

Cisco DNA Service for Bonjour

Contents

Introduction	2
Cisco DNA Service for Bonjour architecture	11
Deploying Wide Area Bonjour – distributed fabric	18
Deploying Wide Area Bonjour – hybrid fabric	24
Deploying Inter-VN service routing	26
Deploying the Wide Area Bonjour application	29
Appendix	52
Summary	53
Reference	53

SD-Access Wired and Wireless Deployment Guide – version 1.0

Introduction

Bonjour technology was invented and standardized by Apple. It is a zero-configuration solution that simplifies network configuration and enables communication between connected devices, services, and applications. Bonjour leverages link-local multicast DNS (mDNS) and is designed to enable peer-to-peer communication on a single Layer 2 domain. It is ideal for small, flat, single-domain setups, such as home networks.

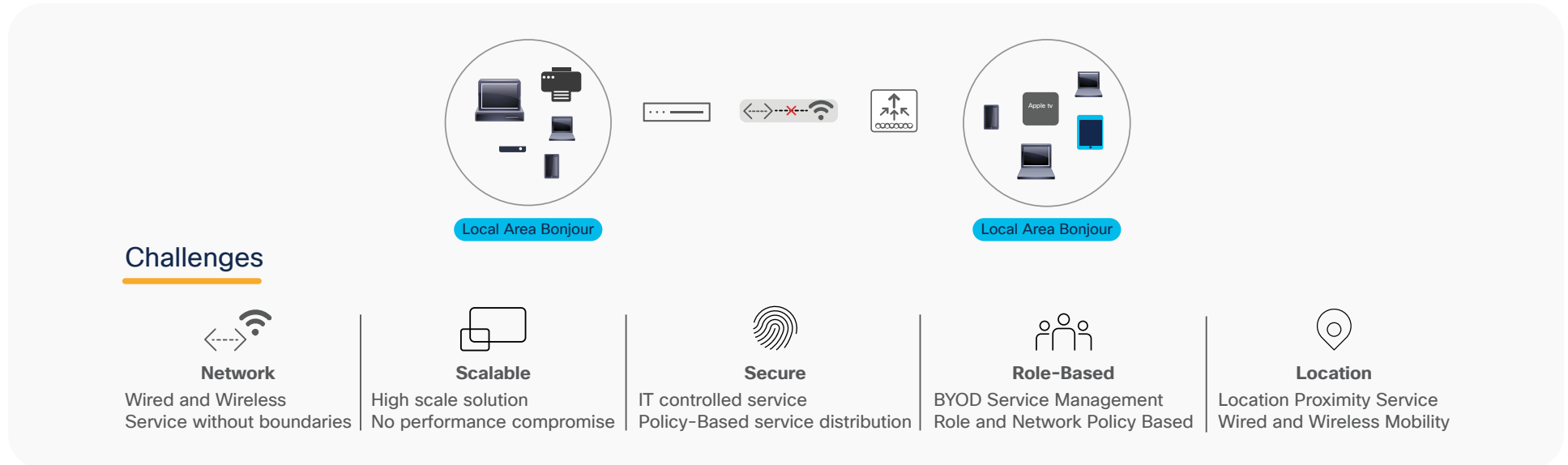
The mDNS enabled services on consumer products, digital conference rooms, Internet of Things (IoT) devices, and more are pervasive in service-oriented enterprise network. Cisco DNA Service for Bonjour eliminates the single Layer 2 domain constraint and expands the scope to enterprise-grade traditional wired and wireless networks, next-generation fabric-based overlay networks such as Cisco® Software-Defined Access (SD-Access), and industry-standard Border Gateway Protocol (BGP) Ethernet VPN (EVPN) with Virtual Extensible LAN (VXLAN). The Cisco Catalyst® 9000 family of LAN switches and Cisco Catalyst 9800 Series Wireless Controllers follow the industry-standard, RFC 6762-based mDNS specification to support interoperability with various compatible wired and wireless consumer products in enterprise networks.

Challenges

Enterprise networks are going through constant digital transformation as more and more smart and services-rich devices are being connected. While every device is designed with different purposes, the user-centric application and operational simplicity in their operation remains the core focus in technology. The plug-and-play service discovery and distribution using Bonjour technology in networks eases IT's task of managing devices.

The IT administrator faces several challenges in large and complex enterprise networks to seamlessly introduce a Bonjour technology that was originally designed to operate in a single Layer 2 broadcast domain. Since the proliferation of Bonjour devices and mandatory service requirements, networking vendors have introduced a gateway solution that allows services discovery between local network segments. The solution overcomes the initial challenge but continues to be limited, as the service discovery and distribution occur up to a single gateway only, without any end-to-end solution. The centralized architecture of a single gateway quickly becomes a bottleneck as the network expands, demanding more scale and performance and impacting other core networking functions. The figure below illustrates the challenges and requirements Bonjour brings to enterprise networks.

Figure 1. Bonjour challenges in enterprise networks



Following are key Bonjour challenges in large-scale enterprise networks:

- **Networks** – The mDNS providers and receivers across disjointed and complex enterprise wired and wireless networks cannot be connected without extending network-wide flood boundaries to central service gateway point.
- **Scalable** – The central service architecture may operate at limited scale, as next-generation networks, endpoints and mDNS service scale increases multi-dimensionally it may degrade overall network and user-experience with un-sustainable classic flood-n-learn gateway solution.
- **Secure** – In flood-n-learn based wired and wireless networks, the IT organizations have limited to no mDNS security control to manage specific services and enforce policy based on locations etc. The networks or consumer endpoints may become vulnerable for possible security attacks.
- **Role-Based** – The network access control may be enforced based on roles and profiling, however the service access control may not be possible

as network cannot distinctly identify mDNS providers or receivers roles in flooded networks to enforce mDNS service security policy.

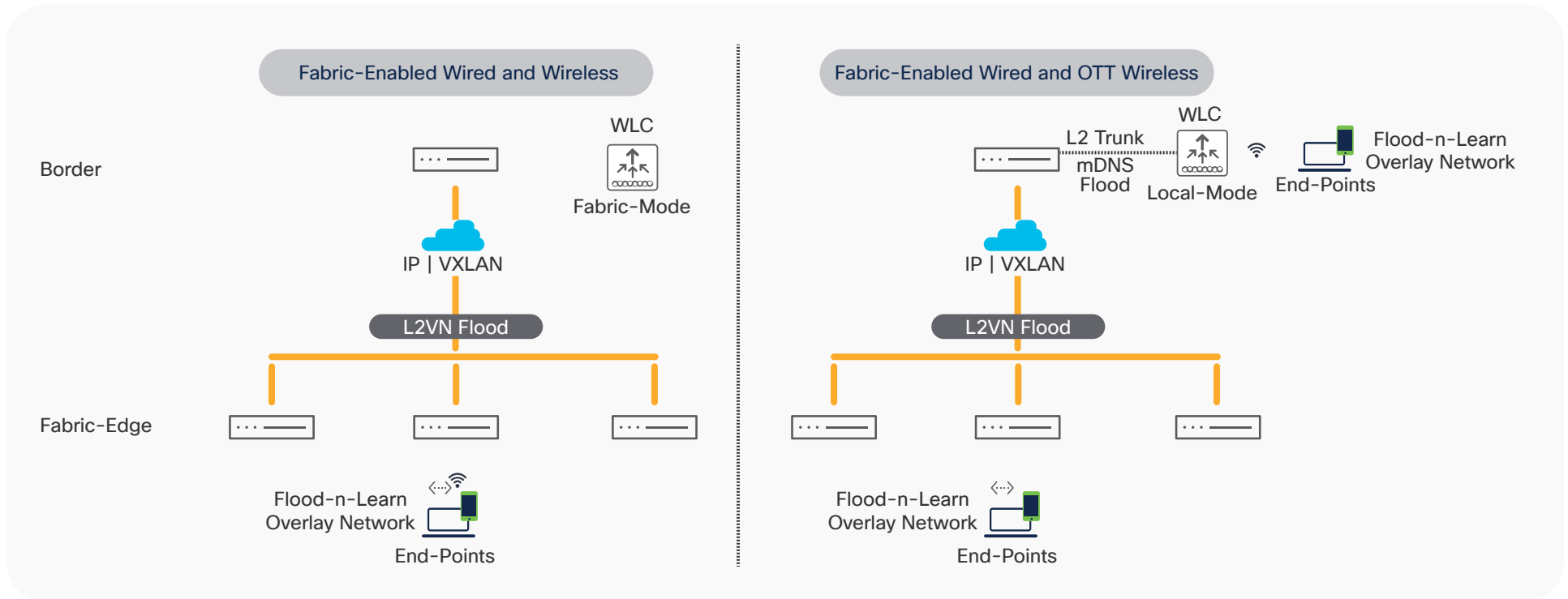
- **Location** – The intuitive user-experience demands dynamic service discovery within close-proximity to quickly locate and use. The granular location-based mDNS service management is challenging in large Layer 2 flooded traditional or fabric-based network environments.

Cisco SD-Access is a turnkey enterprise networking solution that enables IT organizations to transform traditional networks into new, intuitive, and modern Software-Defined Networking (SDN) solutions supporting a complete network lifecycle of design, build, and manage phases from Cisco DNA Center. Cisco SD-Access replaces traditional Spanning-Tree based Layer 2 networks in a LAN with simple Layer 3 routed networks while supporting Layer 2 extensions in overlay virtual networks. The user experience is further enhanced by shifting centralized wireless networks to fully distributed wireless deployments using Cisco SD-Access technology.

As the traditional Layer 2 network design changes for LAN and wireless, the applications and services relying on link-local Layer 2 multicast such as mDNS may be affected. The mDNS service boundary becomes limited to a single IP gateway SD-Access Fabric-Edge (FE) switch, impacting the user's ability to share or browse services across fabric-enabled wired and wireless networks. In addition, Cisco SD-Access allows the flexibility to transition networks in phases. The LAN can transition to SD-Access while retaining the Cisco wireless design with centralized local mode switching. In such hybrid networking designs, the mDNS service discovery boundary between fabric-enabled LAN and traditional wireless LAN is further divided to provide a seamless transition.

The interim alternative to both deployment models can be solved through Layer 2 Virtual Network (L2VN) flooding over the SD-Access fabric. The L2VN flooding extends the broadcast domain across the IP core backbone network within the SD-Access fabric network and beyond. In small to midsize fabric environments, this workaround may be sufficient. However, as the network grows multidimensionally with a higher number of VNs, users, and services, it may not scale. The standard design principle for underlay or overlay networks is to keep the Layer 2 network contained, providing better security and a fault domain across wired and wireless networks. The figure below illustrates two commonly deployed Cisco SD-Access fabric-enabled wired and wireless networks with L2VN flooding to enable an interim mDNS solution.

Figure 2. Cisco SD-Access L2VN flooding challenge



The following are key L2VN flooding challenges in large-scale Cisco SD-Access wired and wireless networks:

- **Single VLAN:** The mDNS flood boundary is limited to a single IP pool or VLAN. The mDNS services between IP pools within the same VN cannot be discovered and distributed. For example, a wired printer in the print VLAN cannot be discovered by users in the wireless VLAN.
- **Scale:** The enterprise-grade fabric network may consist of several VNs and IP pools, each supporting a large number of user groups and mDNS services. As the network becomes more multidimensional, the core network scale and performance may be compromised with a large amount of flooded L2VN bridging broadcast, unknown unicast, and multicast category traffic across the core backbone.
- **Security:** The network security and fault domain size are the same as for the Layer 2 flood domain. Enterprise network systems, endpoints, and applications may become vulnerable by extending several VLANs over L2VN across the fabric core network.
- **Experience:** The flood-and-learn-based networks cannot distinguish user roles, networks, or location. The end-user experience is impacted by this, as it lacks security, close proximity-based services, and reliable service connection.

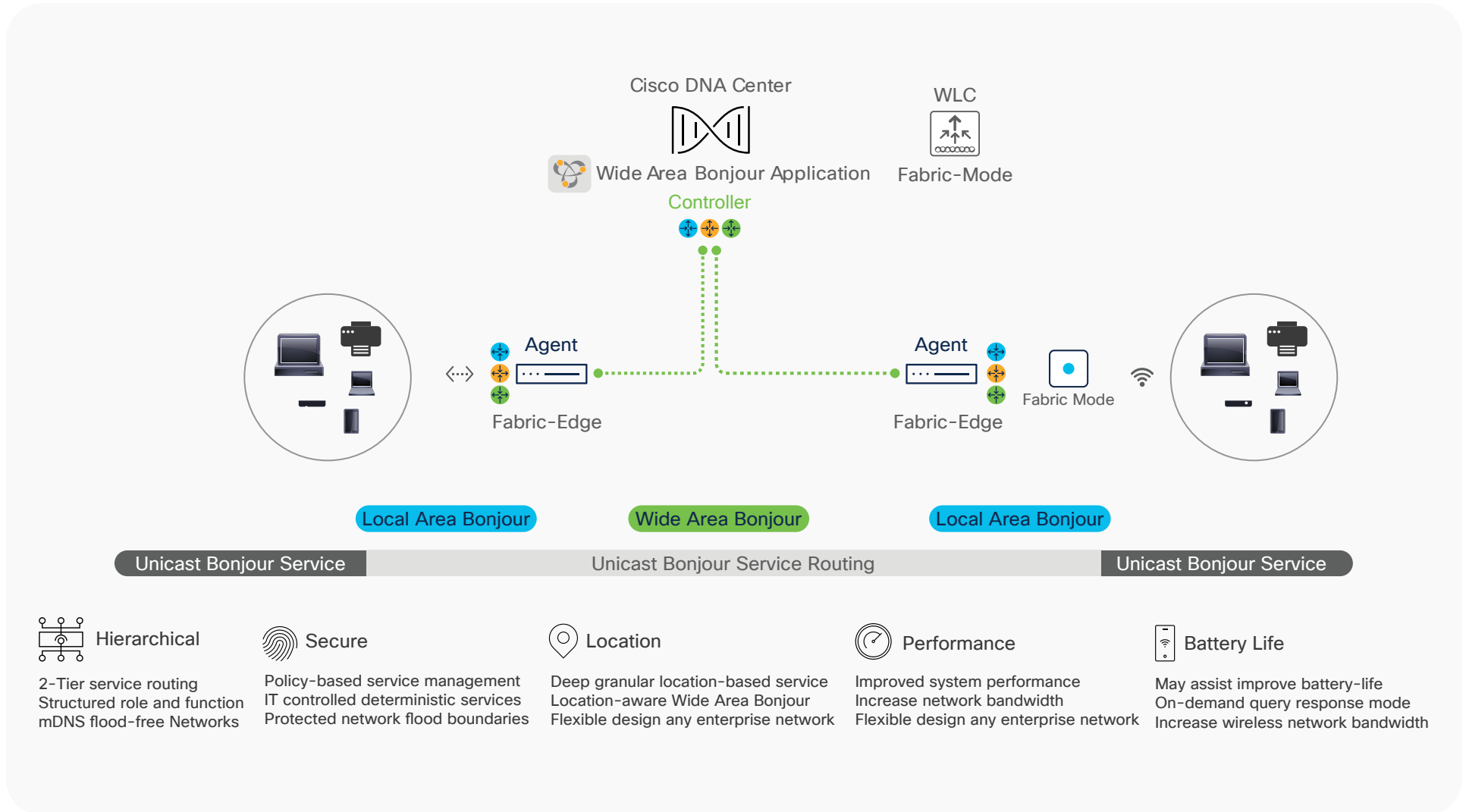
Cisco DNA Service for Bonjour solution overview

The Cisco Digital Network Architecture (Cisco DNA) Service for Bonjour solution enables end-to-end secure Virtual Routing and Forwarding (VRF)-aware Bonjour service routing for Cisco SD-Access wired and wireless networks. It addresses security, policy enforcement, and services administration challenges for large-scale network deployments. The new distributed service architecture eliminates mDNS flooding over L2VN across the core backbone and transitions to simple, secure, and scalable unicast-based service routing, providing policy enforcement points and enabling the management of Bonjour services. With Cisco DNA Service for Bonjour, enterprise networks can seamlessly introduce new services into the existing Cisco SD-Access enterprise environment without modifying the existing network design or configuration.

The enhanced intuitive Cisco DNA Center Wide Area Bonjour application GUI provides centralized access control and real-time service routing to enable a scalable and high-performance solution for large-scale Cisco SD-Access networks. The Wide Area Bonjour application supports detail assurance capabilities comprising end-to-end service-routing, mDNS service providers, and network solution components for the IT administrator to centrally manage various day-2 operational tasks.

The following figure illustrates how the Cisco DNA Service for Bonjour operates across two integrated Cisco SD-Access wired and wireless networks with end-to-end unicast-based service routing.

Figure 3. Cisco DNA Service for Bonjour Solution



Following are key Cisco DNA Service for Bonjour solution benefits:

- **Hierarchical** – The distributed mDNS processing across wired and wireless networks replaces enables flood-free with two-tier hierarchical and structured unicast service-routing. The RFC 6762 compatible mDNS endpoints supports unicast communication to enable enterprise-grade scalable solution.
- **Secure** – The IT organization gains end-to-end policy-based permitted mDNS services discovery and distribution control in network. The unicast based mDNS communication prohibits out-of-policy services and protects the networks and endpoints with advanced security.
- **Location** – The zero-configuration user-experience becomes uppermost as services are dynamically discovered within close-proximity and automatically adjusted with user mobility. The IT can implement flexible design location-based service-routing plan at building, floor or deep zone-levels.
- **Performance** – The de-centralization processing enables any technology for multi-dimensional scale. The network-wide ethernet switch and WLC enables unicast-based local mDNS processing and performs service-routing. The unicast-based distributed service-routing architecture significantly increases network, systems, and endpoint performance.
- **Battery-Life** – As enterprise wired and wireless networks transitions to unicast-based mDNS communication, the constant disruption and processing on mobile devices may ease and possibly assist in improving performance and battery-life.

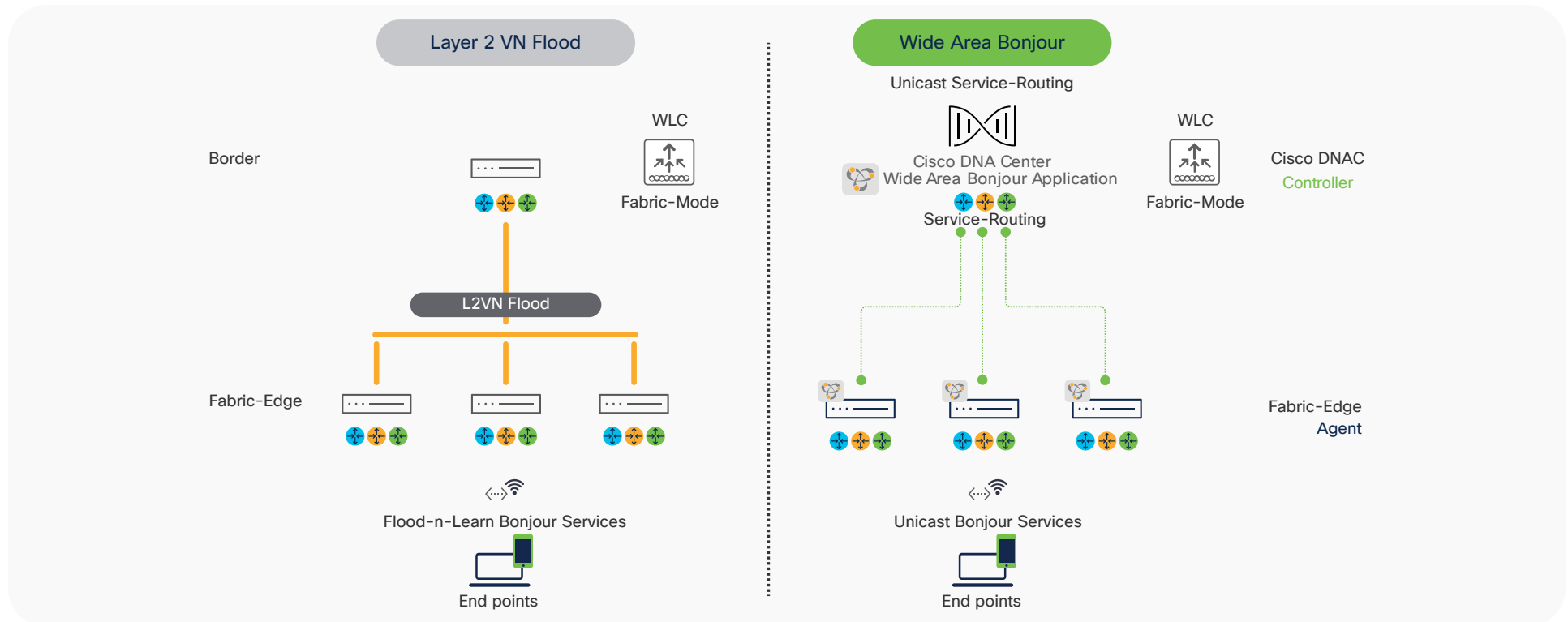
The hierarchical service-routing architecture in Cisco DNA Service for Bonjour is divided into the following two domains:

- **Local Area Bonjour domain:** In a Cisco SD-Access fabric network, the Local Area Bonjour domain consists of a single IP network gateway switch, such as a fabric-edge switch in access, directly attached to an mDNS endpoint. The unicast-based mDNS service routing boundary is limited within the Local Area Bonjour domain across the same or different fabric-enabled wired and wireless VLANs. For extended fabric networks, the unicast-based service-routing capability can be extended to a Policy Extended Node (PEN) or, on the Catalyst 9800 WLC, to supporting traditional local mode wireless.
- **Wide Area Bonjour domain:** The Wide Area Bonjour domain is required for mDNS services and needs to be discovered beyond the single fabric-edge switch. The Catalyst 9000 fabric-edge switches should be enabled in Service Discovery Gateway (SDG) agent mode to establish a lightweight, stateful, and reliable communication channel with Cisco DNA Center running the Cisco Wide Area Bonjour application. The service routing between the SDG agents and the controller operates over a standard underlay IP network to support policy and location-based mDNS service management.

Cisco DNA Service for Bonjour solution benefits

The Cisco DNA Service for Bonjour solution replaces mDNS flood-and-learn based service discovery and distribution to unicast mode through end-to-end hierarchical service routing in enterprise networks. The RFC 6762 based mDNS endpoints communicate with first-hop wired and wireless fabric-edge switches that adhere to the IT-defined policies to securely route services within the Layer 2 network boundary and beyond. The figure below illustrates the difference between mDNS flood-and-learn over L2VN and the unicast-based Wide Area Bonjour service-routing solution, solving known challenges related to discovery boundaries, scale, security, and more for fabric-enabled Cisco SD-Access wired and wireless networks.

Figure 4. Cisco DNA Service for Bonjour solution benefits



The following section highlights the key benefits of Cisco DNA Service for Bonjour across enterprise-grade wired and wireless networks:

- **End to end:** The Cisco DNA Service for Bonjour solution extends mDNS service discovery and distribution across enterprise-grade Cisco SD-Access wired and wireless networks without network boundaries. Enterprise IT can build end-to-end, hierarchical, and structured service-oriented networks without introducing a network redesign that would require new hardware.
- **Scale:** The distributed mDNS service-routing solution across fabric-edge switches replaces networkwide L2VN flooding for each VLAN to support increased network bandwidth and better system performance and enable a multidimensional scalable services solution.
- **Secure:** Enterprise IT gains control to introduce new services based on policy set on location, by role, and more. The new unicast-based model eliminates the flood-and-learn-based mDNS service model, and thus the use of unchecked or out-of-policy services is implicitly denied as consumer products introduce new capabilities.
- **Experience:** The end-user service discovery and distribution experience remain intact between residential and secure enterprise networks. With a service-routing solution that involves no learning curve and agentless mDNS, IT can adapt new services as they are introduced in consumer products without a major network infrastructure redesign.

Solution components

Cisco DNA Service for Bonjour 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 domains. The table below provides complete a Cisco DNA Service for Bonjour solution matrix, service-routing support over commonly deployed enterprise networks, operation, and more.

Table 1. Cisco DNA Service for Bonjour Solution support matrix

	Appliance	Wide Area Bonjour App	Catalyst 9600	Catalyst 9500	Catalyst 9400	Catalyst 9300	Catalyst 9200	Catalyst 9800 WLC	Nexus 9000
Platform Series	DN2-HW-APL DN2-HW-APL-L DN2-HW-APL-XL	–	Any	Any	Any	Any	Catalyst 9200	Any	9300 Series
Minimum Software	2.2.2.0	2.2.2.0	17.6.2	17.6.2	17.6.2	17.6.2	17.6.2	17.6.2	10.2.(3)F
Supported Mode	Platform	Controller	SDG-Agent Service-Peer	SDG-Agent Service-Peer	SDG-Agent Service-Peer	SDG-Agent Service-Peer	SDG	Service Peer	SDG Agent
Wide-Area Support	–	●	●	●	●	●	Not Supported	–	●
Local-Area Support	–	●	●	●	●	●	●	●	●
Service Scale	–	150000	15000	12000	10000	7500	1000	14000	4300
Software License									
Local and Wide-Area License	–	–	Cisco DNA Advantage	Cisco DNA Advantage	Cisco DNA Advantage	Cisco DNA Advantage	Cisco DNA Advantage	Cisco DNA Advantage	Cisco Advantage
System Mode									
Cluster	HA Cluster	Multi-Instance	StackWise Virtual	StackWise Virtual	StackWise Virtual	StackWise-480	StackWise-160	HA Cluster	vPC Domain
Default	Single Host	Single Instance	Standalone	Standalone	Standalone	Standalone	Standalone	Standalone	Standalone
Wired/Wireless Network Support									
Wired-Multilayer	–	●	●	●	●	●	●	–	●
Wired-Routed Access	–	●	●	●	●	●	●	–	●
Wireless-Local Mode	–	●	●	●	●	●	●	●	●
Wireless-FlexConnect mode	–	●	●	●	●	●	●	Switch mDNS Gateway	–
Wireless-Catalyst 9100 EWC Mode	–	●	●	●	●	●	●	Switch mDNS Gateway	–

	Appliance	Wide Area Bonjour App	Catalyst 9600	Catalyst 9500	Catalyst 9400	Catalyst 9300	Catalyst 9200	Catalyst 9800 WLC	Nexus 9000
Overlay Network Support									
Cisco SD-Access	–	●	●	●	●	●	●	–	–
Cisco SD-Access Wireless	–	●	●	●	●	●	●	Switch mDNS Gateway	–
BGP EVPN VXLAN	–	●	●	●	●	●	●	–	●
MPLS VPN	–	●	●	●	●	●	●	–	–
Multi-VRF	–	●	●	●	●	●	●	–	●
Operation									
Assurance	–	●	●	–	–	–	–	–	●
SNMP MIB Support	–	–	–	●	●	●	●	–	–

Note: Cisco Catalyst 9200 series mDNS gateway support is limited to Local Area Bonjour using classic flood-n-learn method. The Catalyst 9200 series switches as Fabric-Edge switch do not support SDG-Agent mode to enable end-to-end unicast-based Wide Area Bonjour service-routing. The Cisco SD-Access fabric with Catalyst 9200 series switches in Fabric-Edge role must enable L2VN Flooding in overlay to discover remote mDNS service from same Layer 2 VLAN.

Endpoint compatibility

As described earlier, the Cisco DNA Service for Bonjour solution follows industry-standard RFC 6762 to communicate with mDNS-capable endpoints. Thus, the solution is compatible with any vendors following the standard, including Apple, Google, Microsoft, printer manufacturers, audio/video endpoints, IoT devices, and many more.

Target audience

This deployment guide is targeted for Cisco SD-Access-enabled wired and wireless network administrators requiring guidance on designing and deploying end-to-end Bonjour services. The content focuses primarily on how to enable Bonjour services seamlessly into various types of enterprise network designs and topologies. The guide provides guidance to evaluate existing network designs and system inventory along with simple step-by-step configurations and guidelines for successful deployments.

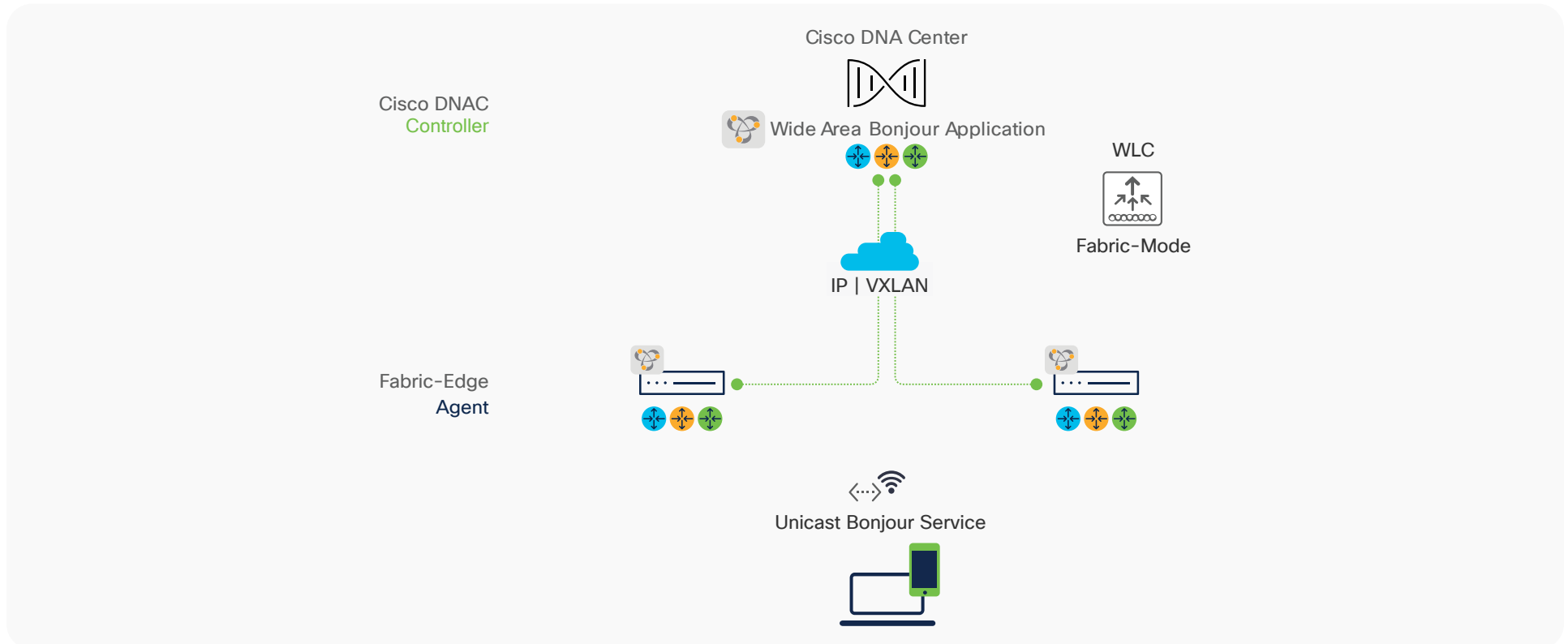
This document does not cover the basics of Bonjour implementation, and we highly recommend that you refer to the [About Bonjour overview](#) document and [RFC 6762](#) to learn about Bonjour terminology and operation.

Cisco DNA Service for Bonjour architecture

The Cisco DNA Service for Bonjour solution supports a three-tier distributed service-routing solution across a broad-range of complex enterprise network designs. mDNS service routing enables secure, targeted, and stateful peering and operates on network devices and optionally with a central Cisco DNA Center controller if service discovery is required beyond a single IP network boundary. mDNS service routing does not interfere with existing underlay or overlay unicast or multicast routing protocols, as it is designed to dynamically discover and distribute mDNS services from a local Layer 2 network and route them across complex wired and wireless networks based on granular policies defined by enterprise IT.

This section describes network device modes, functions, and the range of supporting Cisco SD-Access fabric-enabled wired and wireless network designs. The distributed service-routing architecture of Cisco DNA Service for Bonjour assists in building a scalable, reliable, and resilient solution. IT can design a fabric-enabled wired and wireless network with multitier mDNS service routing to replace end-to-end mDNS flood-and-learn with hierarchical and structured unicast-based service-routing. The figure below provides an overview of the multitier service-routing architecture.

Figure 5. Cisco DNA Service for Bonjour architecture



- **Cisco DNA controller:** The Cisco DNA controller builds the Wide Area Bonjour domain with networkwide and distributed trusted SDG agents using a secure communication channel for centralized services management and controlled service routing.
- **SDG agent:** The fabric-edge Cisco Catalyst 9000 switch functions as an SDG agent and builds reliable communication with Cisco DNA Center. At Layer 3 access, it communicates with directly attached fabric-enabled wired and wireless mDNS service endpoints.
- **Endpoints:** An mDNS endpoint is any device that advertises or queries mDNS services conforming to RFC 6762. The mDNS endpoints can be in either LANs or WLANs. The Cisco Wide Area Bonjour solution is designed to integrate with RFC 6762 compliant Bonjour services, including AirPlay, Google Chromecast, AirPrint, Audinate Dante, and more.



The Cisco Catalyst 9800 WLC requires no mDNS configuration in fabric-enabled wireless deployments.

Local Area Bonjour service routing

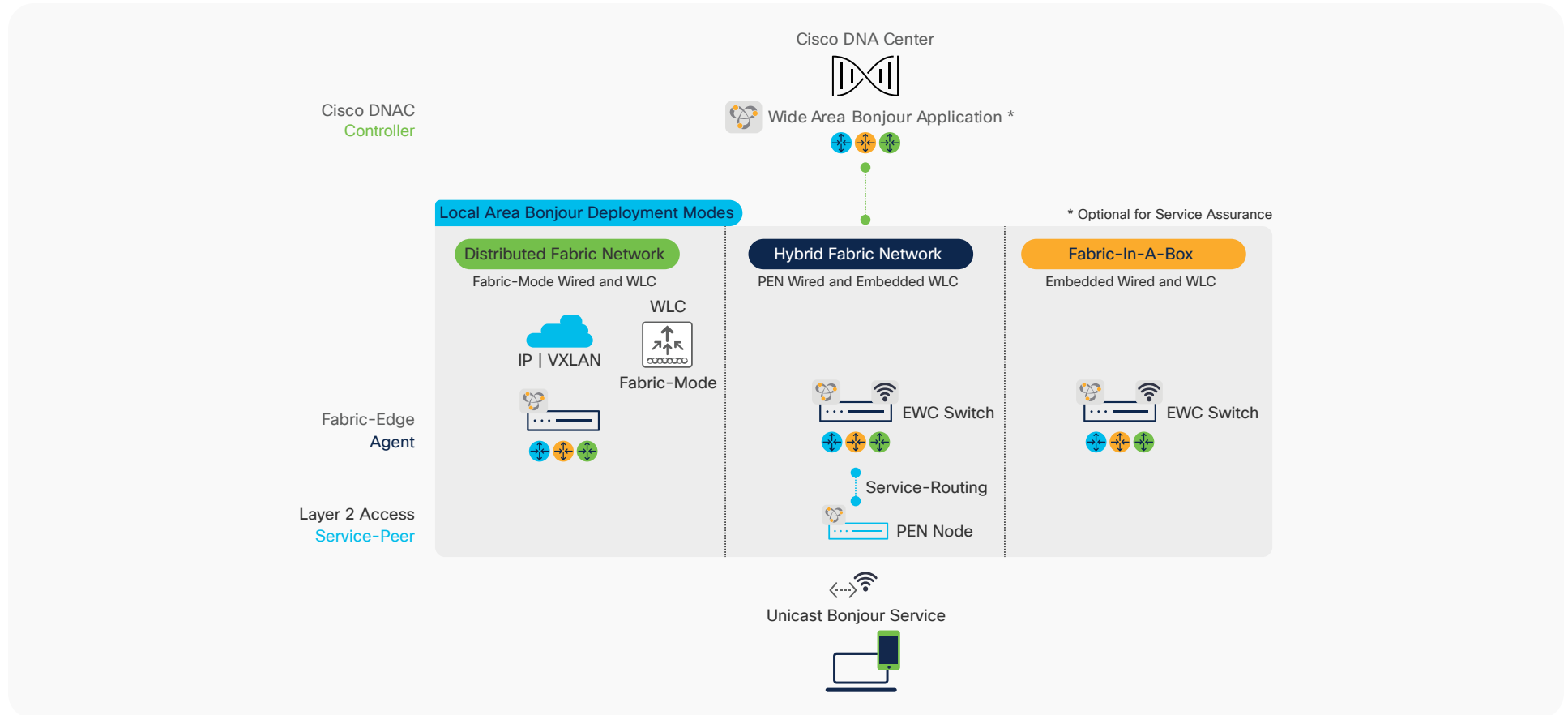
The Local Area Bonjour domain limits the mDNS service-routing function to a single IP gateway, that is, the fabric-edge switch. Cisco SD-Access supports various flexible network deployment models supporting a large or midsize enterprise campus and micro-branch office network with “fabric-in-a-box,” embedding multifunction capability to support integrated wired and wireless networks. The unicast-based mDNS service routing is supported on all deployment models, providing a consistent and enhanced user experience with rich mDNS services.

In most standard Cisco SD-Access deployments, the fabric-edge switch terminates the Layer 2/Layer 3 boundary at access with directly attached fabric-edge wired and wireless endpoints. In an alternative Cisco SD-Access deployment, the fabric boundary may start at the distribution layer with the Layer 2 network extended with a downstream Policy Extended Node (PEN),

providing network security and segmentation. Cisco SD-Access further provides a flexible and robust wireless networking solution to address next-generation high-speed WiFi 6 deployments.

In a Local Area Bonjour service-routing domain, as the fabric-edge switch provides mDNS service routing between directly or indirectly attached wired and wireless mDNS endpoints, it can optionally be paired with Cisco DNA Center to enable networkwide mDNS service assurance in real time. This section provides a brief solution overview to support unicast-based Local Area Bonjour service routing within a single Layer 2/Layer 3 network boundary based on various Cisco SD-Access fabric-mode wired and wireless deployment models in enterprise networks. Cisco DNA Center can optionally be deployed to manage networkwide service-assurance.

Figure 6. Cisco SD-Access Local Area Bonjour deployment modes



Wide Area Bonjour service routing

The Cisco SD-Access fabric architecture provides the flexibility to stretch single Layer 2 VLAN ID and overlay IPv4/v6 networks supporting enterprise-grade mobility. To protect enterprise core backbone network performance, the fabric retains the broadcast domain boundary limited to a single fabric-edge switch. Wide Area Bonjour provides second-tier unicast-based mDNS service routing and is required when an mDNS service discovery boundary is required beyond the single IP gateway. The Wide Area Bonjour

service-routing function enables secure and policy-based mDNS service discovery and distribution across the core network without enabling L2VN flooding.

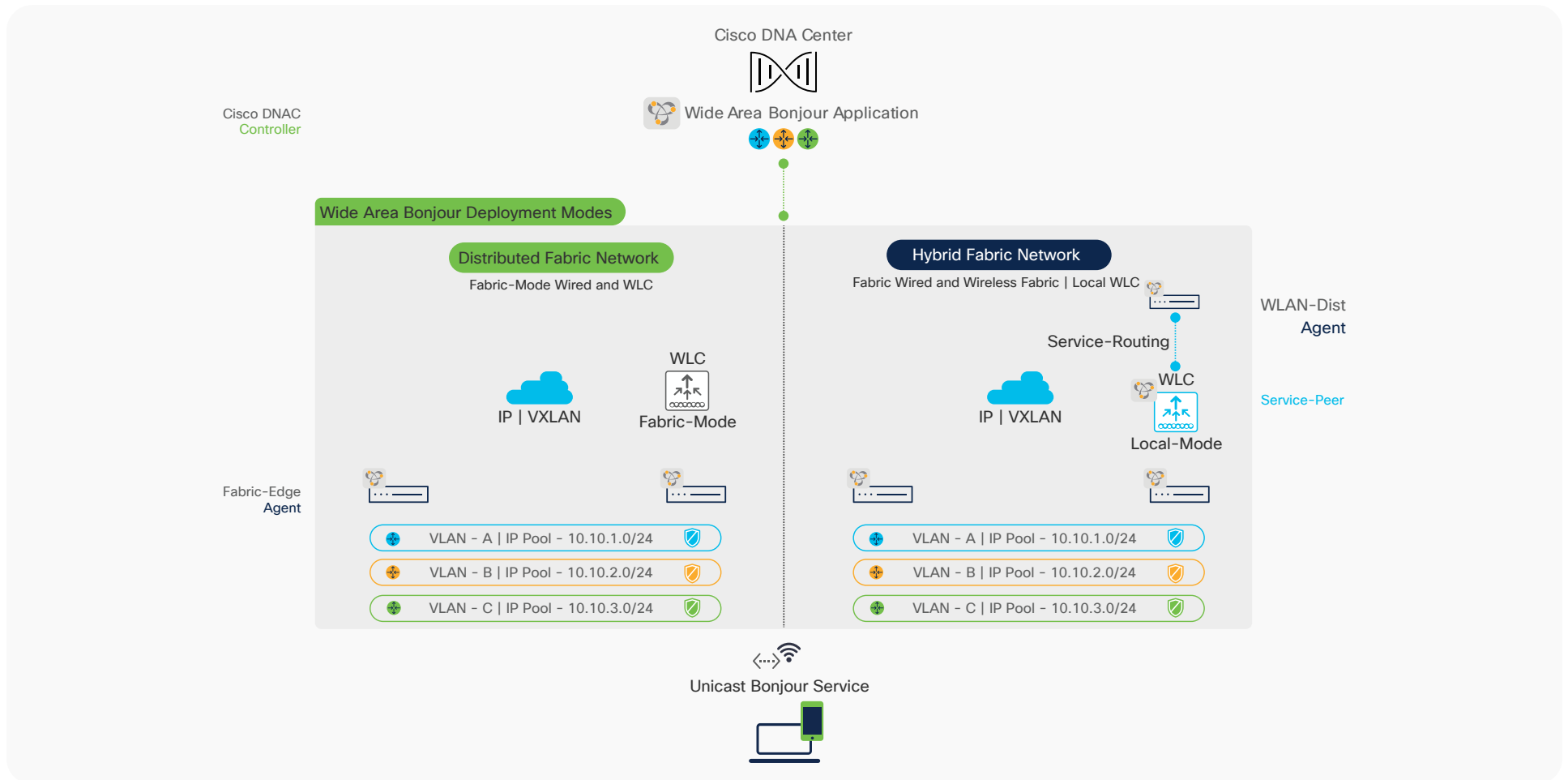
Wide Area Bonjour is a borderless service-routing solution that enables IT-defined policy and location-based mDNS service discovery from one network point to another based on business or technical requirements.

The fabric-edge Cisco Catalyst switch in SDG agent mode builds stateful service-routing communication with Cisco DNA Center to export locally discovered mDNS services or relay remote service discovery requests received from attached fabric-enabled wired and wireless endpoints. IT organizations can design and build common or customized service-routing topologies to limit mDNS policy between Local and Wide Area Bonjour domains. For example, Apple TV and a printer can be discovered

over the Wide Area Bonjour domain, but screen sharing or RealVNC should be limited within the Local Area Bonjour domain boundary.

The figure below illustrates various fabric-enabled distributed wired and wireless network designs sharing common VLANs and IP subnet IDs across the fabric domain. Instead of L2VN flooding, the fabric edge enables unicast and policy-based service routing to networkwide connected mDNS endpoints through policies defined in Cisco DNA Center.

Figure 7. Cisco SD-Access Wide Area Bonjour deployment modes

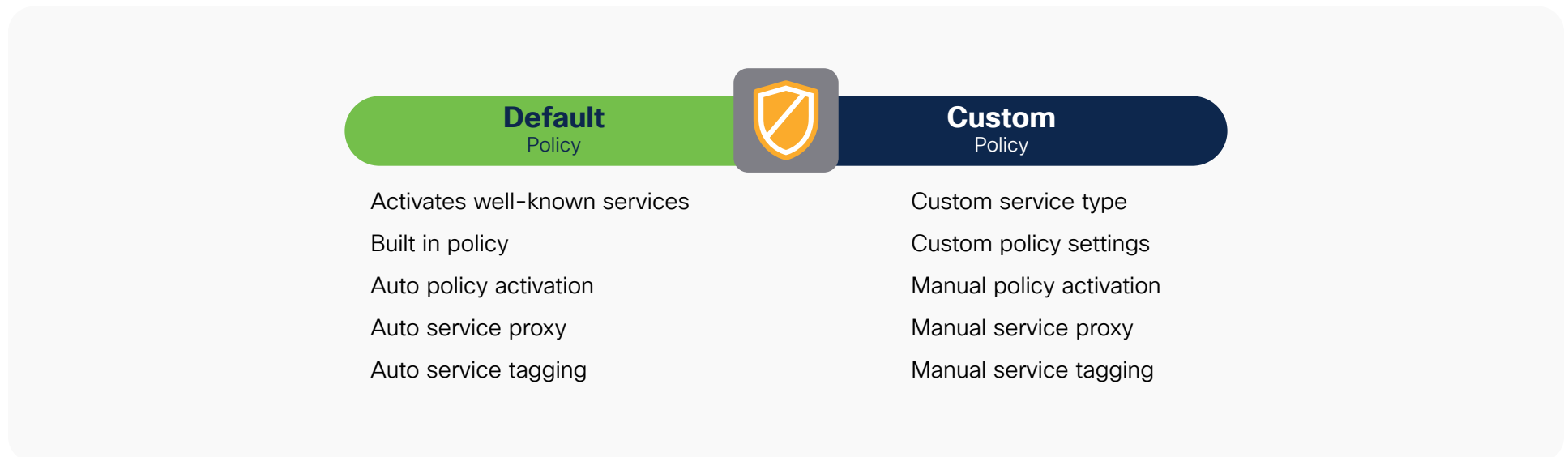


Policy management

A Cisco SD-Access overlay network becomes less secure and more vulnerable when it supports mDNS with L2VN flooding. Network administrators have limited controls and visibility to identify, secure, and manage mDNS services in overlay Layer 2 network environments. As the Cisco Catalyst LAN switching and wireless portfolio introduces unicast-based mDNS service management, it enables new possibilities for IT organizations to build end-to-end secure service routing in Cisco SD-Access-enabled enterprise networks.

Cisco IOS XE® Software Release 17.6.2 introduces a flexible policy configuration model that enables network administrators to design and build simplified or custom-tailored mDNS service routing in wired and wireless networks. The figure below illustrates this new built-in default policy model to activate unicast-based mDNS service routing on a fabric-enabled wired and wireless endpoint VLAN. The Cisco Catalyst switch continues to support custom mode policy when upgrading the software or when tailored policies are needed.

Figure 8. Flexible Cisco IOS XE service-routing policy modes



Cisco IOS-XE® supports the coexistence of default and custom policies on the same switch. The administrator can implement policy in either or both modes per fabric-enabled wired and wireless overlay user VLAN automated by the Cisco SD-Access fabric application.

Table 2. Flexible Cisco IOS-XE® service-routing policy comparison

	Default mode	Custom mode
Local Area Bonjour – service-list permit	Built in Default bidirectional services permitted*	Custom User-defined unidirectional custom service permission
Local Area Bonjour – service policy	Built in Automatically binds default service list	Custom User-defined custom service-list binding
Local Area Bonjour – service policy	Built in Automatically associates default policy to the mDNS gateway enabled wired VLAN and wireless profile	Custom User-defined manual policy association to mDNS gateway enabled wired VLAN and wireless profile
Local Area Bonjour – Intra-VN Inter-VLAN service proxy	Built in Automatic inter-VLAN service proxy	Custom User-defined manual Inter-VLAN location filter
Local Area Bonjour – Inter-VN Inter-VLAN service proxy	Not supported	Custom User-defined manual inter-VN location filter
Wide Area Bonjour – service-list permit	Built in Default controller services permitted*	Custom User-defined controller-bound custom service policy
Wide Area Bonjour – service policy	Built in Automatically binds default controller service list	Custom User-defined custom controller service-list binding
Location tag – wired port	Built in Default tag (0) to wired port	Built in or custom Default tag (0) or custom tag assigned to wired port

* Apple TV, AirPrint, Apple Home Sharing, Apple Remote Login (SSH), Apple Screen Share, Apple-Windows file sharing (SMB), Google ChromeCast, Google Expeditions, multifunction printers (print, scan, fax), secure printing services are whitelisted by default in the service-list policy.

Location-group-based service routing

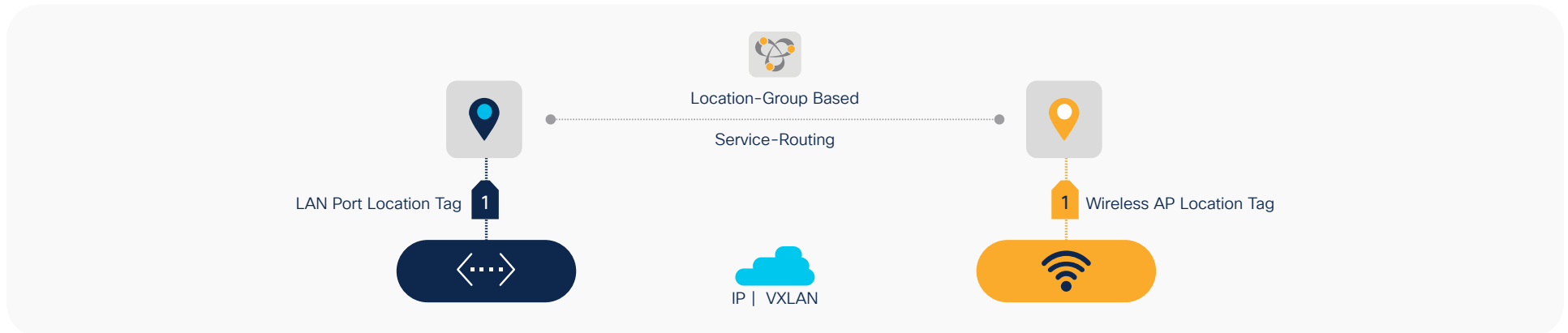
L2VN-based mDNS flood-and-learn network deployments cannot distinguish the originating network point of presence for the service provider and receiver to provide an enhanced user experience with granular location-based mDNS services. Depending on the overall size of the Layer 2 flooded network, the mDNS endpoints may find an overwhelming number of providers during discovery and may not easily locate the intended services within the desired proximity. This may affect the end user's ability to intuitively use mDNS services in large-scale fabric-enabled wired and wireless networks.

Cisco DNA Service for Bonjour enables zero-configuration vision with the introduction of mDNS service routing based on location-group ID tags

assigned to fabric-enabled wired LAN ports and Cisco wireless access points in local mode supporting Over-The-Top (OTT) deployments. The fabric-mode Cisco wireless access points currently do not support location group IDs. However, with the unique Wide Area Bonjour service-routing architecture, the administrator can design and deploy best-in-class location-based mDNS service-routing for Cisco SD-Access networks.

The fabric-edge switches in SDG agent mode and Cisco DNA Center expand policy capabilities with the inclusion of matching location-group ID tags to discover and distribute mDNS services. The mDNS service location-group tags on wired LAN ports are dynamically synchronized across the fabric without introducing extensive hardware changes to the wired and wireless network that would impact mission-critical network environments.

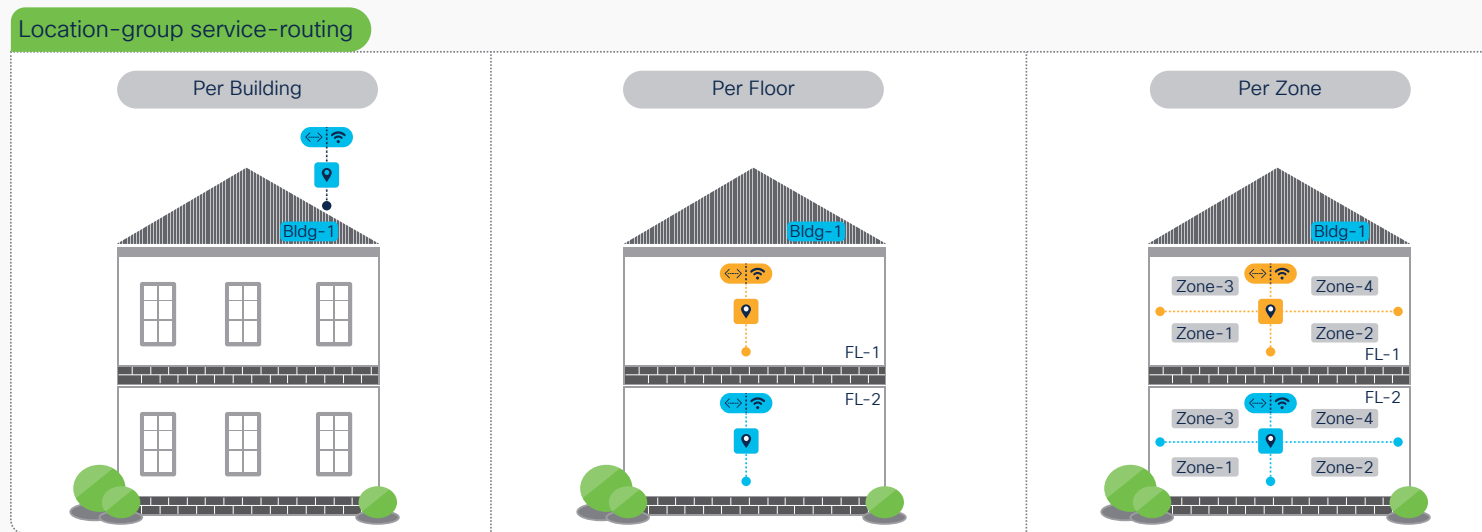
Figure 9. Location-group-based service routing



As end-to-end mDNS processing transforms to unicast-based service and provides flexibility to tag mDNS services for granular service routing, the Cisco DNA Service for Bonjour enables new possibilities for IT organization. To provide a best-in-class user-experience, the IT administrator can design and build location-group tag-based dynamic mDNS service boundaries at individual building, floor, or micro-segmented service zones on each floor. As the mDNS service discovery boundary shrinks, the user experience improves due to the ability to easily navigate a limited IT-managed or peer-to-peer service provider list within tailored close proximity.

The IT organization can design and build mDNS policies, enabling a secure service experience to end users. For example, in Bldg-1, James can discover and use a wired Apple TV and printer from his iPhone. In Bldg-2, James should see only the Apple TV, and he will not be able to find any mDNS services when connected to the Bldg-3 wired or wireless network. The figure below illustrates some common use cases for location-group tags that IT can enable across enterprise wired and wireless networks:

Figure 10. Location-group-based mDNS use cases

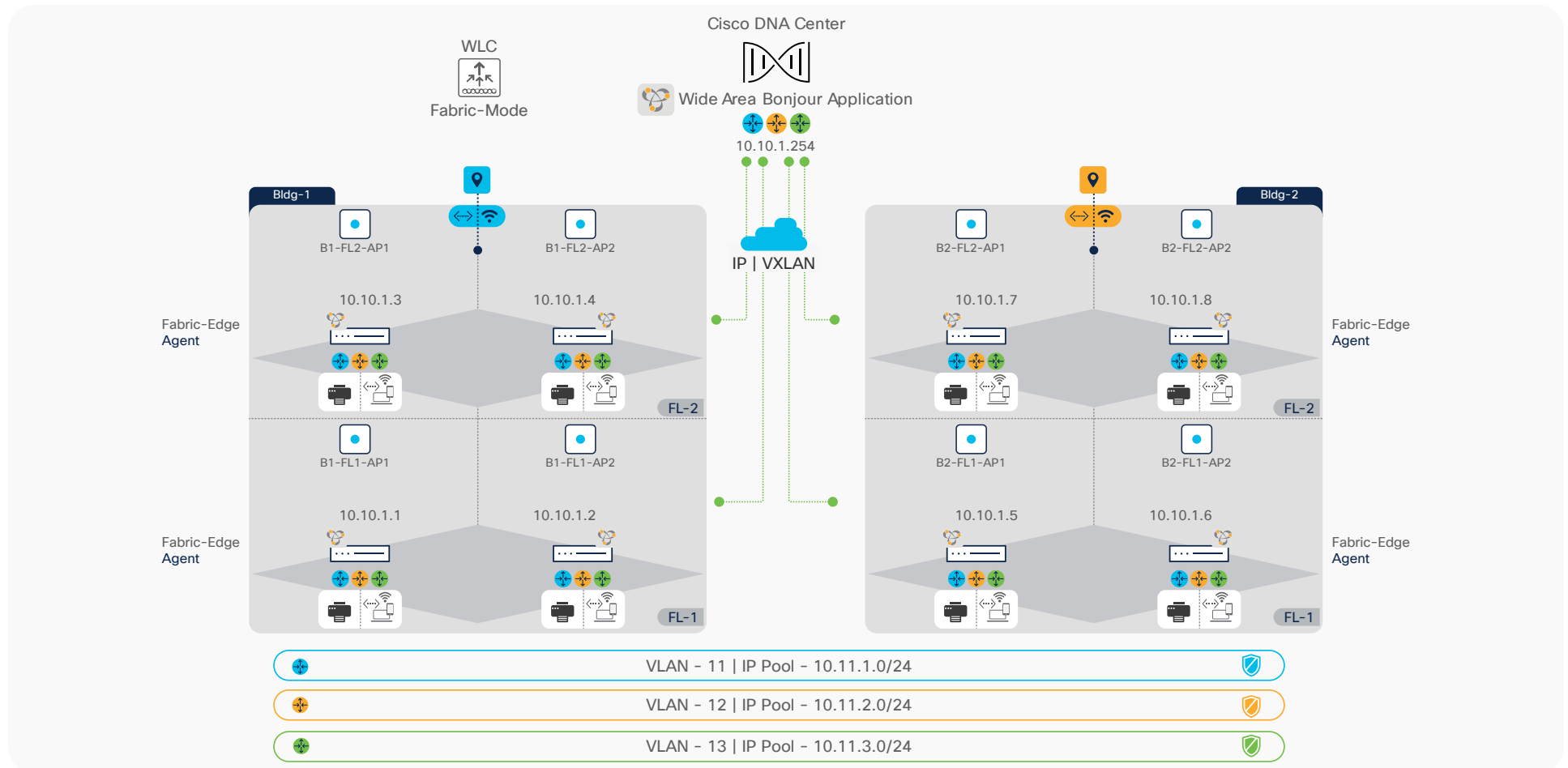


Deploying Wide Area Bonjour – distributed fabric

This section provides guidelines for implementing unicast-based mDNS service routing in Local and Wide Area Bonjour domains supporting Cisco SD-Access fabric-enabled wired and wireless networks. The fully distributed control and data plane processing at each fabric-edge switch enables the mDNS gateway function for directly attached fabric-enabled wired and wireless endpoints. The centralized Cisco WLC does not intersect with any mDNS processing in this deployment model.

This section provides common deployment guidance for fully distributed fabric-enabled wired and wireless networks. The figure below illustrates a reference unicast-based Wide Area Bonjour domain that provides service-routing capabilities across Cisco SD-Access, enabling wired and wireless networks to share a common VLAN ID and IP subnet.

Figure 11. Distributed fabric Wide Area Bonjour design



Distributed fabric prerequisite configuration

Before configuring mDNS service-routing capabilities in a Cisco SD-Access-enabled wired and wireless network, it is imperative to apply the following basic prerequisite configurations to targeted network devices to successfully implement unicast-based mDNS service routing:

- **Software and license:** The minimum Cisco IOS-XE® Software Release 17.6.2 and network devices with Cisco DNA Advantage licenses are required to implement the capabilities described in this guide.
- **Cisco DNA Center:** Ensure that all fabric-edge Ethernet switches and Catalyst 9800 Series WLCs are added to the Cisco DNA Center inventory. Ensure that all the devices have successfully reached Managed status.

- **Fabric automation:** The network administrator must complete the building of the Cisco SD-Access fabric wired and wireless network before enabling the Wide Area Bonjour domain to support service routing across fabric. The fabric network must be enabled with underlay IP multicast.
- **IP multicast:** Ensure that a Cisco Catalyst 9800 Series WLC supporting fabric-mode access points or a Catalyst 9300 Series Switch in EWC mode is enabled with AP multicast. The Cisco fabric mode wireless access points assigned to INFRA_VN VLAN must join the IP multicast group announced by the WLC. IP multicast on the wired and wireless client IP pool interface is optional and not required for mDNS.

This section provides reference configuration guidelines for using default and custom mode policy for Cisco SD-Access-enabled wired and wireless networks, as illustrated in the reference network design in Figure 11. The table below provides the default mode policy reference configuration enabling mDNS service routing on a fabric-edge switch as SDG agent. In this mode, several well-known whitelisted mDNS service types are permitted by default in the Local and Wide Area Bonjour domains.



The Cisco DNA Center Wide Area Bonjour application supports service-routing and service-assurance capabilities. The Cisco SD-Access Fabric application or Wide Area Bonjour application currently do not support mDNS policy automation. The network administrator can create a CLI template with a standard configuration and automate it across the fabric-edge switches.

Default mode policy configuration

Table 3. Default mode policy configuration for distributed wired and wireless

Fabric-edge switch

SDG agent

Step 1: Default mode – Local Area Bonjour mDNS service routing

```
!  
mdns-sd gateway  
mode sdg-agent  
active-query timer 1  
!  
vlan configuration 11,12,13  
! Printer, Wired and Wireless User VLAN  
mdns-sd gateway  
!
```

Fabric-edge switch

Step 2: Default mode – Wide Area Bonjour mDNS service routing

```
!  
service-export mdns-sd controller DNAC  
controller-address 10.10.1.254  
controller-source-interface Loopback 0  
!
```

Step 3: Enable Wide Area Bonjour policy on Cisco DNA Center

Refer to [Deploying the Wide Area Bonjour Application](#) to implement Bonjour policy on Cisco DNA Center.

Custom mode policy configuration

Advanced mode mDNS service routing can be deployed with a user-defined custom service-type, service-list and service-policy for distributed fabric-enabled wired and wireless networks. The default and custom mode policy can coexist on the same mDNS gateway system; hence, Cisco IOS XE provides the flexibility to use default and custom policies on the same Catalyst fabric-edge Ethernet switches. The Cisco IOS XE built-in default mDNS policy is replaced with the custom policy once it is applied under targeted wired and wireless users or endpoint VLANs. The table below provides the custom mode policy reference configuration enabling mDNS service routing on fabric-edge switches, as illustrated in Figure 11.

Table 4. Custom mode policy configuration for distributed wired and wireless

Fabric-edge switch

SDG agent

Step 1: Custom mode – Local Area Bonjour mDNS service routing

```
!  
mdns-sd gateway  
mode sdg-agent  
active-query timer 1  
!
```

Fabric-edge switch

Step 2: Custom mode – Local Area Bonjour mDNS service policy

```
!  
mdns-sd service-definition CUSTOM-SERVICE-LIST  
  service-type _classroom._tcp.local  
!  
mdns-sd service-list LOCAL-AREA-BONJOUR-IN IN  
  match apple-airprint  
  match CUSTOM-SERVICE-LIST  
!  
mdns-sd service-list LOCAL-AREA-BONJOUR-OUT OUT  
  match apple-airprint  
  match CUSTOM-SERVICE-LIST  
!  
mdns-sd service-policy LOCAL-AREA-BONJOUR-POLICY  
  service-list LOCAL-AREA-BONJOUR-IN IN  
  service-list LOCAL-AREA-BONJOUR-OUT OUT  
!
```

Step 3: Custom mode – Local Area Bonjour mDNS service-policy association

```
! Wired Printer (11), Wired User VLAN (12) and Wireless User VLAN (13)  
vlan configuration 11,12,13  
  mdns-sd gateway  
  service-policy LOCAL-AREA-BONJOUR-POLICY  
!
```

Fabric-edge switch

Step 4: Custom mode – Wide Area Bonjour mDNS service policy

! Only outbound filter is required, inbound is trusted and managed from Cisco DNA Center Policy.

```
mdns-sd service-list WIDE-AREA-BONJOUR-OUT OUT
match apple-airprint
!
mdns-sd service-policy WIDE-AREA-BONJOUR-POLICY
service-list WIDE-AREA-BONJOUR-OUT OUT
!
```

Step 5: Custom mode – Wide Area Bonjour mDNS service routing

```
!
service-export mdns-sd controller DNAC
controller-service-policy WIDE-AREA-BONJOUR-POLICY out
controller-address 10.10.1.254
controller-source-interface Loopback 0
!
```

Step 6: Enable Wide Area Bonjour policy on Cisco DNA Center

Refer to [Deploying the Wide Area Bonjour Application](#) to implement Bonjour policy on Cisco DNA Center.

Deploying Wide Area Bonjour – hybrid fabric

Cisco SD-Access enabled wired and wireless can be deployed in a hybrid network environment to meet business and technical requirements. Hybrid fabric network designs enable enterprise customers with traditional wired and wireless networks using classic and disparate technologies to gradually converge and transition toward a unified and distributed fabric network to gain key benefits of the Cisco SD-Access architecture.

Cisco SD-Access supports a hybrid wired and wireless network design. The network administrator can deploy a consistent unicast-based mDNS service experience to wired and wireless endpoints independently of the operating network design:

- **Hybrid wired fabric:** The fabric edge in the distribution layer provides physical network aggregation and an IP gateway to wired endpoints connected through one or more downstream intermediate Layer 2 Ethernet access switches. The Cisco DNA Center managed Layer 2 access switch deployed as a Policy Extended Node (PEN) provides seamless network security, segmentation, and unicast-based mDNS service routing to directly attached endpoints. It builds trusted service-routing peering upstream to the SDG agent switch to eliminate mDNS flood-and-learn on standard Layer 2 networks.
- **Hybrid wireless fabric:** Cisco SD-Access provides the following flexible wireless networking solution in enterprise networks:
 - **Local mode:** The Cisco WLC can continue to support central switching in a local mode wireless network while the wired network is transitioning toward Cisco SD-Access fabric. Such coexistence of traditional and fabric-enabled network architectures provides IT organizations an opportunity for seamless migration. Wide Area

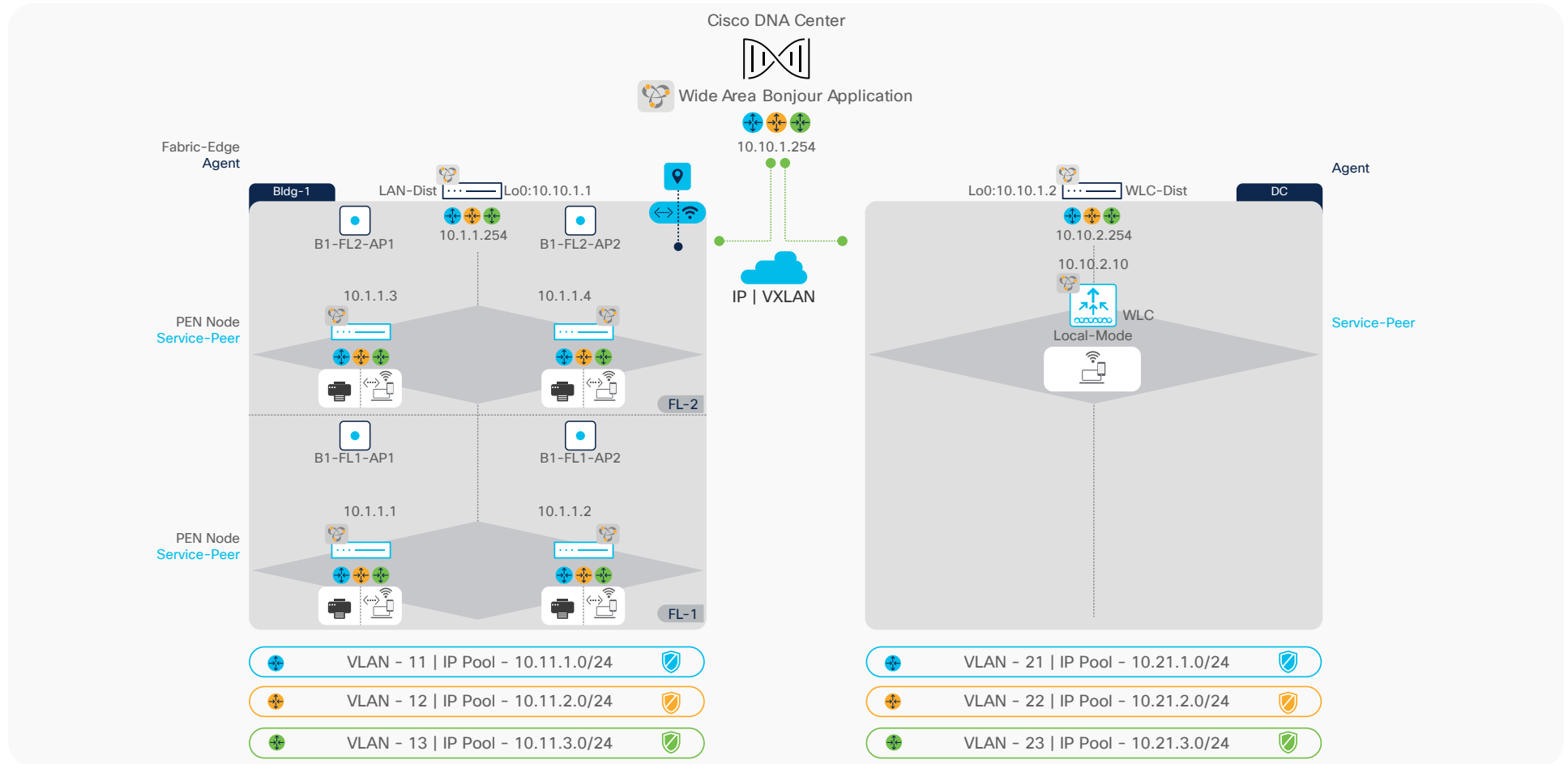
Bonjour provides end-to-end unicast-based mDNS service routing between fabric-enabled wired and traditional local mode wireless without L2VN flooding across the fabric and beyond.

- **EWC on switch:** Small or midsize enterprise networks can be deployed with a controllerless wireless solution by using an Embedded Wireless Controller (EWC) function on the Cisco Catalyst 9300 Series Switches. In EWC mode the Catalyst 9300 Series Switch at the distribution layer provides the IP gateway function to wired and wireless endpoints. The EWC mode switch terminates wireless endpoints by supporting a central data switching model, while wired endpoints may get connected through one or more downstream intermediate Layer 2 PEN Ethernet access switches. Wide Area Bonjour provides an end-to-end unicast-based mDNS service-routing solution without flooding across local Layer 2 trunk ports or L2VN flooding over the core backbone if mDNS service routing is required beyond a single IP gateway at the EWC switch.

This section provides guidelines for implementing unicast-based mDNS service routing in the Wide Area Bonjour domain for a hybrid wired and wireless fabric network. The Layer 2 Ethernet access switch and local mode Cisco WLC must be implemented in mDNS gateway service-peer mode to enable unicast-based service routing in a Layer 2 wired and wireless environment. The network administrator can refer to [Cisco DNA Service for Bonjour Deployment Guide](#) for traditional LAN and wireless local mode design and deployment.

The figure below illustrates a reference unicast-based Local Area and Wide Area Bonjour domain enabling end-to-end service-routing capabilities comprising wired and wireless local mode and Cisco DNA Center.

Figure 12. Hybrid mode wired and wireless Wide Area Bonjour design



Hybrid fabric prerequisite configuration

Before configuring mDNS service-routing capabilities, it is imperative to apply the following basic prerequisite configurations to targeted network devices to successfully implement unicast-based mDNS service-routing:

- **Software and license:** The minimum Cisco IOS XE Software Release 17.6.2 and network devices with Cisco DNA Advantage licenses are required to implement the capabilities described in this guide.
- **Cisco DNA Center:** Ensure that all fabric-edge Ethernet switches and Catalyst 9800 Series WLCs are added to the Cisco DNA Center inventory. Ensure that all the devices have successfully reached Managed status.

- **Fabric automation:** The network administrator must finish building the Cisco SD-Access fabric wired and wireless network before enabling the Wide Area Bonjour domain to support service routing across fabric. The fabric network must be enabled with underlay IP multicast.
- **IP multicast:** Ensure that a Cisco Catalyst 9800 Series WLC supporting traditional local mode access points or a Cisco Catalyst 9300 Series Switch in EWC mode is enabled with AP multicast. The Cisco fabric mode wireless access points assigned to INFRA_VN VLAN must join the IP multicast group announced by the WLC. IP multicast on the wired and wireless client IP pool interface is optional and not required for mDNS.
- **Interdomain routing:** Ensure that the Cisco SD-Access-enabled wired and wireless networks have external IP routing domain connectivity through the border node, allowing fabric-enabled wired or wireless endpoints to have IP reachability with traditional local mode wireless endpoints.

Hybrid fabric configuration reference



The hybrid wired and wireless network follows all traditional device role and service-routing capabilities. The Wide Area Bonjour network design and deployment guidelines are common between traditional and Cisco SD-Access hybrid mode wired and wireless networks. Hence, the network administrator can refer to the [Cisco DNA Service for Bonjour Deployment Guide](#) for traditional LAN and wireless local mode design and deployment to implement Wide Area Bonjour for hybrid mode.

Deploying Inter-VN service routing

Cisco SD-Access fabric-enabled wired and wireless networks may logically divide into separate Layer 2 VLANs or Layer 3 VNs, providing segmentation with network virtualization. The fabric-edge switch in SDG agent mode is a VRF-Aware service-routing system supporting advanced mDNS discovery and distribution between fabric-enabled wired and wireless endpoints associated to the same or different VNs. The Cisco SD-Access fabric edge provides unicast-based secure mDNS service routing in the following segmented network modes:

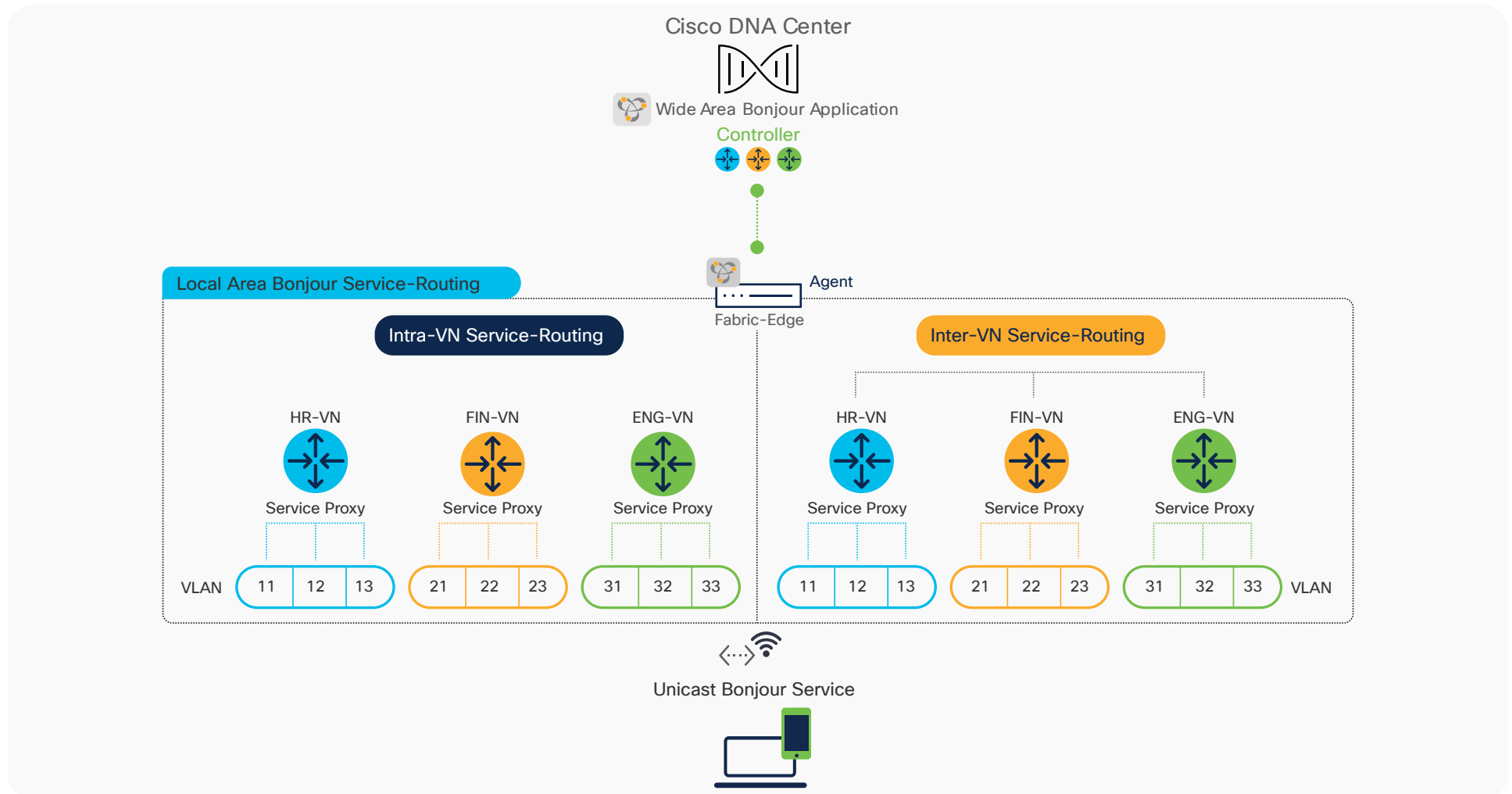
- **Intra-VN mDNS service:** The fabric-edge switch by default dynamically discovers and distributes mDNS services between locally connected wired and wireless endpoints connected to the same or different VLANs or IP pools mapped to same VN, for example, HR-VN. This commonly deployed intra-VN service-routing function can be enabled through the built-in or

default policy to manage mDNS information that is logically aligned to several other VN security requirements.

- **Inter-VN mDNS service:** The fabric-edge switch supports conditional mDNS “service leaking” between locally connected wired and wireless endpoints to different VLANs or IP pools mapped to different VNs. For example, HR Wired Printer in VLAN-11 must be shared with wireless users in VLAN-12 of FIN-VN. To support inter-VN service leaking, the network administrator must create a secure custom mode mDNS policy and build a forwarding path through an external firewall or fusion router to permit communication.

The figure below illustrates a brief example of unicast-based intra-VN and inter-VN mDNS service proxy to directly attached fabric-enabled wired and wireless mDNS endpoints on a single fabric-edge switch.

Figure 13. Wide Area Bonjour – Intra-VN and Inter-VN service routing



Inter-VN service routing prerequisite configuration

Depending on the SD-Access-enabled wired and wireless networks, the prerequisite steps described in [Distributed Fabric Prerequisite Configuration](#) or [Hybrid Fabric Prerequisite Configuration](#) should be implemented to support inter-VN service-routing.

As part of the prerequisites, the network administrator must ensure that inter-VN routing is configured through an external firewall or fusion router to allow closed user group communication.

Custom mode policy configuration

Inter-VN service routing requires network administrator involvement to identify an mDNS service provider source VN network to be conditionally distributed in the outbound mDNS service policy for receiver endpoints in logically separated VNs. To support such tailored mDNS service routing, a flexible custom mode policy must be implemented.

The table below provides the custom mode policy reference configuration enabling inter-VN mDNS service routing on fabric-edge switches supporting directly attached wired and wireless mDNS endpoints as illustrated in the reference network design in Figure 13. In this reference configuration example, the mDNS service printer from HR-VN (VLAN-11) is distributed to mDNS receivers on any VLAN mapped to FIN-VN while continuing to provide mDNS service routing within the local VN.

Table 5. Custom mode policy configuration for inter-VN distributed wired and wireless

Fabric-edge switch

SDG agent

Step 1: Custom mode - Local and Wide Area Bonjour mDNS service routing

Complete the steps for configuring a custom mode policy described in Table 4 for initial Local and Wide Area Bonjour service-routing configuration. The mDNS service list and policy must be given unique names on a per-VN basis.

Step 2: Custom mode - Local Area Bonjour mDNS service policy

```
! Creating Location-filter matching Printer VLAN 11 mapped on HR-VN
mdns-sd location-filter HR-VN-PRINT-SERVICE
  match location-group default 11
!
```

Step 3: Custom mode - Enable HR-VN to FIN-VN service routing

```
! Assign HR-VN Location-filter to FIN-VN outbound mDNS service-filter
mdns-sd service-list FIN -VN-SERVICE-OUT out
  match printer location-filter HR-FIN-VN-PRINT-SERVICE
!
mdns-sd service-policy FIN-VN-BONJOUR-POLICY
  service-list FIN -VN-SERVICE-OUT out
!
```

Step 4: Custom mode: Associate FIN-VN mDNS service policy to VLAN

```
!
vlan configuration 13
  mdns-sd gateway
    service-policy FIN-VN-BONJOUR-POLICY
!
```

Deploying the Wide Area Bonjour application

The Cisco Wide Area Bonjour application is an add-on service in Cisco DNA Center that enables the Bonjour controller function to be paired with networkwide distributed and managed Cisco Catalyst 9000 switches in SDG agent mode. Wide Area Bonjour supports stateful service-routing peering with networkwide SDG agents and provides a broad range of assurance capabilities to manage and monitor Bonjour services throughout the Wide Area Bonjour domain. This section provides guidelines for deploying, managing, and monitoring the Bonjour services in the Wide Area Bonjour domain from Cisco DNA Center.

Cisco Wide Area Bonjour application prerequisites

The network administrator must follow the prerequisites procedure to complete the requirements of Wide Area Bonjour before implementing networkwide service routing. Three simple steps are required before you can start using the Wide Area Bonjour application:

- **Install application:** Cisco Wide Area Bonjour is a default application of Cisco DNA Center. The network administrator must download and install it from the catalog server.
- **Software and license:** The minimum Cisco IOS XE Software Release 17.6.2 and network devices with Cisco DNA Advantage licenses are required to implement the capabilities described in this guide.
- **Cisco DNA Center:** Ensure that all mDNS gateway Ethernet switches and Catalyst 9800 Series WLCs are added to the Cisco DNA Center inventory

with appropriate credentials. Ensure that all devices have IP connectivity and have successfully reached Managed status.

After successful installation, the Cisco Wide Area Bonjour application can be found in the Tools section. The figure below illustrates the application icon for the Cisco Wide Area Bonjour application.

Figure 14. Cisco Wide Area Bonjour application



The Cisco Wide Area Bonjour application in Cisco DNA Center is a standalone application and is not fully integrated with the other applications and tools of Cisco DNA Center, such as Site and Building Hierarchy, Topology, etc. In a future release, application enhancements will enable unified service function following the same principles as all other Cisco DNA Center applications.

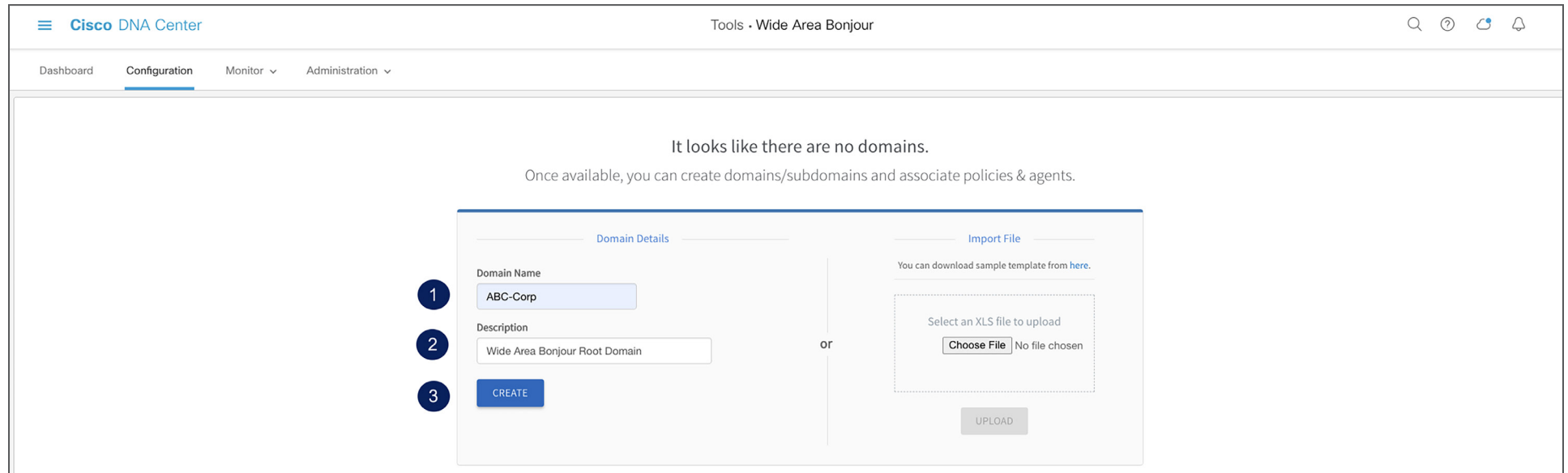
Configuring Cisco Wide Area Bonjour service domains

The Cisco Wide Area Bonjour application supports logical service domain constructs that can be used to build hierarchical global service-routing policies. The domain consists of two simple structure levels that the network administrator must create before starting to build a global service-routing policy to discover the mDNS service from one or more sources and routes to the receiver or querying SDG agent across the Wide Area Bonjour domain network.

Root domain

The service root domain is the first step in building a policy hierarchy in the Cisco Wide Area Bonjour application. The root domain holds a complete logical grouping of policies, the service-cache database, service assurance, and more. In this initial configuration step, the network administrator can create the root domain with any user-defined name, such as ABC-Corp representing the organization name. The figure below illustrates the initial step to configure the Cisco Wide Area Bonjour application.

Figure 15. Cisco Wide Area Bonjour application root domain configuration



The screenshot displays the Cisco DNA Center interface for configuring a Wide Area Bonjour Root Domain. The page title is "Tools - Wide Area Bonjour". The navigation menu includes "Dashboard", "Configuration", "Monitor", and "Administration". The main content area shows a message: "It looks like there are no domains. Once available, you can create domains/subdomains and associate policies & agents." Below this message is a form titled "Domain Details" with two sections: "Domain Details" and "Import File".

Domain Details

- 1 Domain Name: ABC-Corp
- 2 Description: Wide Area Bonjour Root Domain
- 3 CREATE

Import File

You can download sample template from [here](#).

Select an XLS file to upload

Choose File No file chosen

UPLOAD

Sub-Domains

A subdomain is a logical and flexible structure of service filters for Wide Area Bonjour. The network administrator can create one or more subdomains with the parent root domain. For example, two new subdomains can be created under the ABC-Corp domain. Each subdomain can be uniquely labeled as Bldg-1 and Bldg-2 to align with the building structure of ABC-Corp.

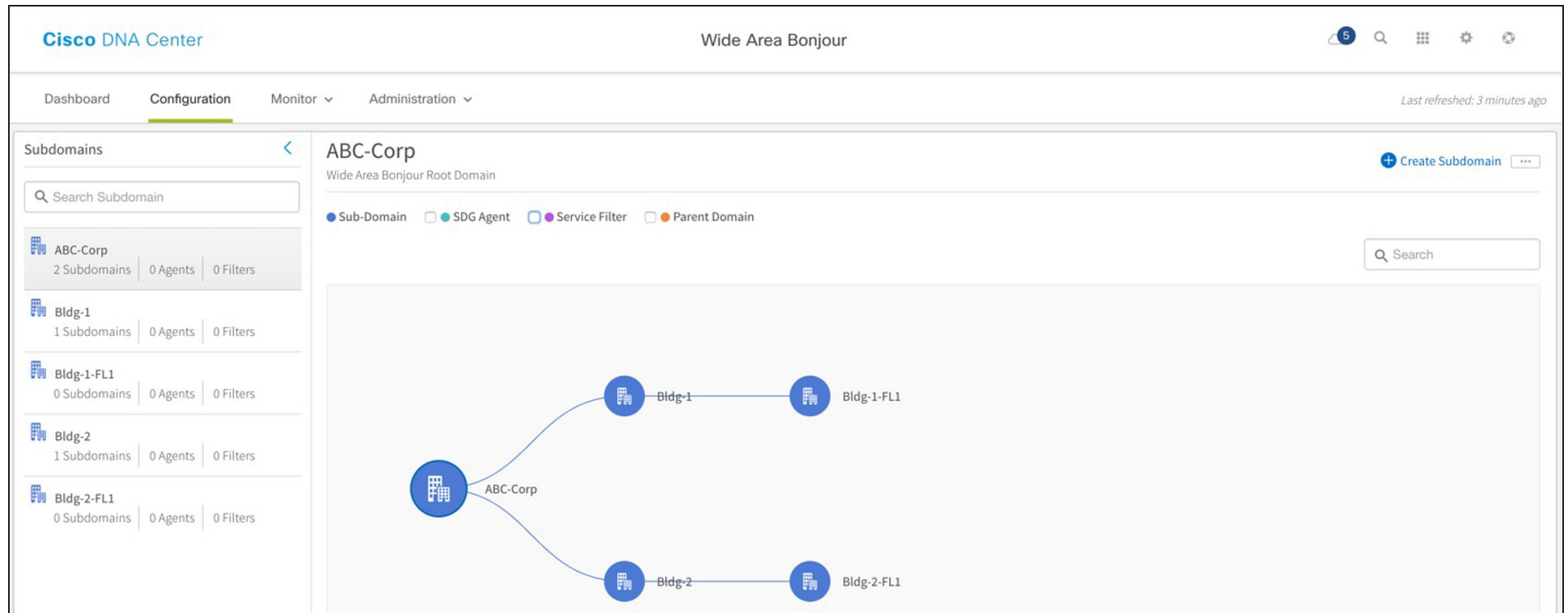
The network administrator can create additional subdomains for different floor plans for each parent subdomain, enabling a complete building hierarchy. The table below provides step-by-step guidance for building a subdomain hierarchy under the root domain.

Table 6. Cisco Wide Area Bonjour Sub-Domain Configuration Task

Step	Task	Procedure
Step-1	Select Root domain	Click to select ABC-Corp from left-panel
Step-2	Create first-tier sub-domains to the Root domain.	Click + Create Subdomain to add a new sub-domain, i.e. Bldg-1 and click Create button
Step-3	Select sub-domain from domain-list in left-panel.	Click to select Bldg-1 from left-panel
Step-4	Create second-tier sub-domains.	Click + Create Subdomain to add new sub-domain, i.e. Bldg-1-FL1 and click Create button

The figure below provides a diagram of a Wide Area Bonjour domain and subdomain hierarchy in the application as the initial configuration.

Figure 16. Cisco Wide Area Bonjour subdomain hierarchy



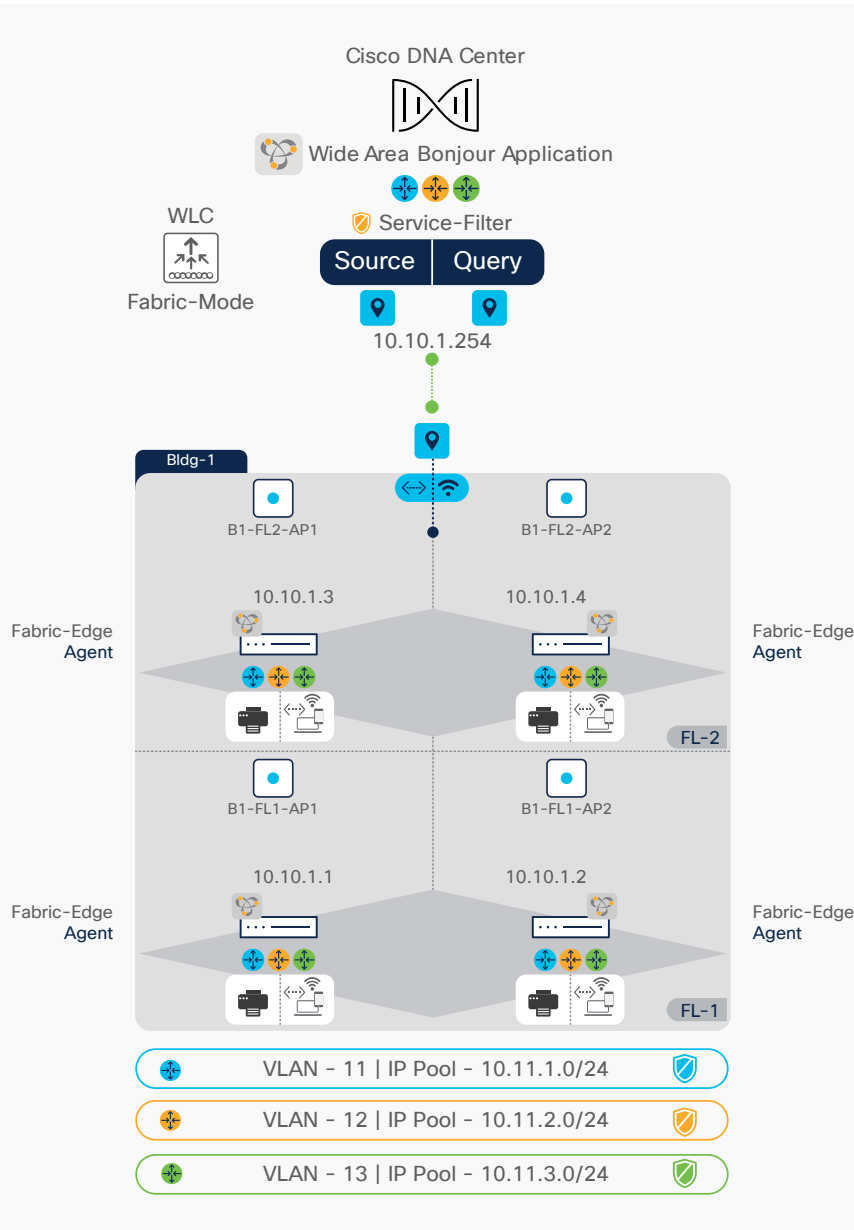
In summary, the domain structure and hierarchy in the Wide Area Bonjour application provides network administrators flexible configuration and assurance capabilities to build a site and network hierarchy for managing global service-routing policies.

Configuring Cisco Wide Area Bonjour policy

The global service-routing structure in the Wide Area Bonjour application provides flexibility to enable service routing from any to any in large-scale environments. The service announcement or service query request must pass all implemented policies for the Wide Area Bonjour application to accept the service provider information to be transmitted to the requesting SDG agent. Before building the global policy on Cisco DNA Center, the network administrator must understand the end-to-end network environment and service types to be activated on targeted wired and wireless networks.

This guide provides a reference configuration based on a Cisco SD-Access fabric-enabled wired and wireless environment as illustrated in the figure below. The intent of configuring policy on Cisco DNA Center is to enable wired printer discovery across the IP core to the wireless Apple iPad user. In addition, service discovery will be based on specific location groups as described in [Location-Group-Based Service Routing](#).





Figure 17. Cisco Wide Area Bonjour Policy reference network design



Service filter

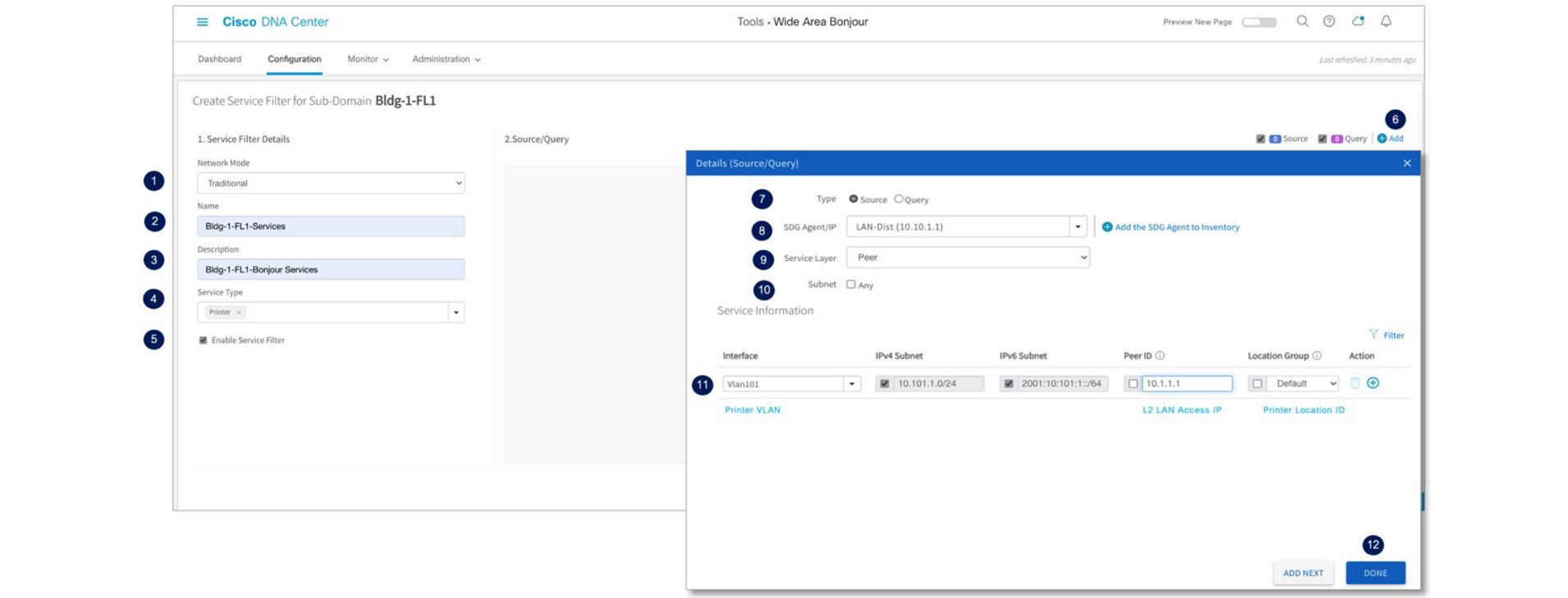
The service filter is a global service-routing policy that can be created at any level of the domain in the Wide Area Bonjour application. The simplified policy structure allows the network administrator to configure basic parameters and SDG agents with specific role and network information to enable service routing. The table below provides configuration guidelines to create a new service filter to enable Bonjour service discovery from a wired SDG agent and distribution to another wireless SDG agent switch:

Table 7. Cisco Wide Area Bonjour service-filter navigation

Task	Step
<p>Select the subdomain.</p> <p>Select Service Filter from the configuration panel to expand the policy panel.</p>	<p>Click the subdomain in the left-panel, such as Bldg-1-FL1.</p> <p>Click to select   Service Filter the subdomain, and click the service filter. </p>
<p>Create a new service filter.</p>	<p>Click  Create Service Filter to add a new service filter.</p>

The intuitive and flexible service-filter configuration supports various service-routing topologies using a single service-filter policy. To construct the policy, it is imperative to understand the constructs and function of service filters to enable service discovery and distribution from a distributed SDG agent, downstream service peer devices, and network details. The figure below illustrates a reference service-filter configuration to implement source SDG agent service routing for the network illustrated in Figure 17 under the selected subdomain.

Figure 18. Cisco Wide Area Bonjour service filter – fabric-edge source SDG agent



The Wide Area Bonjour service filter consists of two-sided fabric-edge SDG agents and respective configurations – source and query. The fabric-edge source SDG agent advertises mDNS services to Cisco DNA Center, whereas the fabric-edge query SDG agent sends mDNS service lookup requests to Cisco DNA Center. The table below provides a step-by-step configuration task to build a fabric-edge source SDG agent service filter on the selected subdomain.

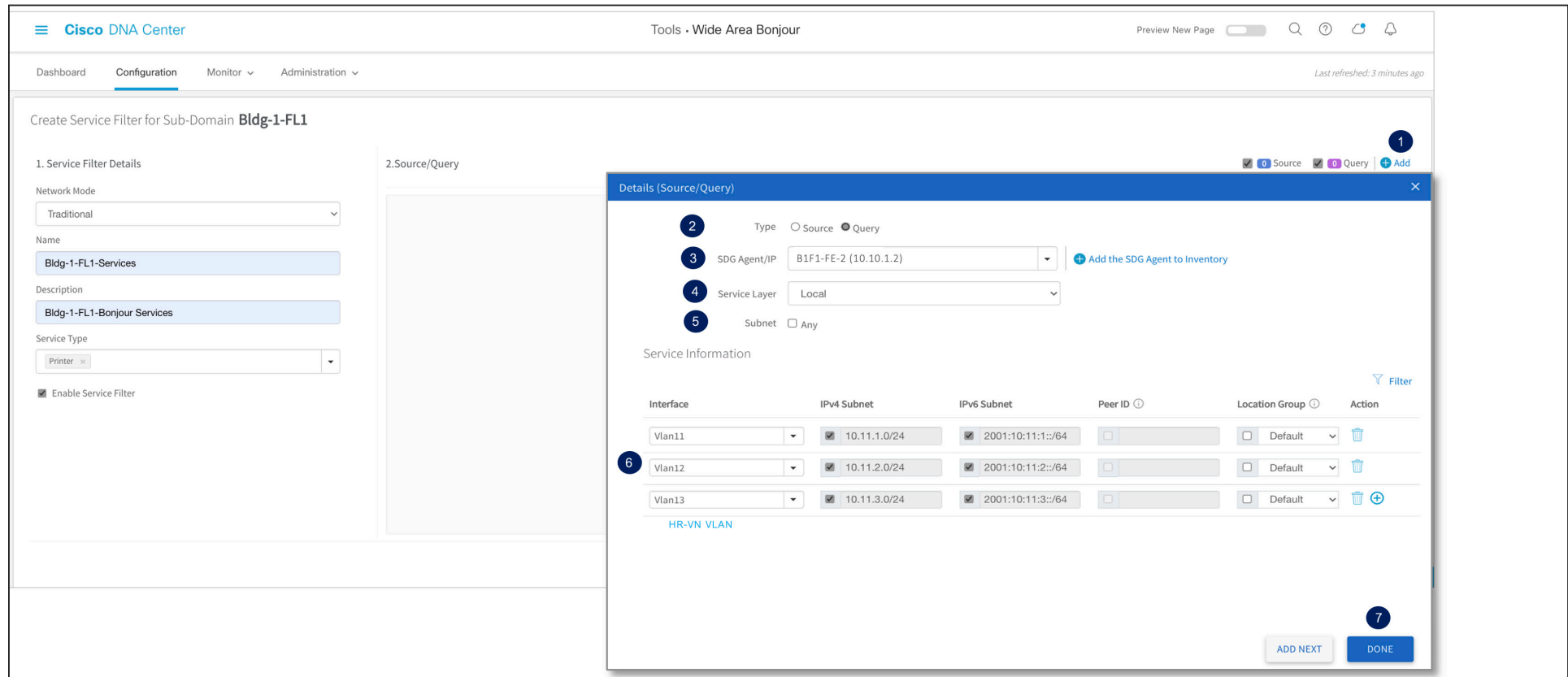
Table 8. Cisco Wide Area Bonjour source SDG agent service-filter configuration task

Step	Task	Procedure
Step-1	Select the network mode.	Select Traditional Network Mode. This is the default.
Step-2	Create a new service filter.	Create a new unique service-filter name, for example, Bldg-1-FL1-SERVICES.
Step-3	Add a description (optional).	Enter a description of the service filter.
Step-4	Select Wide Area Bonjour services.	Click the drop-down menu under Service Type to select Printer for this service filter. Create a custom service from Administration → Service Type for additional services.
Step-5	Enable the service filter in the Wide Area Bonjour domain.	Click <input checked="" type="checkbox"/> Enable service filter to activate the service filter. Uncheck to allow service-filter configuration but disable processing. The default is enabled.
Step-6	Add a source SDG agent to the service filter.	Click + Add to open a new SDG agent configuration panel.
Step-7	Select Source as the Type.	Click <input checked="" type="radio"/> Source to select the SDG agent advertising mDNS service from LAN or WLAN networks to Cisco DNA Center.
Step-8	Select the source SDG agent device.	Select the source SDG agent Catalyst switch from the drop-down menu, for example, B1F1-FE-1 10.10.1.1.
Step-9	Select the service layer mode.	There are two available service layer modes: Local: Select if the mDNS endpoint is directly attached to the fabric-edge SDG agent switch, for example, Layer 3 mode access. Peer: Select if the mDNS endpoint is indirectly attached to the fabric-edge SDG agent switch and is learning or receiving service requests from a downstream Layer 2 service peer, for example, a LAN access PEN switch or Catalyst 9800 Series WLC in local mode.
Step-10	Specify any subnet filtering for the source SDG agent (optional).	Click the Any checkbox to accept mDNS messages from the source SDG agent originated from the IPv4/IPv6 network, service-peer ID, and location tag.

Step	Task	Procedure
Step-11	Specify selective subnet filtering for the source SDG agent.	Select one or more service-provider interface VLAN IDs matching the mDNS policy. Select Default as the Location Group if no location ID is assigned on the Ethernet switch port.
Step-12	Complete configuration of the fabric-edge source SDG agent.	Click DONE to complete configuration of the fabric-edge source SDG agent.

To complete the service filter, the receiver or fabric-edge query SDG agent configuration must be created, enabling end-to-end service routing between fabric-enabled wired and wireless networks. The figure below illustrates a reference service-filter configuration to implement query SDG agent service routing for the network illustrated in Figure 17 under the selected subdomain.

Figure 19. Cisco Wide Area Bonjour service filter – fabric-edge query SDG agent



The screenshot shows the Cisco DNA Center interface for configuring a service filter. The main configuration area is titled 'Create Service Filter for Sub-Domain Bldg-1-FL1'. It includes sections for '1. Service Filter Details' and '2. Source/Query'. A modal window titled 'Details (Source/Query)' is open, showing configuration options for a query agent. The modal includes a table for 'Service Information' with columns for Interface, IPv4 Subnet, IPv6 Subnet, Peer ID, and Location Group. The table lists three VLANs: Vlan11, Vlan12, and Vlan13, each with corresponding IPv4 and IPv6 subnets and a 'Default' location group. A 'Filter' icon is visible in the top right of the table. The modal also has 'ADD NEXT' and 'DONE' buttons at the bottom right.

The table below provides a step-by-step configuration task to build a fabric-edge query SDG agent service filter on the selected subdomain.

Table 9. Cisco Wide Area Bonjour query SDG agent service-filter configuration task

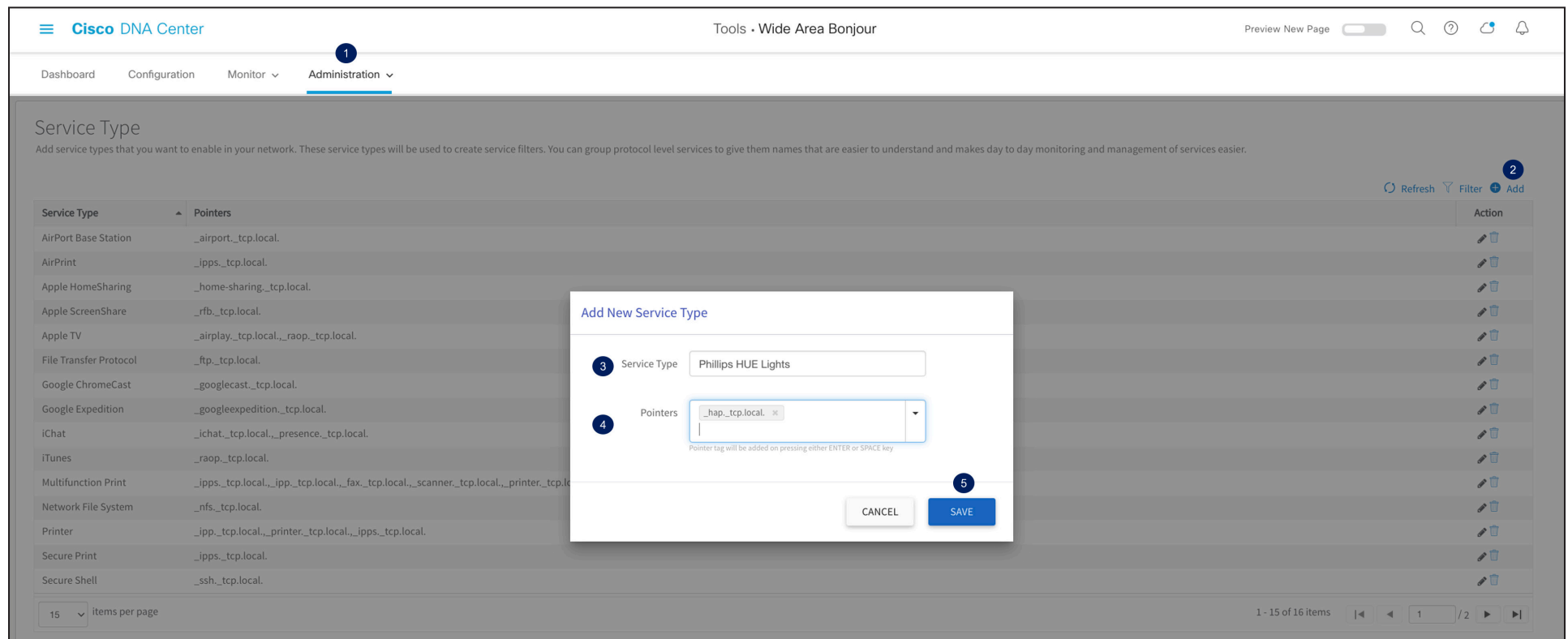
Step	Task	Step
Step-1	Add a query SDG agent to the service filter.	Click + Add to open a new fabric-edge SDG agent configuration panel.
Step-2	Select Query as the Type.	Click ● Query to select the SDG agent advertising mDNS service from LAN or WLAN networks to Cisco DNA Center. For example, B1F1-FE-2 10.10.1.2.
Step-3	Select the service layer mode.	There are two available service layer modes: Local: Select if the mDNS endpoint is directly attached to the fabric-edge SDG agent switch, for example, Layer 3 mode access. Peer: Select if the mDNS endpoint is indirectly attached to the fabric-edge SDG agent switch and is learning or receiving service requests from a downstream Layer 2 service peer, for example, a LAN access PEN switch or Catalyst 9800 Series WLC in local mode.
Step-4	Specify any subnet filtering for the query SDG agent (optional).	Click the Any checkbox to accept mDNS messages from the query SDG agent originated from the IPv4/IPv6 network, service-peer ID, and location tag.
Step-5	Specify selective subnet filtering for the query SDG agent.	Select one or more service-provider interface VLAN IDs matching the mDNS policy. Select Default as the Location Group if no location ID is assigned on the Ethernet switch port.
Step-6	Complete the configuration of the query SDG agent.	Click DONE to complete configuration of the fabric-edge query SDG agent.
Step-7	Complete the configuration of the service filter.	Click CREATE to create the Wide Area Bonjour global service-routing policy.

Configuring a Cisco Wide Area Bonjour service list

The Bonjour service provider may provide one or more types of subservices, such as a single multifunction printer named Bldg-1-PRN, which may advertise print, mobile print, scan, fax, and more subservices in the network. Each of these subservices is announced in mDNS PoinTeR (PTR) records that need to be part of the policy in the Local Area and Wide Area Bonjour domains to permit service discovery and distribution in the global network. The Cisco Wide Area Bonjour application supports a built-in service list for Bonjour services commonly found in the network. By default, the application pairs the common type of PTR records enabling subservices in the network.

The network administrator can leverage the default service list or create a custom entry to enable new services across the Wide Area Bonjour domain network. The mDNS PTR records are in a simple regular-expression format that each endpoint supports with a unique record name for specific services. The service name and transport protocol port numbers may be IANA (Internet Assigned Numbers Authority) registered or unregistered. The network administrator must identify the custom PTR record from the manufacturer or use service scanner tools to discover custom service PTRs from targeted network segments before creating custom entries. The figure below provides a reference diagram for creating a custom service-list entry in Cisco DNA Center.

Figure 20. Cisco Wide Area Bonjour custom service-list entry



The screenshot shows the Cisco DNA Center interface for configuring Wide Area Bonjour service types. A modal dialog titled "Add New Service Type" is open, allowing the user to create a new entry. The dialog contains the following fields and elements:

- 1**: Navigation menu with "Administration" selected.
- 2**: "Add" button in the top right of the table.
- 3**: "Service Type" input field containing "Phillips HUE Lights".
- 4**: "Pointers" dropdown menu containing "_hap_tcp.local".
- 5**: "SAVE" button.

Service Type	Pointers	Action
AirPort Base Station	_airport_tcp.local.	[Edit] [Delete]
AirPrint	_ipp_tcp.local.	[Edit] [Delete]
Apple HomeSharing	_home-sharing_tcp.local.	[Edit] [Delete]
Apple ScreenShare	_rfb_tcp.local.	[Edit] [Delete]
Apple TV	_airplay_tcp.local._raop_tcp.local.	[Edit] [Delete]
File Transfer Protocol	_ftp_tcp.local.	[Edit] [Delete]
Google ChromeCast	_googlecast_tcp.local.	[Edit] [Delete]
Google Expedition	_googleexpedition_tcp.local.	[Edit] [Delete]
iChat	_ichat_tcp.local._presence_tcp.local.	[Edit] [Delete]
iTunes	_raop_tcp.local.	[Edit] [Delete]
Multifunction Print	_ipp_tcp.local._ipp_tcp.local._fax_tcp.local._scanner_tcp.local._printer_tcp.local.	[Edit] [Delete]
Network File System	_nfs_tcp.local.	[Edit] [Delete]
Printer	_ipp_tcp.local._printer_tcp.local._ipp_tcp.local.	[Edit] [Delete]
Secure Print	_ipp_tcp.local.	[Edit] [Delete]
Secure Shell	_ssh_tcp.local.	[Edit] [Delete]

The table below provides step-by-step tasks to create a new custom service-list entry in Cisco Wide Area Bonjour.

Table 10. Cisco Wide Area Bonjour custom service type configuration

Task	Step
Go to the Administration section.	Click Administration → Service Type and click + Add to create a new custom service-list entry.
Add the service-list name and record(s).	Add a new and unique service type name, for example, Phillips HUE Light. In the Pointers section, add the mDNS PTR record for this service, for example, hap._tcp.local. It is important to end each PTR with a period (.) and press Return or Enter to create the new entry. For multiple PTR records, add a comma (,) as a delimiter between records.
Step 5. Save the custom service list.	Click SAVE to save the custom service list in the application database.

Cisco Wide Area Bonjour application assurance

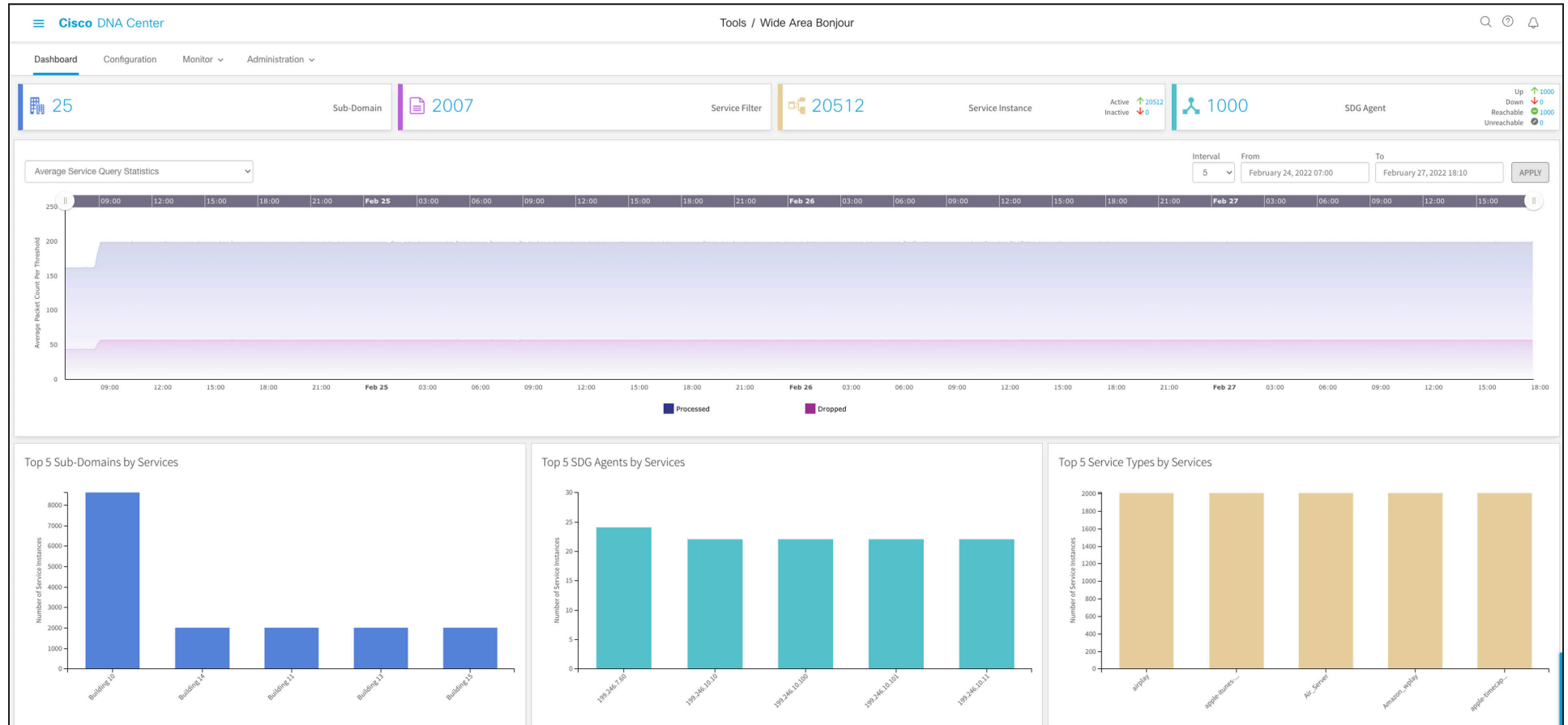
To manage, monitor, and troubleshoot the Wide Area Bonjour domain for day-n operation, the Cisco Wide Area Bonjour application supports various levels of integrated service assurance capabilities. The network administrator can monitor networkwide activities at various levels ranging from services and SDG agent statistics to a per subdomain-level services count and validating the agents and policy operational status. The end-to-end service-routing detail in Wide Area Bonjour can be monitored on a per-instance level, providing granular details from the origination point, advertising SDG agent, domain policy, and much more.

This section focuses on providing operational details for four different types of Cisco Wide Area Bonjour application assurance capabilities – dashboard, Subdomain 360°, detail view, and troubleshooting.

Dashboard

The Cisco Wide Area Bonjour dashboard provides real-time aggregated information about service counts and state visibility combined with top talkers across the Wide Area Bonjour domain. From this startup screen of Wide Area Bonjour, the network administrator can verify the overall health of the Wide Area Bonjour domain with SDG agent device reachability, service-routing status, and query statistics in real time to identify next steps to resolve any challenges. The figure below provides a reference view of the Wide Area Bonjour dashboard screen.

Figure 21. Cisco Wide Area Bonjour dashboard

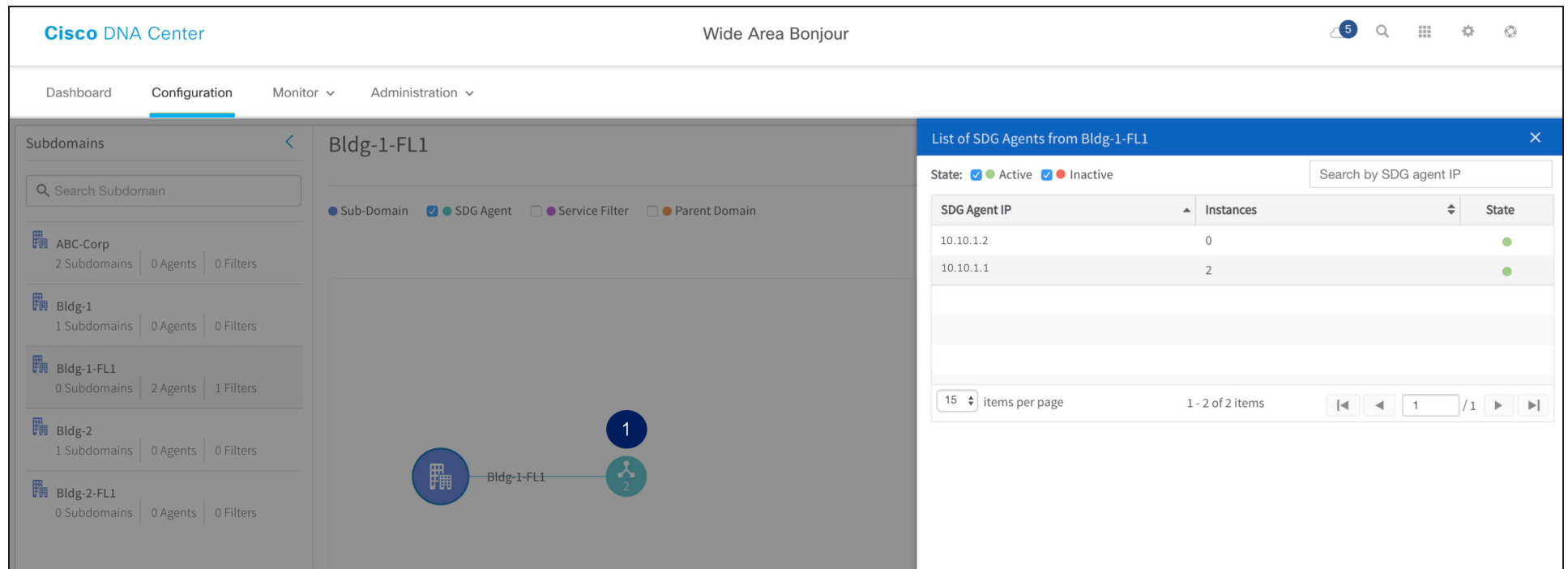


Subdomain 360°

The network administrator can get a 360° statistics view of the subdomain and associated parameters from the Configuration tab. The key objective of 360° statistics is to provide brief information at the individual subdomain level instead of the global-level visualization in the dashboard. Subdomain 360° gives the ability to navigate the different levels of the hierarchical domain structure and verify the aggregated statistics for policy configuration, service-instance count, and much more.

The Subdomain 360° view can be grouped in two-level parameters comprising the policy and SDG agent of the selected subdomain. The figure below illustrates a reference Subdomain 360° view of SDG agent statistics:


Figure 22. Subdomain 360° sub-agent statistics



The screenshot displays the Cisco DNA Center interface for the 'Wide Area Bonjour' environment. The 'Configuration' tab is active, showing a 'Subdomains' list on the left and a detailed view for 'Bldg-1-FL1' on the right. A modal window titled 'List of SDG Agents from Bldg-1-FL1' is open, displaying a table of agent statistics.

SDG Agent IP	Instances	State
10.10.1.2	0	Active
10.10.1.1	2	Active

Table 11. Cisco Wide Area Bonjour Subdomain 360° sub-agent statistics

Task	Step
Select a subdomain from the left panel.	Select a subdomain to open 360° statistics view.
Select SDG Agent.	Click the SDG Agent checkbox to expand the selected subdomain hierarchy, providing aggregated SDG agent count information.
Expand the SDG agent information.	Click  to open a 360° view of each SDG agent of the selected subdomain.
Verify SDG Agent 360° status.	<p>Verify three key indicators of one or more SDG Agents from selected Sub-Domain:</p> <ul style="list-style-type: none"> • SDG Agent IP: An IP address of the SDG agent selected based on service-filter policy configuration. • Instances: Aggregated count of Bonjour services discovered from each source SDG agent network device. • State: The service-routing state between Cisco DNA Center and the SDG agent device. In the normal up and operational state, this is green; it will be red when peering is down.

The service filter 360° provides two key options for the network administrator to build and manage the global policies. The network administrator can select SDG Agent and Service Filter to view or create a new service filter on the selected subdomain. The figure below illustrates a reference Subdomain 360° view of service-filter statistics.

Figure 23. Sub-Domain 360° Service-Filter Statistics

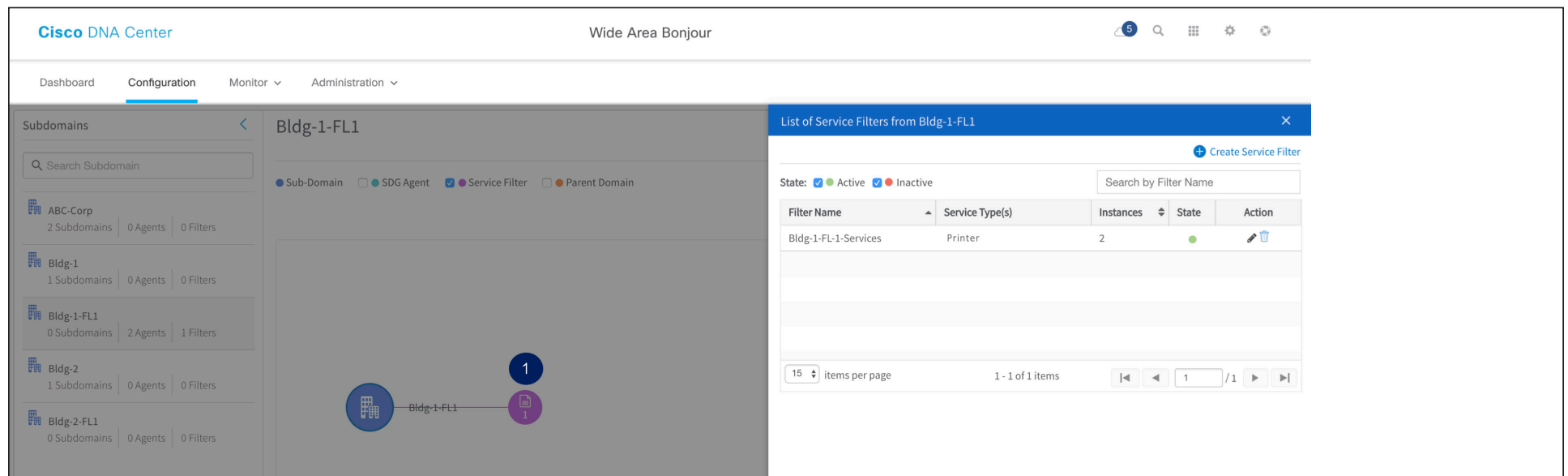



Table 12. Cisco Wide Area Bonjour Subdomain 360° service-filter statistics

Task	Step
Select the subdomain from the left panel.	Search or select a subdomain to view the 360° statistics.
Select Service Filter.	Click the Service Filter checkbox to expand the selected subdomain hierarchy providing aggregated service filter count information.
Expand the SDG agent information.	Click  to open 360° views of each service filter of the selected subdomain.
Verify the SDG agent's 360° status	<p>Verify five key indicators of one or more service filters from the selected subdomain:</p> <ul style="list-style-type: none"> • Filter name: The administrator-created global service filter on the selected subdomain. • Service type(s): Types of Bonjour service(s) allowed for global discovery and distribution. • Instances: Total aggregated service-instance count discovered from one or more source SDG agents on each service filter. • State: A service filter in the Active state enables service-routing peering, service discovery and distribution between all SDG agents. In the Inactive state, service-routing is disabled between all SDG agents that are part of this service filter. • Action: The network administrator can edit or delete the selected service filter.

Detail view

The Cisco Wide Area Bonjour application supports detail monitoring and service-routing status from the Monitor tab. The detail view can also help with troubleshooting if there are service-routing issues at the individual service-instance or SDG agent level. The Monitor section is subdivided into the following categories:

- **SDG agent detail:** This page provides detailed information to understand the configuration, statistics, and status of each SDG agent. In addition,

the network administrator can select one or more source SDG agents to manually force service cache resynchronization to update global information in Cisco DNA Center.


- **Service instance detail:** This page provides detailed information on each Bonjour service instance, and the routing status can be verified.

The figure below provides a reference detail view of the SDG agent listing and various parameters associated with each network device.

Figure 24. Monitoring SDG agent detail

SDG Agent	Management IP	Source Interface	Domain	Service Filter	Role(s)	Available Services	Reachability	State	Last Sync	Resync Status
<input type="checkbox"/> 10.10.1.1	10.155.255.1	Loopback0	Bldg-1-FL1	Bldg-1-FL1-Services	Source	1	Reachable	Active	2022-02-27 21:00:31	Successful
<input type="checkbox"/> 10.10.1.2	10.156.255.1	Loopback0	Bldg-1-FL1	Bldg-1-FL1-Services	Query	0	Reachable	Active		Not Initiated

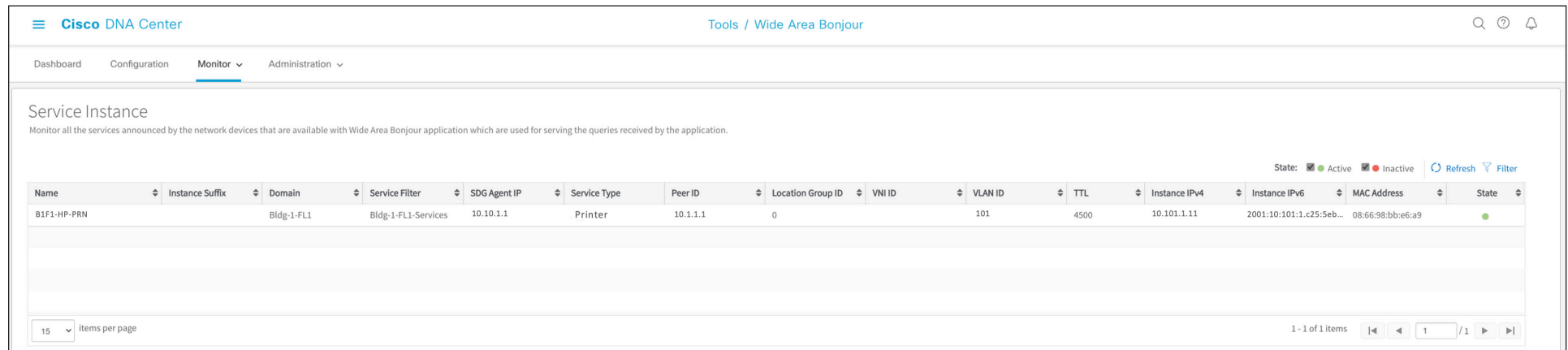
Table 13. Cisco Wide Area Bonjour SDG agent monitoring

Task	Step
<p>Go to Detail SDG Agent Monitoring.</p> <p>Perform manual services resynchronization in the Wide Area Bonjour domain (optional).</p> <p>Verify SDG agent detail status.</p>	<p>Click Monitor tab → and select SDG agents from the submenu.</p> <p>Click checkbox to select one or more SDG-Agents and click  Resync button to start manual service resynchronization process.</p> <p>The SDG agent detail page provides multiple key indicators pertaining to configuration and operational state:</p> <ul style="list-style-type: none"> ▪ SDG Agent: List of SDG agents that are part of one or more service-filter policy configurations. ▪ Management IP: An SDG agent IP address used to manage the network device. ▪ Source Interface: An SDG agent IP address used to establish a service-routing session. ▪ Domain: The name of one or more subdomains where each SDG agent is associated. ▪ Service Filter: The name of one or more service filters where each SDG agent is associated.

Task	Step
	<ul style="list-style-type: none"> ▪ Role(s): The SDG agent can be in the source role, advertising services to Cisco DNA Center, or the query role, requesting services from Cisco DNA Center. In a bidirectional scenario, the same SDG agent is in both source and query roles. ▪ Available Services: Total service-instance count received from each source SDG agent. ▪ Reachability: SDG agent network reachability and SNMP manageability status. ▪ State: Service-routing peering status between Cisco DNA Center and each SDG agent. ▪ Last Sync: Timestamp of services synchronization between Cisco DNA Center and the source SDG agent. ▪ Resync Status: Manual service-instance resynchronization status.

The figure below provides a reference detail view of the mDNS service-instance listing and various associated network and policy parameters discovered from various source SDG agents based on the service-filter policy configuration.

Figure 25. Monitoring service-instance detail



The screenshot shows the Cisco DNA Center interface for monitoring service instances. The breadcrumb navigation is 'Tools / Wide Area Bonjour'. The main heading is 'Service Instance' with a sub-note: 'Monitor all the services announced by the network devices that are available with Wide Area Bonjour application which are used for serving the queries received by the application.' The interface includes a table with columns for Name, Instance Suffix, Domain, Service Filter, SDG Agent IP, Service Type, Peer ID, Location Group ID, VNI ID, VLAN ID, TTL, Instance IPv4, Instance IPv6, MAC Address, and State. A single entry is visible for 'B1F1-HP-PRN' with a state of 'Active'. The bottom of the interface shows a pagination control for 15 items per page, currently displaying 1 of 1 items.

Name	Instance Suffix	Domain	Service Filter	SDG Agent IP	Service Type	Peer ID	Location Group ID	VNI ID	VLAN ID	TTL	Instance IPv4	Instance IPv6	MAC Address	State
B1F1-HP-PRN		Bldg-1-FL1	Bldg-1-FL1-Services	10.10.1.1	Printer	10.1.1.1	0		101	4500	10.101.1.11	2001:10:101:1:c25:5eb...	08:66:98:bb:e6:a9	Active

Table 14. Cisco Wide Area Bonjour application service-instance monitoring

Task	Step
<p>Go to the Service Instance section.</p> <p>Verify Bonjour service-instance detail status.</p>	<p>Click the Monitor tab → and select Service Instance from the submenu.</p> <p>The Service Instance page displays the status of each service instance, as well as the origination point, policy, and reachability information in the Wide Area Bonjour domain:</p> <ul style="list-style-type: none"> ▪ Name: The mDNS service provider endpoint name. ▪ Instance Suffix: Optional text string appended to the original service-instance name for any type of administrative purpose. ▪ Domain: Name of subdomain from which the service is discovered. ▪ Service Filter: Service filter name that was verified and permitted to accept services from the source SDG agent network device. ▪ SDG Agent IP: Source SDG agent advertising mDNS service(s). ▪ Service Type: mDNS service type announced by provider. ▪ Peer ID: Original source service-peer PEN switch or Catalyst 9800 WLC local mode IP address announcing service to SDG agent. ▪ Location Group ID: The location group tag associated with the mDNS service-provider LAN port or wireless access point. ▪ VNI ID: The mDNS service provider mapped to the overlay BGP EVPN VXLAN Layer 2 or Layer 3 network. The VNI ID is an overlay virtual network ID. ▪ VLAN ID: The Layer 2 VLAN ID mapped to a wired or wireless mDNS service provider endpoint. ▪ TTL: The long-lived mDNS TTL value of 4500 seconds remains intact across the Wide Area Bonjour domain. ▪ IPv4 Address: An IPv4 address (A record) of mDNS endpoints. ▪ IPv6 Address: A globally routed IPv6 address (AAAA record) of mDNS endpoints. ▪ MAC Address: The original wired or wireless MAC address of an mDNS endpoint. ▪ Status: The service instance will be distributed to the query SDG agent if the state is Active. The service-instance entries marked as Inactive will be prevented from global distribution if withdrawn from the source SDG agent. The Inactive entries are automatically purged after 24 hours.

Cisco Wide Area Bonjour application administration

The administration section of the Cisco Wide Area Bonjour application allows the network administrator to build and manage global services parameters and policy configuration file management. The features in this section can be used during initial or any day-n deployment stage to complete regular network operation tasks. The network administrator can manage application services, database, and SDG agent global parameters from the Administration menu tab. The policy configuration management is flexible to manage importing or exporting at the domain level of the hierarchy without causing any service-routing disruption or downtime.

This section is divided into multiple subsections that focus on different application administration capabilities that the network administrator can use to manage the Wide Area Bonjour domain.

Global parameters

The global parameters are a common configuration set that is applied to all SDG agents paired with the Cisco Wide Area Bonjour application. The network administrator can secure the service peering communication with all SDG agents using MD5 authentication and can adjust default keepalive timer settings to maintain service peering. In the Cisco Wide Area Bonjour architecture, these service routing parameters are part of the initial handshake and are set based on values configured in the global settings.

Because these global configuration parameters are centrally managed in the control plane from Cisco DNA Center, there are no relevant commands automated to network devices. The network administrator can update the service-routing parameters that are dynamically adjusted without resetting an existing peering session, thus providing best-in-class service resiliency in the network. The figure below provides a reference view of the global parameter settings.

Figure 26. Cisco Wide Area Bonjour global parameters

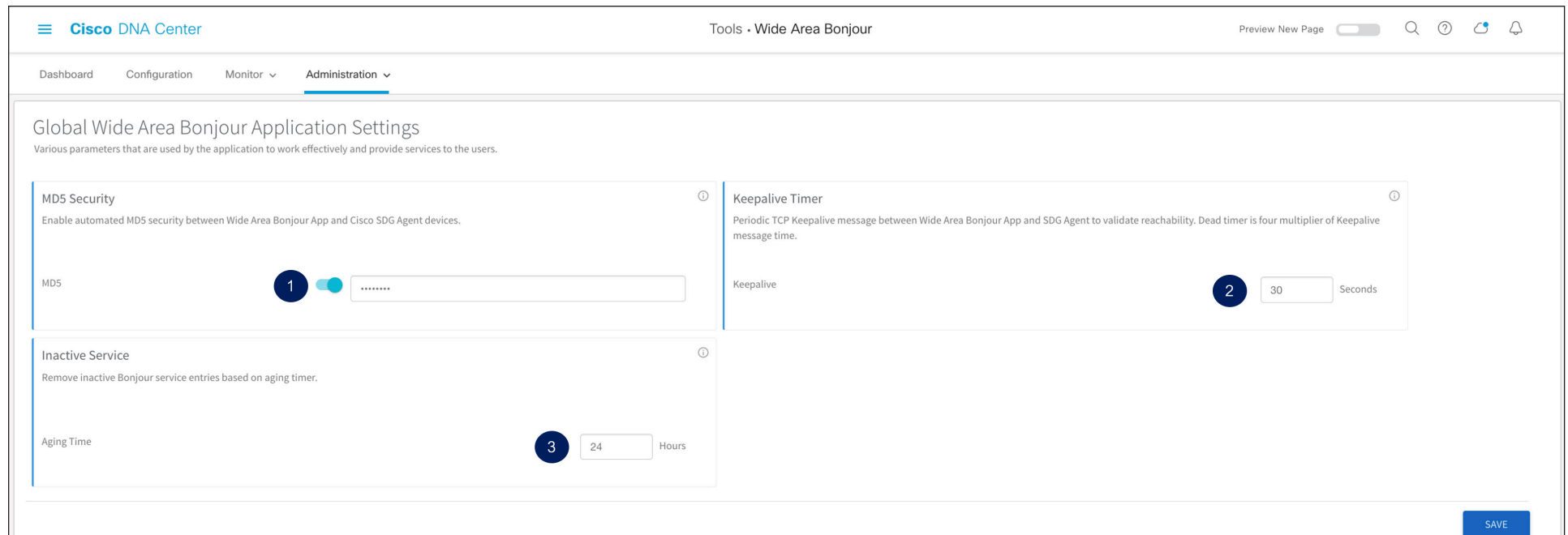



Table 15. Cisco Wide Area Bonjour global parameter configuration

Task	Step
Go to the Global Application Settings section	Click the Administration tab  and select Global from the submenu.
Secure SDG agent service peering sessions.	Slide the button to enable MD5 authentication security between Cisco DNA Center and SDG agent devices.
Adjust service peering timers.	By default, the Hello message timer between Cisco DNA Center and SDG agents is set to 30 seconds with a multiplier of 4 for a 120-second dead-interval timer. The value can be adjusted between 15 and 120 seconds.
Inactive Service Maintenance.	Cisco DNA Center holds inactive services information for up to 24 hours by default. The value can be adjusted between 1 and 24 hours.

Service-type database

Cisco DNA Center supports a built-in service-type database with a user-friendly Bonjour service name paired with the minimum required mDNS PTR records to enable and use the services across the Wide Area Bonjour domain. Like the Cisco IOS XE operating system, the Cisco DNA Center Bonjour service-type database provides flexibility to create custom service entries if default values do not meet the requirements. The figure below provides a reference view of the service type in the Cisco Wide Area Bonjour application.

Figure 27. Cisco Wide Area Bonjour application service-type database



The screenshot shows the Cisco DNA Center interface for the 'Administration' section, specifically the 'Service Type' database. The page title is 'Tools / Wide Area Bonjour'. The navigation menu includes Dashboard, Configuration, Monitor, and Administration. The main content area is titled 'Service Type' and includes a description: 'Add service types that you want to enable in your network. These service types will be used to create service filters. You can group protocol level services to give them names that are easier to understand and makes day to day monitoring and management of services easier.' There are 'Refresh', 'Filter', and 'Add' buttons. A table lists the service types and their pointers:

Service Type	Pointers	Action
AirPort Base Station	_airport_tcp.local.	 
Apple TV	_airplay_tcp.local._raop_tcp.local.	 
Apple-file-transfer	_smb_tcp.local._afp_tcp.local.	 
File Transfer Protocol	_ftp_tcp.local.	 
iChat	_ichat_tcp.local._presence_tcp.local.	 
iTunes	_raop_tcp.local.	 
Network File System	_nfs_tcp.local.	 
Printer	_ipp_tcp.local._printer_tcp.local._ipps_tcp.local.	 
Secure Shell	_ssh_tcp.local.	 
SMB-service	_smb_tcp.local.	 

At the bottom, there is a pagination control showing '15 items per page' and '1 - 10 of 10 items'.

Table 16. Cisco Wide Area Bonjour service-type configuration

Task	Step
Go to the Service Type section.	Click the Administration tab → and select Service Type from the submenu.
Verify the default built-in service type.	<p>The service-type table provide the following information:</p> <ul style="list-style-type: none">• Service Type: System-defined and user-friendly name of the mDNS service.• Pointers: One or more mDNS PTR records for each service type.

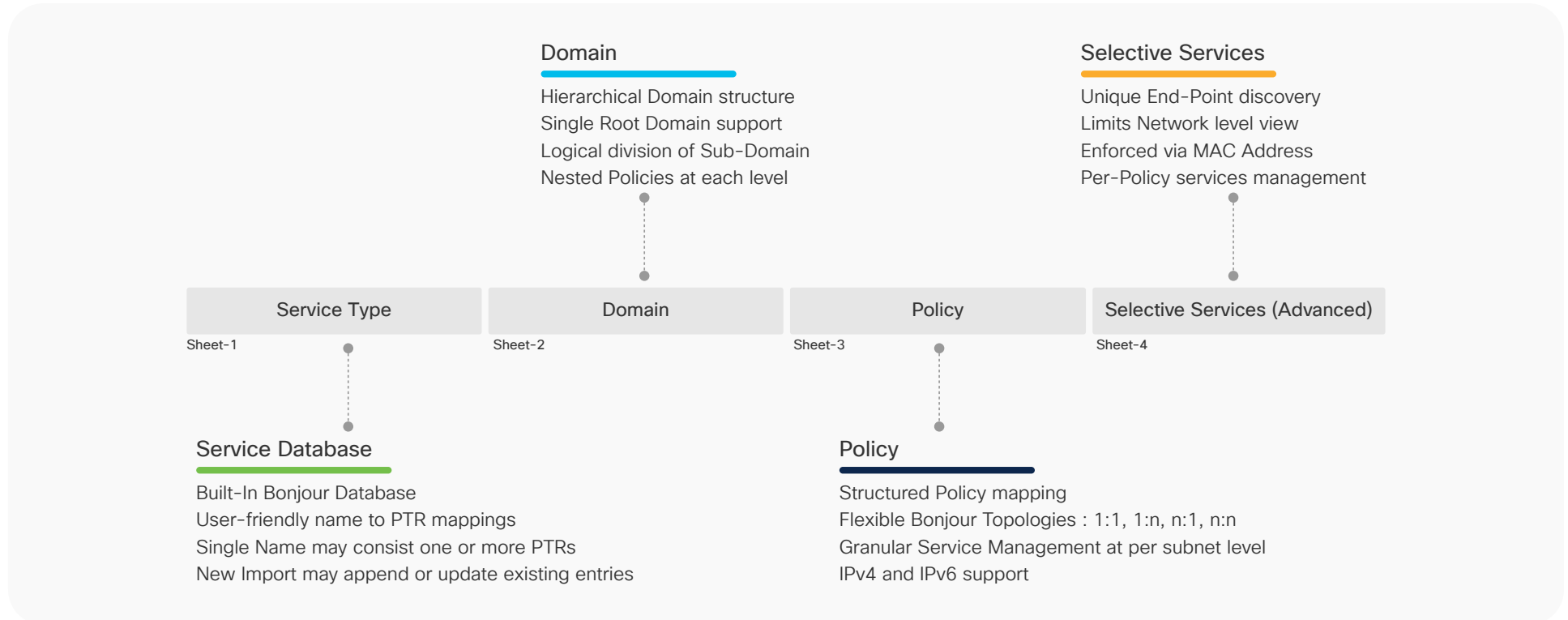
Managing policy configuration

The Cisco Wide Area Bonjour application provides the flexibility to build and manage service-filter policies manually or can be provisioned in bulk during any stage of deployment. Refer to Table 8 and 9, Cisco Wide Area Bonjour Service Filter Configuration Task, for a step-by-step manual procedure for building the service filter. This section focuses on bulk policy provisioning and managing configuration files for backup.

The service-filter policy configuration template is based on the Microsoft Excel XLS format. The network administrator can download a prebuilt

structured and formatted blank XLS template file from the Cisco Wide Area Bonjour application. It can be downloaded during the initial application provisioning stage of building the root domain, or an XLS configuration can be exported from any level of the domain hierarchy with an up-to-date configuration. The XLS template file is divided into four different worksheets, each crosslinked with the details required to automate large-scale service-filter policies. The figure below gives a brief overview of each worksheet that must be configured to build and provision bulk service-filter policies.

Figure 28. Cisco Wide Area Bonjour policy template



The Cisco Wide Area Bonjour XLS template file contains predefined column and respective names that must remain intact; otherwise importing the modified file may fail. The network administrator must feed the required data into the respective column of each worksheet based on the following reference configuration model. The Selective Services worksheet is optional and can be used in advanced service-routing scenarios where service distribution from Cisco DNA Center must be limited to user-defined static MAC addresses. For example, if Cisco DNA Center discovered up to 10 AirPrint-capable printers with Selective Services support, the network administrator could statically assign the MAC addresses of two printers to be responded from when it receives queries from the receiver SDG agent.

Import/export policy configuration

The Cisco Wide Area Bonjour application provides flexibility in managing bulk configuration with import and export capabilities. The application domain and policies can be built and imported as an initial day-0 configuration for bulk provisioning instead of using a manual process. The existing policy configuration can be downloaded to a local computer in XLS format to update existing policies and for backup purposes.

The policy configuration import is seamless in operation and can be appended to the Cisco Wide Area Bonjour application while in the operational state. The new imported file may include new service types in the database, services being added to existing policies, or new subdomains

with new policies. During configuration import, the application and service peering with existing SDG agents remains intact, providing nondisruptive bulk provisioning capabilities to scale up the network and services in the Wide Area Bonjour domain. The network administrator can import the configuration at any domain hierarchy of an application.

The export function downloads the latest configuration snapshot from the Cisco Wide Area Bonjour application to a local computer. The downloaded file can be updated with new bulk changes and reimported to update the configuration. The network administrator can use the export function as a configuration backup to be restored as needed.

Figure 29. Cisco Wide Area Bonjour application – import/export policy configuration

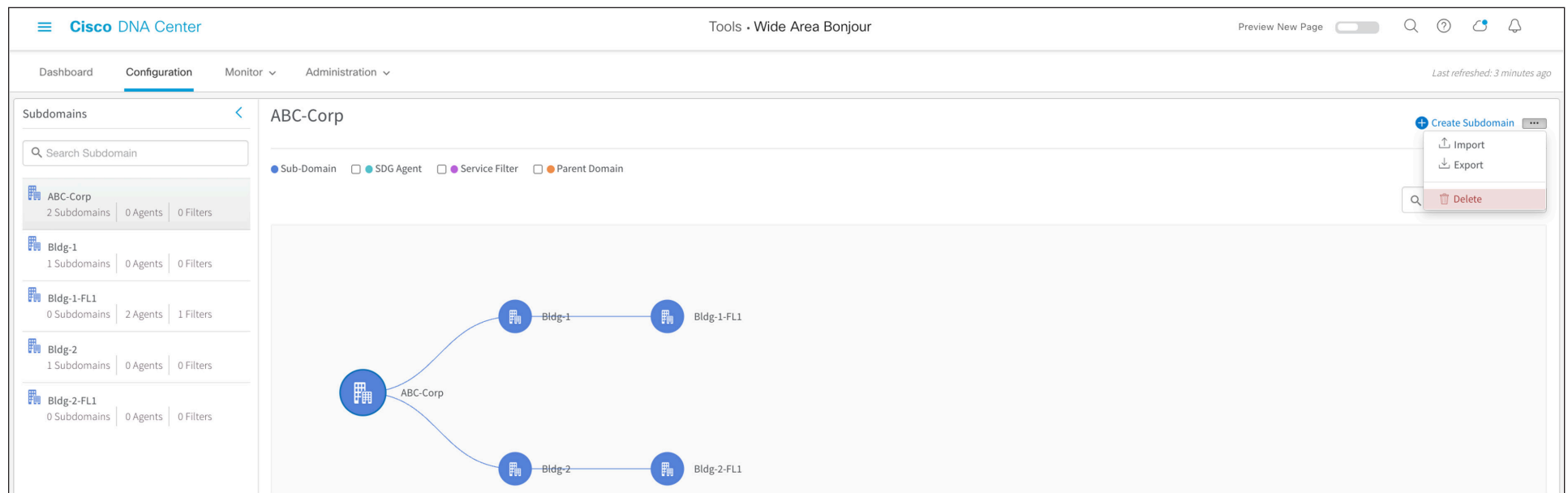


Table 17. Cisco Wide Area Bonjour service-type configuration

Task	Step
Select a domain for import/export configuration.	Click the Configuration tab → and select Root or Subdomain from the left panel to import or export the configuration.
Select import or export.	Click Import or Export to manage the configuration file for the selected domain.

Appendix

Scale and performance support matrix

Cisco DNA Service for Bonjour is a fully distributed mDNS service-routing solution; hence it provides a high-scale solution for large enterprise networks. Each product in the overall solution scales differently due to different levels of system resources.

Table 18. Cisco DNA Center Wide Area Bonjour scale and performance matrix

Cisco DNA Center	Service scale	Release
DN2-HW-APL DN2-HW-APL-L DN2-HW-APL-XL	150,000 services 1000 SDG agents	Cisco DNA Center 2.2.3 Cisco Wide Area Bonjour application

Table 19. Cisco IOS XE mDNS scale and performance matrix

Platform	Mode	Service scale	Release
Cisco Catalyst 9300 Series	Service peer or agent	7500	17.6.2
Cisco Catalyst 9400 Series	Service peer or agent	10,000	17.6.2
Cisco Catalyst 9500 Series	Service peer or agent	12,000	17.6.2
Cisco Catalyst 9500H Series	Service peer or agent	12,000	17.6.2
Cisco Catalyst 9600 Series	Service peer or agent	15,000	17.6.2
Cisco Catalyst 9800-80 WLC	Service peer	14,000	17.6.2
Cisco Catalyst 9800-40 WLC	Service peer	12,000	17.6.2
Cisco Catalyst 9800-L WLC	Service peer	4000	17.6.2
Cisco Catalyst 9800-CL WLC for Cloud	Service peer	2000	17.6.2

Summary

Cisco DNA Service for Bonjour is an enterprise-grade Wide Area Bonjour solution designed to seamlessly integrate into a complex wired and wireless network infrastructure. It retains the original end-user experience for using Bonjour technology in an enterprise network. In addition, the new solution provides plug-and-play service-routing capabilities without any hardware changes in DHCP/DNS servers or manual MAC address management.

The new distributed architecture supports unparalleled scale, performance, security, and redundancy that offers a vendor-agnostic solution to enable an end-to-end services-rich network infrastructure between computers, IoT devices, and more.

Reference

Cisco.com

[Cisco DNA Service for Bonjour – solution landing page](#)

At-A-Glance

[Cisco DNA Service for Bonjour Solution At-A-Glance](#)

Deployment Guide

[Cisco DNA Service for Bonjour Deployment Guide – Traditional LAN and Wireless Local Mode](#)

[Cisco DNA Service for Bonjour Deployment Guide – Traditional LAN and FlexConnect Wireless Mode](#)

Quick Configuration guides

[Cisco DNA Service for Bonjour Quick Configuration Guide](#)

Cisco DNA Service for Bonjour Cisco.com configuration guides

[Cisco Catalyst 9300 Series Switches](#)

[Cisco Catalyst 9400 Series Switches](#)

[Cisco Catalyst 9500 Series Switches](#)

[Cisco Catalyst 9600 Series Switches](#)

[Cisco Catalyst 9800 Series WLC](#)

Cisco Embedded Wireless Controller on Catalyst Access Points

[Cisco DNA Center – Wide Area Bonjour User Guide](#)