Using Services

mDNS

Information about Multicast Domain Name System

Multicast Domain Name System (mDNS) service discovery provides a way to announce and discover the services on the local network. The mDNS service discovery enables wireless clients to access Apple services such as Apple Printer and Apple TV advertised in a different Layer 3 network. mDNS performs DNS queries over IP multicast. mDNS supports zero-configuration IP networking. As a standard, mDNS uses multicast IP address 224.0.0.251 as the destination address and 5353 as the UDP destination port.

Location Specific Services

The processing of mDNS service advertisements and mDNS query packets support Location Specific Services (LSS). All the valid mDNS service advertisements that are received by the controller are tagged with the MAC address of the AP that is associated with the service advertisement from the service provider while inserting the new entry into the service provider database. The response formulation to the client query filters the wireless entries in the SP-DB using the MAC address of the AP associated with the querying client. The wireless service provider database entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service. If LSS is disabled for any service, the wireless service provider database entries are not filtered when they respond to any query from a wireless client for the service.

LSS applies only to wireless service provider database entries. There is no location awareness for wired service provider devices.

The status of LSS cannot be enabled for services with the ORIGIN set to wired and vice versa.

mDNS Policy

This section explains how you can define a policy to access a specific service provider. The access policy explains the client attributes, the constructs, and the rule components that make up the policy; and how rules and policies are evaluated. This helps in deciding whether the given service provider should be included in the mDNS response for the client (that made the mDNS query).

When LSS is enabled, it provides the information only about nearby service providers. But, MDNS Policy enables you to define a policy that is even more granular.

mDNS policies can be framed based on:

- User
- Role
- AP Name
- AP Location
- AP Group

mDNS Policy Limitations

The limitations of the mDNS policy are as follows:

- LSS cannot be applied in conjunction with the mDNS policy.
- Role and User info is provided from the ISE server.
- If the keyword **`Any`** is used as a rule parameter value, then that check is bypassed.
- Since the rule is applied based on Service Provider MAC, the rule is evaluated for all the services advertised by the service provider.
- mDNS Policy is applied based on Service Provider MAC and not based on the mDNS Service.
- mDNS Policy will be active only when mDNS Snooping is enabled.
- The maximum number of policies that can be configured per MAC address is limited to five policies.

Client Attributes in an mDNS Policy

Any client initiating an mDNS query is associated with a set of attributes that describe the context of the client. The list of attributes can be Role, User-Id, associated AP Name, associated AP Location, and associated AP Group. Only these enumerated attributes are used to articulate an access policy rule.

The attribute Location, for example, dynamically changes when the client move to a different location. You can formulate a rule by combining these attributes with logical OR operations and attach the rule to the policy.

A service group can have one or more rules.

mDNS AP

The mDNS AP feature allows the controller to have visibility of the wired service providers that are on VLAN. You must configure VLANs on all APs. VLAN visibility on the controller is achieved by the APs that forward the mDNS advertisements to the controller.

Use the configurable knob that is provided on the controller to start or stop mDNS packet forwarding, through the internal AP. You can also use this configuration to specify the VLANs from which the AP should snoop the mDNS advertisements from the wired side. The maximum number of VLANs that an AP can snoop is 10.

Note By default, the mDNS AP does not snoop on any VLAN, you must specify the Management VLAN to snoop on the mDNS packets.

The mDNS AP configuration is retained on those mDNS APs even if global mDNs snooping is disabled.

Priority MAC Support

You can configure up to 50 MAC addresses per service; these MAC addresses are the service provider MAC addresses that require priority. This guarantees that any service advertisements originating from these MAC addresses for the configured services are learned even if the service provider database is full by deleting the last nonpriority service provider from the service that has the highest number of service providers. When you configure the priority MAC address for a service, there is an optional parameter called **ap-group**, which is applicable only to wired service providers to associate a sense of location to the wired service provider devices. When a client mDNS query originates from this **ap-group**, the wired entries with priority MAC and **ap-group** are looked up and the wired entries are listed first in the aggregated response.

Origin-Based Service Discovery

You can configure a service to filter inbound traffic that is based on its origin, that is either wired or wireless. All the services that are learned from an mDNS AP are treated as wired. When the learn origin is wired, the LSS cannot be enabled for the service because LSS applies only to wireless services.

A service that has its origin set to wireless cannot be changed to wired if the LSS status is enabled for the service because LSS is applicable only to wireless service provider database. If you change the origin between wired and wireless, the service provider database entries with the prior origin type are cleared.

Restrictions for Configuring Multicast DNS

- mDNS over IPv6 is not supported.
- mDNS is not supported on remote LANs.
- Third-party mDNS servers or applications are not supported on the controller using the mDNS feature. Devices that are advertised by the third-party servers or applications are not populated on the mDNS service or device table correctly on the controller.
- In a Layer2 network, if Apple servers and clients are in the same subnet, mDNS snooping is not required on the controller. However, this relies on the switching network to work. If you use switches that do not work as expected with mDNS snooping, you must enable mDNS on the controller.
- Video is not supported on Apple iOS 6 with WMM in enabled state.
- mDNS APs cannot duplicate the same traffic for the same service or VLAN.
- LSS filtering is restricted to only wireless services.
- The LSS, mDNS AP, Priority MAC address, and origin-based discovery features cannot be configured using the controller GUI.
- mDNS-AP feature is not supported in CAPWAP V6.
- mDNS user profile mobility is not supported in guest anchors.

- Apple devices such as iPads and iPhones can discover Apple TV through Bluetooth. This might result in Apple TVs being visible to end users.

Configuring Multicast DNS

Step 1 Configure the global mDNS parameters and the Master Services Database by following these steps:

a) Click the **Switch to Expert View** icon. A message is displayed, confirming if you want to switch to the expert view. Click Yes.

b) Choose **Services** > **mDNS**.

c) Use the **mDNS Global Snooping** toggle button to enable or disable snooping of mDNS packets, respectively.

d) Enter the mDNS query interval in minutes. The query interval is the frequency at which the controller queries for a service. Default is 15 minutes.

e) Click the Add VLAN Id button to add a list of VLANs for internal AP snooping.

Note
- VLANs added from the ME GUI will be configured on all the APs (Internal and External). Individual AP VLANs can be configured only by running the **config mdns ap vlan add vlan-id ap-name** command.
- The 'mDNS VLAN Mapping' table on the GUI only lists the VLANs that are set on the internal AP. Since you can configure VLAN specifically on the external APs only by running the **config mdns ap vlan add vlan-id ap-name** command, you can view the VLANs added on all the APs (both internal and external) only by running the **show ap summary** command. GUI does not show the VLANs, if any, set on the external APs.

f) Complete the details in the following tabs:

1. **Master Services Database** – to view the services listed in the primary database. The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services Database. The controller can snoop and learn a maximum of 64 services.
   - Click the **Add Service** button to add a new service in the primary database.
   - In the **Add/Edit mDNS Service** window, specify the **Service Name**, **Service String**, **Query Status**, **Location Services**, and **Origin**.
   - Click **Update**.
2. **mDNS Profiles** – to view the list of mDNS profiles.
   - Click the **Add Profile** button to add a new profile.
   - In the **Add/Edit mDNS** window, enter the profile name that can be later mapped to the WLAN.
3. **Domain Names** – to view domain names and add domain names from the discovered list.
4. **mDNS Browser** – to view the number of mDNS services running.

g) Click **Apply**.

Step 2 Map an mDNS profile to a WLAN by following these steps:

a) Choose **Wireless Settings** > **WLANs**.

b) Click **Add new WLAN**. The Add new WLAN window is displayed.
c) In the Add new WLAN window, select the **Advanced** tab.
d) Use the **mDNS** toggle button to enable or disable mDNS.
e) From the **mDNS Profile** drop-down list, choose a profile.
f) Use the **Passive Client** toggle button to enable the passive client. Ensure that you enable Global Multicast in Services > Media Stream, as Passive Client will not work when Global Multicast is disabled.
g) Enter the **Multicast IP** address.
h) Use the **Multicast Direct** toggle to enable multicast direct.
i) Click **Apply**.

Note The wireless controller advertises the services from the wired devices (such as Apple TVs) learned over VLANs, when:

- mDNS snooping is enabled in the WLAN Advanced options.
- mDNS profile is enabled either at the interface or WLAN.

Configuring mDNS Policy

Configure the mDNS policy by following these steps:

a) Click the **Switch to Expert View** icon. A message is displayed, confirming if you want to switch to the expert view. Click Yes.
b) Choose **Services** > **mDNS**.
c) Use the **mDNS Global Snooping** toggle button to enable or disable snooping of mDNS packets, respectively.
d) Use the **mDNS Policy** toggle button to enable or disable mDNS policy, respectively.
e) Enter the mDNS query interval in minutes. The query interval is the frequency at which the controller queries for a service. Default is 15 minutes.
f) Click the **mDNS Policy** tab.
The number of mDNS policies are displayed.
g) Click the **Add mDNS Policy** button.

In the Add mDNS Policy window, you must first add the mDNS Service Group.

1. Enter the **mDNS Service Group Name** and the **Description**.
2. Click the **Add Service Instance** button. The Add Service Instance window is displayed. Complete the following details to add a service instance:
    - **Mac Address**
    - **Name**
    - **Location Type** - Choose the Location Type by AP Group, AP Name, or AP Location.
    - **Location** - Based on the Location Type selected.
3. Click **Apply**.

The service instance created is displayed in the mDNS Policy window.

h) Enter the **Policy/Rule** and click **Apply**.

Cisco Umbrella

Overview of Cisco Umbrella on Cisco Mobility Express

The Cisco Umbrella platform is a cloud-delivered network security solution. At the Domain Name System (DNS) level, it provides real-time insights that help protect devices from malware and breach. As of Cisco Mobility Express Release 8.8, Cisco Umbrella mapping is supported only at the WLAN level.

Cisco Umbrella works in the following manner in Cisco Mobiliry Express:

- Wireless clients join a wireless controller and send DNS queries when they initiate traffic to the Internet. Cisco Umbrella transparently intercepts the DNS traffic and redirects the DNS queries to the Cisco Umbrella cloud servers.
- Security policies based on fully qualified domain names (FQDN) in a DNS query are defined in the Cisco Umbrella cloud servers.
- Based on the FQDN in a DNS query, Cisco Umbrella returns one of the following responses:
    - Malicious FQDN: Returns Cisco Umbrella-blocked page IP to the corresponding client.
    - Safe FQDN: Returns Destination IP address.

Cisco Umbrella Support in Cisco Mobility Express

- Up to 10 different Cisco Umbrella profiles are supported, each with a unique device ID.
- In the context of mapping Cisco Umbrella profiles or device IDs to wireless entities, only WLAN level mapping is supported.
- In the context of provisioning device IDs to APs, AP snoops the DNS packets and applies EDNS tags.
- Forced or Ignore Open modes are supported.
- The new DHCP-6 override option is supported at the WLAN level.

Limitations

This feature does not work with the following:

- This feature does not work with the following:
    - Cisco IOS APs
    - Local-auth
    - IPv6 addresses
-
- If an application or host uses an IP address directly, instead of using DNS to query domain names.

- If a client is connected to a web proxy and does not send a DNS query to resolve the server address.
- Wired guests and clients behind Workgroup Bridges (WGB).
- Virtual Wireless LAN Controller (WLC).
- The application of wireless Cisco Umbrella profiles on wireless entities, like WLAN, through configuration, is dependent on the success of the registration of the device.
- The Cisco Umbrella Cloud provides two IPv4 addresses. WLC/AP uses the first server address that is configured. It does not load balance across servers.

Configuring Cisco Umbrella on Cisco Mobility Express (GUI)

Configure Cisco Umbrella on Cisco Mobility Express by doing these steps:

Before you begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

Step 1 Click the **Switch to Expert View** icon.

A message is displayed, confirming if you want to switch to the expert view. Click **Ok**.

Step 2 Choose **Services** > **Umbrella**.

Step 3 Use the **Umbrella Global Status** toggle button to enable or disable the Umbrella status, respectively.

Step 4 Enter the **Umbrella API Token** that you obtained from Cisco Umbrella.

Step 5 Click **Apply** to enable Cisco Umbrella.

Step 6 Click **Add Profile** to create a new profile.

The Add Profile Name window is displayed.

Step 7 Enter the **Profile Name** and click **Apply**.

A new profile is created.

Step 8 Map a Cisco Umbrella profile to WLAN by following these steps:

a) Choose **Wireless Settings** > **WLANs**.
b) Click **Add new WLAN/RLAN.** The Add new WLAN/RLAN window is displayed.
c) In the Add new WLAN window, select the **Advanced** tab.
d) From the **Umbrella Profile** drop-down list, choose a profile.
e) From the **Umbrella Mode** drop-down list, choose either **Ignore** or **Forced**.
f) Use the **Umbrella DHCP Override** toggle button to enable the Cisco Umbrella DHCP override.
g) Click **Apply**.

What to do next

1. From Cisco Umbrella Dashboard, verify that your Cisco WLC shows up under **Device Name**, along with their identities
2. Create classification rules for the user roles, for example, rules for employees and nonemployees.
3. Configure policies on the Cisco Umbrella server.

Configuring Cisco Umbrella on Cisco Mobility Express (CLI)

This section describes the procedure to configure Cisco Umbrella on Cisco Mobility Express:

Before you begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

Step 1 To enable or disable Cisco Umbrella, use the **config opendns** {**enable** | **disable**}

Example:

```
(Cisco Controller) > config opendns enable
```

Enables or disables the Cisco Umbrella global configuration.

Step 2 **config opendns api-token** *api-token*

Example:

```
(Cisco Controller) > config opendns api-token D0986C18DC334FB2E3AA46148D600A4001E5997
```

Registers the Cisco Umbrella API token on the network.

Step 3 **config opendns profile** {**create** |**delete** | **refresh**}*profilename*

Example:

```
(Cisco Controller) > config opendns profile create profile1
```

Creates, deletes, or refreshes a Cisco Umbrella profile that can be applied over a WLAN.

Step 4 **config wlan opendns-profile** *wlan-id profile-name* {**enable** | **disable**}

Example:

```
(Cisco Controller) > config wlan opendns-profile 1 profile-name enable
```

Maps the Cisco Umbrella profile identity to a WLAN.

Step 5 **config wlan opendns-dhcp-opt6** *wlan-id* {**enable** | **disable**}

Example:

```
(Cisco Controller) >config wlan opendns-dhcp-opt6 1 enable
```

Enables or disables DHCP option 6 per WLAN.

Step 6 **config wlan opendns-mode** *wlan-id* {**ignore** | **forced**}

Example:

```
(Cisco Controller) >config wlan opendns-mode 1 forced
```

Ignores or Forces the Cisco Umbrella mode on the WLAN.

TLS

TLS Secure Tunnel

Transport Layer Security (TLS) provides secure and reliable signaling and data transfer between two systems or devices, by using secure ports and certificate exchange. To overcome the challenge of multi-site deployment Cisco Mobility Express uses TLS Secure Tunnel to establish a secure connection from Cisco Mobility Express to the central data center. Inbound traffic includes SSH, SNMP, Ping, HTTP, HTTPS, and TFTP; and outbound traffic includes SNMP, RADIUS, and TFTP

TLS Tunnel has two components:

- TLS Client: TLS Client has been embedded in the Cisco Mobility Express code and will run on the primary AP.
- TLS Gateway: This is a Virtual Machine which is deployed at the central site to establish the TLS Tunnel. TLS Gateway has two network interfaces – Public Network and Private Network.

Following are the features of the TLS Client:

- Zero Touch Provisioning support with PnP
- FQDN support for TLS Gateway
- PSK-based authentication
- Dead Peer Detection (DPD)
- Implicit and Explicit configuration for traffic tunneling
- NAT and Firewall traversal support
- Support System information for device parameters - serial number, MAC address, and system name

Following are the features of TLS-Gateway:

- VMware based Virtual Security Solution
- Dynamic IP allocation to TLS client - Static Pool based IP allocation with TLS-GW internal DHCP server.
- Dead Peer Detection (DPD) and Periodic Re-keying - Configuring DPD and Rekey intervals, DPD – in sync with NAT timeout.
- PSK Authentication - Pre-Shared Key (PSK) based authentication, multiple PSK configurations, and encrypted storage of PSK on the Gateway.
- Internal DNS Server - Configurable DNS server for the TLS client for DNS resolution.

- Connection Rate Limiting - Connection Rate limit of 50 connections per second.
- Scale Characteristic - Scale limit of 10000 tunnels per instance.
- IP Event Notification - Notify events when the TLS client tunnel is connected, disconnected, and reconnected (rekey); to Notify Server [syslog server] Netconf/Restconf.
- Serviceability - Configuration CLIs, Debug Stats (Gateway level and Device Level), and Logging supported.
- SSH login control - Support for enabling and disabling SSH login to TLS Gateway VM (only on private interface).

The Cisco Mobility Express Secure Tunnel supports:

- Outbound - SNMP Traps, RADIUS (Authentication/Accounting)
- Inbound - SNMP, SSH, Ping, HTTPS, and HTTP
- TLS Gateway FQDN
- PSK based authentication
- Inbound traffic - TFTP, SFTP, and FTP
- Rekey Mechanism
- Implicit and Explicit ways of configuration for tunneling the traffic. Implicit Tunneling enables the application for tunneling. For example, SNMP Traps or RADIUS. Explicit Tunneling adds the host or network for tunneling. For example, SSH and PI/SNMP, and Cisco DNA Center.

Following is the sequence of steps given below when configuring the TLS Secure Tunnel for Cisco Mobility Express:

1. Deploying the TLS Gateway - Follow the steps listed here to deploy the TLS Gateway at the central site.
2. CLI Configuration - For more information, refer to the Mobility Express Controller Commands section.
3. Configuring TLS (GUI) - For more information, refer to Configuring TLS Tunnel.

Configuring TLS Tunnel

Follow the procedure given below to configure TLS Tunnel:

Step 1 Click the **Switch to Expert View** icon.
A message is displayed, confirming if you want to switch to the expert view. Click **Yes**.

Step 2 Choose **Services** > **TLS**.
The TLS Tunnel Settings page is displayed.

Step 3 Use the **TLS Tunnel** toggle button to enable or disable TLS Tunnel.

Step 4 On the TLS Tunnel Settings page, configure the following parameters:

- Enter the **TLS Gateway URL/IP Address**
- Enter the PSK ID

- Enter the PSK Key
- Enable RADIUS and SNMP

Step 5 Click Apply.