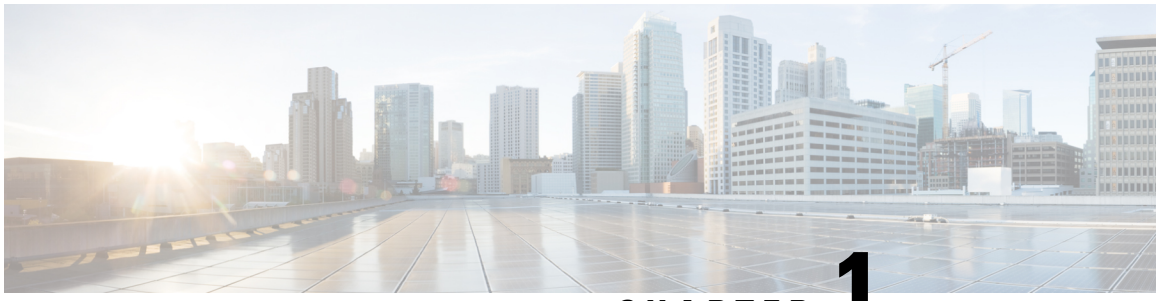
Cisco DNA Service for Bonjour Configuration Guide, Cisco IOS XE Cupertino 17.8.x (Catalyst 9600 Switches)

First Published: 2022-04-09

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

CONTENTS



CHAPTER 1

Cisco DNA Service for Bonjour Solution Overview

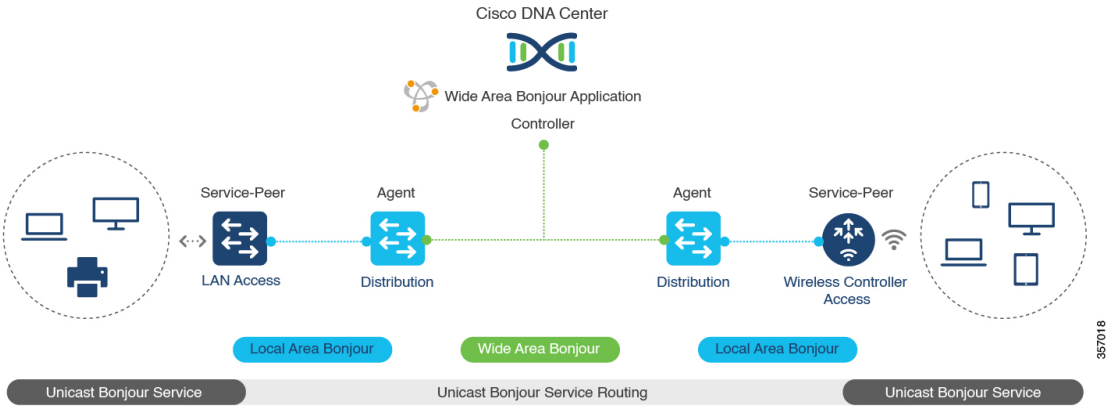
About the Cisco DNA Service for Bonjour Solution

The Apple Bonjour protocol is a zero-configuration solution that simplifies rich services and enables intuitive experience between connected devices, services, and applications. Using Bonjour, you can discover and use IT-managed, peer-to-peer, audio and video, or Internet of Things (IoT) services with minimal intervention and technical knowledge. Bonjour is originally designed for single Layer 2 small to mid-size networks, such as home or branch networks. The Cisco DNA Service for Bonjour solution eliminates the single Layer 2 domain constraint and expands the matrix 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, Cisco Nexus 9300 Series Switches, and Cisco Catalyst 9800 Series Wireless Controller 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 on Cisco DNA Center enables mDNS service routing to advertise and discover services across enterprise-grade wired and wireless networks. 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.

The following figure illustrates how the Cisco Wide Area Bonjour application operates across two integrated service-routing domains.

Figure 1: Cisco Wide Area Bonjour Solution Architecture



- **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 the Layer 2 unicast address enables flood-free LAN and wireless networks. Cisco Catalyst 9000 Series Switches and Cisco Catalyst 9800 Series Wireless Controller in Layer 2 mode introduce a new service-peer role, replacing the classic flood-n-learn, for new unicast-based service routing support in the network. The service-peer switch and wireless 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 and Cisco Nexus 9300 Series 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. The SDG agents route locally discovered services based on the export policy.

Note The classic Layer 2 multicast flood-n-learn continues to be supported on wired and wireless networks with certain restrictions to support enhanced security and location-based policy enforcement. The Cisco Catalyst and Cisco Nexus 9300 Series Switches at Layer 3 boundary function as an SDG to discover and distribute services between local wired or wireless VLANs based on applied policies.

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**: Cisco Catalyst Switches and Cisco Wireless Controllers 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 Catalyst SDG agent in the distribution layer.

Note Cisco Nexus 9300 Series Switches don't support unicast-based service routing with downstream Layer 2 access network devices.

- **Cisco SDG Agent**: Cisco Catalyst and Cisco Nexus 9300 Series Switches function as an SDG agent and communicate 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 wireless controller, or local Layer 2 networks, 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 2.3.2.3
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 License and Software Requirements

Supported Platform	Supported Role	Local Area SDG	Wide Area SDG	Minimum Software
Cisco Catalyst 9200 Series Switches	SDG agent	Cisco DNA Advantage	Unsupported	Cisco IOS XE Bengaluru 17.6.2
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 17.6.2

Supported Platform	Supported Role	Local Area SDG	Wide Area SDG	Minimum Software
Cisco Catalyst 9400 Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9500 Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9500 High Performance Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9600 Series Switches	Service peer SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9800 Wireless Controller	Service peer	Cisco DNA Advantage	Unsupported	Cisco IOS XE Bengaluru 17.6.2
Cisco Catalyst 9800-L Wireless Controller	Service peer	Cisco DNA Advantage	Unsupported	Cisco IOS XE Bengaluru 17.6.2
Cisco Nexus 9300 Series Switches	SDG agent	Cisco DNA Advantage	Cisco DNA Advantage	Cisco NX-OS Release 10.2(3)F

Supported Network Design

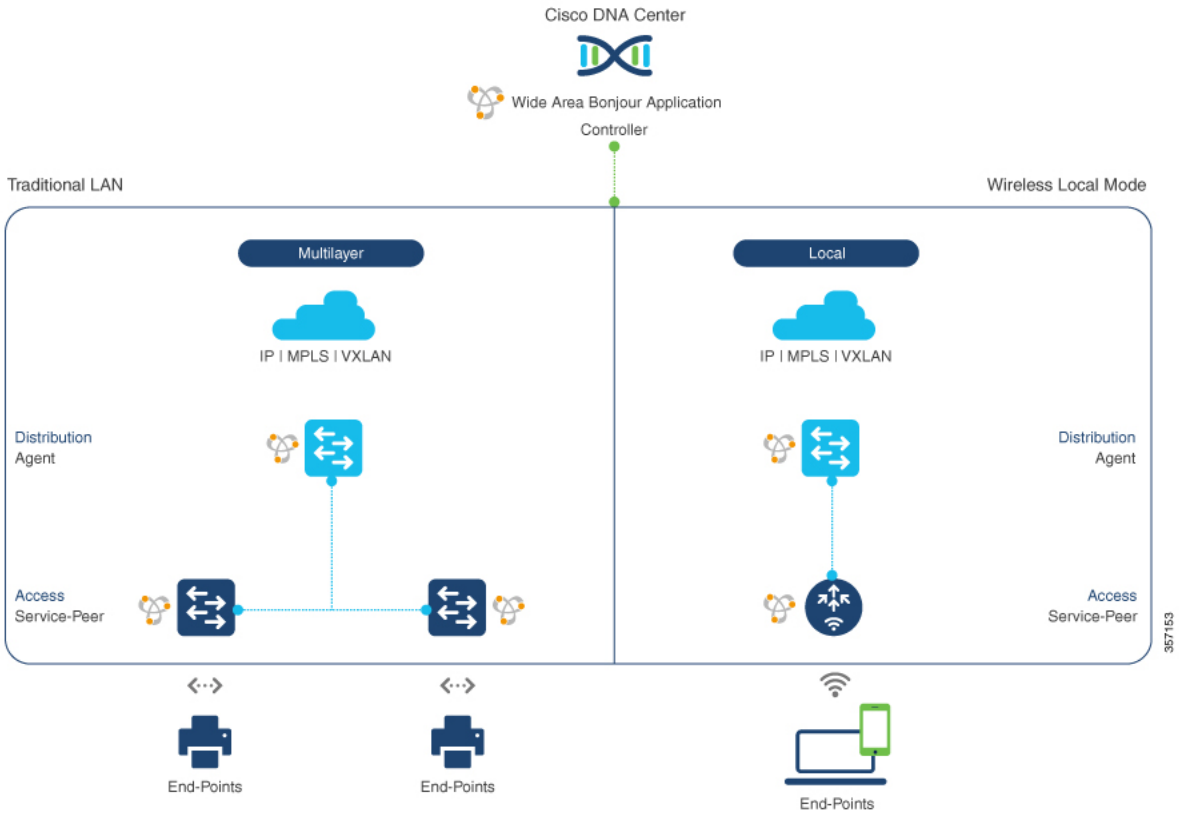
The Cisco DNA Service for Bonjour supports a broad range of enterprise-grade networks. The end-to-end unicast-based Bonjour service routing is supported on traditional, Cisco SD-Access, and BGP EVPN-enabled wired and wireless networks.

Traditional Wired and Wireless Networks

Traditional networks are classic Layer 2 or Layer 3 networks for 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 and replace flood-n-learn-based deployment with a unicast mode-based solution.

The following figure illustrates traditional LAN and central-switching wireless local mode network designs that are commonly deployed in an enterprise.

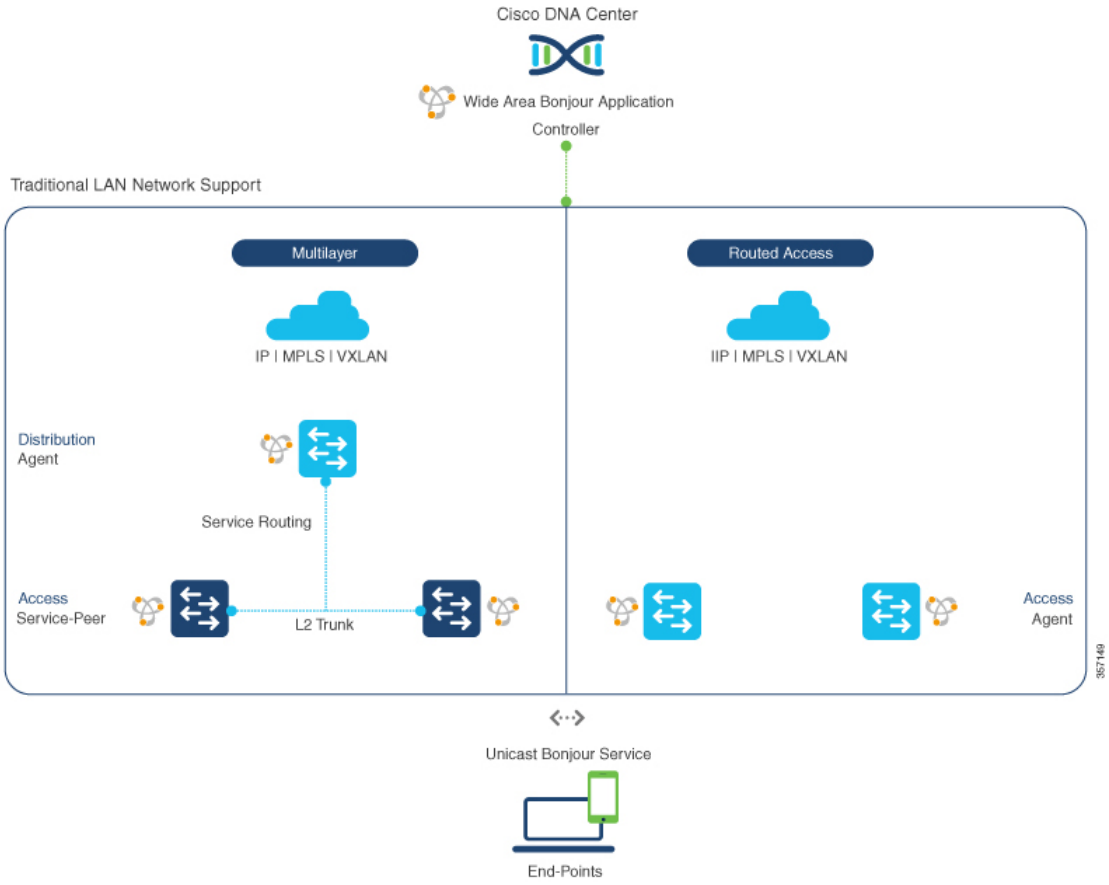
Figure 2: Enterprise Traditional LAN and Wireless Local Mode Network Design



Wired Networks

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

Figure 3: Enterprise Wired Multilayer and Routed Access Network Design



The Cisco Catalyst or Cisco Nexus 9300 Series Switches in SDG agent role that provide Bonjour gateway functions are typically IP gateways for wired endpoints that could reside in the distribution layer in multilayer network designs, or in the access layer in Layer 3 routed access network designs:

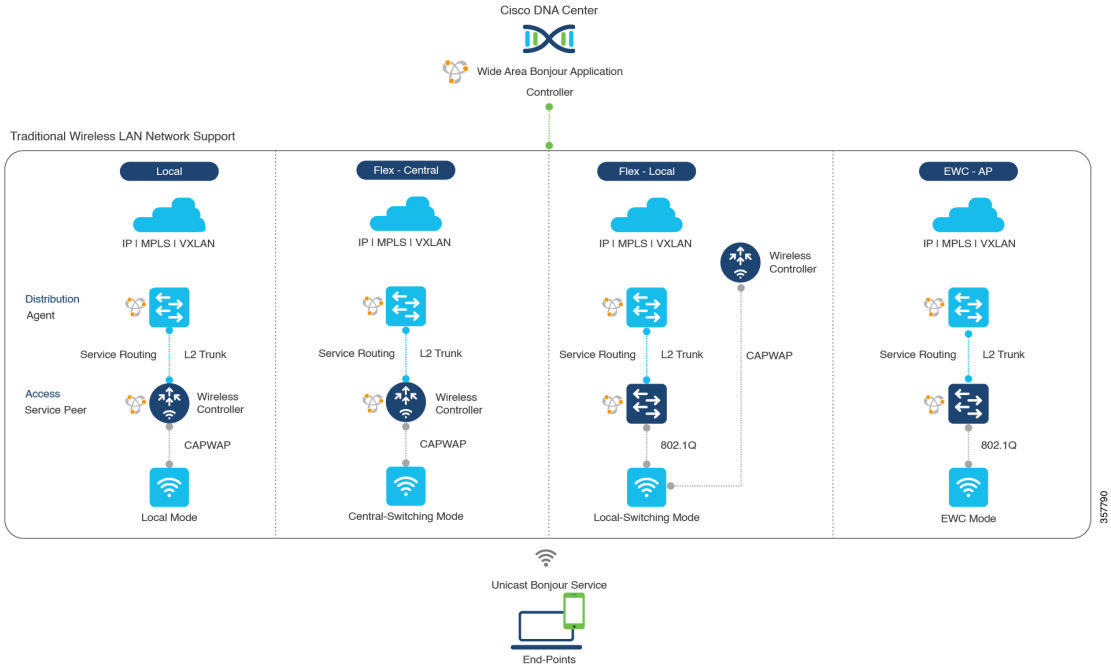
- **Multilayer LAN—Unicast Mode**: In this deployment mode, the Layer 2 access switch provides the first-hop mDNS gateway function to locally attached wired endpoints. In unicast mode, the mDNS services are routed to the distribution layer systems providing IP gateway and SDG agent mode. The policy-based service routing between the SDG agents is performed by the Cisco DNA Center controller.
- **Multilayer LAN—Flood-n-Learn Mode**: In this deployment mode, the Layer 2 access switch or wireless controller are in mDNS passthrough modes with the Cisco Catalyst or Cisco Nexus 9300 Series Switches operating in the SDG agent mode. The mDNS gateway function at distribution layer in a network enables inter-VLAN mDNS local proxy. It also builds stateful Wide Area Bonjour unicast service routing with the Cisco DNA Center to discover or distribute mDNS services beyond a single IP gateway.
- **Routed Access**: In this deployment mode, the first-hop Cisco Catalyst or Cisco Nexus 9300 Series 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 extends the single wireless controller mDNS gateway function into the Wide Area Bonjour solution. The mDNS gateway on Cisco Catalyst 9800 Series Wireless Controller can be deployed in an enhanced mode as a service peer. In this mode, the wireless controller builds unicast service routing with an upstream Cisco Catalyst gateway switch for end-to-end mDNS service discovery. It replaces the classic flood-n-learn mDNS services from wired network using mDNS AP or other methods.

The following figure shows the supported traditional wireless LAN network designs that are commonly deployed in an enterprise. Based on the wireless network design, the mDNS gateway function may be on the wireless controller, or first-hop Layer 2 or Layer 3 Ethernet switch of an Access Point in local-switching mode.

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 the central switching wireless deployment mode, the m-DNS traffic from local mode Cisco access points is terminated on the Cisco Catalyst 9800 Series Wireless Controller. The Cisco Catalyst 9800 Series Wireless Controller extends the mDNS gateway function to the new service peer mode. The wireless controller can discover and distribute services to local wireless users and perform unicast service routing over a wireless management interface to the upstream Cisco Catalyst Switch in the distribution layer, which acts as the IP gateway and the SDG agent.
- **FlexConnect—Central**: The mDNS gateway function for Cisco access point in FlexConnect central switch SSID functions consistently as described in **Local Mode**. The new extended mDNS gateway mode on the Cisco Wireless Controller and upstream service routing with SDG agent operate consistently to discover services across network based on policies and locations.
- **FlexConnect—Local**: In FlexConnect local switching mode, the Layer 2 access switch in mDNS gateway service peer mode 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 and enable

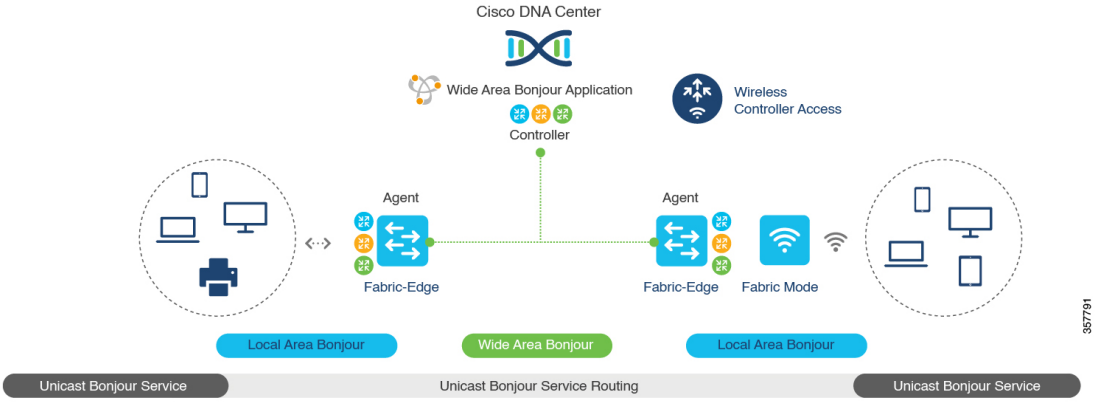
mDNS service-routing across all Layer 2 ethernet switches to support unicast-based service routing to LAN and wireless LAN user groups.

- **Embedded Wireless Controller—Access Point**: The Layer 2 access switch in service peer mode provides unified mDNS gateway function to wired and wireless endpoints associated with Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Series Access Points. 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.

Cisco SD-Access Wired and Wireless Networks

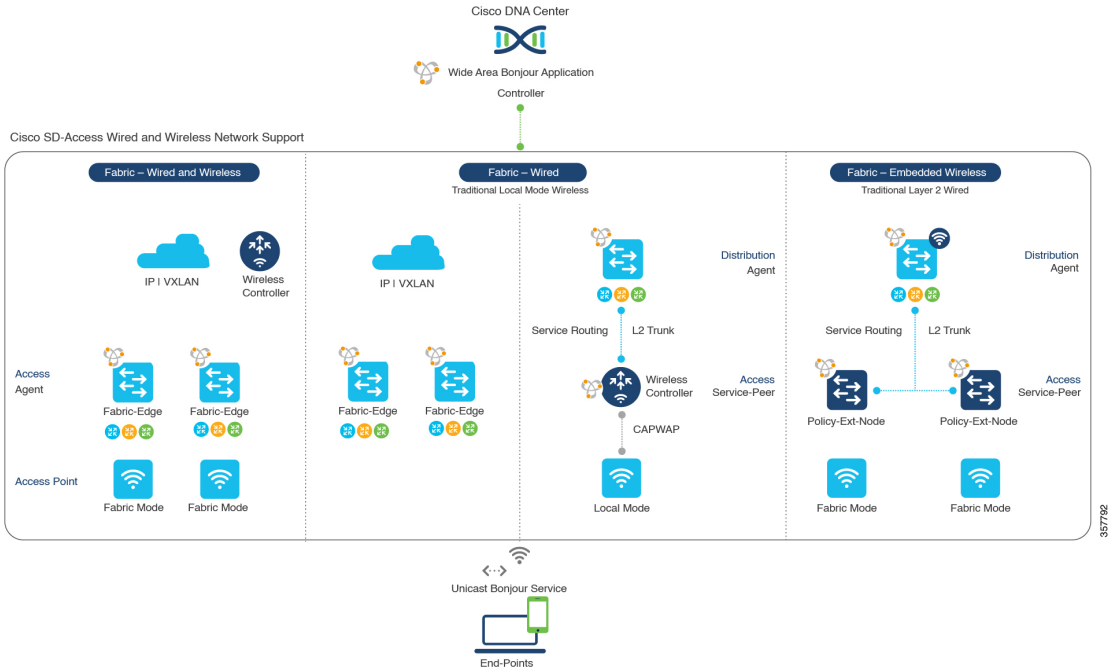
Cisco SD-Access-enabled wired and wireless networks support Cisco DNA Service for Bonjour across fabric networks. The Cisco Catalyst 9000 Series Switches support VRF-aware Wide Area Bonjour service routing to provide secure and segmented mDNS service discovery and distribution management for virtual networks. The VRF-aware unicast service routing eliminates the need to extend Layer 2 flooding, and improves the scale and performance of the fabric core network and endpoints.

Figure 5: Cisco SD-Access Wired and Wireless Network Design



Cisco SD-Access supports flexible wired and wireless network design alternatives to manage fully distributed, integrated, and backward-compatible traditional network infrastructure. Wide Area Bonjour service routing is supported in all network designs providing intuitive user experience. The following figure illustrates the various SD-Access enabled wired and wireless network design alternatives.

Figure 6: Cisco SD-Access Wired and Wireless Network Design Alternatives



The Cisco DNA Service for Bonjour for SD-Access enabled wired and fabric, or traditional mode-wireless networks use two-tier service routing providing end-to-end unicast-based mDNS solution. Based on the network design, each solution component is enabled in a unique role to support the Wide Area Bonjour domain:

- **Fabric Edge SDG Agent**: The Layer 3 Cisco Catalyst Fabric Edge switch in the access layer configured as SDG agent provides unicast-based mDNS gateway function to the locally attached wired and wireless endpoints. The VRF-aware mDNS service policy provides network service security and segmentation in a virtual network environment. The mDNS services can be locally distributed and routed through centralized Cisco DNA Center.
- **Policy Extended Node**: The Layer 2 Cisco Catalyst access layer switch enables first-hop mDNS gateway function without flooding across the Layer 2 broadcast domain. The unicast-based service routing with upstream Fabric Edge switch in the distribution layer enables mDNS service routing within the same Layer 2 network block. It can also perform remote service discovery and distribution from centralized Cisco DNA Center.
- **Cisco Wireless Controller**: Based on the following wireless deployment modes, Cisco Wireless Controller supports unique function to enable mDNS service routing in Cisco SD-Access enabled network:
  - **Fabric-Enabled Wireless**: Cisco Wireless Controller doesn't require any mDNS gateway capability to be enabled in distributed fabric-enabled wireless deployments.
  - **Local Mode Wireless**: As Cisco Wireless Controller provides central control and data plane termination, it provides mDNS gateway in service peer mode for wireless endpoints. The wireless controller provides mDNS gateway between locally associated wireless clients. The wireless controller builds service routing with upstream SDG agent Catalyst switch providing IP gateway and service routing function for wireless endpoints.
  - **Embedded Wireless Controller—Switch**: The Cisco Embedded Wireless Controller solution enables the lightweight integrated wireless controller function within the Cisco Catalyst 9300 Series

Switch. The Cisco Catalyst switches in the distribution layer function as SDG agents to the wired and wireless endpoints. The SDG agent in the distribution layer provides unicast service routing across all wireless access points and Layer 2 service peer switches without mDNS flooding.

- **Cisco DNA Center Controller**: The Cisco Wide Area Bonjour application on Cisco DNA Center supports policy and location-based service discovery, and distribution between network-wide distributed Fabric Edge switches in SDG agent mode.

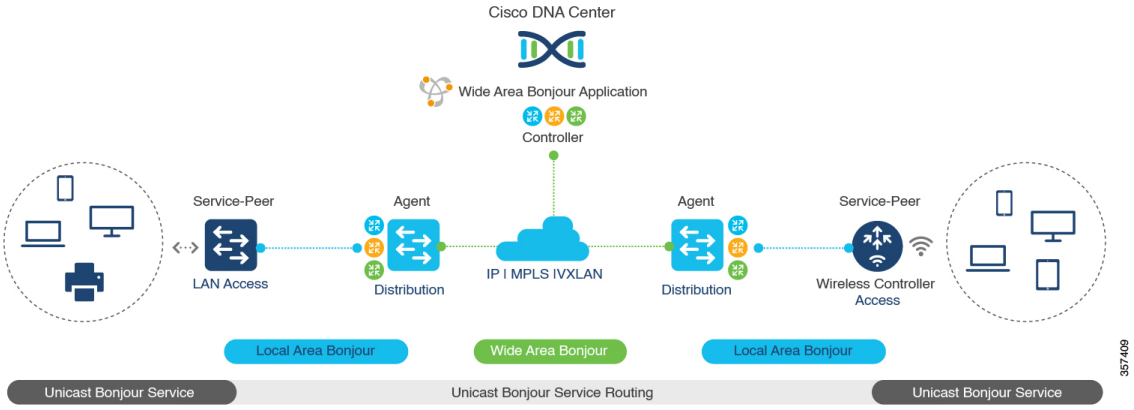
The Wide Area Bonjour communication between the SDG agent and controller takes place through the network underlay. Based on policies, the SDG agent forwards the endpoint announcements or queries to the Cisco DNA Center. After discovering a service, the endpoints can establish direct unicast communication through the fabric overlay in the same virtual network. The inter-virtual network unicast communication takes place through the Fusion router or external Firewall system. This communication is subject to the configured overlay IP routing and Security Group Tag (SGT) policies.

BGP EVPN Networks

The BGP EVPN-based technology provides a flexible Layer 3 segmentation and Layer 2 extension overlay network. The VRF and EVPN VXLAN-aware Wide Area Bonjour service routing provides secure and segmented mDNS service solution. The overlay networks eliminate mDNS flooding over EVPN-enabled Layer 2 extended networks and solve the service reachability challenges for Layer 3 segmented routed networks in the fabric.

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

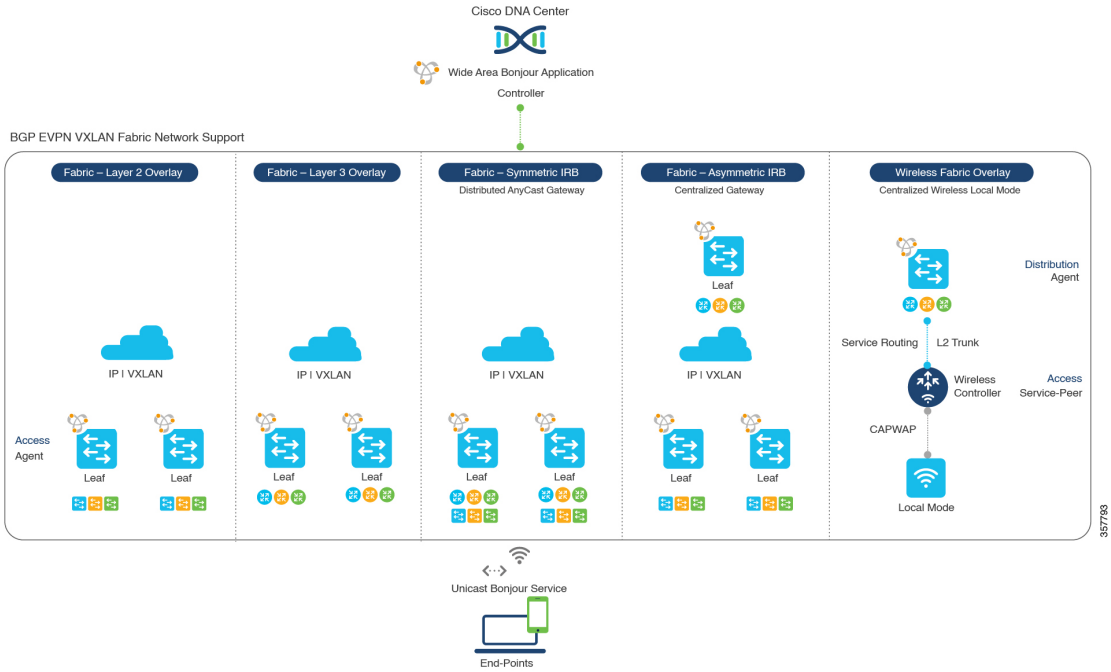
Figure 7: Overlay Bonjour Service for a BGP EVPN-Enabled Enterprise Network



Cisco DNA Service for Bonjour supports all the industry-standard overlay network designs enabling end-to-end unicast-based mDNS service routing, and preventing flooding and service boundary limitation across wired and wireless networks.

The following figure illustrates the various BGP EVPN VXLAN reference overlay network design alternatives. This network design enables end-to-end mDNS service discovery and distribution based on overlay network policies.

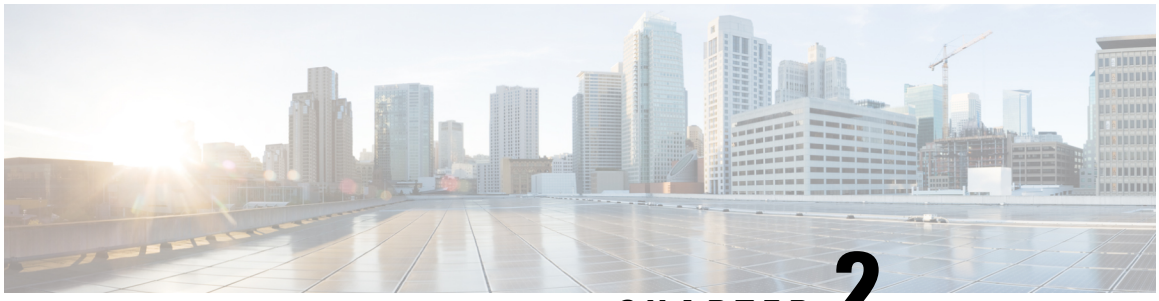
Figure 8: BGP EVPN VXLAN Wired and Wireless Design Alternatives



The Cisco Catalyst and Cisco Nexus 9000 Series Switches can be deployed in Layer 2 or Layer 3 leaf roles supporting mDNS service routing for a broad range of overlay networks. In any role, the mDNS communication is limited locally and supports end-to-end unicast-based service routing across Wide Area Bonjour domain:

- **Layer 2 Leaf SDG Agent**: The Cisco Catalyst or Cisco Nexus switches can be deployed as Layer 2 leaf supporting end-to-end bridged network with IP gateway within or beyond BGP EVPN VXLAN fabric network. By default, the mDNS is flooded as Broadcast, Unknown Unicast, Multicast (BUM) over the fabric-enabled core network. This mDNS flooding may impact network performance and security. The Layer 2 leaf, enabled as SDG agent, prevents mDNS flooding over VXLAN and supports unicast-based service routing.
- **Layer 3 Leaf SDG Agent**: The Cisco Catalyst or Cisco Nexus switches can be deployed as SDG agent supporting Layer 3 overlay network in BGP EVPN VXLAN fabric. The IP gateway and mDNS service boundary is terminated at the SDG agent switches and remote services can be discovered or distributed through centralized Cisco DNA Center.
- **Local Mode Wireless**: The centralized wireless local mode network can be terminated within or outside the EVPN VXLAN fabric domain to retain network segmentation and service discovery for wireless endpoints. The Cisco Catalyst 9800 Series Wireless Controller in service peer mode can build unicast service routing with distribution layer IP and SDG agent Cisco Catalyst switch to discover services from BGP EVPN VXLAN fabric overlay network.
- **Cisco DNA Center**: Cisco DNA Center supports Wide Area Bonjour capability to dynamically discover and distribute mDNS services based on Layer 2 or Layer 3 Virtual Network ID (VNID) policies to route the mDNS services between SDG agent switches in the network.

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

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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	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
		• **air-print-helper**: Enables IOS devices like iPADs to discover and use older printers that support Bonjour • **cache-memory-max**: Configures the percentage memory for cache • **ingress-client**: Configures Ingress Client Packet Tuners • **rate-limit**: Enables rate limiting of incoming mDNS packets • **service-announcement-count**: Configures maximum service advertisement count • **service-announcement-timer**: Configures advertisements announce timer periodicity • **service-query-count**: Configures maximum query count • **service-query-timer**: Configures query forward timer periodicity **Note** For **cache-memory-max**, **ingress-client**, **rate-limit**, **service-announcement-count**, **service-announcement-timer**, **service-query-count**, and **service-query-timer** commands, you can retain the default value of the respective parameter for general deployments. Configure a different value, if required, for a specific deployment.
Step 4	**exit** **Example:** `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	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-definition** *service-definition-name* **Example:** `Device(config)# mdns-sd service-definition CUSTOM1`	Configures mDNS service definition. **Note** 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	**service-type** *string* **Example:** `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	**exit** **Example:** `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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**mdns-sd service-list** *service-list-name* {**in** | **out**} **Example:** `Device(config)# mdns-sd service-list VLAN100-list in`	Configures mDNS service list.
Step 4	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] **Example:** `Device(config-mdns-sl-in)# match PRINTER-IPPS message-type announcement`	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. **Note** 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: **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]. If the mDNS service list is set to OUT, the applicable command syntax is: **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] [**location-filter** *location-filter-name*] [**source-interface** {*mDNS-VLAN-number* | *mDNS-VLAN-range*}].
Step 5	**exit** **Example:** `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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Configures mDNS service policy.

Step 4	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`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.

Step 5	**exit** **Example:** `Device(config-mdns-ser-pol)# exit`	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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-name* **Example:** `Device(config)# interface Vlan 601`	Enters interface mDNS configuration mode and enables interface configuration.

	Command or Action	Purpose
Step 4	**mdns-sd gateway** **Example:** `Device(config-if)# mdns-sd gateway`	Configures mDNS gateway on the interface. Enter the following commands in the interface mDNS gateway configuration mode to enable the respective functionalities: • **active-query**: 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. **Note** 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. • **service-instance-suffix**(Optional) : Appends the service instance suffix to any announced service name that is forwarded to the controller. • **service-mdns-query** [**ptr** | **all**]: Configures mDNS query request message processing for the specified query types. If the **service-mdns-query** 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 **service-mdns-query ptr** command. • **service-policy** *policy-name*: 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. **Note** Service policies can only be attached at interface level.

	Command or Action	Purpose
		• **transport** [**all** | **ipv4** | **ipv6**] (Optional): Configures BCP parameter. It is recommended to use **transport ipv4** command, except in those networks where the Bonjour clients send only IPv6 announcements and queries.
Step 5	**exit** **Example:** `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.

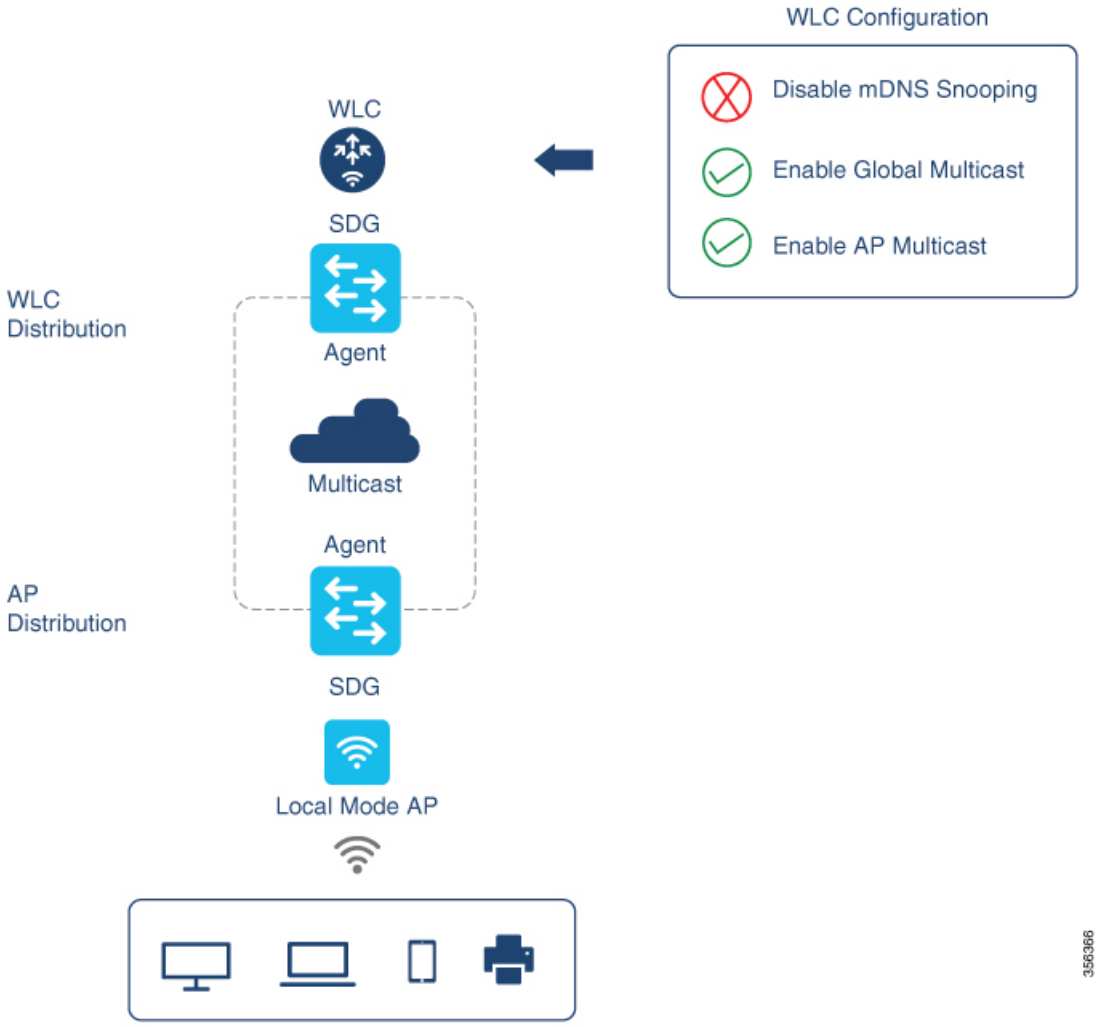
The Bonjour protocol operates on service announcements and queries. Each query or advertisement is sent to the mDNS IPv4 address 224.0.0.251 and IPv6 address FF02::FB. The mDNS messages are carried over well-known industry standard UDP port 5353, over both Layer 3 transport types.

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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	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: • **air-print-helper**: Enables IOS devices like iPADs to discover and use older printers that support Bonjour • **cache-memory-max**: Configures the percentage memory for cache • **ingress-client**: Configures Ingress Client Packet Tuners • **rate-limit**: Enables rate limiting of incoming mDNS packets • **service-announcement-count**: Configures maximum service advertisement count • **service-announcement-timer**: Configures advertisements announce timer periodicity • **service-query-count**: Configures maximum query count • **service-query-timer**: Configures query forward timer periodicity **Note** For **cache-memory-max**, **ingress-client**, **rate-limit**, **service-announcement-count**, **service-announcement-timer**, **service-query-count**, and **service-query-timer** commands, you can retain the default value of the respective parameter for general deployments. Configure a different value, if required, for a specific deployment.

	Command or Action	Purpose
Step 4	**exit** **Example:** `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	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-definition** *service-definition-name* **Example:** `Device(config)# mdns-sd service-definition CUSTOM1`	Configures mDNS service definition. **Note** 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	**service-type** *string* **Example:** `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	**exit** **Example:** `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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-list** *service-list-name* {**in** | **out**} **Example:** `Device(config)# mdns-sd service-list VLAN100-list in`	Configures mDNS service list.
Step 4	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] **Example:** `Device(config-mdns-sl-in)# match PRINTER-IPPS message-type announcement`	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. **Note** 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: **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]. If the mDNS service list is set to OUT, the applicable command syntax is: **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] [**location-filter** *location-filter-name*] [**source-interface** {*mDNS-VLAN-number* | *mDNS-VLAN-range*}].
Step 5	**exit** **Example:** `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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy mdns-policy1`	Configures mDNS service policy.

Step 4	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`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.

Step 5	**exit** **Example:** `Device(config-mdns-ser-pol)# exit`	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     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** 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.

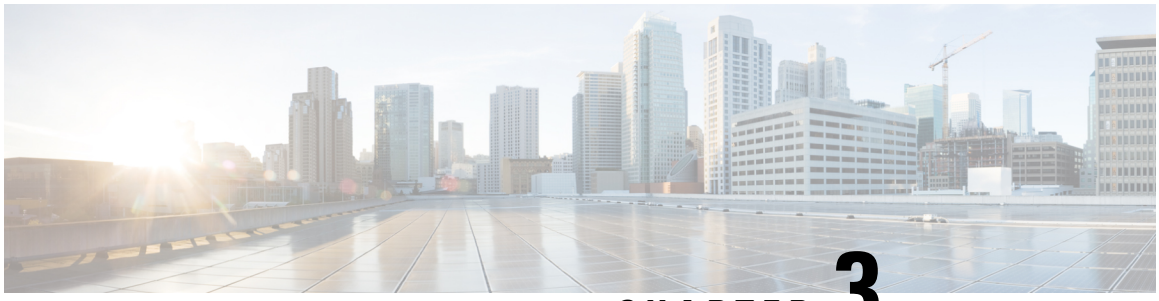
```
Device# show mdns controller detail

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 Local Area Bonjour in Unicast Mode for LAN Networks

Cisco Catalyst 9000 Series switches and Cisco Catalyst 9800 Series WLC introduce the unicast mode function in Local Area Bonjour network domain. The new enhanced gateway function at the first hop of wired and wireless networks communicates directly with any industry standard RFC 6762 compliant mDNS end point in Layer 2 unicast mode. The new unicast mode communication eliminates the Layer 2 mDNS flood challenge in large-scale enterprise-grade LAN and WLAN networks. The unicast mode provides enhanced security, bandwidth, scale, and performance within the network.

Prerequisites for Local Area Bonjour in Unicast Mode for LAN Networks

You must ensure that the Cisco Catalyst devices are successfully configured and are operational prior to implementing Cisco Local Area Bonjour in unicast mode for LAN networks. The following are the prerequisites that need to be verified on a Cisco Catalyst Switch before deploying it in SDG-Agent mode or Service-Peer mode:

- Verify that the targeted Cisco Catalyst switch platform is supported in SDG-Agent or Service-Peer mode from the support matrix.
- Verify that the targeted Cisco Catalyst SDG-Agent and Service-Peer switch are running the minimum required Cisco IOS XE software version.
- The Cisco Catalyst switch in SDG-Agent and Service-Peer mode must have the valid Cisco DNA Advantage license installed and running.
- In a Multilayer network with Layer 2 unicast service-routing, ensure that the SDG-Agent in distribution-layer and Service-Peer is interconnected through a Layer 2 trunk in static mode.

- Ensure that the SDG-Agent and Service-Peer switches have IP reachability on the same IPv4 subnet in global routing.

Restrictions for Local Area Bonjour in Unicast Mode for LAN Networks

- Local Area Bonjour in Unicast Mode for LAN Networks is not supported on Cisco Catalyst 2900 Series, Cisco Catalyst 3850 Series, Cisco Catalyst 3650 Series, Cisco Catalyst 4500 Series, Cisco Catalyst 6500 Series, Cisco Catalyst 6800 Series switches, C9500X-28C8D model of the Cisco Catalyst 9500 Series Switches, and Cisco Catalyst 9600 Series Supervisor 2 Module.
- Cisco SD-Access for wired and wireless networks is supported only for releases starting from Cisco IOS XE Amsterdam 17.3.3.
- Cisco Embedded Wireless Controller on a Cisco Catalyst Series switch is supported only for releases starting from Cisco IOS XE Amsterdam 17.3.3.
- The Cisco Bonjour gateway solution follows the industry standard RFC 6762 Multicast DNS (mDNS) guidelines and only supports wired or wireless end points that comply with unicast mode.
- The Catalyst Switch Management Port is not supported for local area service-routing.
- mDNS doesn't support the split of transport with dual stack on FHRP between SDG agents. You can either enable IPv4 or IPv6 management VLAN and make one switch as FHRP active.
- You can configure either Local Area Bonjour in Unicast Mode or Local Area Bonjour in Multicast DNS mode, and not both, on the same SDG agent or the same service peer.

Information About Local Area Bonjour in Unicast Mode for LAN Networks

The zero-configuration service discovery and distribution capabilities use the link-local mDNS protocol to discover rich services intuitively without extensive user knowledge and intervention. RFC 6762 provides guidelines to discover services via Layer 2 multicast or Layer 2 unicast in a local segment. The receiving end point may request service discovery over an IPv4 and IPv6 network to collect information prior to use. The Layer 2 multicast frames are broadcast-category packets in a LAN and WLAN environment. Thus, they are flooded based on the Layer 2 flood boundary size across the network.

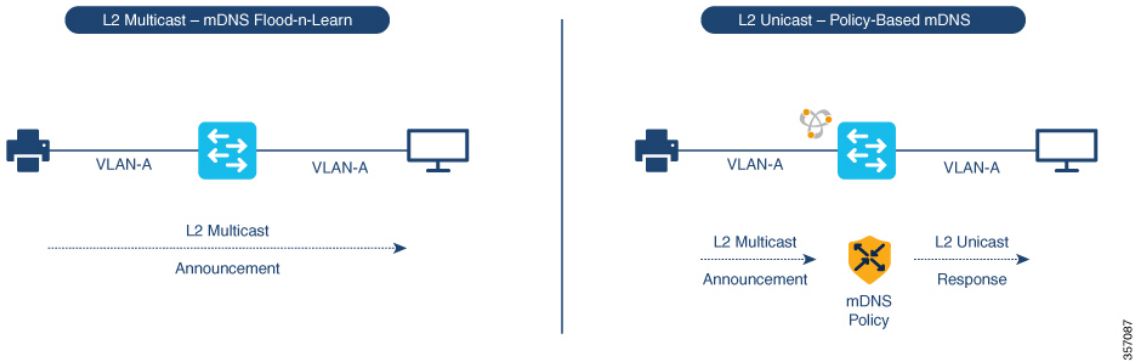
The Layer 2 or Layer 3 network boundary varies broadly in an enterprise network for LAN and wireless designs. The Local Area Bonjour domain introduces two new unicast communication modes. The unicast communication modes prevent mDNS flooding in the network for any current or evolving network deployment models. The following are the two new aspects of Local Area Bonjour Unicast modes:

- Unicast mode end points
- Unicast mode Layer 2 network

End Points for Unicast Mode

Starting with Cisco IOS XE Amsterdam Release 17.3.2, Cisco Catalyst 9000 Series switches and Cisco Catalyst 9800 Series WLCs introduce Layer 2 unicast service gateway solution. The mDNS endpoint continues to advertise or query services over Layer 2 mDNS. However, with the unicast mode settings enabled, the incoming mDNS IPv4 and IPv6 frames are handled uniquely. The unicast technique eliminates the mDNS flood challenges and provides a policy-based service query response to the requesting end points over a unicast MAC address. The following figure illustrates the functional difference between the new Layer 2 unicast (flood-free) and the traditional Layer 2 Multicast (flood) communication with wired and wireless end points.

Figure 9: Layer 2 Unicast Mode End Points



Layer 2 Network for Unicast Mode

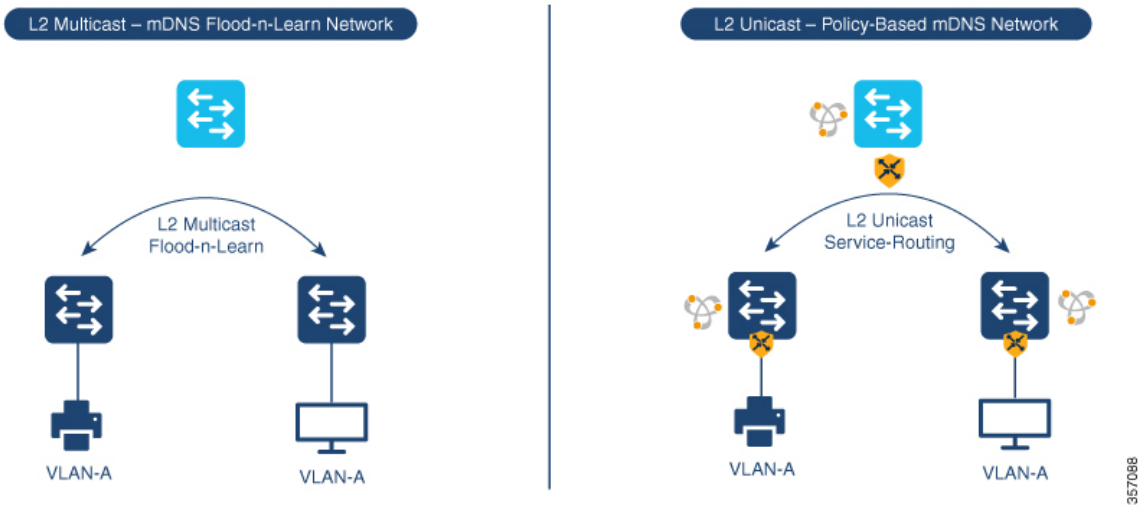
The Layer 3 boundary for wired and wireless networks can reside in the distribution layer with Layer 2 connections extended over trunk ports to an access layer switch or WLC. The association of the nonpruned or common VLAN ID to the trunk ports extends the Layer 2 flood boundary across the network.

Starting with Cisco IOS XE Amsterdam Release 17.3.2, Cisco Catalyst 9000 Series switches and Cisco Catalyst 9800 Series WLCs introduce the Service Peer role to eliminate transmitting mDNS flood over trunk ports. The Service Peer establishes a unicast Layer 3 IPv4-based service-routing session with the distribution layer system in Service Discovery Gateway (SDG) role. The Service Peer establishes the session over the existing Layer 2 trunk ports without modifying any existing Layer 2 VLAN configuration. The new mDNS trust port between access layer and distribution layer uses the existing out-of-band management network to statefully discover and distribute services (based on policies) to replace traditional flood-n-learn methods from the Layer 2 network.

If the Layer 3 boundary in a LAN environment is at the access layer, then the SDG mode provides integrated Service Peer role. Further, the SDG mode needs only Wide Area Bonjour with Cisco DNA Center for service-routing in a Layer 3 IP network.

The following figure illustrates a Layer 2 Network with the unicast mode and a traditional Layer 2 network with mDNS flood:

Figure 10: Unicast Mode Layer 2 Network



Default mDNS Service Configurations

Starting with Cisco IOS XE Bengaluru 17.6.1, an intuitive approach to configuring mDNS services, known as the default mDNS service configuration, is introduced. The default service configuration contains a default service policy that creates a service list with default service-types that is automatically enforced in the ingress or egress direction. The following figure illustrates the default mDNS service configurations:

Figure 11: Default mDNS Service Configuration

The default mDNS service configurations accelerates solution adoption, increases user productivity, and reduces operation overhead. Additionally you can define a custom policy and define a service list with custom-defined service types and enforce it in the ingress or egress direction.

HSRP-Aware mDNS Service-Routing

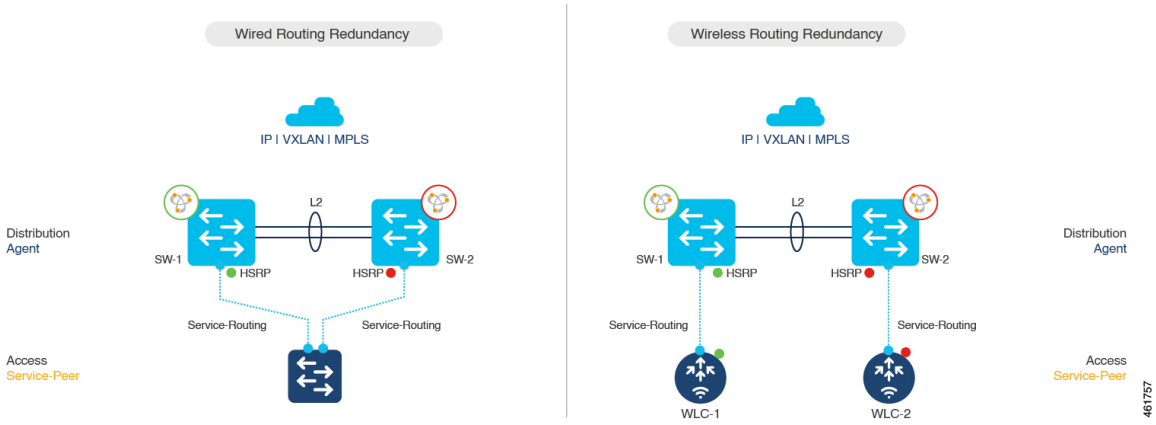
Starting from Cisco IOS XE Bengaluru 17.6.1, Hot Standby Router Protocol-aware (HSRP-aware) mDNS Service-Routing is supported between Service Peers and SDG agents in a multilayer network. During a changeover, that is when the primary SDG agent fails and the secondary SDG agent becomes the new primary, the service-routing session between the Service Peer and the SDG agent remains uninterrupted. The new primary SDG agent establishes a session with the Service Peer and cache information is resynced.

mDNS Service-Routing is performed over the management VLAN between the Service Peer and the SDG Agent. The HSRP virtual IP address of the management VLAN is enabled on the SDG agent using the **standby** *group_number* **ip** *ip_address* command. The HSRP virtual IP address needs to configured on the Service Peer as the IP address of the SDG agent.

Note The HSRP virtual IP address must be reachable and in active state during a changeover.

The following figure illustrated a wired and wireless network that supports HSRP-aware mDNS Service-Routing:

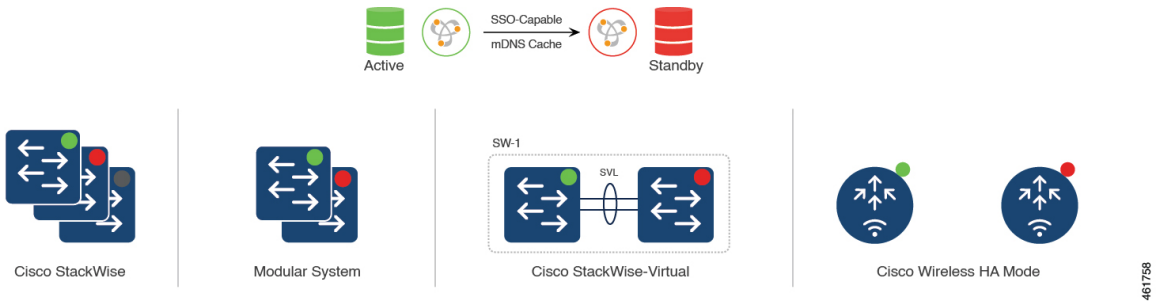
Figure 12: HSRP-Aware mDNS Service-Routing on a Wired and Wireless Network



mDNS Service-Gateway SSO Support

Starting from Cisco IOS XE Bengaluru 17.6.1, mDNS Stateful Switchover (SSO) is supported on network devices configured in Service Peer role and SDG agent role. In SSO-enabled devices, one device is selected as an active device and the other as a standby device. The cache information learnt by the active device is synced with the standby device. When the active device fails, the standby device becomes the new active device and continues the mDNS service discovery process.

Figure 13: mDNS Service-Gateway SSO



Note Use the **show mdns-sd summary** command to check whether SSO is in active or disabled state.

mDNS service-gateway SSO is supported on Cisco Catalyst 9600 Series Switches configured with either redundant supervisor engine module in SSO state or with Cisco StackWise Virtual.

How to Configure Local Area Bonjour Unicast Mode for LAN Networks

This section shows how to configure the first-hop Layer 2 LAN access switch in Service Peer mode, to enable mDNS gateway function with policies, and to enable peering with upstream Layer 3 gateway in SDG Agent mode. The procedure also applies to the first-hop Layer 3 LAN access switch and the first-hop Layer 3 gateway switch in SDG Agent mode.

Configuring mDNS Gateway Mode

To configure mDNS gateway mode, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enables mDNS on the Layer 2 switch and enters mDNS gateway configuration mode. Enter the following commands in mDNS gateway configuration mode to enable the respective functionalities: • **active-query timer** [**min**]: Enables refresh of discovered services and their records with a periodic mDNS query message for the permitted service types. The value ranges from 1 to 120 minutes.

	Command or Action	Purpose
		Note Starting from Cisco IOS XE Bengaluru 17.6.1, the **active-query timer** command can be configured globally in Service-Peer for multilayer networks and in SDG agent for routed access networks. • **air-print-helper**: Enables communication between Apple iOS devices like iPhones and iPads to discover and use older printers that do not support driverless AirPrint function. • **air-print-helper**: Enables communication between Apple iOS devices like iPhones and iPads to discover and use older printers that do not support driverless AirPrint function. • **cache-memory-max**: Configures the percentage memory for cache. • **rate-limit**: Enables rate limiting of incoming mDNS packets. • **service-announcement-count**: Configures maximum service announcement count per scheduler to upstream SDG-Agent or Cisco DNA Center controller. Service advertisement count ranges from 10 to 500 . • **service-announcement-timer periodicity**: Configures service advertisement time scheduler in seconds to upstream SDG-Agent or Cisco DNA Center controller. The value ranges from 5 to 36000 seconds. • **service-query-count**: Configures maximum service query request count per scheduler to upstream SDG-Agent or Cisco DNA Center controller. The value ranges from 10 to 500 service query count. • **service-query-timer periodicity**: Configures service query request time scheduler in seconds to upstream SDG-Agent or Cisco DNA Center

	Command or Action	Purpose
		controller. The value ranges from 5 to 36000 seconds. • **service-mdns-query** {**ptr**|**srv**|**txt**}: Permits processing a specific query type. The default value is **ptr**. **Note** Starting from Cisco IOS XE Bengaluru 17.6.1, the **service-mdns-query** command can be configured globally on the Layer 2 switch.

Step 4	**mode** {**service-peer** | **sdg-agent**}
	Example:
	`Device(config-mdns-sd)# mode sdg-agent`
	OR
	`Device(config-mdns-sd)# mode service-peer`
		Configure mDNS gateway in either of the following modes based on system settings:
		• **service-peer**: Enables the Layer 2 Catalyst Series switch in mDNS Service Peer mode.
		• **sdg-agent**: Enables the Layer 3 Catalyst Series switch in SDG Agent mode to peer with Cisco DNA Center controller for Wide Area Bonjour service-routing.
		This is the default mode.

Step 5	**end** **Example:** `Device(config-mdns-sd)# end`	Returns to privileged EXEC mode.

Configuring mDNS Service Policy

The mDNS service policy creates a service list that permits built-in or user-defined custom service-types. It then associates the service-list to a service-policy to enforce it in ingress or egress direction. It then applies the service-policy to the new VLAN configuration mode. This configuration remains the same on a Cisco Catalyst Series switch in both Service Peer and SDG Agent mode.

To configure an mDNS service policy and apply it on a target VLAN in Service Peer mode, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-list** *service-list-name* { **in** | **out**} **Example:** `Device(config)# mdns-sd service-list VLAN100-LIST-IN in`	Configures the incoming mDNS service list to classify one or more service types. A unique service list is required to process the incoming mDNS message and the outbound response to the requesting end points.

Step 4	**match** {**all** | *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] }
	Example:
	`Device(config-mdns-sl-in)# match APPLE-TV`
	`Device(config-mdns-sl-in)# match PRINTER-IPPS message-type announcement`
		Checks the inbound service-list. The switch either accepts or drops the incoming mDNS service type (like Apple TV) advertisement or query matching message type.
		The service list contains an implicit deny at the end.
		The default message-type is **any**.
		Note Starting from Cisco IOS XE Bengaluru 17.6.1, the **match all** command can be configured under a service-list to accept all mDNS service-types.

Step 5	**exit** **Example:** `Device(config-mdns-sl-in)# exit`	Returns to global configuration mode.
Step 6	**mdns-sd service-list** *service-list-name* {**in** | **out**} **Example:** `Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`	Configures the outgoing mDNS service list to classify one or more service types. A unique service list is required to process the incoming mDNS message and the outbound response to the requesting end points.

Step 7	**match** {**all** | *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] [**location-filter** *location-filter-name*] [**source-interface** {*mDNS-VLAN-number* | *mDNS-VLAN-range*}] }
	Example:
	`Device(config-mdns-sl-out)# match APPLE-TV`
	`Device(config-mdns-sl-out)# match PRINTER-IPPS`
		Checks the outgoing service-list. The switch provides a local service proxy function by responding with a matching service-type to the requesting end point. For example, the Apple-TV and Printer learned from VLAN 100 are distributed to the receiver in the same VLAN 100.
		The service-list contains an implicit deny at the end.
		The message-type for an outbound service list is optional.

	Command or Action	Purpose
		Note Starting from Cisco IOS XE Bengaluru 17.6.1, the **match all** command can be configured under a service-list to accept all mDNS service-types.
Step 8	**exit** **Example:** `Device(config-mdns-sl-out)# exit`	Returns to global configuration mode.
Step 9	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy VLAN100-POLICY`	Creates a unique mDNS service-policy.

Step 10	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config-mdns-ser-policy)# service-list VLAN100-LIST-IN in`
	`Device(config-mdns-ser-policy)# service-list VLAN100-LIST-OUT out`
		Configures an mDNS service policy to associate with the service list for each direction.

Step 11	**exit** **Example:** `Device(config-mdns-ser-policy)# exit`	Returns to global configuration mode.

Step 12	**vlan configuration** *vlan-id*
	Example:
	`Device(config)# vlan configuration 100`
	`Device(config)# vlan configuration 101-110, 200`
		Enables VLAN configuration for advanced service parameters. One or more VLANs can be created for the same settings.

Step 13	**mdns-sd gateway** **Example:** `Device(config-vlan)# mdns-sd gateway`	Enables the mDNS gateway on the specified VLAN IDs.
Step 14	**service-policy** [*service-policy-name*] **Example:** `Device(config-vlan-mdns)# service-policy VLAN100-POLICY`	Associates an mDNS service policy with the specified VLAN IDs. **Note** Starting from Cisco IOS XE Bengaluru 17.6.1, if no service policy is configured, the default service policy is used.
Step 15	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-vlan-mdns)# end`	

(Optional) Configuring mDNS Location-Group on Service Peer

A Cisco Catalyst Series switch in service-peer mode provides granular mDNS service-routing based by assigning Location-Group ID tags to its Wired LAN Ports. You can expand policy capabilities with inclusion of matching Location-Group ID tag to discover and distribute mDNS services. You can design and build Location-Group tag based dynamic mDNS service boundaries at micro-segmented service-zones on each floor.

To enable mDNS location-group on service peer, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd location-group** *location-group-id* **vlan** *vlan-id* **Example:** `Device(config)# mdns-sd location-group 1 vlan 100`	Configures a location-group tag to a VLAN
Step 4	**interface** *interface-name* **Example:** `Device(config-vlan)# interface gigabitethernet 1/0/1`	Assigns location-group tag to individual or group of Ethernet ports.
Step 5	**end** **Example:** `Device(config-vlan)# end`	Returns to privileged EXEC mode.

Configuring mDNS Location-Filter

A Cisco Catalyst Series switch in Unicast network mode provides, by default, a local service proxy between the mDNS service provider and the receiver connected in the same Layer 2 VLAN. Also, you can configure the mDNS location filter to allow service discovery and distribution between locally configured VLAN IDs. The configuration remains the same for both Service Peer and SDG Agent modes.

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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd location-filter** *location-filter-name* **Example:** `Device(config)# mdns-sd location-filter LOCAL-PROXY`	Configures a unique location filter.

Step 4	**match location-group** {**all** | **default** | **ID**} **vlan** *vlan-id*
	Example:
	`Device(config-mdns-loc-filter)# match location-group default vlan 100`
	`Device(config-mdns-loc-filter)# match location-group default vlan 101`
		Configures the match criteria that mutually distribute permitted services between grouped VLANs.

Step 5	**exit** **Example:** `Device(config-mdns-loc-filter)# exit`	Returns to global configuration mode.

Step 6	**mdns-sd service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config)# mdns-sd service-list VLAN100-LIST-IN in`
	`Device(config)# mdns-sd service-list VLAN100-LIST-OUT out`
		Configures the mDNS service list to classify one or more service types.
		A unique service list is required to process the incoming mDNS message and the outbound response to the requesting end points.

Step 7	**match** {**all** |*service-definition-name* [**message-type** {**any** | **announcement** | **query**}] [**location-filter** *location-filter-name*] } **Example:** `Device(config-mdns-sl-out)# match APPLE-TV location-filter LOCAL-PROXY`	Checks the outgoing service-list. The switch provides a local service proxy function by responding with a matching service-type to the requesting end point. For example, the Apple-TV and Printer learned from VLAN 100 are distributed to the receiver on different VLAN 101. The service-list contains an implicit deny at the end.

	Command or Action	Purpose
		The message-type for an outbound service list is optional. **Note** Starting from Cisco IOS XE Bengaluru 17.6.1, the **match all** command can be configured under a service-list to accept all mDNS service-types.
Step 8	**exit** **Example:** `Device(config-mdns-sl-out)# exit`	Returns to global configuration mode.
Step 9	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy VLAN100-POLICY`	Creates a unique mDNS service-policy.
Step 10	**service-list** *service-list-name* {**in** | **out**} **Example:** `Device(config-mdns-ser-policy)# service-list VLAN100-LIST-OUT out`	Configures an mDNS service-policy to associate with the service-list for each direction.
Step 11	**exit** **Example:** `Device(config-mdns-ser-policy)# exit`	Returns to global configuration mode.

Step 12	**vlan configuration** *vlan-id*
	Example:
	`Device(config)# vlan configuration 100`
	`Device(config)# vlan configuration 101-110, 200`
		Enables VLAN configuration for advanced service parameters. One or more VLANs can be created for the same settings.

Step 13	**mdns-sd gateway** **Example:** `Device(config-vlan)# mdns-sd gateway`	Enables the mDNS gateway on the specified VLAN IDs.
Step 14	**service-policy** [*service-policy-name*] **Example:** `Device(config)# service-policy VLAN100-POLICY`	Associates an mDNS service-policy with the specified VLAN IDs. **Note** Starting from Cisco IOS XE Bengaluru 17.6.1, configuring a service policy name is optional. If no service policy is configured, then the default service policy is used.

	Command or Action	Purpose
Step 15	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

(Optional) Configuring Custom Service Definition

Cisco IOS XE supports various built-in mDNS service definition types that map the key mDNS PTR records to user-friendly names. For example, a built-in Apple-TV service type is associated with _airplay._tcp.local and _raop._tcp.local PTR records to successfully enable the service in the network. You can create custom service-definitions with matching mDNS PTR records to enable mDNS service-routing in the network.

To create a custom service definition, associate it with the service list and discover mDNS services between local VLANs, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd service-definition** *service-definition-name* **Example:** `Device(config)# mdns-sd service-definition APPLE-CLASSROOM`	Configures a unique location filter.
Step 4	**service-type** *service-type-string* **Example:** `Device(config-mdns-ser-def)# service-type _classroom._tcp.local`	Configures two or more local VLANs and mutually distributes permitted services between the grouped VLANs.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring Service-Routing on Service Peer

The Layer 2 Cisco Catalyst switch in service-peer mode builds service-routing with an upstream distribution-layer switch in SDG Agent mode. To build service-routing the Layer 2 Cisco Catalyst switch

requires at least one interface with valid IP address to reach upstream SDG Agent Catalyst switch. The switch management port is unsupported.

To enable service routing on a Cisco Catalyst Series switch in service-peer mode and configure mDNS trust interface settings, perform the following steps:

Before you begin

The **mdns-sd trust** command must be enabled on the interface configured between the Service Peer and SDG agent.

Procedure

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

Step 3	**vlan configuration** *vlan-id*
	Example:
	`Device(config)# vlan configuration 100`
	`Device(config)# vlan configuration 101-110, 200`
		Enables VLAN configuration for advanced service parameters. One or more VLANs can be created for the same settings.

Step 4	**mdns-sd gateway** **Example:** `Device(config-vlan)# mdns-sd gateway`	Enables the mDNS gateway on the specified VLAN IDs. Enter the following commands in mDNS gateway configuration mode to enable the respective functionalities: • **active-query timer** [**min**]: Enables refresh of discovered services and their records with a periodic mDNS query message for the permitted service types. The value ranges from 1 to 120 minutes.

	Command or Action	Purpose
		Note Starting from Cisco IOS XE Bengaluru 17.6.1, the following changes are applicable for the **active-query timer** command: • The unit of measurement for the timer is changed to minutes from seconds. • This command can also be configured globally on the Layer 2 switch in addition to a VLAN. The VLAN configuration for this command takes precedence over the global configuration. • **service-mdns-query** {**ptr** | **srv** | **txt**}: Permits processing a specific query type. The default value is **ptr**. **Note** Starting from Cisco IOS XE Bengaluru 17.6.1, the **service-mdns-query** command can be configured globally on the Layer 2 switch in addition to a VLAN. The VLAN configuration for this command takes precedence over the global configuration. • **transport** {**ipv4** | **ipv6** | **both**}: Permits processing for IPv4 traffic, IPv6 traffic, or both. We recommend that you add only one network type to reduce redundant processing and avoid responses with same information over two network types. The default value is **ipv4**.

	Command or Action	Purpose
Step 5	**source interface** *interface-id* **Example:** `Device(config-vlan-mdns-sd)# source-interface vlan 4094`	Selects the interface with a valid IP address that sources the service-routing session with the upstream Cisco Catalyst SDG Agent switch. Typically, the management VLAN interface is used.
Step 6	**sdg-agent** *ipv4-address* **Example:** `Device(config-vlan-mdns-sd)# sdg-agent 10.0.0.254`	Configures the IPv4 address for the SDG Agent. Typically, the management VLAN gateway address is used. If FHRP mode is being used, then use the FHRP virtual IP address of the management VLAN.
Step 7	**end** **Example:** `Device(config-vlan-mdns-sd)# end`	Returns to privileged EXEC mode.

Configuring Service-Routing on Service Discovery Gateway

Cisco Catalyst 9000 Series switches at the distribution layer support SDG Agent mode. SDG Agent mode enables the unicast mode of Bonjour service-routing with downstream Layer 2 access layer Ethernet switches and Cisco Catalyst 9800 Series WLCs.

To enable policy-based service discovery and distribution between locally paired service peers network devices, perform the following steps:

Note Configure the mDNS service policy as described in Configuring mDNS Service Policy, on page 36.

Before you begin

The **mdns-sd trust** command must be enabled on the interface configured between the Service Peer and SDG agent.

Procedure

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

	Command or Action	Purpose
Step 3	**mdns-sd service-peer group** **Example:** `Device(config)# mdns-sd service-peer group`	Configures a unique Service Peer group.
Step 4	**peer-group** *group-id* **Example:** `Device(config-mdns-svc-peer)# peer-group 1`	Assigns a unique peer group ID to pair the Service Peers that permit mDNS service discovery and allows distribution within assigned group list. The allowed peer group range is 1 to 1000 for every SDG Agent switch.
Step 5	**service-policy** *service-policy* **Example:** `Device(config-mdns-svc-peer)# service-policy VLAN100-POLICY`	Filters services based on configured service policy. If custom service policy is configured under the service peer group, then SDG agent applies filters based on the custom service policy. If a custom service policy is not configured, the SDG agent applies filters based on the default service policy.

Step 6	**service-peer** [*ipv4-address*] **location-group** {**all** | **default** | **id**}
	Example:
	`Device(config-mdns-svc-peer-grp)# service-peer 10.0.0.1 location-group default`
	`Device(config-mdns-svc-peer-grp)# service-peer 10.0.0.2 location-group default`
		Configures at least one Service Peer to accept mDNS service advertisement or query message. When grouped with more than one Service Peers, the SDG Agent provides Layer 2 unicast mode routing between the configured peers.
		For example, the SDG Agent provides unicast-based service gateway function between the two Layer 2 service peer switches (10.0.0.1 and 10.0.0.2) that match the associated service policy.

Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

(Optional) Configuring HSRP-aware mDNS Service-Routing Support on SDG Agent

To configure HSRP-aware mDNS Service-Routing support on SDG agent, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd gateway** **Example:** `Device(config)# mdns-sd gateway`	Enables mDNS on the Layer 2 switch and enters mDNS gateway configuration mode. Enter the following commands in mDNS gateway configuration mode to enable the respective functionalities: • **active-query timer** [**min**]: Enables refresh of discovered services and their records with a periodic mDNS query message for the permitted service types. The value ranges from 1 to 120 minutes. **Note** Starting from Cisco IOS XE Bengaluru 17.6.1, the **active-query timer** command can be configured globally in Service-Peer for multilayer networks and in SDG agent for routed access networks. • **air-print-helper**: Enables communication between Apple iOS devices like iPhones and iPads to discover and use older printers that do not support driverless AirPrint function. • **cache-memory-max**: Configures the percentage memory for cache. • **rate-limit**: Enables rate limiting of incoming mDNS packets. • **service-announcement-count**: Configures maximum service announcement count per scheduler to upstream SDG-Agent or Cisco DNA Center controller. Service advertisement count ranges from 10 to 500. • **service-announcement-timer periodicity**: Configures service advertisement time scheduler in seconds to upstream SDG-Agent or Cisco DNA

	Command or Action	Purpose
		Center controller. The value ranges from 5 to 36000 seconds. • **service-query-count**: Configures maximum service query request count per scheduler to upstream SDG-Agent or Cisco DNA Center controller. The value ranges from 10 to 500 service query count. • **service-query-timer periodicity**: Configures service query request time scheduler in seconds to upstream SDG-Agent or Cisco DNA Center controller. The value ranges from 5 to 36000 seconds. • **service-mdns-query** {**ptr**|**srv**|**txt**}: Permits processing a specific query type. The default value is **ptr**. **Note** Starting from Cisco IOS XE Bengaluru 17.6.1, the **service-mdns-query** command can be configured globally on the Layer 2 switch.
Step 4	**source interface** *interface-id* **Example:** `Device(config-mdns-sd)# source-interface vlan 4094`	Selects the interface with a valid IP address that sources the service-routing session with the upstream Cisco Catalyst SDG Agent switch. Typically, the management VLAN interface is used.
Step 5	**exit** **Example:** `Device(config-mdns-sd)# exit`	Returns to global configuration mode.
Step 6	**interface** *interface-name* **Example:** `Device(config)# interface vlan 101`	Enters interface mDNS configuration mode and enables interface configuration.
Step 7	**ip address** *ip-address subnet-mask* **Example:** `Device(config-if)# ip address 10.0.1.1 255.255.255.0`	Specifies an IP address for an interface.

	Command or Action	Purpose
Step 8	**standby** *group-number* **ip** *ip-address* **Example:** `Device(config-if)# standby 1 ip 10.1.1.254`	Creates (or enable) the HSRP group using its number and virtual IP address. • *group-number*: The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. • *ip-address*: The virtual IP address of the first hop SDG agent interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces.
Step 9	**standby** *group-number* **priority** *priority* **Example:** `Device(config-if)# standby 1 priority 110`	Sets a priority value that is used in choosing the active SDG agent. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority.
Step 10	**standby** *group-number* **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*] **Example:** `Device(config-if)# standby 1 preempt delay 300`	Configures the router to preempt, which means that when the local router has a higher priority than the active router, it becomes the active router. • *group-number*: The group number to which the command applies. • (Optional) **delay minimum**: Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) **delay reload**: Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) **delay sync**: Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). Use the **no** form of the command to restore the default values.

	Command or Action	Purpose
Step 11	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Verifying Local Area Bonjour in Unicast Mode for LAN Networks

This section provides information about verifying Local Area Bonjour in unicast mode for both Service Peer and SDG Agent modes.

Verifying a Service Peer Catalyst Switch in Local Area Bonjour Domain

The following **show** commands are used to verify the various Local Area Bonjour domain mDNS service configuration parameters, cache records, statistics, and other information on a Cisco Catalyst Series switch configured in Service Peer mode.

Table 3: Commands to Verify a Service Peer Catalyst Switch in Local Area Bonjour Domain

Command	Purpose
show mdns-sd cache {**all** | **interface** | **mac** | **name** | **service-peer** | **static** | **type** | **vlan**}	Displays the available mDNS cache records that support multiple variables and provides granular source details. The following variables are available: • **all**: Displays all available cache records discovered from multiple source connections of a system. • **interface**: Displays the available cache records discovered from specified Layer 3 interface. • **mac**: Displays the available cache records discovered from the specified MAC address. • **name**: Displays the available cache records based on the name of the service provider announced. • **service-peer**: Displays available cache records discovered from the specified Layer 2 Service Peer. • **static**: Displays the locally configured static mDNS cache entries. • **type**: Displays the available cache records based on the specific mDNS record type (PTR, SRV, TXT, A, or AAAA). • **vlan**: Displays the available cache records discovered from the specified Layer 2 VLAN ID in unicast mode.

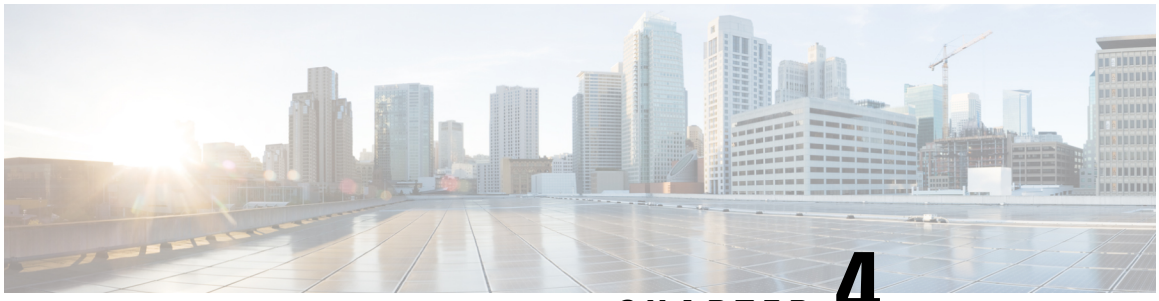
Command	Purpose
show mdns-sd service-definition {**name** | **type**}	Displays the built-in and user-defined custom service definitions and provides the mapping from service name to mDNS PTR records. The service definitions can be filtered by name or by type.
show mdns-sd service-list {**direction** | **name**}	Displays the configured inbound and outbound service lists that classify matching service types for a service policy. The service lists can be filtered by name or by direction.
show mdns-sd service-peer statistics	Displays the detailed mDNS packet statistics (number of packets sent to and received from the client, number of packets sent to and received from SDG-agent, and so on) that is processed by the system, when mDNS is configured in service-peer mode.
show mdns-sd service-policy {**interface** | **name**}	Displays the list of mDNS service policies mapped with inbound and outbound service lists. The service policies list can be filtered by the associated interface or by name.
show mdns-sd statistics {**all** | **cache** | **debug** | **interface** | **service-list** | **service-policy** | **services** | **vlan**}	Displays the detailed mDNS statistics processed bi-directionally by the system on each mDNS-gateway-enabled VLAN, when mDNS is configured in unicast mode. The keywords for the mDNS statistics provide a detailed view on the interface, policy, service list, and services.
show mdns-sd summary {**interface** | **vlan**}	Displays the brief information about mDNS gateway and the key configuration status on all VLANs and interfaces of the system.
show mdns-sd sdg service-peer summary	Displays the service-routing session information of the Service Peer and SDG agent.

Verifying a Service Discovery Gateway Agent Catalyst Switch in Local Area Bonjour Domain

See Verifying a Service Peer Catalyst Switch in Local Area Bonjour Domain, on page 50 for the complete list of **show** commands that are used to verify the various Local Area Bonjour domain mDNS service configuration parameters, cache records, statistics, and other information on a Cisco Catalyst Series switch configured in SDG Agent mode.

Additional References for Local Area Bonjour in Unicast Mode for LAN Networks

Related Topic	Document Title
Cisco Wide Area Bonjour Application on Cisco DNA Center User Guide	Cisco Wide Area Bonjour Application on Cisco DNA Center User Guide, Release 2.1.2
DNA Service for Bonjour Deployment on Cisco Catalyst 9800 WLCs	Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide



CHAPTER 4

Configuring Wide Area Bonjour

Cisco Wide Area Bonjour domain enables global service-routing beyond a single IP gateway for traditional LAN and WLAN networks. In Cisco Wide Area Bonjour domain, Cisco Catalyst LAN switches are deployed in Layer 3 routed mode to act as distributed SDG Agents throughout the network. These SDG agents build a TCP-based, stateful, reliable, and light-weight communication channel with a Cisco DNA Center. The Cisco DNA Center must also be configured with Cisco Wide Area Bonjour application for policy-based global service discovery and distribution.

Restrictions for Wide Area Bonjour for LAN and WLAN Networks

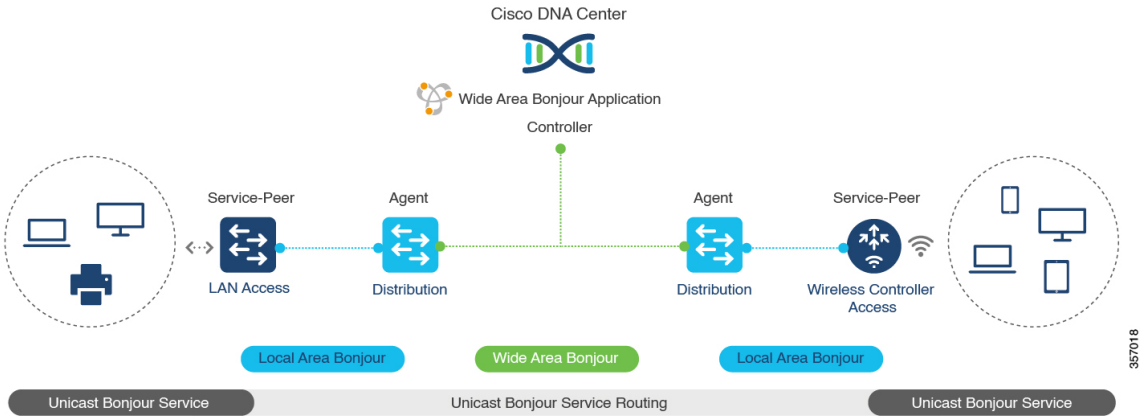
Wide Area Bonjour service-routing between Cisco DNA Center and a Catalyst SDG Agent Switch over management port is not supported. We recommend that you use a switch Loopback interface instead.

Information About Wide Area Bonjour LAN and WLAN Networks

Wide Area Bonjour, by definition, allows service-routing over an IP network without network boundaries. Hence, the core objective of Cisco Wide Area Bonjour is to advertise and browse Bonjour services in a global IP network that is limited to local or remote sites, as required. Typically, the LAN and Wireless LAN IP gateway deployed in SDG Agent mode build the stateful TCP-based unicast connection to the Cisco DNA Center for Wide Area Bonjour service-routing.

The fundamentals of service-routing are based on the policies defined in Local Area and Wide Area Bonjour domains. The policy defines implicit guidelines to accept, process and respond to mDNS services on the SDG Agent and the Cisco DNA-Center. The service policy carries multiple tuples to distinctly classify and distribute the service provider information along with granular network location. The following figure illustrates an end-to-end reference network model for Cisco Wide Area Bonjour.

Figure 14: Cisco Wide Area Bonjour Domain



How to Configure Wide Area Bonjour for LAN and WLAN Networks

This section provides information about how to configure Wide Area Bonjour for LAN and WLAN networks. Configuration of Cisco Wide Area Bonjour requires you to configure the Cisco Catalyst Series switch in SDG Agent mode and build the service policies in Wide Area Bonjour application of Cisco DNA Center.

Configuring Cisco Wide Area Bonjour Service-Routing

To build and apply Wide Area Bonjour export service policy and setup controller parameters that enable service-routing, perform the following steps

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**service-export mdns-sd controller** *controller-name* **Example:** `Device(config)# service-export mdns-sd controller DNAC-BONJOUR-CONTROLLER`	Configures the service export controller to enable Wide Area Bonjour service-routing with Cisco DNA Center. Only one service export can be configured.

	Command or Action	Purpose
Step 4	**controller-address** *ipv4-address* **Example:** `Device(config-mdns-sd-se)# controller-address 100.0.0.1`	Assigns the Cisco DNA Center IPv4 address to pair service-routing. Only one controller address can be configured.
Step 5	**controller-source-interface** *interface-name* **Example:** `Device(config-mdns-sd-se)# controller-source-interface Loopback0`	Configures the source interface to build service-routing from the SDG-Agent and the Cisco DNA Center. We recommend you to use the Loopback interface.
Step 6	**end** **Example:** `Device(config-mdns-sd-se)# end`	Returns to privileged EXEC mode.

What to do next

The default controller service policy is automatically configured, if a customized controller service policy is not configured. To configure a customized controller service policy, see (Optional) Configuring Cisco Wide Area Bonjour Custom Controller Service Policy, on page 55

(Optional) Configuring Cisco Wide Area Bonjour Custom Controller Service Policy

To build and apply the Wide Area Bonjour custom-controller service policy, perform the following steps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mdns-sd controller service-list** *controller-service-list-name* **Example:** `Device(config)# mdns-sd controller service-list WIDE-AREA-SERVICES-LIST`	Configures the mDNS controller service list to classify one or more service types.
Step 4	**match** {**all**|*service-definition-name* [**message-type** {**any**| **announcement**|**query**}	Checks and matches the controller service list. The switch exports locally discovered services

	Command or Action	Purpose

	] [**source-interface** {*mDNS-VLAN-number* | *mDNS-VLAN-range*}] }
	Example:
	`Device(config-mdns-sl-out)# match APPLE-TV`
	`Device(config-mdns-sl-out)# match PRINTER-APPS`
		and requests remote service information from Wide Area Bonjour domain. The service announcement and query request are processed based on permitted, built-in, or custom service types.
		The service list contains an implicit deny at the end.

Step 5	**mdns-sd controller service-policy** *controller-service-policy-name* **Example:** `Device(config)# mdns-sd controller service-policy DNAC-CONTROLLER-POLICY`	Creates a custom mDNS controller service policy.
Step 6	**service-list** *controller-service-list-name* **Example:** `Device(config-mdns-ser-policy)# service-list WIDE-AREA-SERVICES-LIST`	Associates a controller service list to a controller service policy.
Step 7	**exit** **Example:** `Device(config-mdns-sd)# exit`	Returns to global configuration mode.
Step 8	**service-export mdns-sd controller** *controller-name* **Example:** `Device(config)# service-export mdns-sd controller DNAC-BONJOUR-CONTROLLER`	Configures the service export controller to enable Wide Area Bonjour service-routing with Cisco DNA Center. Only one service export can be configured.
Step 9	**controller-service-policy** *controller-service-policy-name* **Example:** `Device(config-mdns-sd-se)# controller-service-policy DNAC-CONTROLLER-POLICY`	Associates the custom mDNS controller service policy for Wide Area Bonjour service-routing.
Step 10	**end** **Example:** `Device(config-mdns-sd-se)# end`	Returns to privileged EXEC mode.

Verifying Wide Area Bonjour for LAN and WLAN Networks

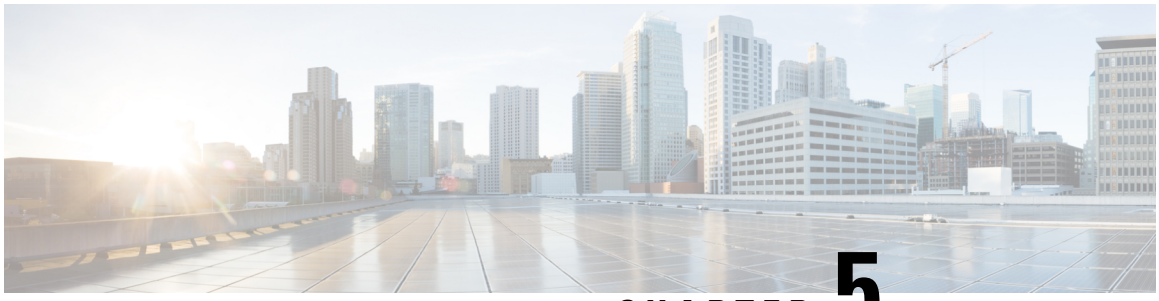
The following **show** commands are used to verify Wide Area Bonjour for LAN and WLAN networks:

- **show mdns-sd controller detail**

- **show mdns-sd controller export-summary**
- **show mdns-sd controller statistics**
- **show mdns-sd controller summary**

Additional References for Wide Area Bonjour for LAN and WLAN Networks

Related Topic	Document Title
Cisco Wide Area Bonjour Application on Cisco DNA Center User Guide	Cisco Wide Area Bonjour Application on Cisco DNA Center User Guide, Release 2.1.2
DNA Service for Bonjour Deployment on Cisco Catalyst 9800 WLCs	Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide



CHAPTER 5

Configuration Examples for Cisco DNA Service for Bonjour

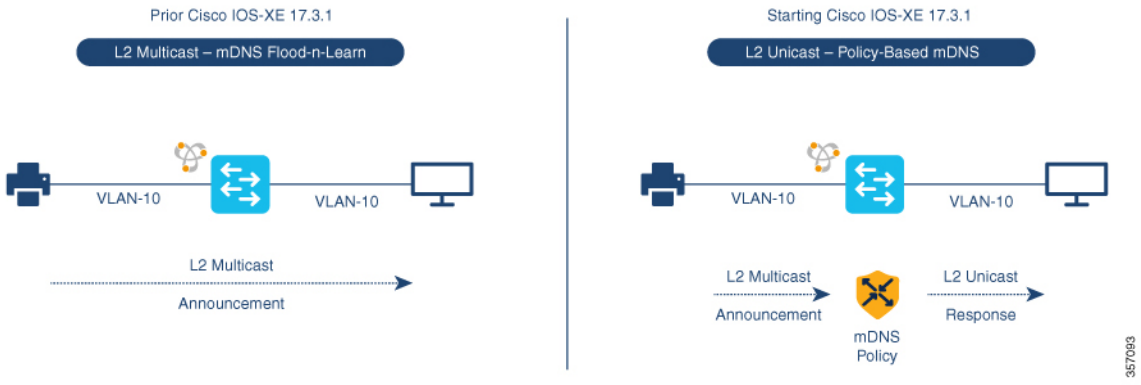
Configuration Examples for Local Area Bonjour in Unicast Mode for LAN Networks

This section provides configuration examples for Local Area Bonjour Domain in unicast mode.

Example: Single-VLAN Unicast Mode Bonjour

This example provides a sample configuration to implement Local Area Bonjour for single-VLAN unicast mode on an access layer switch. The following figure illustrates a single-VLAN unicast mode Bonjour network environment:

Figure 15: Single VLAN Unicast Mode Bonjour Network



The preceding figure illustrates a multiple-VLAN unicast mode Bonjour network environment with an AirPrint-capable printer and a user computer (MacOS or Microsoft Windows). The devices are connected to an Ethernet network and are part of a common Layer 2 VLAN. Once you configure the devices using the

following sample configuration, the user computer can dynamically discover the printer using Layer 2 unicast and policy.

Note The sample configuration provided in this section can be applied on an access layer switch deployed as a Service-Peer (Layer 2 access) or as an SDG Agent (Layer 3 access).

Table 4: Configuring Single VLAN Unicast Mode Bonjour

Configuration Step	Sample Configuration
Step 1: Enable mDNS gateway and set the gateway mode.	! mdns-sd gateway active-query timer 1 mode service-peer !
Step 2: Create a unique mDNS inbound policy to permit ingress AirPrint service announcement from the service provider.	! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipps !
Step 3: Create a unique mDNS outbound policy to permit egress AirPrint service response to the service receiver.	! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipps !
Step 4: Associate the inbound and outbound service lists to a unique service-policy.	! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT !
Step 5: Activate unicast mDNS gateway on VLAN 10 and associate the service-policy with advanced parameters.	! vlan configuration 10 mdns-sd gateway service-policy LOCAL-AREA-POLICY !

Verifying Single VLAN Unicast Mode Bonjour

Sample outputs for the following **show** commands on a Cisco Catalyst Series switch in Service Peer mode show the operational status after the discovery of AirPrint service from the local network:

```
Device# show mdns-sd summary vlan 10
VLAN  :  10
========================================
mDNS Gateway              :       Enabled
mDNS Service Policy       :       LOCAL-AREA-POLICY
Active Query              :       Enabled
                          :       Periodicity 3600 Seconds
Transport Type            :       IPv4
Service Instance Suffix . :       Not-Configured
mDNS Query Type           :       ALL
SDG Agent IP              :       10.0.1.254
```

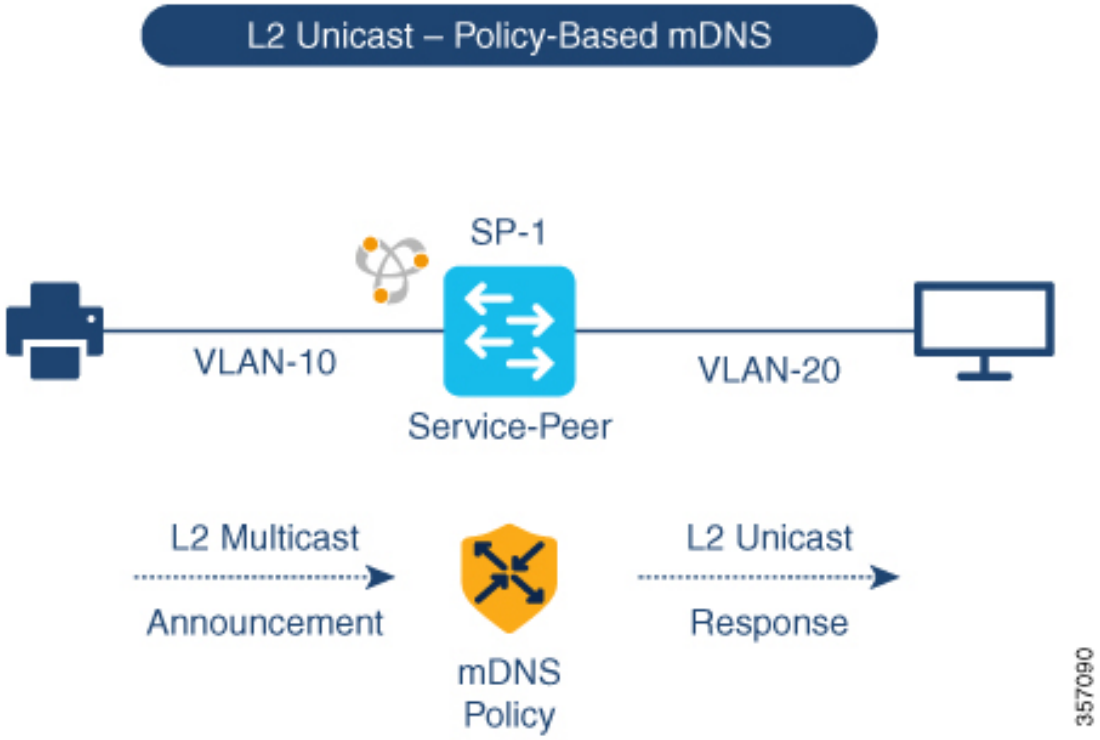
```
Source Interface          :       Vlan4094

Device#


Device# show mdns-sd service-policy name LOCAL-AREA-POLICY
Service Policy Name  Service List IN Name  Service List Out Name
================================================================================
LOCAL-AREA-POLICY                    LOCAL-AREA-SERVICES-IN LOCAL-AREA-SERVICES-OUT

Device#


Device# show mdns-sd cache vlan 10
<NAME>                              TYPE    TTL/Remaining Vlan-Id/If-name  Mac Address
 <RR Record Data>
_universal._sub._ipp._tcp.local    PTR     4500/4486         Vl10        ac18.2651.03fe
Bldg-1-FL1-PRN._ipp._tcp.local
_ipp._tcp.local                    PTR     4500/4486         Vl10        ac18.2651.03fe
Bldg-1-FL1-PRN._ipp._tcp.local
Bldg-1-FL1-PRN._ipp._tcp.local     SRV     4500/4486         Vl10        ac18.2651.03fe
0 0 631 Bldg-1-FL1-PRN.local
Bldg-1-FL1-PRN.local               A       4500/4486         Vl10        ac18.2651.03fe
10.153.1.1
Bldg-1-FL1-PRN.local               AAAA    4500/4486         Vl10        ac18.2651.03fe
2001:10:153:1:79:A40C:6BEE:AEEC
Bldg-1-FL1-PRN._ipp._tcp.local     TXT     4500/4486         Vl10        ac18.2651.03fe
(451)'txtvers=1''priority=30''ty=EPSON WF-3620 Series''usb_MFG=EPSON''usb_MDL=W~'~

Device#


Device# show mdns-sd statistics vlan 10
mDNS Statistics

 Vl10:
  mDNS packets sent                   : 612
     IPv4 sent                        : 612
       IPv4 advertisements sent       : 0
       IPv4 queries sent              : 612
     IPv6 sent                        : 0
       IPv6 advertisements sent       : 0
       IPv6 queries sent              : 0
  Unicast sent                        : 0
  mDNS packets rate limited           : 0
  mDNS packets received               : 42
   advertisements received            : 28
   queries received                   : 14
     IPv4 received                    : 42
       IPv4 advertisements received   : 28
       IPv4 queries received          : 14
     IPv6 received                    : 0
       IPv6 advertisements received   : 0
       IPv6 queries received          : 0
  mDNS packets dropped                : 0
  ========================================
  Query Type                        : Count
  ========================================
  PTR                               : 12
  SRV                               : 0
  A                                 : 0
  AAAA                              : 0
  TXT                               : 0
  ANY                               : 3
```

```
  ================================================
  PTR Name                      Advertisement   Query
  ================================================
_ipp._tcp.local                          9         4

Device#
```

Example: Multiple-VLAN Unicast Mode Bonjour

This example provides a sample configuration to implement Local Area Bonjour for multilpe-VLAN unicast mode on an access layer switch.

Figure 16: Multiple-VLAN Unicast Mode Bonjour Network



The preceding figure illustrates a multiple-VLAN unicast mode Bonjour network environment with an AirPrint-capable printer and a user computer (MacOS or Microsoft Windows). The devices are connected to an Ethernet network and are part of different Layer 2 VLANs for the same Ethernet switch. Once you configure the devices using the following sample configuration, the user computer can dynamically discover the printer using Layer 2 unicast and policy between the different VLANs.

Note The sample configuration provided in this section can be applied on an access layer switch deployed as a Service-Peer (Layer 2 access) or as an SDG Agent (Layer 3 access).

Table 5: Configuring Multiple VLAN Unicast Mode Bonjour

Configuration Step	Sample Configuration
Step 1: Enable mDNS gateway and set the gateway mode.	! mdns-sd gateway active-query timer 1 mode service-peer !
Step 2: Create a location filter to enable local service proxy between the grouped VLANs.	! mdns-sd location-filter LOCAL-PROXY match location-group default vlan 10 match location-group default vlan 20 !
Step 3: Create a unique mDNS inbound policy to permit ingress AirPrint service announcement from service provider.	! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipps !
Step 4: Create a unique mDNS outbound policy to permit egress AirPrint service response to the service receiver. Associate the location filter to share AirPrint service information from grouped VLAN.	! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipps location-filter LOCAL-PROXY !
Step 5: Associate the inbound and outbound service lists to a unique service-policy.	! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT !
Step 6: Activate unicast mDNS gateway on VLAN 10 and VLAN 20. Associate the service-policy with advanced parameters.	! vlan configuration 10,20 mdns-sd gateway service-policy LOCAL-AREA-POLICY !

Verifying Multiple VLAN Unicast Mode Bonjour

Sample outputs for the following **show** commands on a Cisco Catalyst Series switch in Service Peer mode show the operational status after the discovery of AirPrint service from the local network:

```
Device# show mdns-sd summary vlan 10
VLAN  :  10
========================================
mDNS Gateway            :       Enabled
mDNS Service Policy     :       LOCAL-AREA-POLICY
Active Query            :       Enabled
                        :       Periodicity 3600 Seconds
Transport Type          :       IPv4
Service Instance Suffix :       Not-Configured
mDNS Query Type         :       ALL
SDG Agent IP            :       10.0.1.254
Source Interface        :       Vlan4094

Device#
```

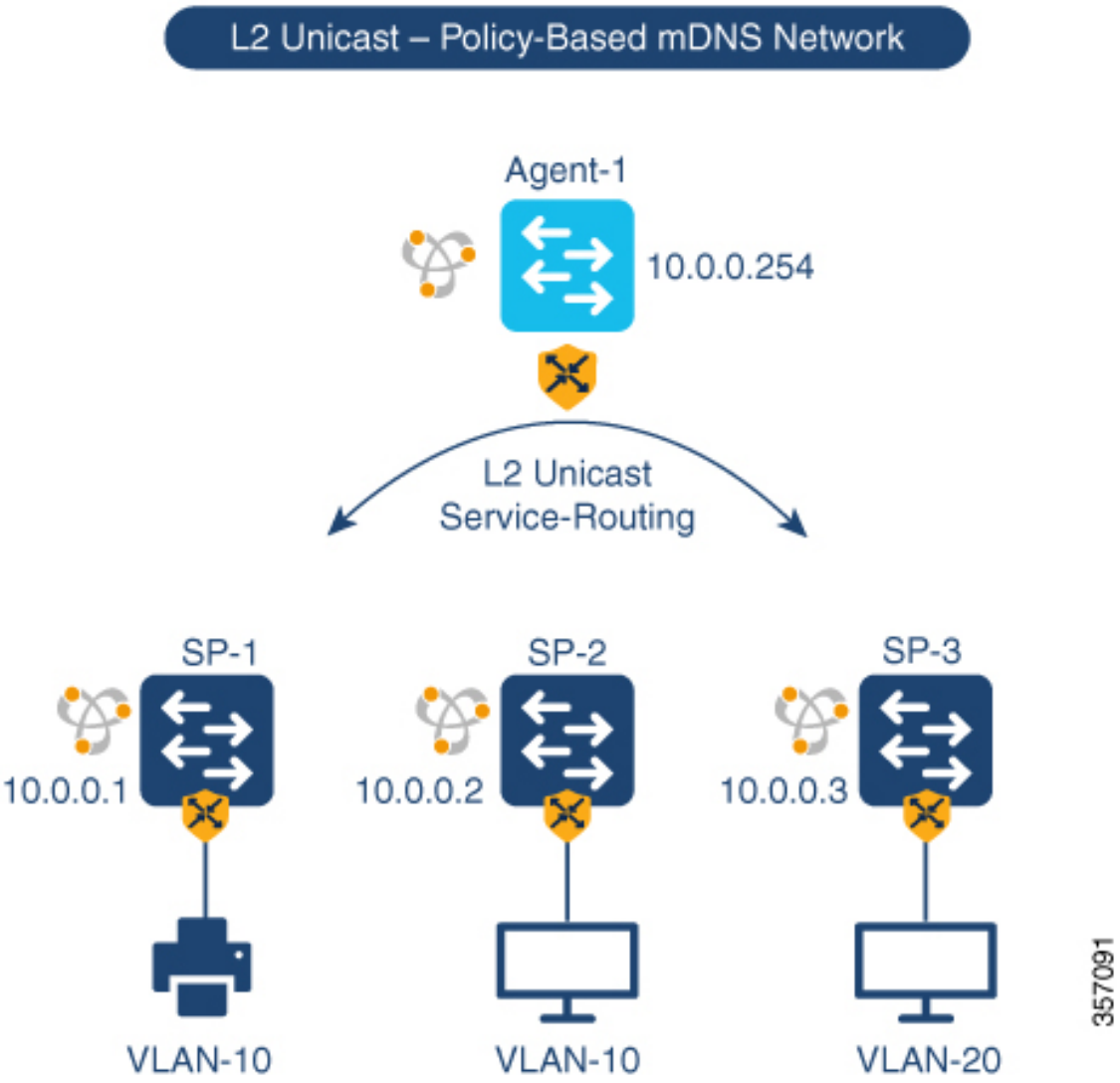
```
Device# show mdns-sd summary vlan 20
VLAN  :  20
========================================
mDNS Gateway            :        Enabled
mDNS Service Policy     :        LOCAL-AREA-POLICY
Active Query            :        Enabled
                        :        Periodicity 3600 Seconds
Transport Type          :        IPv4
Service Instance Suffix :        Not-Configured
mDNS Query Type         :        ALL
SDG Agent IP            :        10.0.1.254
Source Interface        :        Vlan4094

Device#


Device# show mdns-sd service-policy name LOCAL-AREA-POLICY
Service Policy Name  Service List IN Name  Service List Out Name
================================================================================
LOCAL-AREA-POLICY                   LOCAL-AREA-SERVICES-IN LOCAL-AREA-SERVICES-OUT

Device#


Device# show mdns-sd cache vlan 10
<NAME>                          <TYPE>  <TTL>/Remaining    Vlan-Id/If-name   Mac Address
       <RR Record Data>
_universal._sub._ipp._tcp.local    PTR    4500/4486           Vl10           ac18.2651.03fe
    Bldg-1-FL1-PRN._ipp._tcp.local
_ipp._tcp.local                   PTR    4500/4486           Vl10           ac18.2651.03fe
    Bldg-1-FL1-PRN._ipp._tcp.local
Bldg-1-FL1-PRN._ipp._tcp.local     SRV    4500/4486           Vl10           ac18.2651.03fe
    0 0 631 Bldg-1-FL1-PRN.local
Bldg-1-FL1-PRN.local                A    4500/4486           Vl10           ac18.2651.03fe
    10.153.1.1
Bldg-1-FL1-PRN.local              AAAA    4500/4486           Vl10           ac18.2651.03fe
    2001:10:153:1:79:A40C:6BEE:AEEC
Bldg-1-FL1-PRN._ipp._tcp.local     TXT    4500/4486           Vl10           ac18.2651.03fe
    (451)'txtvers=1''priority=30''ty=EPSON WF-3620 Series''usb_MFG=EPSON''usb_MDL=W~'~

Device#


Device# show mdns-sd statistics vlan 10
mDNS Statistics

 Vl10:
  mDNS packets sent              : 612
     IPv4 sent                   : 612
       IPv4 advertisements sent  : 0
       IPv4 queries sent         : 612
     IPv6 sent                   : 0
       IPv6 advertisements sent  : 0
       IPv6 queries sent         : 0
  Unicast sent                   : 0
  mDNS packets rate limited      : 0
  mDNS packets received          : 42
   advertisements received       : 28
   queries received              : 14
     IPv4 received               : 42
       IPv4 advertisements received: 28
       IPv4 queries received     : 14
     IPv6 received               : 0
```

```
      IPv6 advertisements received: 0
      IPv6 queries received      : 0
  mDNS packets dropped           : 0


  ========================================
  Query Type                     : Count
  ========================================
  PTR                            : 2
  SRV                            : 0
  A                              : 0
  AAAA                           : 0
  TXT                            : 0
  ANY                            : 3

  ================================================
  PTR Name                         Advertisement     Query
  ================================================
  _ipp._tcp.local                          21          0

Device#
```

Example: Configuring Customized Service List and Policy in Unicast Mode for Multilayer Networks

This example provides a sample configuration to implement Local Area Bonjour in unicast mode service-routing for a multilayer network. The network has Layer 2 access switches and Layer 2 or Layer 3 boundary at distribution. The mDNS gateway mode on the Layer 2 access switches must be configured as Service Peers. The distribution layer switch gets configured in SDG Agent mode by default once you activate the mDNS gateway on the specified VLANs. The mDNS service discovery and distribution is extended using an IPv4-based service-routing protocol, instead of the Layer 2 mDNS flood-n-learn over the Layer 2 trunk ports.

Figure 17: Customized Service List and Policy in Unicast Mode for a Multilayer Network



The preceding figure illustrates a VLAN unicast mode Bonjour network environment. The network has an AirPrint-capable printer connected in VLAN-10 of SP-1 switch. User-1 computer is connected in same VLAN 10 of SP-2. User-2 computer is connected to a different VLAN 20 of SP-3. Once you configure the devices using the following sample configuration, the user computers can dynamically discover the printer using Layer 2 unicast and policy on same and different VLAN IDs across the Layer 2 network.

Table 6: Configuring Customized Service List and Policy in Unicast Mode for Multilayer Networks

Configuration Step	Service Peer Sample Configuration	SDG Agent Sample Configuration
Step 1: Enable mDNS gateway and set the gateway mode.	! mdns-sd gateway active-query timer 1 mode service-peer !	! mdns-sd gateway mode service-peer !

Configuration Step	Service Peer Sample Configuration	SDG Agent Sample Configuration
Step 2: Create a unique mDNS inbound policy to permit ingress AirPrint service announcement from service provider.	! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipps !	! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipps !
Step 3: Create a unique mDNS outbound policy to permit egress AirPrint service response to the service receiver. Associate the location filter to share AirPrint service information from the grouped VLAN.	! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer location-filter LOCAL-PROXY !	! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer location-filter LOCAL-PROXY !
Step 4: Associate the inbound and outbound service lists to a unique service-policy.	! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT !	! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT !
Step 5: Activate unicast mDNS gateway on VLAN 10 and VLAN 20. Associate the service-policy with advanced parameters. Configure the SDG-Agent IP address and the source interface on Service Peer to enable service-routing. No additional configuration required on SDG-Agent.	! vlan configuration 10,20 mdns-sd gateway service-policy LOCAL-AREA-POLICY source-interface vlan 4094 sdg-agent 10.0.0.254 !	! vlan configuration 10,20 mdns-sd gateway service-policy LOCAL-AREA-POLICY !
Step 6: Configure mDNS Trust on Layer 2 trunk port of the switches.	interface range TenG 1/0/1 - 2 switchport mode trunk mdns-sd trust !	! interface range TenG 1/0/1 - 6 switchport mode trunk mdns-sd trust !
Step 7: Configure service peer-group on the SDG Agent distribution switch and enable service-routing between the assigned Service Peer switch group.	No configuration is needed.	! mdns-sd service-peer group peer-group 1 service-peer 10.0.0.1 location-group default service-peer 10.0.0.2 location-group default service-peer 10.0.0.3 location-group default !

Verifying Customized Service List and Policy in Unicast Mode for Multilayer Networks

Sample outputs for the following **show** commands on a Cisco Catalyst Series switch show the operational status after the discovery of AirPrint service from the local network:

```
Device# show mdns-sd summary vlan 10
VLAN  :  10
========================================
mDNS Gateway               : Enabled
mDNS Service Policy        : LOCAL-AREA-POLICY
Active Query               : Enabled
                           : Periodicity 3600 Seconds
Transport Type             : IPv4
Service Instance Suffix    : Not-Configured
mDNS Query Type            : ALL
SDG Agent IP               : 10.0.1.254
Source Interface           : Vlan4094

Device#


Device# show mdns-sd summary vlan 20
VLAN  :  20
========================================
mDNS Gateway               : Enabled
mDNS Service Policy        : LOCAL-AREA-POLICY
Active Query               : Enabled
                           : Periodicity 3600 Seconds
Transport Type             : IPv4
Service Instance Suffix    : Not-Configured
mDNS Query Type            : ALL
SDG Agent IP               : 10.0.1.254
Source Interface           : Vlan4094

Device#


Device# show mdns-sd service-policy name LOCAL-AREA-POLICY
Service Policy Name  Service List IN Name  Service List Out Name
=================================================================================
LOCAL-AREA-POLICY                    LOCAL-AREA-SERVICES-IN LOCAL-AREA-SERVICES-OUT

Device#


Device# show mdns-sd cache vlan 10
<NAME>                           <TYPE>  <TTL>/Remaining    Vlan-Id/If-name    Mac Address
    <RR Record Data>
_universal._sub._ipp._tcp.local    PTR    4500/4486           Vl10           ac18.2651.03fe
    Bldg-1-FL1-PRN._ipp._tcp.local
_ipp._tcp.local                     PTR    4500/4486           Vl10           ac18.2651.03fe
    Bldg-1-FL1-PRN._ipp._tcp.local
Bldg-1-FL1-PRN._ipp._tcp.local     SRV    4500/4486           Vl10           ac18.2651.03fe
    0 0 631 Bldg-1-FL1-PRN.local
Bldg-1-FL1-PRN.local                 A    4500/4486           Vl10           ac18.2651.03fe
    10.153.1.1
Bldg-1-FL1-PRN.local              AAAA    4500/4486           Vl10           ac18.2651.03fe
    2001:10:153:1:79:A40C:6BEE:AEEC
Bldg-1-FL1-PRN._ipp._tcp.local     TXT    4500/4486           Vl10           ac18.2651.03fe
    (451)'txtvers=1''priority=30''ty=EPSON WF-3620 Series''usb_MFG=EPSON''usb_MDL=W~'~

Device#


Device# show mdns-sd statistics vlan 10
mDNS Statistics

 Vl10:
```

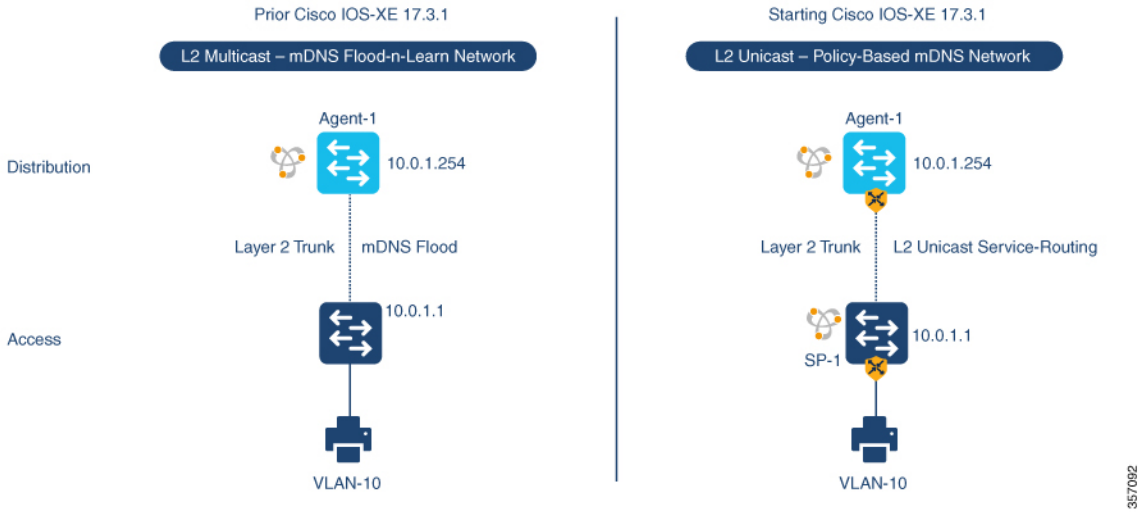
```
  mDNS packets sent               : 612
     IPv4 sent                    : 612
       IPv4 advertisements sent   : 0
       IPv4 queries sent          : 612
     IPv6 sent                    : 0
       IPv6 advertisements sent   : 0
       IPv6 queries sent          : 0
  Unicast sent                    : 0
  mDNS packets rate limited       : 0
  mDNS packets received           : 42
   advertisements received        : 28
   queries received               : 14
     IPv4 received                : 42
       IPv4 advertisements received : 28
       IPv4 queries received        : 14
     IPv6 received                : 0
       IPv6 advertisements received : 0
       IPv6 queries received        : 0
  mDNS packets dropped            : 0

  ========================================
  Query Type                       : Count
  ========================================
  PTR                              : 2
  SRV                              : 0
  A                                : 0
  AAAA                             : 0
  TXT                              : 0
  ANY                              : 3

  ================================================
  PTR Name                           Advertisement     Query
  ================================================
  _ipp._tcp.local                          21          0

Device#


Device# show mdns-sd summary vlan 10
VLAN  :  10
========================================
mDNS Gateway            : Enabled
mDNS Service Policy     : LOCAL-AREA-POLICY
Active Query            : Enabled
                        : Periodicity 3600 Seconds
Transport Type          : IPv4
Service Instance Suffix : Not-Configured
mDNS Query Type         : ALL
SDG Agent IP            : 10.0.1.254
Source Interface        : Vlan4094

Device#


Device# show mdns-sd summary vlan 20
VLAN  :  20
========================================
mDNS Gateway            : Enabled
mDNS Service Policy     : LOCAL-AREA-POLICY
Active Query            : Enabled
                        : Periodicity 3600 Seconds
Transport Type          : IPv4
Service Instance Suffix : Not-Configured
mDNS Query Type         : ALL
```

```
SDG Agent IP            : 10.0.1.254
Source Interface        : Vlan4094

Device#


Device# show mdns-sd service-policy name LOCAL-AREA-POLICY
Service Policy Name  Service List IN Name  Service List Out Name
================================================================================
LOCAL-AREA-POLICY                    LOCAL-AREA-SERVICES-IN LOCAL-AREA-SERVICES-OUT

Device#


Device# show mdns-sd sdg service-peer summary
Cache-Sync Interval: 15
Service-Peer: 40.1.1.10 Port: 10991
Uptime: 30 Hrs 24 Mins 40 secs, Cache-Sync Sent: 117
Last Cache-Sync Time: Thu Apr 16 20:50:27 2020

Service-Peer: 40.1.1.20 Port: 10991
Uptime: 31 Hrs 1 Mins 44 secs, Cache-Sync Sent: 120
Last Cache-Sync Time: Thu Apr 16 20:58:44 2020


Device# show mdns-sd sp-sdg statistics

                                        One min, 5 mins, 1 hour
Average Input rate (pps)     : 15,     5,     2
Average Output rate (pps)    :       5,     14,     2
 Messages received:
  Query                      : 219
  ANY query                  : 0
  Advertisements             : 10
  Advertisement Withdraw     : 19
  Interface down             : 2
  Vlan down                  : 0
  Service-peer ID change     : 0
  Service-peer cache clear   : 0
  Resync response            : 0
 Messages sent:
  Query response             : 129
  ANY Query response         : 0
  Cache-sync                 : 27
  Get service-instance       : 0

Device#
```

Example: Migrating from mDNS Flood to Unicast Mode in Multilayer Networks

Prior to Cisco IOS XE Amsterdam 17.3.1 release, Layer 2 LAN switches functioned as an intermediate pass-through system between an upstream SDG Agent in distribution layer and locally attached wired mDNS end points. This example provides a sample configuration to migrate from mDNS flood to unicast mode in multilayer networks. The network has Layer 2 access switches and Layer 2 or Layer 3 boundary at distribution.

Figure 18: Migration from mDNS Flood to Layer 2 Service-Routing Unicast Mode



The preceding figure illustrates a sample multilayer network that provides key gateway functional difference before and after upgrading to Cisco IOS XE Amsterdam 17.3.1 release.

The following table provides sample configurations for a traditional mDNS flood-based network and a Cisco Catalyst Series switch in SDG Agent mode that operates in a Layer 2 network environment.

Table 7: Layer 2 Access Configuration and Layer 3 SDG Agent Configuration

Layer 2 Access Sample Configuration	Layer 3 SDG Agent Sample Configuration
! interface TenG 1/1 switchport mode trunk switchport trunk allowed vlan 10,4094 ! interface Vlan 4094 description CAMPUS LAN MGMT ip address 10.0.1.1 255.255.255.0 no shutdown !	! interface TenG 1/1 switchport mode trunk switchport trunk allowed vlan 10,4094 ! interface Vlan 4094 description CAMPUS LAN MGMT ip address 10.0.1.254 255.255.255.0 no shutdown ! mdns-sd gateway active-query timer 1 ! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipps ! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipps ! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT ! ! mDNS Flood-based gateway ! interface vlan 10 mdns-sd gateway service-policy LOCAL-AREA-POLICY !

The following table provides sample configurations for migration to a Layer 2 unicast-based network for a Cisco Catalyst switch in SDG Agent and Service Peer mode that operates in a Layer 2 network environment. The Layer 2 unicast routing functions between SDG Agent and Service Peer. Thus, no further controller-bound policy or export configuration change is required for the migration to unicast mode.

Table 8: Configuring Layer 2 Access and Layer 3 SDG Agent for Migration to Layer 2 Service-Routing Unicast Mode

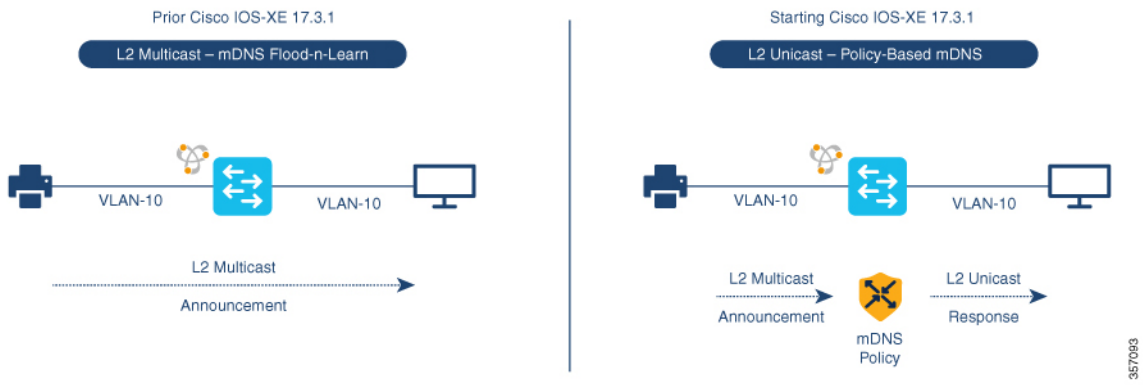
Configuration Step	Layer 2 Access Sample Configuration	Layer 3 SDG Agent Sample Configuration
Step 1: Enable Layer 2 Trunk mode between access and distribution switches.	! interface TenG 1/1 switchport mode trunk switchport trunk allowed vlan 10, 4094 mdns trust !	! interface TenG 1/1 switchport mode trunk switchport trunk allowed vlan 10, 4094 mdns trust !

Configuration Step	Layer 2 Access Sample Configuration	Layer 3 SDG Agent Sample Configuration
Step 2: Configure the LAN management VLAN and assign a valid IP range.	```! interface Vlan 4094 description CAMPUS LAN MGMT ip add 10.0.1.1 255.255.255.0 no shutdown ! ```	```! interface Vlan 4094 description CAMPUS LAN MGMT ip add 10.0.1.254 255.255.255.0 no shutdown ! ```
Step 3: Enable mDNS gateway and modes at access and distribution switches.	```! mdns-sd gateway mode service-peer ! ```	```! mdns-sd gateway mode sdg-agent ! ```
Step 4: Create a unique mDNS inbound policy to permit ingress AirPrint service announcement from the service provider.	```! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipps ! ```	```! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipps ! ```
Step 5: Create a unique mDNS outbound policy to permit egress AirPrint service response to the service receiver. Associate the location filter to share AirPrint service information from the grouped VLAN.	```! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipps ! ```	```! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipps ! ```
Step 6: Associate inbound and outbound service lists to a unique service policy.	```! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT ! ```	```! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT ! ```
Step 7: Disable mDNS gateway from the SVI interface.	No configuration is needed.	```! interface vlan 10 no mdns-sd gateway ! ```
Step 8: Enable a unicast-based mDNS gateway on VLAN 10. Associate the service policy with advanced parameters. Configure the SDG Agent IP address and the source interface settings on the Service Peer.	```! ! mDNS Unicast based gateway ! vlan configuration 10 mdns-sd gateway service-policy LOCAL-AREA-POLICY active-query timer 1 sdg-agent 10.0.0.254 source-interface Vlan 4094 ! ```	```! ! mDNS Unicast based gateway ! vlan configuration 10 mdns-sd gateway ! ```
Step 9: Clear cache on the SDG Agent to remove stale entries which are learnt from the mDNS flood.	No configuration is needed.	```! clear mdns-sd cache ! ```

Example: Migrating from mDNS Flood to Unicast Mode in Routed Access Networks

Prior to Cisco IOS XE Amsterdam 17.3.1 release, a Layer 3 Access LAN switch limits the extension of mDNS flood to the upstream Layer 3 network. However, it continues to flood the incoming mDNS frames to all ports participating in a common Layer 2 broadcast domain. This example provides a sample configuration to migrate from mDNS flood to unicast mode in Layer 3 or routed access networks. The network has Layer 2 access switches and Layer 2 or Layer 3 boundary at distribution.

Figure 19: Migration from mDNS Flood to Layer 3 Unicast Mode



The preceding figure illustrates a sample routed access network that provides key gateway functional difference before and after upgrading to Cisco IOS XE Amsterdam 17.3.1 release.

The following table provides sample configurations for a traditional mDNS flood-based network and a Cisco Catalyst Series switch in SDG Agent mode that operates in a Layer 2 network environment.

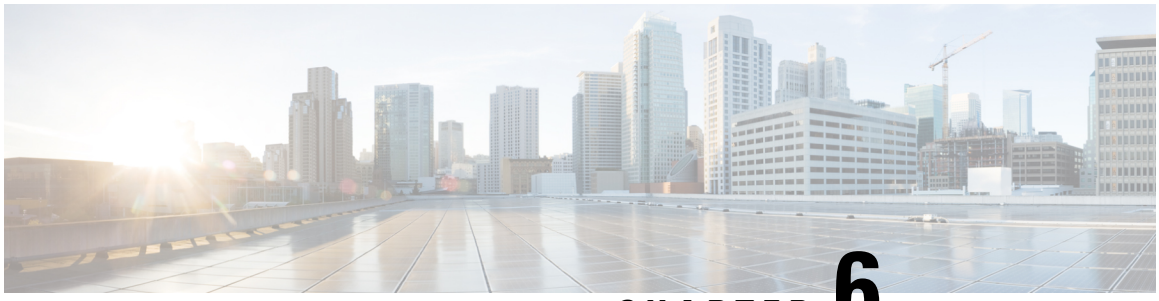
Table 9: Layer 2 Access Configuration and Layer 3 SDG Agent Configuration

Layer 2 Access Sample Configuration	Layer 3 SDG Agent Sample Configuration
! interface TenG 1/1 switchport mode trunk switchport trunk allowed vlan 10,4094 ! interface Vlan 4094 description CAMPUS LAN MGMT ip address 10.0.1.1 255.255.255.0 no shutdown !	! interface TenG 1/1 switchport mode trunk switchport trunk allowed vlan 10,4094 ! interface Vlan 4094 description CAMPUS LAN MGMT ip address 10.0.1.254 255.255.255.0 no shutdown ! mdns-sd gateway active-query timer 1 ! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipps ! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipps ! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT ! ! mDNS Flood-based gateway ! interface vlan 10 mdns-sd gateway service-policy LOCAL-AREA-POLICY !

The following table provides sample configurations for migration to a Layer 2 unicast-based network for a Cisco Catalyst switch in SDG Agent that operates in a Layer 3 network environment. The unicast mode function is a local function on the SDG Agent. Thus, no further controller bound policy or export configuration change required for the migration to unicast mode.

Table 10: Configuring Layer 2 Access and Layer 3 SDG Agent for Migration to Layer 3 Unicast Mode

Configuration Step	Layer 2 Access Sample Configuration	Layer 3 SDG Agent Sample Configuration
Step 1: Enable mDNS gateway and modes at access and distribution switches.	No configuration is needed.	```! mdns-sd gateway active-query timer 1 mode sdg-agent ! ```
Step 2: Create a unique mDNS inbound policy to permit ingress AirPrint service announcement from the service provider.		```! mdns-sd service-list LOCAL-AREA-SERVICES-IN in match printer-ipps ! ```
Step 3: Create a unique mDNS outbound policy to permit egress AirPrint service response to the service receiver. Associate the location filter to share AirPrint service information from the grouped VLAN.		```! mdns-sd service-list LOCAL-AREA-SERVICES-OUT out match printer-ipps ! ```
Step 4: Associate inbound and outbound service lists to a unique service policy.		```! mdns-sd service-policy LOCAL-AREA-POLICY service-list LOCAL-AREA-SERVICES-IN service-list LOCAL-AREA-SERVICES-OUT ! ```
Step 5: Disable mDNS gateway from the SVI interface.		```!! interface vlan 10 no mdns-sd gateway ! ```
Step 6: Enable a unicast-based mDNS gateway on VLAN 10. Associate the service policy with advanced parameters.		```! ! mDNS Unicast based gateway ! vlan configuration 10 mdns-sd gateway service-policy LOCAL-AREA-POLICY ! source-interface vlan 4094 ! ```



CHAPTER 6

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

- 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.
- Ensure that all the prerequisites described in *Configuring Local Area Bonjour in Unicast Mode for LAN Networks* module are completed.

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.

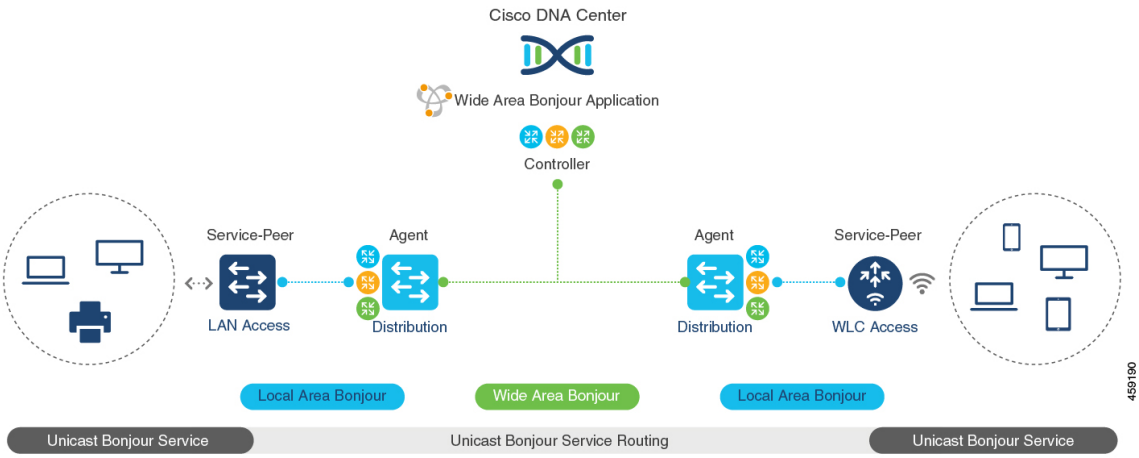
Information about VRF-Aware Local Area Bonjour Services

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, BGP EVPN VXLAN or classic technologies such as Multi-VRF, MPLS.

Figure 20: 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 20: Cisco DNA Service for Bonjour with VRF-Aware Services

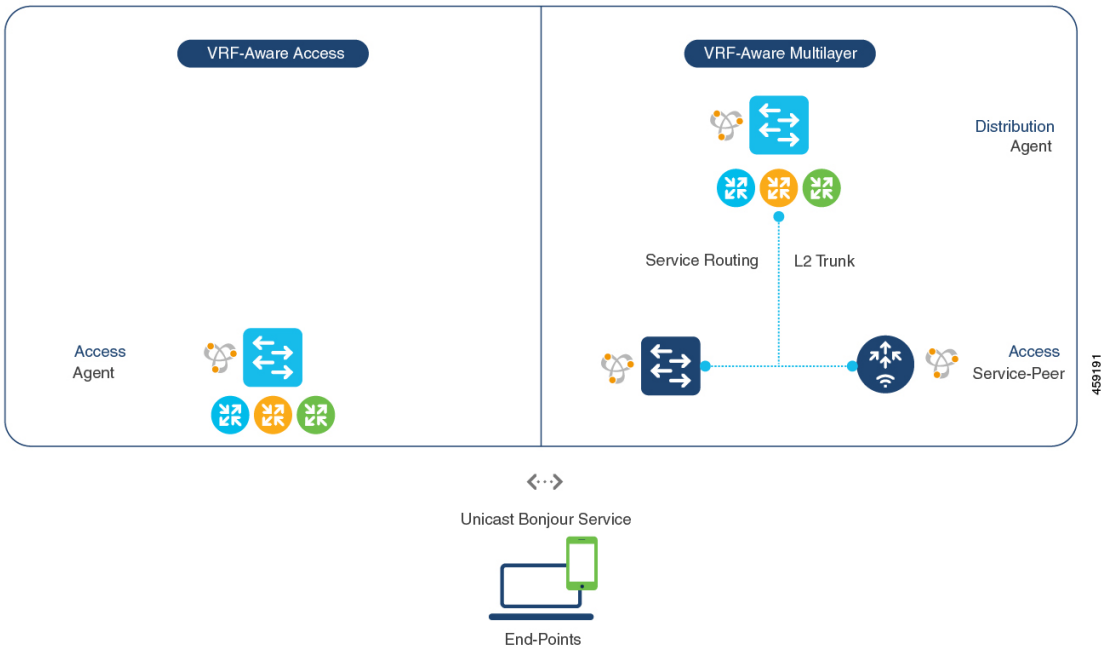


Gateway Modes for VRF-Aware Bonjour Services

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 21: 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 21: 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.

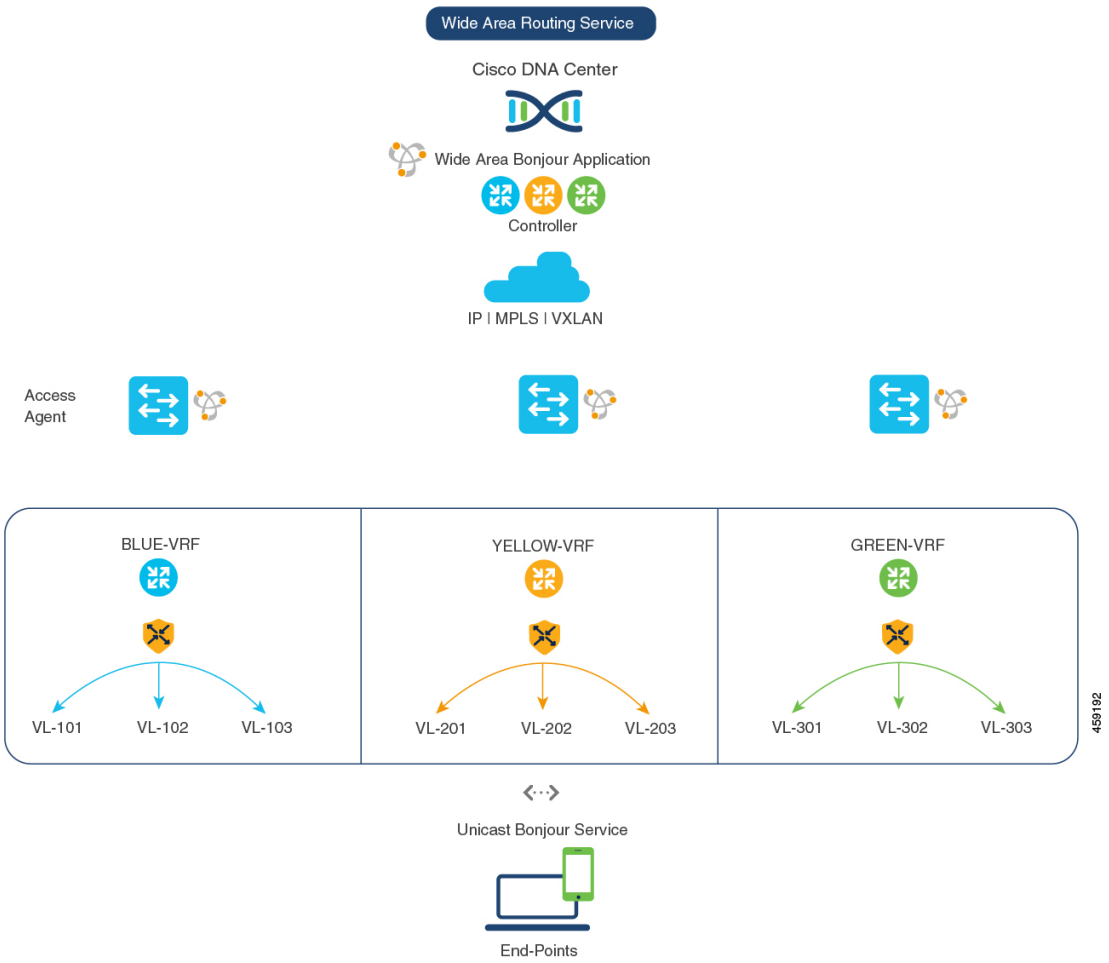
Understanding VRF-Aware Wide Area Bonjour Services

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

Figure 22: VRF-Aware Wide Area Bonjour Services



The *Configuring Wide Area Bonjour* module lists the configuration procedures in detail.

Understanding VRF-Aware Service on Multilayered Wired and Wireless Networks

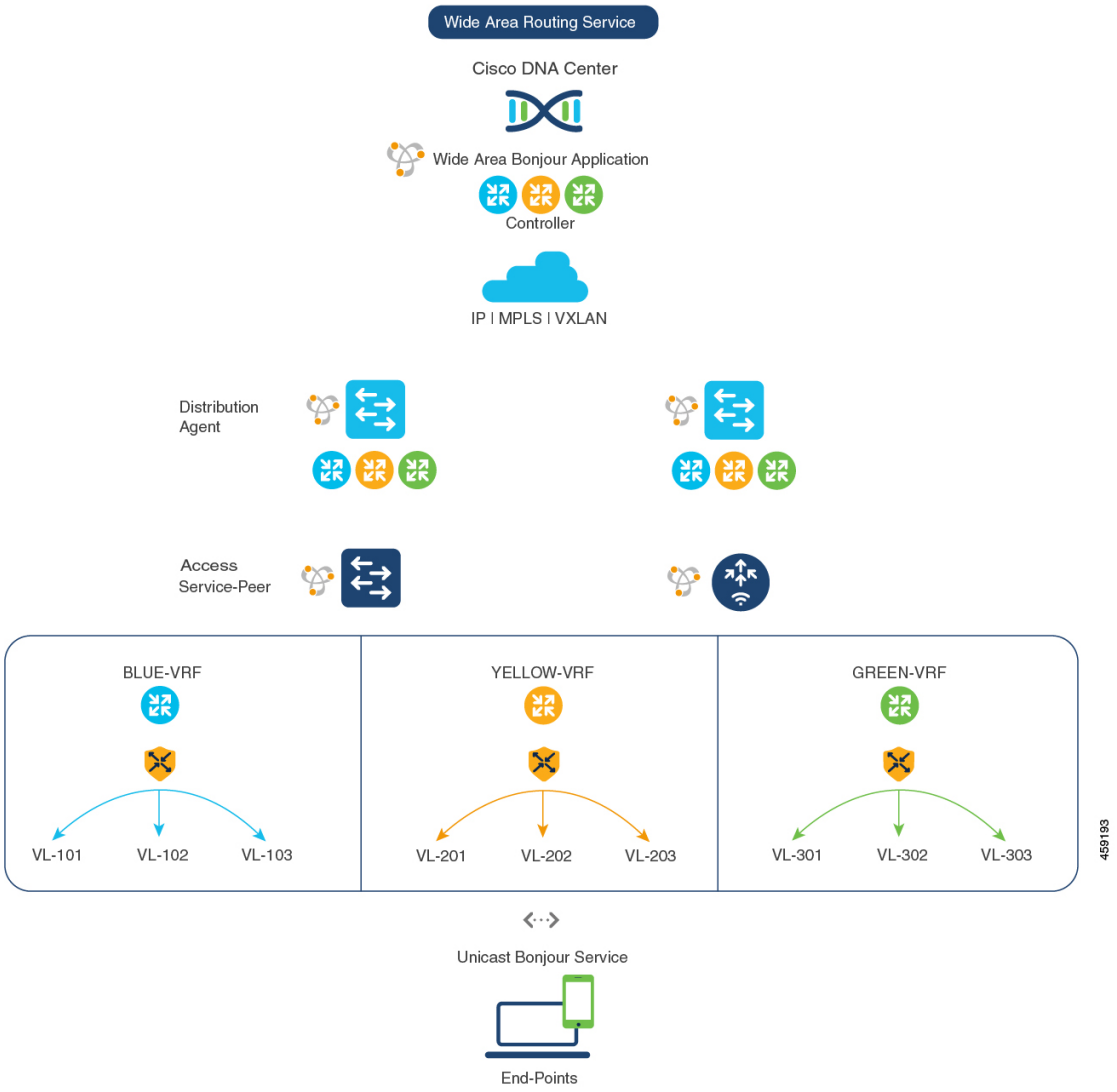
The Cisco Catalyst 9000 Series switches support VRF-Aware service for multilayered Wired and central-switching Wireless-enabled networks. The Layer 2 or Layer 3 network boundary to the Cisco Catalyst 9000 Series switches is extended at the distribution layer with an intermediate Layer 2 Cisco Catalyst 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 80. 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 23: 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 23: VRF-Aware on Multilayered Wired and Wireless Network



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

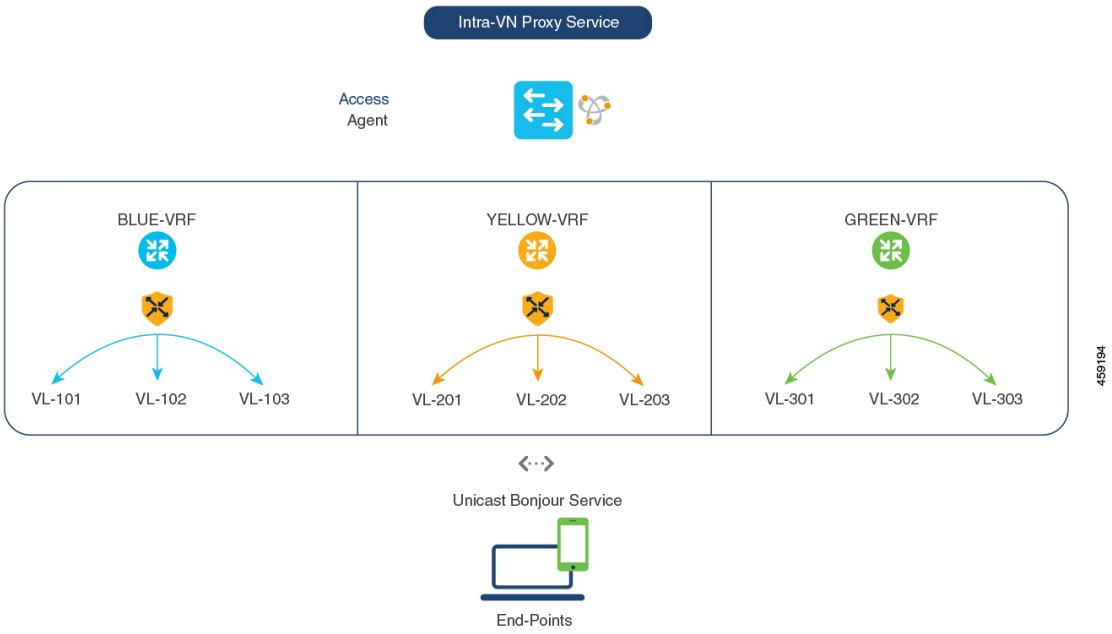
Intra-Virtual Network (Intra-VN) Proxy Service is a policy-based VRF-Aware service discovery and distribution implemented on the IP VRF of a switch in SDG-Agent mode connected to multiple IP networks.

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 24: Intra-VN Service Proxy illustrates VRF-Aware enabled on an Intra-VN proxy service.

Figure 24: Intra-VN Service Proxy



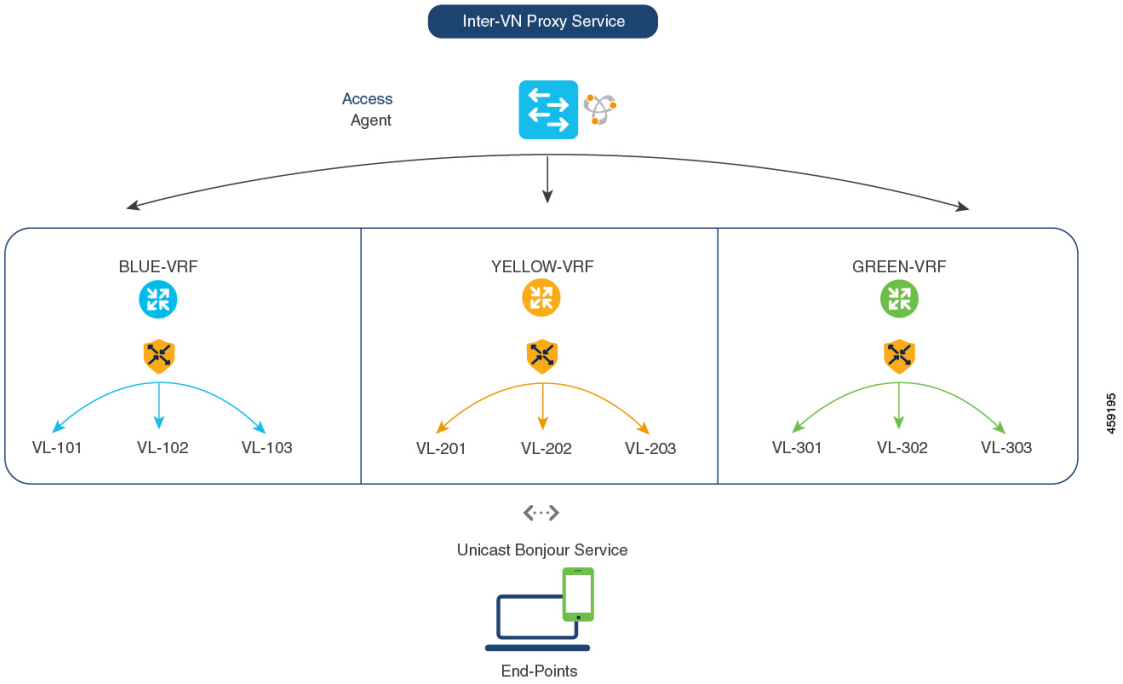
How to configure Inter-Virtual Network Proxy Service on Local Area Bonjour Domain

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 25: Inter-VN Proxy Service shows Inter-VN proxy service for Extranet network.

Figure 25: Inter-VN Proxy Service



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
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**vlan** *ID*
	Example:
	`Device(config)# vlan 101`
	`Device(config-vlan)# name BLUE-VRF`
	`Device(config)# vlan 201`
	`Device(config-vlan)# name YELLOW-VRF`
	`Device(config)# vlan 301`
	`Device(config-vlan)# name GREEN-VRF`
		Configures a VLAN ID in local database for overlay mDNS endpoints.

	Command or Action	Purpose
Step 4	**mdns-sd location-filter** *location-filter-name* **Example:** `Device(config)# mdns-sd location-filter INTER-VN-LOCAL-PROXY`	Configures a unique location-filter.

Step 5	**match location** {**all** | **default** | **ID**} **vlan** [**ID**]
	Example:
	`Device(config-mdns-loc-filter)# match location-group default vlan 101`
	`Device(config-mdns-loc-filter)# match location-group default vlan 201`
	`Device(config-mdns-loc-filter)# match location-group default vlan 301`
		Configures the match criteria that mutually distribute permitted services between grouped VLANs.

Step 6	**mdns-sd service-list** *service-list-name* {**in** | **out**} **Example:** `Device(config)# mdns-sd service-list BLUE-VRF-LIST-OUT out`	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.

Step 7	**match** *service-destination-name* [**message-type** {**any** | **announcement** | **query**}]
	Example:
	`Device(config)# mdns-sd service-list BLUE-VRF-LIST-OUT out`
	`Device(config-mdns-sl-out)# match APPLE-TV location-filter LOCAL-PROXY`
		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.
		The service-list contains implicit deny at the end.
		The message-type for outbound service-list is not required.

Step 8	**mdns-sd service-policy** *service-policy-name* **Example:** `Device(config)# mdns-sd service-policy BLUE-VRF-POLICY`	Creates a unique mDNS service-policy.

Step 9	**service-list** *service-list-name* {**in** | **out**}
	Example:
	`Device(config)# mdns-sd service-policy BLUE-VRF-POLICY`
	`Device(config-mdns-ser-policy)# service-list BLUE-VRF-LIST-OUT out`
		Configures an mDNS service policy to associate with the service-list for each direction.

Step 10	**vlan configuration** *ID* **Example:** `Device(config)# vlan configuration 101-103`	Enables VLAN configuration for advanced service parameters. One or more VLANs can be created for the same settings. For example, the VLAN

	Command or Action	Purpose
		configuration range 101-110 or 200 allows to configure consecutive and nonconsecutive VLAN IDs.
Step 11	**mdns-sd gateway** **Example:** `Device(config-vlan)# mdns-sd gateway`	Enables the mDNS gateway on the specified VLAN IDs.
Step 12	**service-policy BLUE-VRF-POLICY** **Example:** `Device(config-vlan-mdns)# service-policy BLUE-VRF-POLICY`	Associates an mDNS service-policy with the specified VLAN IDs.
Step 13	**end** **Example:** `Device(config-vlan-mdns)# end`	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=0x5A7FFFF7,0x1E''flags=0x44''model=~'~
A01828F29889@RTP-ATV-1._raop._tcp.local      TXT         4500/4495         511
```

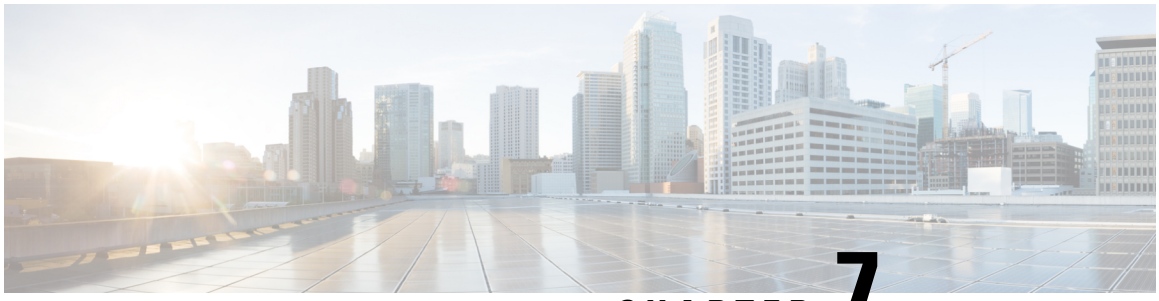
```
   a018.28f2.9889
(177)'cn=0,1,2,3''da=true''et=0,3,5''ft=0x5A7FFFF7,0x1E''md=0,1,2''am=AppleTV3,2'~
```

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 11: Commands to Verify VRF-Aware Services

Command	Purpose
show mdns-sd cache {**all** | **interface** | **mac** | **name** | **service-peer** | **static** | **type** | **vlan** | **vrf**}	Displays all available mDNS cache record that supports multiple variables and provides granular source details. The following variables are available: • **all**: Displays all available cache records discovered from multiple source connections of a system. • **interface**: Displays the available cache records discovered from a specified Layer 3 interface. • **mac**: Displays the available cache records discovered from the specified MAC address. • **name**: Displays the available cache records based on service provider announced name. • **service-peer**: Displays available cache records discovered from the specified Layer 2 Service-Peer. • **static**: Displays the locally configured static mDNS cache entries. • **type**: Displays the available cache records based on the specific mDNS record type (PTR, SRV, TXT, A, or AAAA). • **vlan**: Displays the available cache records discovered from the specified Layer 2 VLAN ID in unicast mode. • **vrf**: Displays each VRF available cache records based on the specific mDNS record type (PTR, SRV, TXT, A, or AAAA).
show mdns-sd service-definition {**name** | **type**}	Displays the built-in and user-defined custom service definitions and provides the mapping from service name to mDNS PTR records. The service-definition can be filtered by name or type.

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



CHAPTER 7

Feature History for Cisco DNA Service for Bonjour

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: • Cisco Catalyst 2960-X Series Switches • Cisco Catalyst 2960-XR Series Switches
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: • Cisco Catalyst 4500-E Series Switches • Cisco Catalyst 4500-X Series Switches

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	Cisco DNA Service for Local Area Bonjour and Wide Area Bonjour (Multicast DNS Mode only) was introduced on the following platforms: • Cisco Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches • Cisco Catalyst 9300 Series Switches • Cisco Catalyst 9400 Series Switches • Cisco Catalyst 9500 Series Switches • Cisco Catalyst 9500 Series Switches - High Performance • Cisco Catalyst 9600 Series Switches • Cisco Catalyst 9800 Series Wireless Controllers • Cisco 5500 Series Wireless Controllers • Cisco 8540 Wireless Controllers • Cisco 4000 Series Integrated Services Routers (ISR)
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	Introduced Cisco DNA Service for Bonjour support for the following: • SD-Access network • Unicast mode for LAN network
Cisco IOS XE Amsterdam 17.3.2a	Introduced Cisco DNA Service for Bonjour support for the following: • Multilayer networks • Location grouping in wired networks • mDNS AP group in wireless networks

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	Introduced support for the following features for Local Area Bonjour in Unicast Mode for LAN networks: • HSRP-aware mDNS Service-Routing • mDNS Service-Gateway SSO Support • Default mDNS Service-list and policy support. The following commands have been modified: • **active-query timer**: Global configuration mode support is introduced. • **active-query timer**: Second-based configuration support is replaced with minute-based global timer setting support. • **service-mdns-query** : Global configuration mode support is introduced
Cisco IOS XE Bengaluru 17.6.2	Configuration of Cisco Wide Area Bonjour requires you to configure the Cisco Catalyst Series switch in SDG Agent mode and optionally build a custom service policy in Wide Area Bonjour application of Cisco DNA Center. If you do not build a custom service policy, then the default service policy is build into the Wide Area Bonjour application. The following commands are modified: • **mdns-sd controller service-list** *controller-service-list-name* • **match** {**all**|*service-definition-name* [**message-type** {**any**| **announcement**|**query**}] [**source-interface** {*mDNS-VLAN-number* | *mDNS-VLAN-range*}] } • **mdns-sd controller service-policy** *controller-service-policy-name* • **service-list** *controller-service-list-name* • **controller-service-policy** *controller-service-policy-name*

Feature History for Cisco DNA Service for Bonjour

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This feature was implemented on supervisor modules C9400X-SUP-2 and C9400X-SUP-2XL, which were introduced in this release.