Cisco DNA Service for Bonjour Solution

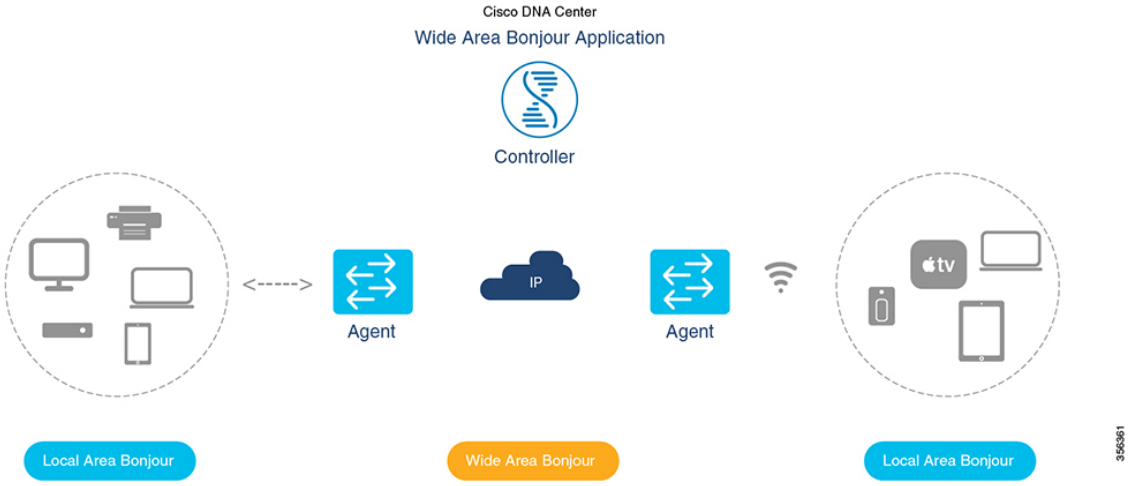
Overview

The Apple Bonjour protocol is a zero-configuration solution, which simplifies network configuration and enables communication between connected devices, services, and applications. Using Bonjour, you can discover and use shared services with minimal intervention and configuration. Bonjour is designed for single Layer-2 domains, which is ideal for small, flat, single-domain setups, such as home networks. The Cisco Wide Area Bonjour solution eliminates the single Layer-2 domain constraint and expands the scope to larger Layer-3 wired and wireless networks, as well as SD-Access networks.

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

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

The Cisco Wide Area Bonjour application operates across two integrated domain networks.



- **Local-Area SDG Domain**: The Cisco Catalyst switches at Layer 3 boundary function as Service Discovery Gateway (SDG) for local cache discovery and distribution functions between local VLANs. In this controller-less Bonjour solution, the SDG gateway switch provides a single gateway solution at the LAN and Wireless Distribution block. The SDG switch communicates with local Bonjour endpoints to build and manages the services information. The Bonjour gateway function is ineffective between Bonjour endpoints in same Layer 2 network, as they follow standards-based flood-and-learn rule.
- **Wide-Area SDG Domain**: The Wide Area Bonjour domain is a Controller-based solution. The Bonjour gateway role and responsibilities of Cisco Catalyst switching is extended from the SDG to an SDG-Agent. The network-wide distributed SDG-Agent devices establish a lightweight, stateful and reliable communication channel with centralized Cisco DNA-Center Controller running the Wide Area Bonjour application. The service routing between the SDG Agents and the Controller operates over regular IP networks using reliable TCP port 9991 between the Cisco DNA Center and the SDG Agent devices. The SDG Agents route locally discovered services based on the export policy.

Restrictions

- Cisco Service Discovery Gateway (SDG) and Wide Area Bonjour gateway function is supported on Cisco Catalyst Switch and Cisco ISR 4000 series routers. See Solution Components, on page 3 for the complete list of supporting platforms, software versions and license levels.
- Cisco IOS supports classic and new method of building local Bonjour configuration policies. The classic method is based on **service-list mdns-sd** CLI whereas the new method is based on **mdns-sd gateway**. We recommend using the new **mdns-sd gateway** method since the classic configuration support will be deprecated in near future releases.
- The classic to new method CLI migration is manual procedure to convert the configuration.
- The Bonjour service policies on Cisco SDG Gateways are effective between local VLANs. In addition to these, a specific egress policy controls the type of services to be exported to the controller. The Layer 2 Multicast-DNS Bonjour communication between two end-points on same broadcast domain is transparent to gateway.

- To enable end-to-end Wide Area Bonjour solution on Wireless networks, the Cisco WLC controller must not enable mDNS Snooping function. The upstream IP gateway on the dedicated Cisco Catalyst switch must have the Bonjour gateway function enabled for wireless clients.
- Cisco Wireless LAN Controller must enable AP Multicast with unique Multicast group. Without AP joining WLC Multicast group the mDNS messages will not be processed between client and gateway switch. Multicast on Client SSID or VLAN is optional for other multicast applications and not mandatory or required for Bonjour solution.
- Cisco Catalyst 9800 WLC can be configured as mDNS Gateway. In this mode, the Cisco Catalyst 9800 WLC supports Local-Area Bonjour gateway solution limited to Wireless only networks. Cisco Catalyst 9800 does not support Wide Area Bonjour. For end-to-end Wired and Wireless Bonjour support, we recommend using upstream Cisco Catalyst Switch as IP and Bonjour gateway.

Solution Components

The Cisco DNA Service for Bonjour solution is an end-to-end solution that includes the following key components:

- **Cisco SDG Agent**: The Cisco Catalyst Switch or an ISR 4000 series router functions as a Service Discovery Gateway (SDG) Agent and communicates with the Bonjour Service endpoints within the Layer 2 domain and central Cisco DNA Center controller.
- **Cisco DNA Controller**: The Cisco DNA Controller provides a secure channel with trusted SDG Agents, for centralized services management and controlled service routing.
- **Cisco Wireless LAN Controller**: The Cisco Wireless LAN Controller (WLC) transparently switches mDNS messages between wireless clients and upstream Bonjour gateway switch in distribution layer network.
- **Endpoints**: A Bonjour endpoint is any device that advertises or queries Bonjour services conforming to RFC 6762. The Bonjour endpoints can be in either LAN or WLANs. The Wide Area Bonjour application is designed to integrate with RFC 6762 compliant Bonjour services, including Apple, Microsoft, Google, HP and more.

Cisco Wide Area Bonjour Service Workflow

The Cisco Wide Area Bonjour solution follows a client-server model. The SDG Agent functions as a client and the Cisco Wide Area Bonjour application Cisco DNA Center functions as a server.

The following sections describe the workflow of service announcement and discovery in the IP network.

Announcing Services to the Network

- The endpoint devices (Source) in the Local Area Bonjour domain send service announcements to the SDG Agent and specify what services they offer. For example, _airplay._tcp.local, _raop._tcp.local, _ipp._tcp.local, and so on.
- The SDG Agent listens to these announcements and matches them against the configured Local Area SDG Agent policies. If the announcement matches the configured policies, the SDG Agent accepts the service announcement and routes the service to the controller.

Discovering Services Available in the Network

- The endpoint device (Receiver) connected to the Local Area SDG Agent sends a Bonjour query to discover the services available, using the mDNS protocol.
- If the query conforms to configured policies, SDG Agent responds with the services obtained from appropriate service routing via the Wide Area Bonjour Controller.

Wide Area Bonjour Multi-Tier Policies

The various policies that can be used to control the Bonjour announcements and queries are classified as the following:

- **Local Area SDG Agent Filters**: Enforced on the SDG Agent in Layer-2 Network Domain. These bi-directional policies control the Bonjour announcements or queries between the SDG Agents and the Bonjour endpoints.
- **Wide Area SDG Agent Filters**: Enforced on the SDG Agent for export control to the Controller. This egress unidirectional policy controls the service routing from the SDG Agent to the controller.
- **Cisco Wide Area Bonjour Policy**: Enforced on Controller for global service discovery and distribution. Policy enforcement, between the controller and the IP network is bi-directional.

Supported Platforms

The following table lists the supported controller, along with its hardware and software version.

Supported Controller	Hardware	Software Version
Cisco DNA Center Appliance	DN2-HW-APL DN2-HW-APL-L DN2-HW-APL-XL	1.3.1.0
Cisco Wide Area Bonjour Application	Cisco DNA Center Appliance	2.4.0.10062

The following table lists the Supported SDG Agents along with their licenses and software requirements.

Supported SDG Agent	Local Area SDG	Wide Area SDG	Minimum Software
Cisco Catalyst 9200 Series Switches	DNA Essentials	Unsupported	17.1.1
Cisco Catalyst 9200L Series Switches	Unsupported	Unsupported	-
Cisco Catalyst 9300 Series Switches	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 9400 Series Switches	DNA Essentials	DNA Advantage	16.11.1

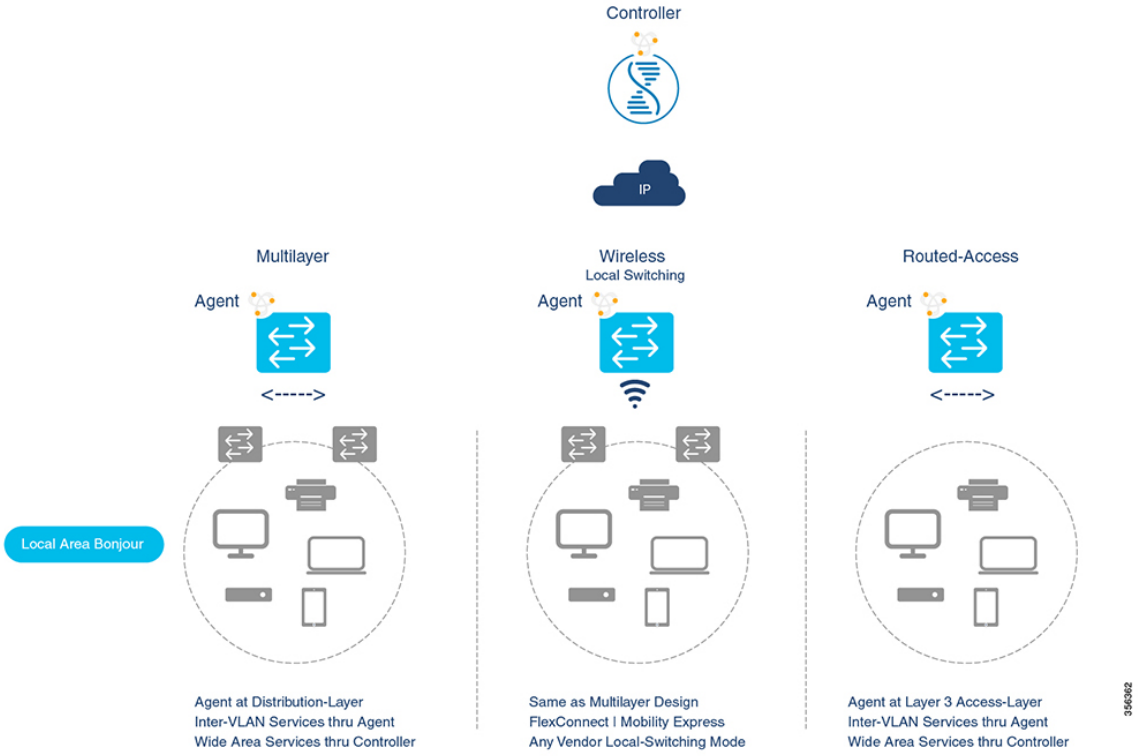
Supported SDG Agent	Local Area SDG	Wide Area SDG	Minimum Software
Cisco Catalyst 9500 Series Switches	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 9500 Series Switches - High Performance	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 9600 Series Switches	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 9800 Series Wireless Controllers	DNA Essentials	Unsupported	16.11.1
Cisco 5500 Series Wireless Controllers	Unsupported	Unsupported	Pass-Thru
Cisco 8540 Wireless Controller	Unsupported	Unsupported	Pass-Thru
Cisco Catalyst 6800 Series Switches	IP Base	IP Services + DNA-Addon	15.5(1)SY4
Cisco Catalyst 4500-E Series Switches	IP Base	IP Services + DNA-Addon	3.11.0
Cisco Catalyst 4500-X Series Switches	IP Base	IP Services + DNA-Addon	3.11.0
Cisco Catalyst 3650 Series Switches	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 3850 Series Switches	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 2960-X Series Switches	LAN Base	Unsupported	15.2.6E2
Cisco Catalyst 2960-XR Series Switches	IP Lite	Unsupported	15.2.6E2
Cisco 4000 Series Integrated Services Routers (ISR)	IP Base	AppX	16.11.1

Cisco Wide Area Bonjour Supported Network Design

Traditional Wired and Wireless Networks

The Cisco DNA Service for Bonjour supports various LAN network designs commonly deployed in the enterprise. The SDG Agent providing Bonjour gateway functions is typically an IP gateway for wired end-points that could be residing in the distribution layer in multilayer network designs, or in the access layer in routed access network designs.

The following figure shows various topologies which are explained further in the section.

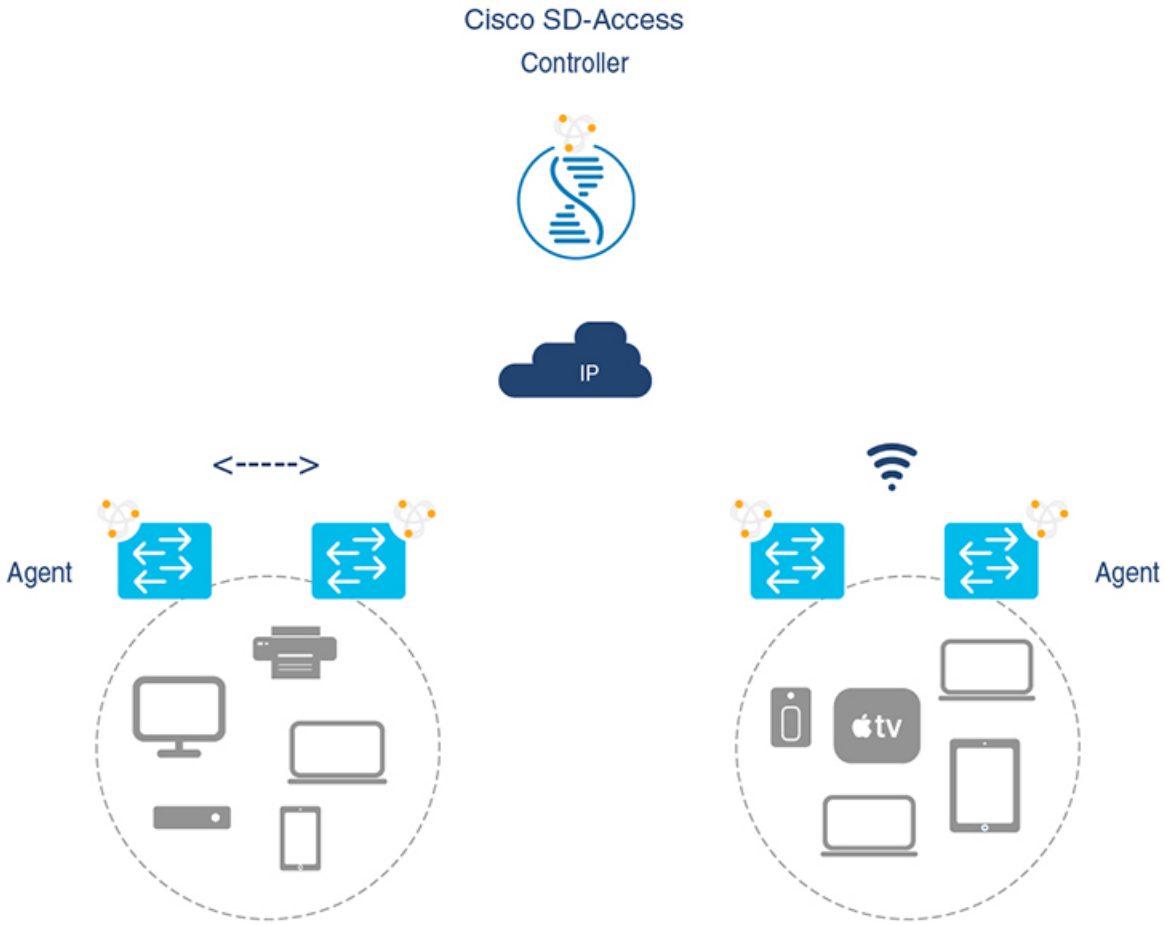


- **Multilayer LAN**: In this deployment mode, the Layer 2 Access switch provides the transparent bridging function of Bonjour services to Distribution-layer systems that act as the IP gateway and SDG Agent. There is no additional configurration or new requirement to modify the existing Layer-2 trunk settings between the Access and Distribution Layer Cisco Catalyst Switches.
- **Routed Access**: In this deployment mode, the first-hop switch is an IP gateway boundary and therefore, it must be combined with the SDG Agent role.

The Cisco DNA Service for Bonjour also supports various Wireless LAN network designs commonly deployed in the Enterprise. The SDG Agent provides consistent Bonjour gateway functions for the wireless endpoints as in wired networks. In general, the IP gateway of the wireless clients is also a Bonjour gateway. However, the placement of the SDG Agent may vary depending on the Wireless LAN deployment mode.

Cisco SD Access Wired and Wireless Networks

In Cisco SD-Access network, the Fabric Edge switch is configured as the SDG Agent for fabric-enabled wired and wireless networks. Wide Area Bonjour policies need to be aligned with the SD-Access network policies with respect to Virtual Networks and SGT policies, if any.



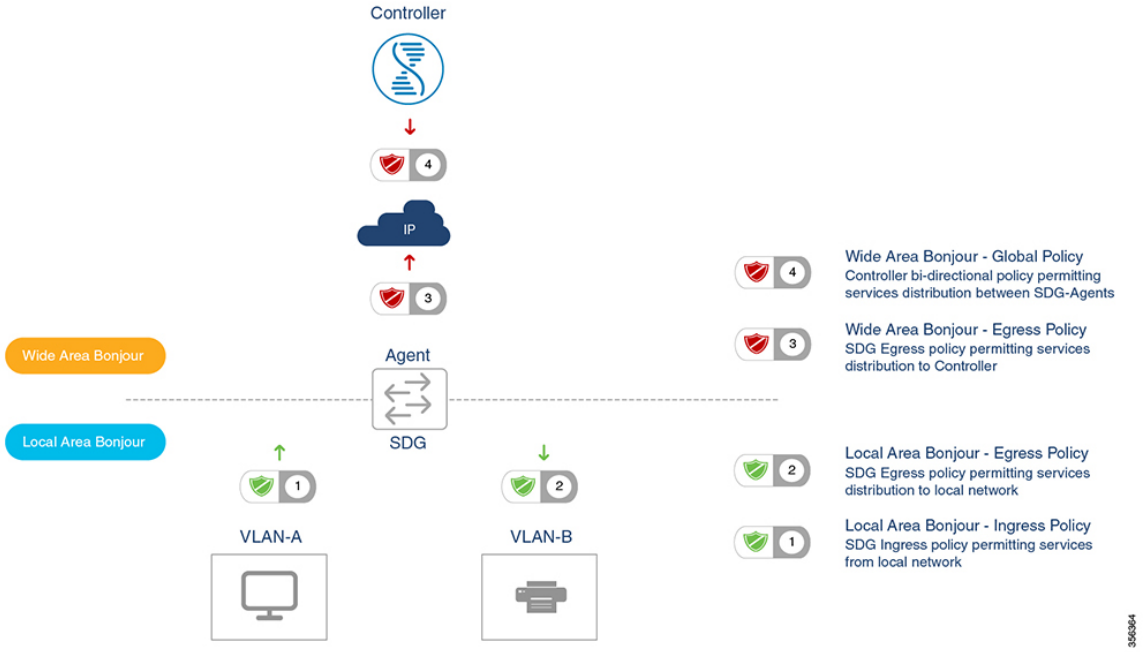
Wide Area Bonjour uses two logical components in a network:

- SDG Agent: The Fabric Edge switch is configured as the SDG Agent, and the configuration is added only after the SD-Access is configured.
- Wide Area Bonjour Controller: The Wide Area Bonjour application in the Cisco DNA Center acts as the Controller.

The Wide Area Bonjour communication between the SDG Agent and the Controller takes place through the network underlay. The SDG Agent forwards the endpoint announcements or queries to the Controller through the fabric underlay. After discovering a service, a Bonjour-enabled application establishes direct unicast communication with the discovered device through the fabric overlay. This communication is subject to any configured routing and SDG policies.

Local and Wide Area Bonjour Policies

The Cisco Wide Area Bonjour policy is divided into four unique function to enable policy based Bonjour services discovery and distribution in two-tier domains. The network administrator must identify the list of Bonjour services that needs to be enabled and set the discovery boundary that can be limited to local or global based on requirements. Figure below illustrates enforcement point and direction of all four types of Bonjour policies at the SDG Agent level and in Cisco DNA-Center Wide Area Bonjour application:

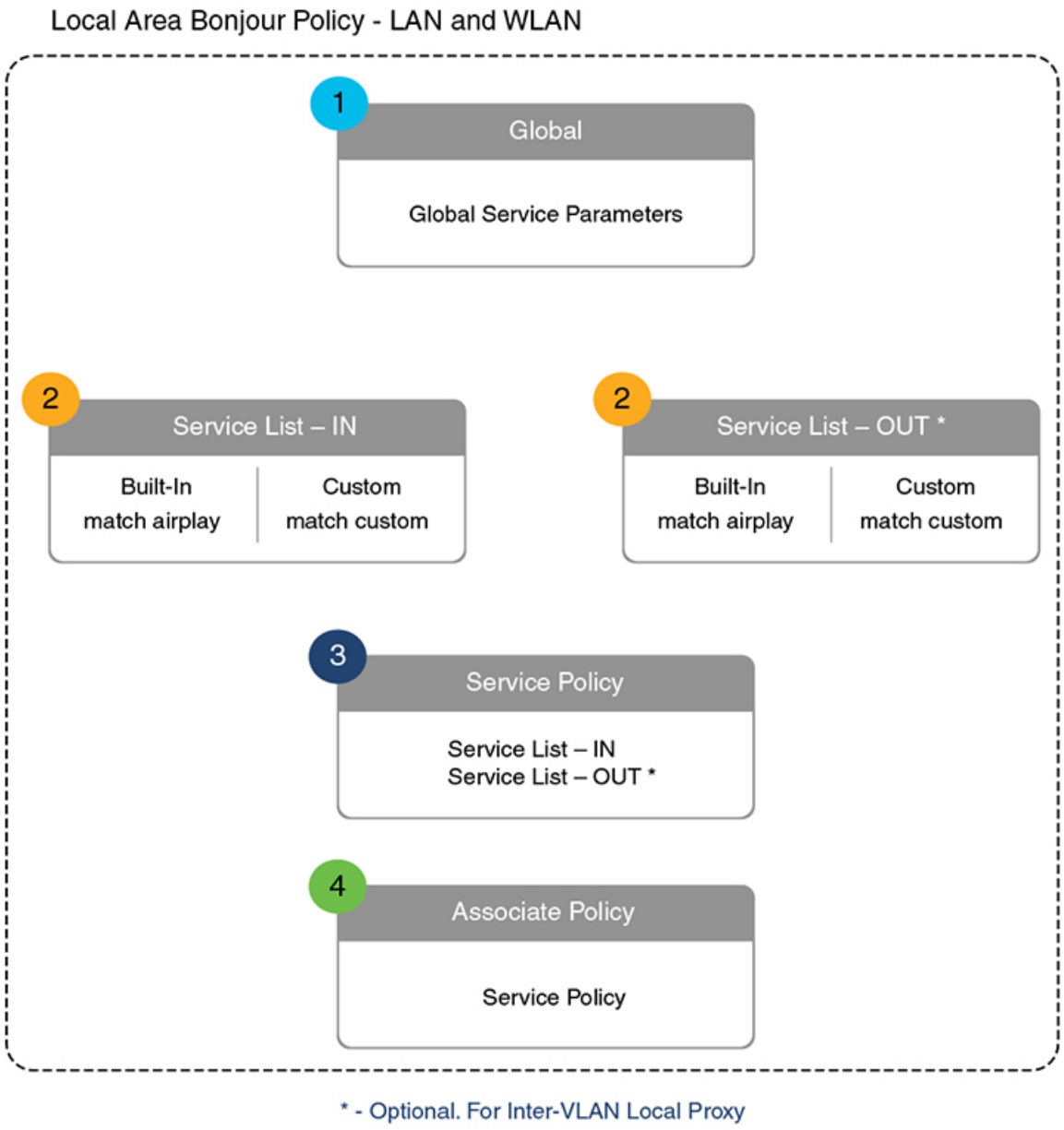


Local Area Bonjour Policy

The Cisco IOS Bonjour policy structure is greatly simplified and scalable with the new configuration mode. The services can be enabled with intuitive user-friendly service-type instead individual mDNS PoinTeR (PTR) records types, for example select AirPlay that automatically enables video and audio service support from Apple TV or equivalent capable devices. Several common types of services in Enterprise can be enabled with built-in service-types. If built-in service type is limited, network administrator can create custom service-type and enable the service distribution in the network.

The policy configuration for the Local Area Bonjour domain is mandatory, and is a three step process. Figure below illustrates the step-by-step procedure to build the Local-Area Bonjour policy, and apply to enable the gateway function on selected local networks:

Figure 1: Local Area Bonjour Policy Hierarchy



To configure local area bonjour policies, enable mDNS globally. For the device to receive mDNS packets on the interface, configure mDNS gateway on the interface. Create a service-list by using filter options within it allow services into or out of a device or interface. After enabling mDNS gateway globally and on the interface, you can apply filters (IN-bound filtering or OUT-bound filtering) on service discovery information by using **service-policy** commands.

Built-In Service List

The Cisco IOS software includes built-in list of services that may consist of one more Bonjour service-type. A single service-list may contain more than one service-type entries with default rule to accept service

announcement from service-provider and the service query request from receiver end-points. If selected service-type contains more than one Bonjour service-types (PTR), then a service announcement or a service query is honoured when the announcement/query is for any one of these included Bonjour service-types. For example, Apple Time Capsule Data service-type consists of both _adisk and _afpovertcp built-in PTRs, however if any end-point announces or requests for only _afpovertcp service, then SDG Agent will successfully classify and process the announcement or request. The service-list contains implicit-deny for all un-defined built-in or custom services entries.

Table below illustrates complete list of built-in Bonjour services that can be used to create policies in local area Bonjour.

Table 1: Cisco IOS Built-In Bonjour Service Database

Service	Service Name	mDNS PTRs
Apple TV	airplay	_airplay._tcp.local
AirServer Mirroring Service	airserver	_airserver._tcp.local _airplay._tcp.local
Apple AirTunes	airtunes	_raop._tcp.local
Amazon Fire TV	amazon-fire-tv	_amzn-wplay._tcp.local
Apple AirPrint	apple-airprint	_ipp._tcp.local _universal._sub._ipp._tcp.local
Apple TV 2	apple-continuity	_companion-link._tcp.local
Apple File Share	apple-file-share	_afpovertcp._tcp.local
Apple HomeKit	apple-homekit	_hap._tcp.local _homekit._ipp.local
Apple iTunes Library	apple-itunes-library	_atc._tcp.local
Apple iTunes Music	apple-itunes-music	_daap._tcp.local
Apple iTunes Photo	apple-itunes-photo	_dpap._tcp.local
Apple KeyNote Remote Control	apple-keynote	_keynotepair._tcp.local _keynotecontrol._tcp.local
Apple Remote Desktop	apple-rdp	_net-assistant._tcp.local _afpovertcp._tcp.local
Apple Remote Event	apple-remote-events	_eppc._tcp.local
Apple Remote Login	apple-remote-login	_sftp-ssh._tcp.local _ssh._tcp.local
Apple Screen Share	apple-screen-share	_rfb._tcp.local

Service	Service Name	mDNS PTRs
Apple Time Capsule Data	apple-timecapsule	_adisk._tcp.local _afpovertcp._tcp.local
Apple Time Capsule Management	apple-timecapsule-mgmt	_airport._tcp.local
Apple MS Window File Share	apple-windows-fileshare	_smb._tcp.local
Fax	fax	_fax-ipp._tcp.local
Google ChromeCast	google-chromecast	_googlecast._tcp.local
Apple HomeSharing	homesharing	_home-sharing._tcp.local
Apple iTunes Data Sync	itune-wireless-devicesharing2	_apple-mobdev2._tcp.local
Multifunction Printer	multifunction-printer	_ipp._tcp.local _scanner._tcp.local _fax-ipp._tcp.local
Phillips Hue Lights	phillips-hue-lights	_hap._tcp.local
Printer – Internet Printing Protocol	printer-ipp	_ipp._tcp.local
Printer – IPP over SSL	printer-ipps	_ipps._tcp.local
Linux Printer – Line Printer Daemon	printer-lpd	_printer._tcp.local
Printer Socket	printer-socket	_pdl-datastream._tcp.local
Roku Media Player	roku	_rsp._tcp.local
Scanner	scanner	_scanner._tcp.local
Spotify Music Service	spotify	_spotify-connect._tcp.local
Web-Server	web-server	_http._tcp.local
WorkStation	workstation	_workstation._tcp.local

Custom Service List

The Custom service list allows network administrator to configure service if built-in Bonjour database does not support specific service or bundled service types. For example, the file-sharing requirement demands to support Apple Filing Protocol (AFP) between macOS users and Server Message Block (SMB) file transfer capability between macOS and Microsoft Windows devices. For such requirements the network administrator can create an custom service list combining AFP (_afpovertcp._tcp.local) and SMB (_smb._tcp.local).

The Service-List provides flexibility to network administrator to combine built-in and custom service definition under single list. There is no restriction on numbers of custom service definitions list and association to single service-list.

Policy Direction

The Local Area Bonjour policy in Cisco IOS provides flexibility to network administrator to construct service policies that can align service announcement and query management in same or different local networks. The service-policies can be tied to either ingress or egress direction to enforce service control in both directions. The following sub-sections provide more details on service policy configuration.

Ingress Service Policy

The ingress service policy is a mandatory configuration element that is used to permit the processing of incoming mDNS service announcement and query requests. Without ingress service policy, the Bonjour gateway function on a targeted Wired or Wireless network is not enabled. The ingress service policy provides flexibility to permit service announcement and query on each user-defined service-types, i.e. permit accepting AirPlay service announcement and query request, but enable Printer service query request only.

Egress Service Policy

The egress service policy is an optional configuration and not required in following two conditions:

- The egress service policy is not applicable in local VLAN where the expected Bonjour end-points are service-provider only, i.e. Service-VLAN network may contain only IT managed service-provider end-points such as Apple TV, Printers etc. as these end-points do not query for other service-types in the network.
- The Wired or Wireless users must receive services only from Wide Area Bonjour domain by Cisco DNA-Center, and not from other Bonjour end points connected to the same SDG Agent.. The egress service policy configuration is only required when an SDG-Agent must distribute locally discovered Bonjour services information from one VLAN to other. For example, based on ingress service policy the SDG-Agent discovered and cache the AirPrint capable Printer from VLAN-A, if the receiver endpoint in VLAN-B wants to discover Printer information from VLAN-A then the SDG-Agent must have ingress and egress service policy permitting AirPrint service on both VLANs.

Conditional Egress Service Policy

The network administrator can optionally customize the egress service policy to enable conditional service response from sourced from specific VLAN network. For example, based on ingress service policy the SDG-Agent may discover AirPrint capable Printers from VLAN-A and VLAN-C networks. With conditional Local Area Bonjour egress service policy rule, the network administrator may limit distributing Printer information discovered from VLAN-A to the receivers in VLAN-B network and automatically filters VLAN-C Printers. The conditional egress service policy support is optional setting and only applicable on out direction service policy.

Service Status Timer Management

The Bonjour service-provider end-points may announces one or more services in the network combining mDNS records and time-to-live (TTL) service timers for each record. The TTL value provides assurance of end-point availability and serviceability in the network. The SDG Agents ensures that it contains up to date information in its local and updates global services in Controller based on TTL and other events in Local Area Bonjour domain. The network administrator must configure the service status timer where service-provider endpoint discovery is permitted.

Wide Area Bonjour Policy

The SDG-Agent mandatorily requires the controller bound Wide Area Bonjour service export policy to control routing local services and discover remote services from Cisco DNA-Center. As the Cisco DNACenter and SDG-Agent builds trusted communication channel the remote service response from Wide Area Bonjour App

is implicitly permitted at SDG-Agent. Hence the Wide Area Bonjour policy is unidirectional it only requires egress service policy towards controller.

The Wide Area Bonjour policy hierarchy and structure is identical as described in Local Area Bonjour Policy structure section. Following sub-section provides step-by-step reference configuration to build and enforce the policy to enable the successful communication with Wide Area Bonjour App in Cisco DNA-Center.

Service List – Built-In and Custom

The network administrator must create new controller bound egress service list for the Wide Area Bonjour domain. In most common network deployment model, the Wide Area Bonjour service list may contain same service-types as the Local Area Bonjour to implement common services between both domains. Based on requirements, certain services can be limited to Local Area and prevent routed in Wide Area Domain, then by default only allowed service list entries are permitted and rest are dropped with implicit deny rule.

Ingress Policy Direction

The ingress service policy for Wide Area Bonjour domain is not required and cannot be associated to the controller.

Egress Policy Direction

As described the Bonjour policy structure between Local Area and Wide Area is consistent, however the enforcement point is different. We recommend configuring separate Service-List and Service-Policy for Wide Area Bonjour domain as it may help building unique policy set for each domain.

Conditional Egress Service List

The Wide Area Bonjour egress service list configuration can be customized to conditionally route the service or query request to the Cisco DNA-Center. With this alternative configuration settings, the network administrator can route the service or query the request in Wide Area Bonjour domain from specific local source VLAN network instead globally from entire system.

Wide Area Bonjour Service Status Timer Management

The Cisco DNA-Center centralizes the services information from large scale distributed SDG-Agents across the network. To maintain a scale and performance of controller the services routing information is transmitted and synchronized periodically by each SDG-Agent network devices. To protect system and network performance the scheduler base service information exchange allows graceful and reliable way to discover and distribute Bonjour services across Wide Area Bonjour domain.

In most large-scale network environment, the default Bonjour service timers on SDG-Agents are by default fine-tuned and may not need any further adjustments. Cisco recommends retaining the interval timer values to default and adjust only based on any user experience issue and consider modified parameters do not introduce scale and performance impact.