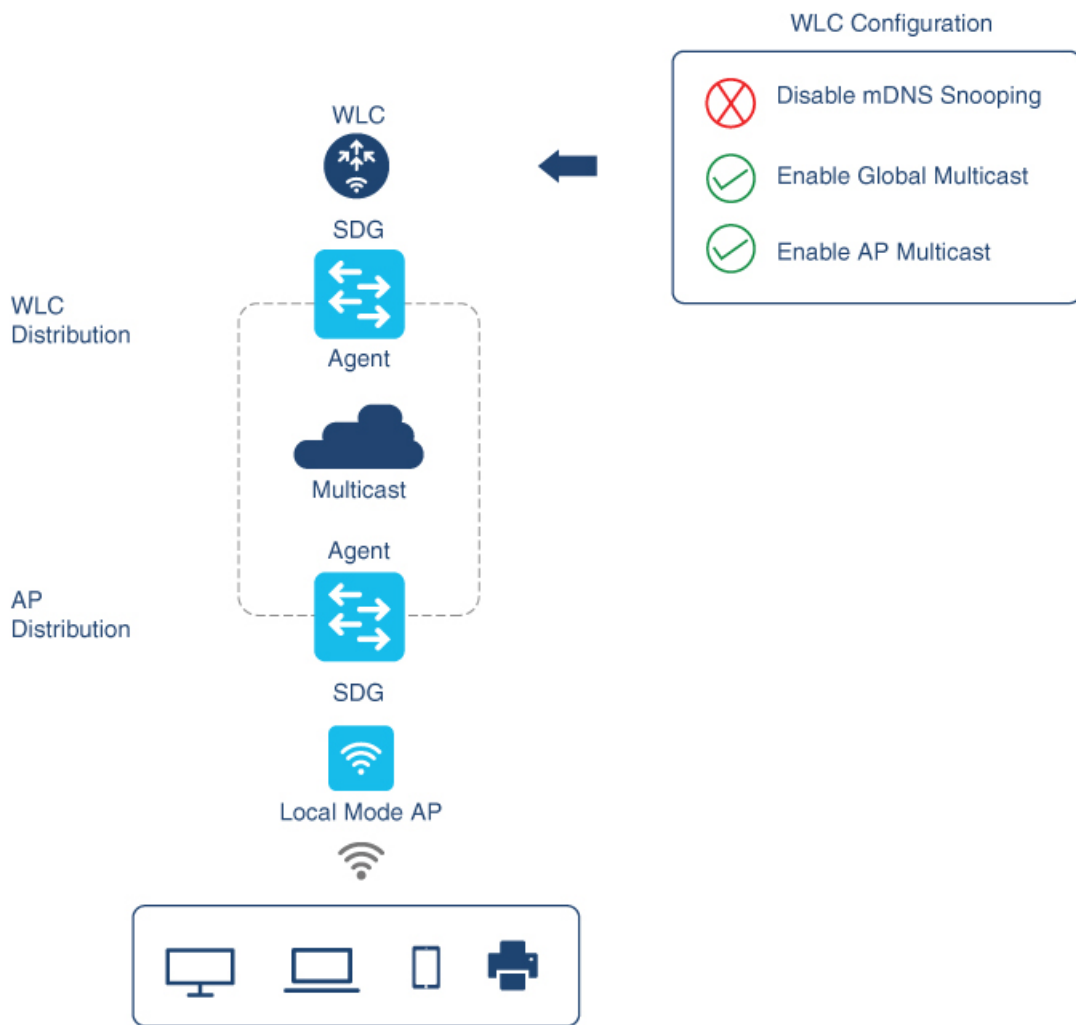
The Bonjour protocol operates on service announcements and queries. Each query or advertisement is sent to the Bonjour multicast address ipv4 224.0.0.251 (ipv6 FF02::FB). This protocol uses mDNS on UDP port 5353.

The address used by the Bonjour protocol is link-local multicast address and therefore is only forwarded to the local L2 network. As, multicast DNS is limited to an L2 domain for a client to discover a service it has to be part of the same L2 domain, This is not always possible in any large scale deployment or enterprise.

In order to address this issue, the Cisco Catalyst 9800 Series Wireless Controller acts as a Bonjour Gateway. The controller then listens for Bonjour services, caches these Bonjour advertisements (AirPlay, AirPrint, and so on) from the source or host. For example, Apple TV responds back to Bonjour clients when asked or requested for a service. This way you can have sources and clients in different subnets.

By default, the mDNS gateway is disabled on the controller. To enable mDNS gateway functionality, you must explicitly configure mDNS gateway using CLI or Web UI.

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



3563366

The Cisco WLC and Access Points by default prevents forwarding 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 unique Multicast Group to advertise in 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 does not require any Multicast requirements on Wireless Client VLAN; thus, it is optional and applicable only for other Layer 3 Multicast applications.

The core network must be configured with appropriate Multicast routing allowing AP’s to join WLC Multicast Group. The Multicast configuration must be enabled on Cisco WLC management VLAN and on Cisco Access Point of their own respective distribution layer switch.

## Enabling mDNS Gateway on the Device

To configure mDNS on the device, 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 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 advertisements</li> <li>• <b>service-announcement-timer</b>: Configures advertisements announce timer periodicity</li> <li>• <b>service-query-count</b>: Configures maximum queries</li> <li>• <b>service-query-timer</b>: Configures query forward timer periodicity</li> <li>• <b>service-type-enumeration</b>: Configures service enumeration</li> </ul>

	Command or Action	Purpose
		<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>, <b>service-query-timer</b>, and <b>service-type-enumeration</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>	<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, 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<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.  <p><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.</p>
<b>Step 4</b>	<b>service-type</b> <i>string</i>  <b>Example:</b> Device(config-mdns-ser-def)# service-type _custom1._tcp.local	Configures mDNS service type.

	Command or Action	Purpose
<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)# 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

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	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)# mdns-sd service-list VLAN100-list in	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)# match PRINTER message-type announcement	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 OFF, the applicable command syntax is: <b>match <i>service-definition-name</i></b> .

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

# Verifying Local and Wide Area Bonjour Domains

## Verifying Service Discovery Gateway

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  Vl200

```

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** [**interface** *interface-name*] command.

```

Global mDNS Gateway
=====
mDNS Gateway           : Enabled
Rate Limit             : 60 PPS (default)
AirPrint Helper        : Disabled

Interface : Vlan601
=====
mDNS Gateway           : Enabled
mDNS Service Policy    : policy1
Active Query           : Enabled
                        : Periodicity 60 Seconds
Transport Type         : Both IPv4 & IPv6
Service Instance Suffix : ghalwasi

```

```

mDNS Query Type           : ALL

Interface : Vlan602
=====
mDNS Gateway           : Enabled
mDNS Service Policy    : int602
Active Query           : Enabled
                        : Periodicity 100 Seconds

Transport Type         : Both IPv4 & IPv6
Service Instance Suffix : 602
mDNS Query Type       : ALL

```

## Verifying Controller

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 for Wired and Wireless Networks

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

```

mdns-sd gateway
  rate-limit 100
  service-query-count 100
  service-announcement-count 100

mdns-sd service-definition custom1
  service-type _airplay._tcp.local
  service-type _raop._tcp.local
  service-type _ipp._tcp.local
  service-type _afpovertcp._tcp.local
  service-type _nfs._tcp.local
  service-type _ssh._tcp.local
  service-type _dpap._tcp.local
  service-type _daap._tcp.local

```

```
service-type _ichat._tcp.local
service-type _presence._tcp.local
service-type _http._tcp.local
service-type _ipps._tcp.local
service-type _printer._tcp.local
service-type _smb._tcp.local
service-type _ftp._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 APIC-EM
controller-address 99.99.99.10
controller-port 9991
controller-service-policy policy1 OUT
controller-source-interface Loopback0
```





## CHAPTER 3

# Feature History for Cisco DNA Service for Bonjour

- [Feature History for DNA Service for Bonjour, on page 29](#)

## Feature History for 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 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 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 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 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 and Wide Area Bonjour was introduced on Cisco Catalyst 9200 Series Switches.