サービスの使用

mDNS

マルチキャスト ドメイン ネーム システムについて

マルチキャスト ドメイン ネーム システム（mDNS）サービス ディスカバリは、ローカル ネットワークでサービスを通知し、検出する手段を提供します。mDNS サービス ディスカバリを使用すれば、ワイヤレス クライアントは、別のレイヤ 3 ネットワーク上でアドバタイズされた Apple プリンタや Apple TV などの Apple サービスにアクセスすることができます。mDNS は IP マルチキャスト経由で DNS クエリを実行します。また、mDNS は 0 設定 IP ネットワーキングをサポートします。通常どおり、mDNS は宛先アドレスとしてマルチキャスト IP アドレス 224.0.0.251 を使用し、UDP 宛先ポートとして 5353 を使用します。

Location Specific Services（ロケーション固有サービス）

mDNS サービス アドバタイズメントおよび mDNS クエリ パケットの処理では、ロケーション固有サービス（LSS）をサポートしています。コントローラが受信するすべての有効な mDNS サービス アドバタイズメントは、新しいエントリをサービス プロバイダーのデータベースに挿入する際に、サービス プロバイダーからのサービス アドバタイズメントに関連付けられた AP の MAC アドレスにタグ付けされます。クライアント クエリーに対する応答記述では、クエリー送信するクライアントに関連付けられた AP の MAC アドレスを使用して SP-DB のワイヤレス エントリをフィルタリングします。ワイヤレス サービス プロバイダーのデータベース エントリは、LSS がサービスに対して有効になっている場合、AP-NEIGHBOR-LIST に基づいてフィルタリングされます。LSS がサービスに対して無効になっている場合、ワイヤレス サービス プロバイダーのデータベース エントリは、そのサービスに対するワイヤレス クライアントからのクエリに応答する場合、フィルタリング対象ではありません。

LSS は、ワイヤレス サービス プロバイダーのデータベース エントリだけに適用されます。有線サービス プロバイダー デバイスのロケーションは認識されません。

LSS の状態は、ORIGIN が有線に設定されているサービスに対して有効にすることはできません。この逆も同じです。

mDNS ポリシー

ここでは、特定のサービスプロバイダーにアクセスするためのポリシーの定義方法について説明します。アクセスポリシーでは、クライアント属性、構造、およびポリシーを構成するルール要素（ルールとポリシーの評価方法）が定義されます。これは、mDNS クエリを作成したクライアントに対する mDNS 応答に、特定のサービスプロバイダーを含める必要があるかどうかを判断する際に役立ちます。

LSS が有効になっている場合、近隣するサービスプロバイダーに関する情報だけが提供されますが、MDNS ポリシーでは、さらに詳細なポリシーを定義できます。

mDNS ポリシーは、次の情報に基づいてフレーム化できます。

- ユーザ
- Role
- AP 名
- AP Location
- [AP グループ（AP Group）]

mDNS ポリシーの制限事項

MDNS ポリシーの制限事項は次のとおりです。

- LSS は、mDNS ポリシーと組み合わせて適用できません。
- ロールとユーザ情報は、ISE サーバから提供されます。
- キーワード **Any** がルールパラメータ値として使用されている場合、チェックはバイパスされます。
- ルールはサービスプロバイダーの MAC アドレスに基づいて適用されるため、サービスプロバイダーによってアドバタイズされるすべてのサービスに対してルールが評価されます。
- mDNS ポリシーは、mDNS サービスに基づくものではなく、サービスプロバイダーの MAC アドレスに基づいて適用されます。
- mDNS ポリシーは、mDNS スヌーピングが有効になっている場合にのみアクティブになります。
- MAC アドレスごとに設定できるポリシーの最大数は、5 つです。

mDNS ポリシーのクライアント属性

mDNS クエリを開始するクライアントは、クライアントのコンテキストを表す一連の属性に関連付けられます。属性として使用できるのは、ロール、ユーザ ID、関連付けられた AP 名、関

連付けられた AP の場所、および関連付けられた AP グループです。アクセスポリシールールを明確化するために、ここに列挙された属性のみを使用します。

たとえば属性が場所の場合、クライアントが異なる場所に移動すると動的に変更されます。ユーザは、論理 OR 演算を使用してこれらの属性を組み合わせてルールを定式化し、そのルールをポリシーにアタッチできます。

サービスグループには、1 つまたは複数のルールを設定できます。

mDNS AP

mDNS AP 機能により、コントローラは VLAN 上の有線サービス プロバイダーの可視性を獲得できます。すべての AP で VLAN を設定する必要があります。コントローラの VLAN の可視性は、AP が mDNS アドバタイズメントをコントローラに転送することで実現されます。

内部 AP による mDNS パケット転送を開始または停止するには、コントローラで提供される設定可能なノブを使用します。また、この設定を使用して、AP が有線側から mDNS アドバタイズメントをスヌープする必要のある VLAN を指定できます。AP がスヌープできる VLAN の最大数は 10 です。

（注） デフォルトでは、mDNS AP は VLAN をスヌーピングしないため、管理 VLAN を指定して mDNS パケットをスヌーピングする必要があります。

mDNS AP 設定は、グローバル mDNs スヌーピングを無効にしてもそれぞれの mDNS AP で保持されます。

プライオリティ MAC サポート

サービスごとに最大 50 の MAC アドレスを設定できます。これらの MAC アドレスは、プライオリティを必要とするサービス プロバイダーの MAC アドレスです。これによって、サービス プロバイダーのデータベースがフルであっても、サービス プロバイダー数が最多であるサービスから最新の非プライオリティ サービス プロバイダーを削除することによって、設定されたサービスの MAC アドレスから発信されるあらゆるサービス アドバタイズメントが学習されることが保証されます。サービスのプライオリティ MAC アドレスを設定する場合は、**ap-group** と呼ばれるオプションのパラメータがあります。これは有線サービスプロバイダーにのみ適用され、有線サービスプロバイダーのデバイスにロケーションの検知を関連付けます。クライアントの mDNS クエリがこの **ap-group** から発信されると、プライオリティ MAC アドレスおよび **ap-group** による有線エントリが検索されて、集約応答の最初に表示されます。

Origin-Based Service Discovery

発信元（有線または無線）に基づいて着信トラフィックをフィルタするようにサービスを設定できます。mDNS AP から学習されたすべてのサービスは有線として扱われます。認識元が有線である場合、LSS は無線サービスにのみ適用されるため、LSS サービスに対して有効にすることはできません。

LSS ステータスがサービスに対して有効である場合、LSS は無線サービス プロバイダーのデータベースのみに適用されるため、発信元が無線に設定されたサービスを有線に変更することはできません。発信元を有線と無線で変更した場合、変更前の発信元タイプを持つサービス プロバイダーのデータベース エントリは削除されます。

マルチキャスト DNS の設定の制限

- IPv6 を介した mDNS はサポートされません。
- ローカル側で切り替えられた WLAN およびメッシュ アクセス ポイントでは、FlexConnect モードのアクセス ポイントで mDNS はサポートされていません。
- mDNS はリモート LAN ではサポートされません。
- サードパーティの mDNS サーバまたはアプリケーションは mDNS 機能を使用するコントローラではサポートされていません。サードパーティのサーバまたはアプリケーションによってアドバタイズされるデバイスは、コントローラで mDNS のサービスまたはデバイス テーブルに正しく入力されません。
- レイヤ 2 ネットワークで Apple のサーバとクライアントが同じサブネット内に存在する場合、コントローラでの mDNS スヌーピングは不要です。ただし、これはスイッチング ネットワークの動作に依存します。使用しているスイッチが mDNS スヌーピングと想定どおりに連動しない場合は、コントローラで mDNS を有効にする必要があります。
- ビデオは、WMM が有効な状態の Apple iOS 6 ではサポートされていません。
- mDNS AP は同じサービスまたは VLAN に対して同じトラフィックを複製することはできません。
- LSS フィルタリングはワイヤレス サービスのみに制限されます。
- LSS、mDNS AP、プライオリティ MAC アドレスおよび送信元ベースの検出機能は、コントローラの GUI を使用して設定できません。
- mDNS AP 機能は CAPWAP V6 ではサポートされません。
- mDNS のユーザ プロファイル モビリティは、ゲスト アンカーではサポートされません。
- iPad、iPhone などの Apple デバイスは、Bluetooth を使用して Apple TV を検出できます。このため、Apple TV がエンド ユーザに表示されることがあります。

マルチキャスト DNS の設定

ステップ 1 次の手順に従って、グローバル mDNS パラメータおよびマスター サービス データベースを設定します。

a) [Switch to Expert View] アイコンをクリックします。エキスパート ビューに切り替えるかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

b) [Services] > [mDNS] を選択します。

c) [mDNS Global Snooping] トグル ボタンを使用して、mDNS パケットのスヌーピングを有効または無効にします。
d) 分単位で mDNS クエリー間隔を入力します。クエリー間隔はコントローラがサービスを検索する頻度です。デフォルトは 15 分です。
e) [Add VLAN Id] ボタンをクリックして内部 AP スヌーピング用の VLAN のリストを追加します。

（注）
- ME の GUI から追加された VLAN は、すべての AP（内部および外部）に設定されます。**config mdns ap vlan add vlan-id ap-name** コマンドを実行するだけで、個々の AP VLAN を設定できます。
- GUI の [mDNS VLAN Mapping] テーブルには、内部 AP に設定されている VLAN のみが表示されます。**config mdns ap vlan add vlan-id ap-name** コマンドを実行するだけで、外部 AP に具体的に VLAN を設定できるので、**show ap summary** コマンドを実行すれば、すべての AP（内部と外部の両方）に追加された VLAN を表示できます。外部 AP に VLAN が設定されていても、GUI には表示されません。

f) 次のタブで詳細を入力します。

1. [Master Services Database]：マスター データベースに記載されているサービスを表示します。コントローラは、マスター サービス データベースで mDNS サービスが利用できる場合にのみ、このサービスのアドバタイズメントをスヌーピングおよび学習します。コントローラは、最大 64 のサービスをスヌープおよび学習できます。
   - [Add Service] ボタンをクリックしてマスター データベースに新しいサービスを追加します。
   - [Add/Edit mDNS Service] ウィンドウで、[Service Name]、[Service String]、[Query Status]、[Location Services]、および [Origin] を指定します。
   - [Update] をクリックします。
2. [mDNS Profiles]：mDNS プロファイルのリストを表示します。
   - [Add Profile] ボタンをクリックして新しいプロファイルを追加します。
   - [Add/Edit mDNS] ウィンドウで、後で WLAN にマッピングする可能性があるプロファイル名を入力します。
3. [Domain Names]：ドメイン名を表示し、検出されたリストからドメイン名を追加します。
4. [mDNS Browser]：実行している mDNS サービスの数を表示します。

g) [Apply] をクリックします。

ステップ 2 次の手順に従って、WLAN に mDNS プロファイルをマッピングします。

a) [Wireless Settings] > [WLANs] の順に選択します。
b) [Add new WLAN] をクリックします。[Add new WLAN] ウィンドウが表示されます。
c) [Add new WLAN] ウィンドウで [Advanced] タブを選択します。
d) [mDNS] トグル ボタンを使用して、mDNS を有効または無効にします。
e) [mDNS Profile] ドロップダウン リストから、プロファイルを選択します。

f) [Passive Client] トグル ボタンを使用してパッシブ クライアントを有効にします。[Services] > [Media Stream] で [Global Multicast] が有効になっていることを確認してください。パッシブ クライアントは [Global Multicast] が無効になっていると機能しません。
g) [Multicast IP] アドレスを入力します。
h) [Multicast Direct] トグルを使用してマルチキャスト ダイレクトを有効にします。
i) [Apply] をクリックします。

（注） ワイヤレスコントローラは、次の場合にVLAN経由で学習した有線デバイス（Apple TV など）からサービスをアドバタイズします。

- [WLAN Advanced] オプションで mDNS スヌーピングが有効になっている。
- インターフェイスまたは WLAN で mDNS プロファイルが有効になっている。

mDNS ポリシーの設定

次の手順に従って、mDNS ポリシーを設定します。

a) [Switch to Expert View] アイコンをクリックします。エキスパート ビューに切り替えるかどうかを確認するメッセージが表示されます。[Yes] をクリックします。
b) [Services] > [mDNS] を選択します。
c) [mDNS Global Snooping] トグル ボタンを使用して、mDNS パケットのスヌーピングを有効または無効にします。
d) [mDNS Policy] トグルボタンを使用して、mDNS ポリシーをそれぞれ有効または無効にします。
e) 分単位で mDNS クエリー間隔を入力します。クエリー間隔はコントローラがサービスを検索する頻度です。デフォルトは 15 分です。
f) [mDNS Policy] タブをクリックします。
mDNS ポリシー数が表示されます。
g) [Add mDNS Policy] ボタンをクリックします。
[Add mDNS Policy] ウィンドウで、最初に mDNS サービスグループを追加する必要があります。

1. [DNS Service Group Name] と [Description] を入力します。
2. [Add Service Instance] ボタンをクリックします。[Add Service Instance] ウィンドウが表示されます。サービスインスタンスを追加するには、次の詳細情報を入力します。
   - **Mac Address**
   - **Name**
   - [Location Type]：AP グループ、AP 名、または AP ロケーションでロケーションタイプを選択します。
   - [Location]：選択したロケーションタイプに基づきます。
3. [Apply] をクリックします。

[mDNS Policy] ウィンドウに作成されたサービスインスタンスが表示されます。

h) [Profile Name] を入力して、[Apply] をクリックします。

Cisco Umbrella

Cisco Mobility Express に搭載された Cisco Umbrella の概要

Cisco Umbrellaプラットフォームは、クラウドで提供されるネットワークセキュリティソリューションです。ドメインネームシステム（DNS）レベルでは、マルウェアや侵害からデバイスを保護するのに役立つリアルタイムの洞察を提供します。Cisco Mobility Express リリース 8.8 以降では、Cisco Umbrella マッピングは WLAN レベルでのみサポートされます。

Cisco Umbrella は、Cisco Mobiliry Express で次のように動作します。

- ワイヤレスクライアントがワイヤレスコントローラに接続すると、インターネットへのトラフィックを開始するときに DNS クエリを送信します。Cisco Umbrella は、DNS トラフィックを透過的に代行受信し、DNS クエリを Cisco Umbrella クラウドサーバにリダイレクトします。
- DNS クエリの完全修飾ドメイン名（FQDN）に基づくセキュリティポリシーは、Cisco Umbrella クラウドサーバで定義されます。
- Cisco Umbrella は、DNS クエリの FQDN に基づいて次のいずれかの応答を返します。
  - 悪意のある FQDN：Cisco Umbrella がブロックしたページの IP を対応するクライアントに返します。
  - 安全な FQDN：宛先 IP アドレスを返します。

Cisco Mobility Express に搭載された Cisco Umbrella のサポート内容

- 最大 10 個の異なる Cisco Umbrella プロファイルがサポートされます。各プロファイルには、固有のデバイス ID が割り当てられます。
- Cisco Umbrella プロファイルやデバイス ID のワイヤレスエンティティへのマッピングについては、WLAN レベルのマッピングのみがサポートされます。
- AP へのデバイス ID のプロビジョニングについては、AP が DNS パケットをスヌーピングし、EDNS タグを適用します。
- 強制や無視オープンモードがサポートされます。
- 新規の DHCP-6 オーバーライドオプションは、WLAN レベルでサポートされます。

制限事項

Cisco Umbrella は、次では機能しません。

- Cisco Umbrella は、次では機能しません。
  - Cisco IOS AP
  - ローカル認証
  - IPv6 アドレス
-
- アプリケーションまたはホストが、DNS を使用する代わりに IP アドレスを直接使用してドメイン名をクエリしている場合。
- クライアントが Web プロキシに接続されていて、サーバ アドレスを解決するための DNS クエリを送信しない場合。
- ワークグループブリッジ（WGB）の背後にある有線ゲストとクライアント。
- 仮想ワイヤレス LAN コントローラ（WLC）
- WLAN などのワイヤレスエンティティで、設定によるワイヤレス Cisco Umbrella プロファイルの適用が、デバイスの登録が成功したかどうかによって決まる場合。
- Cisco Umbrella クラウドが 2 つの IPv4 アドレスを提供している場合。WLC/AP では、最初に設定されたサーバアドレスが使用されます。サーバ間でロードバランシングは行われません。

Cisco Mobility Express での Cisco Umbrella の設定（GUI）

次の手順を実行して、Cisco Mobility Express で Cisco Umbrella を設定します。

始める前に

- Cisco Umbrella のアカウントが必要です。
- Cisco Umbrella からの API トークンが必要です。

ステップ 1 [Switch to Expert View] アイコンをクリックします。
エキスパート ビューに切り替えるかどうかを確認するメッセージが表示されます。[OK] をクリックします。

ステップ 2 [Services] > [Umbrella] を選択します。

ステップ 3 [Umbrella Global Status] トグルボタンを使用して、Umbrella ステータスをそれぞれ有効または無効にします。

ステップ 4 Cisco Umbrella から取得した **Umbrella API トークン**を入力します。

ステップ 5 [Apply] をクリックして Cisco Umbrella を有効にします。

ステップ 6 [Add Profile] をクリックして新しいプロファイルを作成します。

[Add Profile Name] ウィンドウが表示されます。

ステップ 7 [Profile Name] を入力して、[Apply] をクリックします。

新しいプロファイルが作成されます。

ステップ 8 次の手順に従って、WLAN に Cisco Umbrella プロファイルをマッピングします。

a) [Wireless Settings] > [WLANs] を選択します。
b) [Add new WLAN/RLAN] をクリックします。[Add new WLAN/RLAN] ウィンドウが表示されます。
c) [Add new WLAN] ウィンドウで [Advanced] タブを選択します。
d) [Umbrella Profile] ドロップダウンリストから、プロファイルを選択します。
e) [Umbrellaモード] ドロップダウンリストで、[Ignore] または [強制（Forced）] を選択します。
f) [Umbrella DHCP Override] トグルボタンを使用して、Cisco Umbrella DHCP オーバーライドを有効にします。
g) [Apply] をクリックします。

次のタスク

1. [Cisco Umbrella] ダッシュボードで、[Device Name] の下に、Cisco WLC とその ID が表示されていることを確認します。
2. ユーザ ロールの分類ルール（従業員のルールや従業員以外のルールなど）を作成します。
3. Cisco Umbrella サーバでポリシーを設定します。

Cisco Mobility Express（CLI）での Cisco Umbrella の設定

ここでは、Cisco Mobility Express で Cisco Umbrella を設定する手順について説明します。

始める前に

- Cisco Umbrella のアカウントが必要です。
- Cisco Umbrella からの API トークンが必要です。

ステップ 1 Cisco Umbrella を有効または無効にするには、 **config opendns** {**enable** | **disable**} を使用します。

例：

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

Cisco Umbrella のグローバル設定を有効または無効にします。

ステップ 2 **config opendns api-token** *api-token*

例：

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

ネットワークに Cisco Umbrella の API トークンを登録します。

ステップ 3 **config opendns profile** {**create** | **delete** | **refresh**} *profilename*

例：

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

WLAN 経由で適用できる Cisco Umbrella プロファイルを作成、削除、または更新します。

ステップ 4 **config wlan opendns-profile** *wlan-id profile-name* {**enable** | **disable**}

例：

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

Cisco Umbrella プロファイル ID を WLAN にマッピングします。

ステップ 5 **config wlan opendns-dhcp-opt6** *wlan-id* {**enable** | **disable**}

例：

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

WLAN ごとに DHCP オプション 6 を有効または無効にします。

ステップ 6 **config wlan opendns-mode** *wlan-id* {**ignore** | **forced**}

例：

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

WLAN で Cisco Umbrella モードを無視するかまたは適用します。

TLS

TLS セキュアトンネル

Transport Layer Security（TLS）はセキュア ポートと証明書交換を使用して、2 つのシステム間またはデバイス間でセキュアで信頼できるシグナリングとデータ転送を実現します。マルチサイト展開の課題を克服するために、Cisco Mobility Express は、TLS セキュアトンネルを使用して、Cisco Mobility Express から中央のデータセンターへのセキュアな接続を確立します。インバウンドトラフィックには、SSH、SNMP、Ping、HTTP、HTTPS、および TFTP が含まれ、アウトバウンドトラフィックには、SNMP、RADIUS、および TFTP が含まれます。

TLS トンネルには 2 つのコンポーネントがあります。

- TLS クライアント：Cisco Mobility Express コードに組み込まれ、マスター AP 上で実行されます。

- TLS ゲートウェイ：中央サイトで展開されて TLS トンネルを確立するための仮想マシンです。TLS ゲートウェイは、2 つのネットワークインターフェイス（パブリックネットワークとプライベートネットワーク）を備えています。

TLS クライアントの機能は次のとおりです。

- PnP でゼロタッチプロビジョニングをサポート
- TLS ゲートウェイ向け FQDN をサポート
- PSK ベースの認証
- Dead Peer Detection（DPD）
- トラフィックトンネリングの暗黙的および明示的設定
- NAT およびファイアウォール トラバーサルをサポート
- デバイスパラメータのシステム情報（シリアル番号、MAC アドレス、システム名）をサポート

TLS ゲートウェイの機能は次のとおりです。

- VMware を基盤とした仮想セキュリティソリューション
- TLS クライアントに対するダイナミック IP 割り当て：TLS ゲートウェイの 内部 DHCP サーバを使用した静的プールベースの IP 割り当て。
- デッドピア検出（DPD）と定期的なキー再生成：DPD とキー再生成間隔の設定、DPD と NAT タイムアウトの同期化。
- PSK 認証：事前共有キー（PSK）ベースの認証、複数の PSK 設定、およびゲートウェイでの PSK の暗号化ストレージ。
- 内部 DNS サーバ：DNS 解決用に設定可能な TLS クライアントの DNS サーバ。
- 接続レート制限：接続レート制限（1 秒あたり 50 接続）。
- スケール特性：インスタンスごとに 1 万トンネルのスケール制限。
- IP イベント通知：TLS クライアントトンネルの接続、切断、再接続（キー再生成）イベント時の通知（サーバ [syslog サーバ] Netconf/Restconf に通知）
- 有用性：設定 CLI、デバッグ統計情報（ゲートウェイレベルとデバイスレベル）、およびロギングをサポート。
- SSH ログイン制御：TLS ゲートウェイ VM への SSH ログインの有効化と無効化をサポート（プライベート インターフェイスのみ対象）。

Cisco Mobility Express セキュアトンネルは、次をサポートしています。

- アウトバウンド：SNMP トラップ、RADIUS（認証/アカウンティング）
- インバウンド：SNMP、SSH、Ping、HTTPS、HTTP

- TLS ゲートウェイ FQDN
- PSK ベースの認証
- インバウンドトラフィック：TFTP、SFTP、FTP
- キー再生成メカニズム
- トラフィックトンネリングの暗黙的および明示的な設定方法。暗黙的トンネリングにより、アプリケーションのトンネリングが可能になります。たとえば、SNMP トラップや RADIUS などです。また、明示的トンネリングにより、トンネリング用のホストやネットワークが追加されます。たとえば、SSH、PI/SNMP、DNAC などです。

Cisco Mobility Express に TLS セキュアトンネルを設定する際の一連の手順を以下に示します。

1. TLS ゲートウェイの展開：中央サイトで TLS ゲートウェイを展開するには、ここに記載されている手順に従います。
2. CLI の設定：詳細については、「Mobility Express コントローラのコマンド」のセクションを参照してください。
3. TLS の設定（GUI）：詳細については、「TLS トンネルの設定」を参照してください。

TLS トンネルの設定

TLS トンネルを設定するには、次の手順を実行します。

ステップ 1 [Switch to Expert View] アイコンをクリックします。
エキスパート ビューに切り替えるかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

ステップ 2 [Services] > [TLS] の順に選択します。
[TLS Tunnel Settings] ページが表示されます。

ステップ 3 [TLS Tunnel] トグルボタンを使用して、TLS トンネルを有効または無効にします。

ステップ 4 [TLS Tunnel Settings] ページで、次のパラメータを設定します。

- [TLS Gateway URL/IP Address] を入力します。
- PSK ID を入力します。
- PSK キーを入力します。
- RADIUS と SNMP を有効にします。

ステップ 5 [Apply] をクリックします。