Services

Cisco Business Wireless Access Points provides the following services:

- **Media Stream** – The Media Stream (formerly VideoStream) feature makes the IP multicast stream delivery reliable over the air, by converting the multicast frame to a unicast frame over the air. Each Media Stream client acknowledges receiving a video IP multicast stream.
- **mDNS** – Multicast Domain Name System (mDNS) service discovery provides a way to announce and discover the Apple services to the Wireless clients connected to the CBW AP.
- **Cisco Umbrella** – The Cisco Umbrella is a cloud-delivered network security solution. It provides real-time insights that help protect devices from malware and breach.

This chapter contains the following sections:

Media Steam

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. As a result, if any multicast packet is lost in the air, it is not sent again which may lead to poor quality of IP multicast stream.

The Media Stream (formerly VideoStream) feature makes the IP multicast stream delivery to the wireless clients more reliable over the air and facilitates better usage of wireless bandwidth, by converting the multicast frame to a unicast frame over the air. Each Media Stream client acknowledges receiving a video IP multicast stream.

Configure Media Stream Parameters

Configure the global multicast parameters by the following steps:

1. Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of the Primary AP.

   A message is displayed to confirm if you want to switch to the expert view.

2. Click **Ok**.
3. Navigate to **Services** > **Media Stream**.

4. Enable **Global Multicast** to support multicast traffic on Primary AP. The default value is **Disabled**.

Important Global multicast cannot be enabled without configuring IPv4 multicast address in WLAN page.

5. Enable **Multicast Direct** to enhance the video streaming for wireless clients. The default value is **Disabled**.

Note The wireless clients must re-join the multicast stream after enabling the multicast direct feature on the Primary AP.

6. Select **Session Announcement State** toggle button to enable the session announcement mechanism. If the session announcement state is enabled, clients are informed each time a Primary AP is not able to serve the multicast direct data to the client. The following parameters need to be filled only if Session Announcement State is enabled.
   a. **Session Announcement URL**— Enter the URL where the client can find more information when an error occurs during the multicast media stream transmission.
   b. **Session Announcement E-mail**— Enter the e-mail address of the person who can be contacted.
   c. **Session Announcement Phone**— Enter the phone number of the person who can be contacted.
   d. **Session Announcement Note**— Enter a reason as to why a particular client cannot be served with a multicast media.
7. Click **Apply**.

Configuring a New Media Stream

To add a new Media stream switch to **Expert View** and navigate to **Services** > **Media Stream**.

1. Click **Add New Stream** to configure a new media stream.
2. Enter the media stream name in the **Stream Name** text box. The stream name can be up to 64 characters.
3. Enter the starting IPv4 address of the multicast media stream in the **Multicast Start IP Address** text box.
4. Enter the ending IPv4 address of the multicast media stream in the **Multicast End IP Address** text box.
5. Enter the maximum expected bandwidth that you want to assign to the media stream into the **Maximum Expected Bandwidth (Kbps)** text box. The range is 1 to 35000 kbps.

Note We recommend that you use a template to add a media stream to the Primary AP.

6. From the **Select from Predefined Templates** drop-down list under **Resource Reservation Control (RRC) Parameters**, choose one of the following options to specify the details about the resource reservation control:
   - Very Coarse (below 300 kbps)

- Coarse (below 500 kbps)
- Ordinary (below 750 kbps)
- Low (below 1 Mbps)
- Medium (below 3 Mbps)
- High (below 5 Mbps)

Note When you select a predefined template from the drop-down list, the following text boxes under the **Resource Reservation Control (RRC) Parameters** list their default values that are assigned with the template.

7. Specify the average packet size in the **Average Packet Size** field. The value can be in the range of 100 to 1500 bytes. The default value is 1200.
8. Enable the RRC (Resource Reservation Control Check) Periodic update in the **RRC Periodic update** field. By default, this option is enabled.

   RRC periodically updates the admission decision on the admitted stream according to the correct channel load. As a result, it may deny certain low priority admitted stream requests.
9. Specify the priority bit set in the media stream in the **RRC Priority** field. The priority can be any number between 1 and 8.

   The larger the value means the priority is higher. For example, a priority of 1 is the lowest value and a value of 8 is the highest value. The default priority is 4. The low priority stream may be denied in the RRC periodic update.
10. Specify the action to perform in case of a violation after a re-RRC in the **Traffic Profile Violation** field. Choose an action from the drop-down list. The possible values are as follows:
    - **Best Effort**— Specifies that a stream is set to Best Effort class on periodic revaluation. This is the default value.
    - **Drop**— Specifies that a stream is dropped on periodic revaluation.
11. Click **Apply**.

    The newly created Media stream is displayed in the table along with details of **Stream Name**, **Start/End IP Address**, and **Operation Status**.

Viewing Media Stream Clients

Media stream clients will be displayed under this section with the following details:

- **Client MAC**—Displays the MAC address of the client.
- **Stream Name**—Shows the Media stream name. If the **Multicast Direct** toggle disabled, the Stream Name will be null for clients that are connected to the WLAN.
- **Multicast IP**—Displays the Multicast Group Address configured in the WLAN page.
- **AP Name**—Displays the AP Name connected to the client.

- **VLAN**—Displays the Client VLAN.
- **Type**—Displays **Multicast Only** or **Multicast Direct** based on which toggle was configured in the WLAN.

About Multicast Domain Name System

Multicast Domain Name System (mDNS)

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.

Bonjour Advertisements for CBW device discovery

The Cisco Business Wireless Access Point sends Bonjour Advertisements to the local network to support CBW device discovery in the Cisco Business Dashboard probe. Using these advertisements, CBD probe obtains details of individual AP and the Primary AP.

Note During the initial setup phase, if there is more than one Primary Capable AP in the network, only one AP will get DHCP IP, and sends VRRP and Bonjour Advertisements. The rest of the APs will wait for the AP to be configured and then join the Primary AP.

Location Specific Services

The processing of mDNS service advertisements and mDNS query packets support Location Specific Services (LSS). All the valid mDNS service advertisements received by the Primary AP 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, such as Apple TV database.

The response to the client query filters the wireless entries in the SP-DB using the MAC address of the AP associated with the querying client. 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 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.

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. 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.
- If the keyword **Any** is used as a role parameter value, then that check is bypassed.
- mDNS Policy will be active only when mDNS Snooping is enabled.
- The maximum number of policies that can be configured per MAC address is five.

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 based on Role, User-id, associated AP Name, associated AP Location, and associated AP Group.

mDNS AP

The mDNS AP feature allows the Primary AP to have visibility of the wired service providers. This is in-built in the Primary AP.

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 non-priority 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 wired or wireless origin. All the services that are learned from an mDNS AP are treated as wired. When the 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 devices. 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 is not supported on access points in **AP Only** mode within a locally switched WLAN and mesh access points.
- mDNS is not supported on remote LANs.
- Third-party mDNS servers or applications are not supported on the Primary AP 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 Primary AP.
- In a Layer2 network, if Apple servers and clients are in the same subnet, mDNS snooping is not required on the Primary AP. However, this relies on the function of switching network. If you use switches that do not work as expected with mDNS snooping, you must enable mDNS on the Primary AP.
- 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 mDNS AP, Priority MAC address, and origin-based discovery features cannot be configured using the Primary AP Web-UI.
- 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

Configure the global mDNS parameters and the Primary Services Database by following these steps:

Step 1 Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of the Primary AP. A message is displayed to confirm if you want to switch to the expert view. Click **Ok**.

Step 2 Navigate to **Services** > **mDNS**.

Step 3 Use the **mDNS Global Snooping** toggle button to enable or disable snooping of mDNS packets, respectively.

Step 4 Use **Bonjour Advertisements** toggle button to enable or disable sending of bonjour advertisement packets to the local network. By default it is **enabled** and advertisements will be sent every minute.

Note
- By enabling this option, CBD probe can discover CBW APs in the network.
- CBW AP sends bonjour packets only in Native VLAN.
- CBW AP sends **Goodbye bonjour** message to CBD probe.
  - If the **Bonjour Advertisements** toggle button is disabled.
  - If the name of the AP joined to Primary AP is changed, or the Primary AP name is changed, a **Goodbye bonjour** message is sent for the old name. A new name will be updated in Bonjour Advertisements at the next interval. A **Goodbye bonjour** message on AP name change will be sent only if the **Bonjour Advertisement** is enabled.

Step 5 Use the **mDNS Policy** toggle button to enable or disable mDNS policy mapping.

Step 6 Enter the mDNS query interval in minutes. The query interval is the frequency at which the Primary AP queries for a service. Default is 15 minutes.

Step 7 Click **Add VLAN Id** to add a list of VLANs for internal AP snooping.

Step 8 Complete the details in the following tabs:

a. **Primary Services Database** —To view the services listed in the Primary database. The Primary AP looks and learns about the mDNS service advertisements only if the service is available in the Primary Services Database. The Primary AP can check 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**.

b. **mDNS Profiles** —To view the list of mDNS profiles. By default, one mDNS profile will be available.

- Click the **Add Profile** button to add a new profile.
- In the **Add/Edit mDNS profile** window, enter the profile name that can be later mapped to the WLAN.

c. **mDNS policy**—To view the mDNS policies. By default, one mDNS policy will be available.

- Click **Add mDNS policy** to add a new policy.
- In the **Edit mDNS policy** window, enter the role name and user name.

d. **Domain Names** —To view domain names and add domain names from the discovered list.

e. **mDNS Browser** —To view the number of mDNS services running.

f. Click **Apply**.

Mapping mDNS Profile to WLAN

Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of Primary AP.

Step 1 Navigate to **Wireless Settings** > **WLANs**.

Step 2 Click **Add new WLAN** to create a new WLAN.

Step 3 In the **Add new WLAN** window, select **Advanced** to configure the mDNS.

Step 4 Use the **mDNS** toggle button to add the mDNS services to the WLAN.

Step 5 From the **mDNS Profile** drop-down list, choose a profile to map the required policy to the WLAN.

Step 6 Click **Apply** to save your changes.

Note The wireless Primary AP broadcasts 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

Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of the Primary AP. A message is displayed to confirm if you want to switch to the expert view. Click **Ok**.

To configure the mDNS policy, do the following:

Step 1 Navigate to **Services** > **mDNS**.

Step 2 Use the **mDNS Global Snooping** toggle button to enable or disable snooping of mDNS packets, respectively.

Step 3 Use the **mDNS Policy** toggle button to enable or disable mDNS policy, respectively.

Step 4 Enter the mDNS query interval in minutes. The query interval is the frequency at which the Primary AP queries for a service. Default is 15 minutes.

Step 5 Click **mDNS Policy**. The number of mDNS policies are displayed.

Step 6 In the **Add mDNS Policy** window, you must add the mDNS Service Group

.

a. Enter the **mDNS Service Group Name** and the **Description**.

b. Click the **Add Service Instance** button. The Add Service Instance window is displayed. Complete the following details to add a service instance:

- **Mac Address**—MAC address of the service provider such as Apple TV.
- **Name**—Add a name for the device.
- **Location Type**—Choose the Location Type by AP Group, AP Name, or AP Location.
- **Location**—Based on the Location Type selected.

c. Click **Apply**.

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

Step 7 Enter the **Policy/Rule** and click **Apply**.

Cisco Umbrella Overview

Cisco Umbrella is a cloud based security platform that provides the first line of defense against threats on the Internet wherever users go. It acts as a gateway between the Internet and your systems and data to block malware, botnets, and phishing over any port, protocol, or app.

At the Domain Name System (DNS) level, it provides real-time insights that help protect devices from malware and breach.

The following points summarizes the way in which Cisco Umbrella works in the Primary AP:

- Wireless clients join a wireless access point 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 for the Primary AP

- 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.

Limitations

This feature does not work with the following:

- Local-auth
- IPv6 addresses

Other limitations include:

- 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.
- 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. The AP uses the first server address that is configured. It does not load balance across servers.

Configuring Cisco Umbrella on Primary AP

To configure Cisco Umbrella on the Primary AP, ensure the following:

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

To generate the API token, do the following:

1. Login into your Cisco Umbrella Account
2. In the Umbrella dashboard, navigate to **Admin** > **API Keys** and click **Create**.
3. Select **Legacy Network Devices** and click **Create**.
4. Expand **Legacy Network Devices** and copy the API token **Your Key**. The API token is a lengthy string of alphanumeric characters.

To configure Cisco Umbrella on the Primary AP, do the following:

Step 1 Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of the Primary AP.

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

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

Step 3 Click the **Umbrella Global Status** toggle button to enable Umbrella status.

Step 4 Enter or paste the **Umbrella API Token** that you copied.

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

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

Step 7 In the **Add Profile** window, enter the **Profile Name** and click **Apply**.

A new profile is created.

Step 8 Verify that the State changes from *Registration in Progress* to *Profile Registered*. This may take a few seconds, and may require you to refresh your browser window.

Step 9 In the Umbrella dashboard, navigate to **Deployments** > **Core Identities** > **Network Devices**. You can check if your device is listed in this window.

Adding Policy to Umbrella Profile

Step 1 Browse to the Cisco Umbrella UI using your Cisco credentials. Add your device details to protect from breach and malware.

Step 2 Navigate to **Policies** > **All Policies** to create rules and map this to your network device.

Step 3 Click **Add** to create new rules.

Step 4 Select **Network Devices** from the list of **Identities** and click **Next**. This helps add your APs in a way so that the whole network is monitored by the umbrella.

Step 5 You can configure the required **Security Settings and Limit Content Access**. These are user configurable and you can select the type of attacks that you want to block such as phishing attack, malware, potentially harmful domains, web page contents such as games, gambling, drugs etc.

Step 6 In the **Application** tab, select the applications that need to be blocked. You can limit access to certain applications like YouTube, Facebook, Google-services, or others if you wish.

Step 7 Specify the **Destination**, **File Analysis**, and **Block Pages** in the network.

Destination List shows the global allowable list and global block list that you configured in the umbrella and **Block pages** define the appearance and bypass options for your block pages.

Note These all are user configurable.

Step 8 Navigate to **Deployments** > **Core Identities** > **Network Devices** and verify if the Policy has been applied to your network device.

Applying Cisco Umbrella Profile to WLAN

Step 1 Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of the Primary AP.

Step 2 Navigate to **Wireless Settings** > **WLANs**.

Step 3 Click **Add new WLAN** to open the **Add new WLAN**.

Step 4 Select **Advanced**.

Step 5 From the **Umbrella Profile** drop-down list, choose a profile that was created for the WLAN.

Step 6 From the drop-down list, choose **Ignore** or **Forced**.

When a client obtains DNS IPs, users can manually change them on the client device, thus bypassing Umbrella policy enforcement.

To prevent this security compromise, configure Umbrella Mode to Forced. This ensures that Umbrella policy enforcement cannot be overridden on the client device.

Step 7 Click the **Umbrella DHCP Override** toggle button to enable the Cisco Umbrella DHCP override.

The DNS IP addresses that a client obtains when connecting to the SSID are configured on the DHCP server. For Umbrella enforcement to work, clients must send out DNS requests to Umbrella IP addresses (208.67.222.222, 208.67.220.220).

Umbrella DHCP Override ignores the DNS IPs configured via DHCP, and forces the Umbrella DNS IPs on the client device. If you set Umbrella Mode to **Forced**, you do not need to enable **Umbrella DHCP Override**.

Step 8 Click **Apply** and then **Save** your configuration.