Wide Area mDNS

The Wide Area mDNS feature helps local networks to learn all services terminated on a Service Discovery Gateway (SDG) through mDNS. These services are discoverable over a Wide Area Network across the enterprise network.

- Information About Wide Area mDNS, on page 1
- How to Configure Wide Area mDNS, on page 5
- Verifying Wide Area mDNS, on page 6
- Additional References for Wide Area mDNS, on page 11
- Feature Information for Configuring DNS, on page 12

Information About Wide Area mDNS

Wide Area mDNS Solution Overview

The Wide Area Multicast DNS (mDNS) feature is based on a distributed and hierarchical Apple Bonjour service-learning and distribution architecture. This architecture consists of the following components:

- Cisco APIC-EM controller
- Wide Area Apple Bonjour application that is installed and enabled on the controller
- Service Discovery Gateway (SDG) agent

The SDG agent supports a two-tier SDG functionality: local Area and wide area SDG. To discover Apple Bonjour services beyond a single Layer-3 boundary, the SDG agent consults the Wide Area Apple Bonjour application that is installed and enabled on the Cisco APIC-EM controller, and receives policy-based remote Apple Bonjour service entries to be distributed in the local network. The boundary remains limited to the SDG agent and is not extended over the IP network. The network communication between Wide Area Apple Bonjour application and agent is based on TCP/IP and does not extend to any mDNS Layer 2 boundary over the enterprise core or WAN network. This two-tier SDG design ensures both network bandwidth and reliability.

The Wide Area Apple Bonjour application provides an end-to-end Enterprise-class Apple Bonjour solution in the network. The Wide Area mDNS is a software-defined, policy-based Apple Bonjour protocol controller that facilitates both multicast and unicast DNS-based service discovery. Wide Area mDNS is designed for the Cisco APIC-EM platform and enables service discovery across the enterprise network and also reduces the load on devices within that network. Information about services learned from the access layer are unicast to the Cisco APIC-EM and stored within its database. The stored service data is also sent to other clients on
different subnets across the network, depending on user-configured filters. The Wide Area Apple Bonjour application enables policy-based Apple Bonjour discovery and distribution across the user-defined network and SDG Agent function.

**Wide Area mDNS**

The following figure displays a topology of how the Cisco Wide Area application enables Bonjour service discovery and distribution in the IP network.

*Figure 1: Wide Area mDNS Topology*

The topology consists of the following components:

- **Bonjour Endpoints**: These are end user devices or end points which are capable of announcing Bonjour services into the network or discovering the services. Examples of services are printers, Apple TV, file transfer services such as SMB or AFP, Philips Hue light and so on.

- **SDG Agent**: SDG agents contain policies and perform service discovery, service caching, and service filtering functions. Cisco ISR 4000 series Integration Services Routers act as SDG agents and listen on both IPV4 and IPV6 multicast addresses, to learn services announced by end clients.

- **Wide Area Bonjour application**: The function of this application is paired with SDG agent to enable centralized Bonjour service caching and provide policy-based service distribution. The Wide Area Bonjour application is supported on Cisco APIC-EM.

The Wide Area topology consists of two layers-Local Area SDG and Wide Area SDG.

- **Local Area SDG**: Local area SDG acts as local Bonjour proxy function between VLANs. The Bonjour endpoints can be on LANs or WLANs.

- **Wide Area SDG**: The Wide Area Bonjour application running on APIC-EM acts as the Wide Area service discovery gateway. It provides proxy functionality among the local area SDGs.

**Announcing Services into the Network**

1. The end-point devices (source) in local area SDG send service announcements to SDG agent and specify the services they are capable of providing. For example: _airplay._tcp.local, raop._tcp.local and so on.
2. The SDG agent listens to these announcements and matches them against the policies (Local Area SDG Agent Policy).
   - If the announcement matches the policy, SDG agent caches it and advertise them to Wide Area Apple Bonjour application through Apple Bonjour Control Protocol based on the configured Wide Area SDG Agent Policy.
   - If the announcement does not match the policy, the announcement is dropped.

3. Based on the policies on the Wide Area Controller Policy Engine, the controller stores the matched service announcements in its centralized Apple Bonjour cache.

**Discovering Services Available in the Network**

1. The endpoint device (receiver) connected to the local area SDG agent sends a Bonjour query to discover the services available using mDNS protocol.

2. The SDG agent listens to these queries and matches them against the Local Area SDG agent filters that are configured. Either of the following scenarios occur:
   - If the query matches one of the filters:
     - Immediate response is sent to the services that match the cache of the SDG agent.
     - The query is replicated to Wide Area Bonjour application, if the Wide Area SDG agent filter allows it, over the IP network using Cisco Bonjour Control Protocol.
   - If the query does not match any of the filters, it will be dropped.

3. When a query is received from SDG agent, the Wide Area Bonjour application matches the configured policies in the applications. If the query is matched, it responds with the corresponding services from its cache to SDG agent using Cisco Bonjour Control Protocol.

4. When responses are received from the Wide Area Bonjour application, the SDG agent forwards them to the corresponding end points using mDNS.

**Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)**


The platform hosts multiple applications (SDN apps) that use open north-bound REST APIs that drive core network automation solutions. The platform also supports a number of south-bound protocols that enable it to communicate with the breadth of network devices that customers already have in place, and extend SDN benefits to both greenfield and brownfield environments.

The Cisco APIC-EM platform supports both wired and wireless enterprise networks across the Campus, Branch and WAN infrastructures. It offers the following benefits:

- Creates an intelligent, open, programmable network with open APIs.
Transforms business-intent policies into a dynamic network configuration
Provides a single point for network-wide automation and control

Every SDG agent establishes a TCP connection to APIC-EM on port 9991. All services learnt from end clients by the SDG agent are exported to APIC-EM. The services learnt from an SDG agent is used by the controller to create a centralized database for the services.

End clients from other SDG agents can fetch the services, which are multiple hops away from APIC-EM through other SDG agents. When an SDG agent is connected to other SDG agents, services learnt from one SDG agent can be forwarded as response to the queries sent by end clients attached to other SDG agents.

**mDNS Snooping SDG Sub-Agent**

Sub-Agent snooping module forwards mDNS query traffic within the port group and also sends a copy to the SDG agent.

The copy sent to SDG agent also contains additional details like Access Switch Id, Source VLAN ID and source port-group id.

When the SDG Sub-Agent receives mDNS query response messages from SDG Agent over UDP, the SDG Sub-Agent extracts VLAN, destination port-group ID, and mDNS packets and sends them to mDNS clients.

Answers or advertisements from mDNS clients on same port group also use similar copy and forward approach. The copy sent to SDG Agent is used to create local cache on SDG Agent.

**mDNS Snooping SDG Agent**

1. An SDG agent is connected to multiple access switches (SDG sub-agent) using trusted trunk ports.
2. SDG maintains the cache with the services learnt from the connected access switches.
3. The snooping module at SDG, receives the UDP packet from the connected access switch and extracts all the information like access switch-id, source port-group id, source vlan-id, and mDNS packet. This information is updated in the SDG cache.
4. If a query is recieved as part of a UDP packet, the SDG module looks up the SDG cache, based on the access switch-id, vlan-id, and service-type. Reply from the SDG agent is based on the global local-proxy configuration. Response is sent over UDP with the additional parameters - access-switch-id, destination port group (where this answer should be flooded), and destination VLAN-id.
5. By default, SDG agent does not cross forward any mDNS packets across sub-agents.
6. By default, SDG agent provides services learnt from different VLAN (excluding VLAN from which query is received) of same sub-agent.
How to Configure Wide Area mDNS

Configure Policy Filters

Use the following commands to configuring policy filters for services to be cached at SDG or be exported to controller:

```
enable
configure terminal
service-list mdns-sd [Filter name] permit 1
match service-type _airplay._tcp.local
!
service-list mdns-sd [Filter name] permit 2
match service-type _raop._tcp.local
!
service-list mdns-sd [Filter name] permit 3
match service-type _ipp._tcp.local
!
service-list mdns-sd [Filter name] permit 4
match service-type _afpovertcp._tcp.local
!
service-list mdns-sd [Filter name] permit 5
match service-type _nfs._tcp.local
!
service-list mdns-sd [Filter name] permit 6
match service-type _ssh._tcp.local
!
service-list mdns-sd [Filter name] permit 7
match service-type _dpap._tcp.local
!
service-list mdns-sd [Filter name] permit 8
match service-type _ichat._tcp.local
!
service-list mdns-sd [Filter name] permit 9
match service-type _presence._tcp.local
!
service-list mdns-sd [Filter name] permit 10
match service-type _http._tcp.local
```

Use the following commands to configure the policy filter of services for the active query:

```
enable
configure terminal
service-list mdns-sd [Filter name] query
!
match service-type _airplay._tcp.local
!
match service-type _raop._tcp.local
!
match service-type _ipp._tcp.local
!
match service-type _afpovertcp._tcp.local
!
match service-type _nfs._tcp.local
!
match service-type _ssh._tcp.local
!
match service-type _dpap._tcp.local
!
match service-type _ichat._tcp.local
```
Configure Ingress Query Suppression

As mDNS queries and responses are all multicast, every query from the network need not be responded to. SDG can respond to a single query per service-type per interface per a specified time period.

Use the following configuration to suppress ingress queries:

```
enable
configure terminal
service-routing mdns-sd
ingress-client query-suppression enable
ingress-client query-suppression gap <time>
ingress-client query-reply count <service count> gap <time>
```

Verifying Wide Area mDNS

Verifying the Controller Summary

Use the following command to verify the controller summary:

```
show mdns controller summary
Controller Summary
-----------------------------------------------
Controller Name : apic-em
```
Controller IP : 10.104.52.241
State : UP
Port : 9991
Interface : Loopback0
Filter List : policy1
Dead Time : 00:01:00

Verifying Controller Export Summary

Use the following command to verify the controller export summary:

```
show mdns controller export-summary
```

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

Verifying Controller Statistics

Use the following command to verify the controller statistics:

```
show mdns controller statistics
```

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

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

Verifying Controller Details

Use the following command to verify controller details:

```
show mdns controller detail
```

Controller : apic-em
IP : 10.104.52.241, Dest Port : 9991, Src Port : 0, State : UP
Source Interface : Loopback0, MD5 Disabled
Hello Timer 0 sec, Dead Timer 0 sec, Next Hello 00:00:01
Uptime 00:00:00
Verifying Local Area SDG

Verifying Global mDNS Statistics
Use the following command to verify global mDNS statistics:

```
show mdns statistics cache all
```

```
MDNS cache statistics :
Number of service types : 15
Number of records of type PTR : 12300
Number of records of type SRV : 3745
Number of records of type A : 295
Number of records of type AAAA : 0
Number of records of type TXT : 12300

Top service types by instances :
Service type : (count of service instances)
_afpovertcp._tcp.local : 820
_airplay._tcp.local : 820
_daap._tcp.local : 820
_dpap._tcp.local : 820
_ftp._tcp.local : 820

Top advertisers of record :
MAC Address : (count of records)
0242.4601.0a43 : 46
0242.4601.0a4b : 46
0242.4601.0a35 : 46
0242.4601.0a3f : 46
0242.4601.0a0d : 46
```

Verifying mDNS Statistics
Use the following command to verify interface mDNS statistics:

```
show mdns statistics interface GigabitEthernet 0/0/0.101
```

```
G10/0/0.101:
MDNS packets sent : 61
IPv4 sent : 61
IPv4 advertisements sent : 0
IPv4 queries sent : 61
IPv6 sent : 0
IPv6 advertisements sent : 0
IPv6 queries sent : 0
Unicast sent : 0
MDNS packets rate limited : 100
MDNS packets received : 16377
```
**Verifying Local Area SDG**

advertisements received : 2227  
queries received : 14150  
IPv4 received : 16377  
IPv4 advertisements received : 2227  
IPv4 queries received : 14150  
IPv6 received : 0  
IPv6 advertisements received : 0  
IPv6 queries received : 0  
mDNS packets dropped : 14061  
mDNS gateway is : Active

---

**Interface mDNS Cache**

Use the following command to verify interface mDNS cache:

```
mDNS CACHE
<NAME> [TYPE] [TTL]/Remaining [IF-name]
<Mac Address> [RR Record Data]
```

```
_http._tcp.local PTR 4500/4482 Gi0/0/0.101
0242.4601.010b vlan101-macbook-http-cat4k-host-1._http._tcp.local
```

```
_vlan101-macbook-http-cat4k-host-1._http._tcp.local SRV 120/102 Gi0/0/0.101
0242.4601.010b 0 0 2001 ea3535b07fb3.local
```

```
ea3535b07fb3.local A 120/102 Gi0/0/0.101
0242.4601.010b 70.1.9.11
```

```
_vlan101-macbook-http-cat4k-host-1._http._tcp.local TXT 4500/4482 Gi0/0/0.101
0242.4601.010b (33)'vlan101-macbook-http-cat4k-host-1'
```

```
_http._tcp.local PTR 4500/4482 Gi0/0/0.101
0242.4601.010b vlan101-macbook-http-cat4k-host-1._http._tcp.local
```

---

**Verifying mDNS Cache Details Without Snooping**

Use the following command to verify interface mDNS cache detail (without snooping enabled on Sub-Agent):

```
show mdns cache interface gi0/0/0.101 detail
```

```
Name : _printer._tcp.local
Type : PTR
Class : IN
TTL/Remaining : 4500/4449
Accessed : 3
Interface : GigabitEthernet0/0/0.101
MAC Address : 0242.4601.010b
Record Data : vlan101-printer-printer-cat2k-host-1._printer._tcp.local
Access Type : Wireline
Preset Buffer : V4
Exported Records : V4
Access switch-id : NA
Vlan/Port-group : 0/0
Name : _ichat._tcp.local
Type : PTR
Class : IN
```
Verifying mDNS Snooping Summary on Sub-Agent

Verifying mDNS Snooping Summary
Use the following command to display mDNS Snooping Summary on Sub-Agent

```
show mdns snooping summary
```

Vlan-Id : 101
Port-Group : 0
  Gi4/0/1
Vlan-Id : 102
  Port-Group : 0
  Gi4/0/1
Total Number of PG's: 2
Trusted Trunks: Gi4/0/2

Verifying mDNS snooping details on Sub-Agent
Use the following command to verify mDNS snooping details on Sub-Agent:

```
show mdns snooping detail
```

SDG-Agent : 11.11.11.1
Source-Interface : Vlan111
UDP sock status : UP
Query Suppression : Disabled
Snooping vlan’s :
  101  102
## Verifying mDNS snooping statistics on Sub-Agent

Use the following command to verify mDNS snooping statistics on Sub-Agent:

```
show mdns snooping statistics
```

mDNS Packet statistics:

- **Packets received from client**:
  - Queries: 216
  - IPv4: 94
  - IPv6: 122
  - Advertisements: 149
    - IPv4: 61
    - IPv6: 88

- **Packets sent to client**:
  - Queries: 113
  - IPv4: 53
  - IPv6: 60

- **Packets sent to SDG**:
  - Queries: 216
  - IPv4: 94
  - IPv6: 122
  - Advertisements: 149
    - IPv4: 61
    - IPv6: 88

- **Packets received from SDG**:
  - Queries: 113
  - IPv4: 53
  - IPv6: 60

## Additional References for Wide Area mDNS

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Command List</td>
<td>Cisco IOS Master Command List</td>
</tr>
<tr>
<td>IP Addressing Services Command Reference</td>
<td>Cisco IOS IP Addressing Services Command Reference</td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1348</td>
<td>DNS NSAP Resource Records</td>
</tr>
</tbody>
</table>

### MIBs

- **MIB**
  - No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.

- **MIBs Link**
  - To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:
    - [http://www.cisco.com/go/mibs](http://www.cisco.com/go/mibs)
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for Configuring DNS

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

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Wide Area mDNS

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring DNS</td>
<td>Cisco IOS XE Fuji 16.9.x</td>
<td>The Wide Area mDNS feature helps local networks to learn all services terminated on a Service Discovery Gateway (SDG) through mDNS. These services are discoverable over a Wide Area Network across the enterprise network. The following commands were introduced: controller-address, controller-port, controller-source-interface, controller-service-policy, service-announcement-count, service-announcement-timer, service-export mdns-sd controller, service-query-count, service-query-timer, service-router mdns-sd</td>
</tr>
</tbody>
</table>