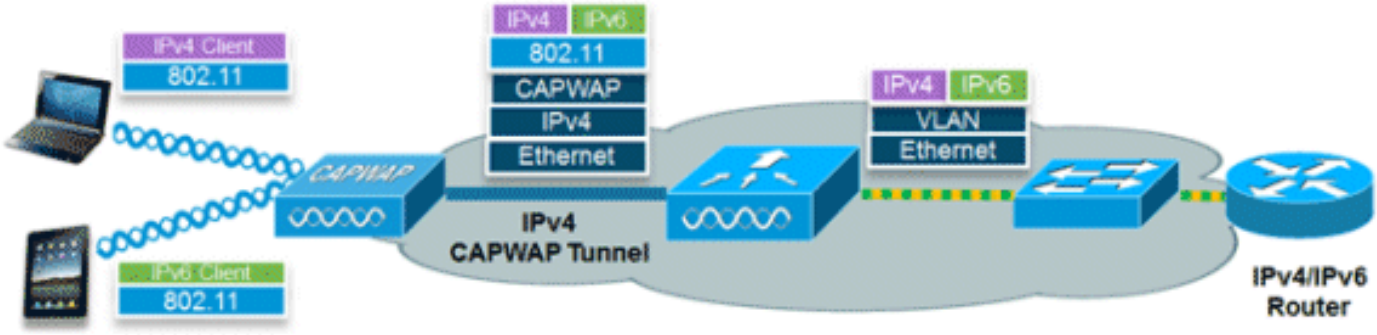
ワイヤレス LAN IPv6 クライアント導入ガイド

内容

はじめに

このドキュメントでは、IPv6 クライアントのサポートに関係する Cisco Unified Wireless LAN ソリューションの動作論理および設定について説明します。

IPv6 ワイヤレス クライアント接続



Cisco Unified Wireless Network ソフトウェア リリース v7.2 で設定される IPv6 機能セットは、ワイヤレス ネットワークが同じワイヤレス ネットワークの IPv4、デュアルスタック、および IPv6 専用のクライアントをサポートできるようにします。Cisco Unified Wireless LAN への IPv6 クライアント サポートの追加の全体的な目標は、モビリティ、セキュリティ、ゲスト アクセス、QoS、およびエンドポイントの可視性を含む IPv4 と IPv6 クライアントとの間の同等の機能を維持することです。

デバイスごとに最大 8 個の IPv6 クライアント アドレスを追跡できます。これにより、IPv6 クライアントは単一インターフェイス上でリンクローカル、ステートレス アドレス自動設定（SLAAC）アドレス、IPv6 用の Dynamic Host Configuration Protocol（DHCPv6）アドレス、および代替プレフィックスのアドレスを持つこともできます。WGB モードで自律アクセス ポイント（AP）のアップリンクに接続されているワークグループ ブリッジ（WGB）クライアントでも、IPv6 をサポートできます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ワイヤレス LAN コントローラ 2500 シリーズ、5500 シリーズ、または WiSM2

- 1130、1240、1250、1040、1140、1260、3500、3600 シリーズ AP、および 1520 または 1550 シリーズ メッシュ AP
- IPv6 対応ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

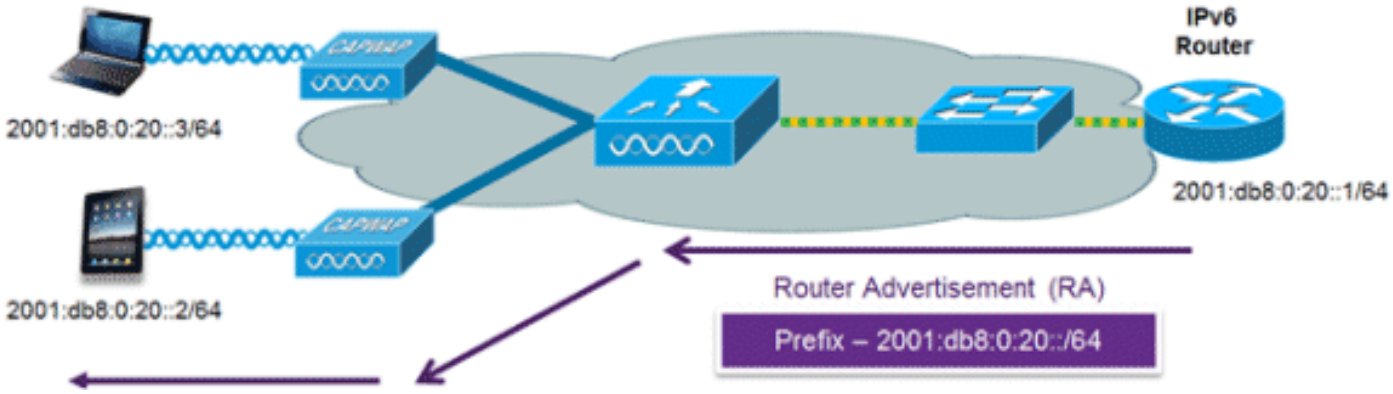
表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

ワイヤレス IPv6 クライアント接続の前提条件

ワイヤレス IPv6 クライアント接続を有効にするには、基礎となる有線ネットワークで、SLAAC または DHCPv6 などの IPv6 ルーティングおよびアドレス割り当て機能をサポートしている必要があります。ワイヤレス LAN コントローラは IPv6 ルータに対する L2 隣接関係が必要です。また、VLAN はパケットがコントローラに着信するときにタグを付ける必要があります。AP は、IPv6 ネットワーク上で接続を必要としません。すべてのトラフィックが AP とコントローラと間の IPv4 CAPWAP トンネル内でカプセル化されるためです。

SLAAC アドレスの設定

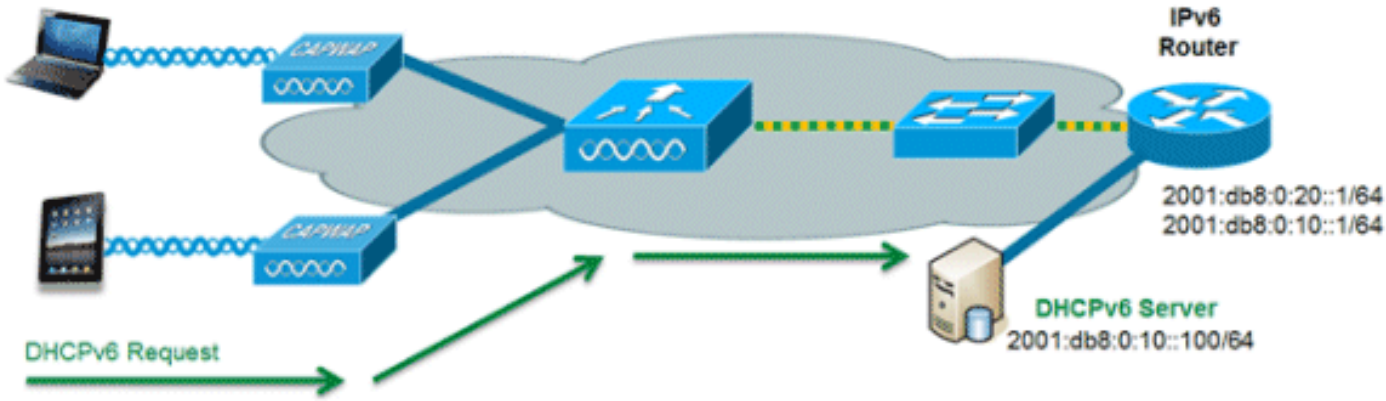


IPv6 クライアント アドレス割り当ての最も一般的な方法は SLAAC です。SLAAC はクライアントが IPv6 プレフィクスに基づいてアドレスを自己割り当てするシンプルなプラグ アンド プレイ接続を提供します。このプロセスは、IPv6 ルータが、使用されている IPv6 プレフィクス（最初の 64 ビット）および IPv6 デフォルト ゲートウェイをクライアントに通知する定期的なルータ アドバタイズメント メッセージを送信するときに実施されます。その時点から、クライアントは2つのアルゴリズム（インターフェイスのMACアドレスに基づくEUI-64、またはランダムに生成されるプライベートアドレス）に基づいて、IPv6アドレスの残りの64ビットを生成できます。アルゴリズムの選択はクライアントに依存し、多くの場合は設定できます。重複アドレス検出は、選択されるランダム アドレスが他のクライアントと重複しないように、IPv6 クライアントによって実行されます。アドバタイズメントを送信するルータのアドレスは、クライアントのデフォルト ゲートウェイとして使用されます。

Cisco 対応 IPv6 ルータからの次の Cisco IOS® コンフィギュレーション コマンドを使用して、SLAAC のアドレッシングとルータ アドバタイズメントを有効にします。

```
ipv6 unicast-routing
interface Vlan20
 description IPv6-SLAAC
 ip address 192.168.20.1 255.255.255.0
 ipv6 address 2001:DB8:0:20::1/64
 ipv6 enable
end
```

DHCPv6 アドレスの設定



DHCPv6 の使用は、SLAAC がすでに導入されている場合は、IPv6 クライアント接続で要求されません。DHCPv6 には「ステートレス」および「ステートフル」という 2 種類の動作モードがあります。

DHCPv6 ステートレス モードは、ルータ アドバタイズメントで使用できない追加のネットワーク情報をクライアントに提供するために使用しますが、これは IPv6 アドレスではありません。すでに SLAAC によって提供されているためです。この情報には DNS ドメイン名、DNS サーバ、その他の DHCP ベンダー固有オプションを含めることができます。このインターフェイス設定は、SLAAC をイネーブルにしてステートレス DHCPv6 を実装する Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
interface Vlan20
 description IPv6-DHCP-Stateless
 ip address 192.168.20.1 255.255.255.0
 ipv6 enable
 ipv6 address 2001:DB8:0:20::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:DB8:0:10::100
end
```

マネージド モードとも呼ばれる DHCPv6 ステートフル オプションは、DHCPv4 に対して同じよ

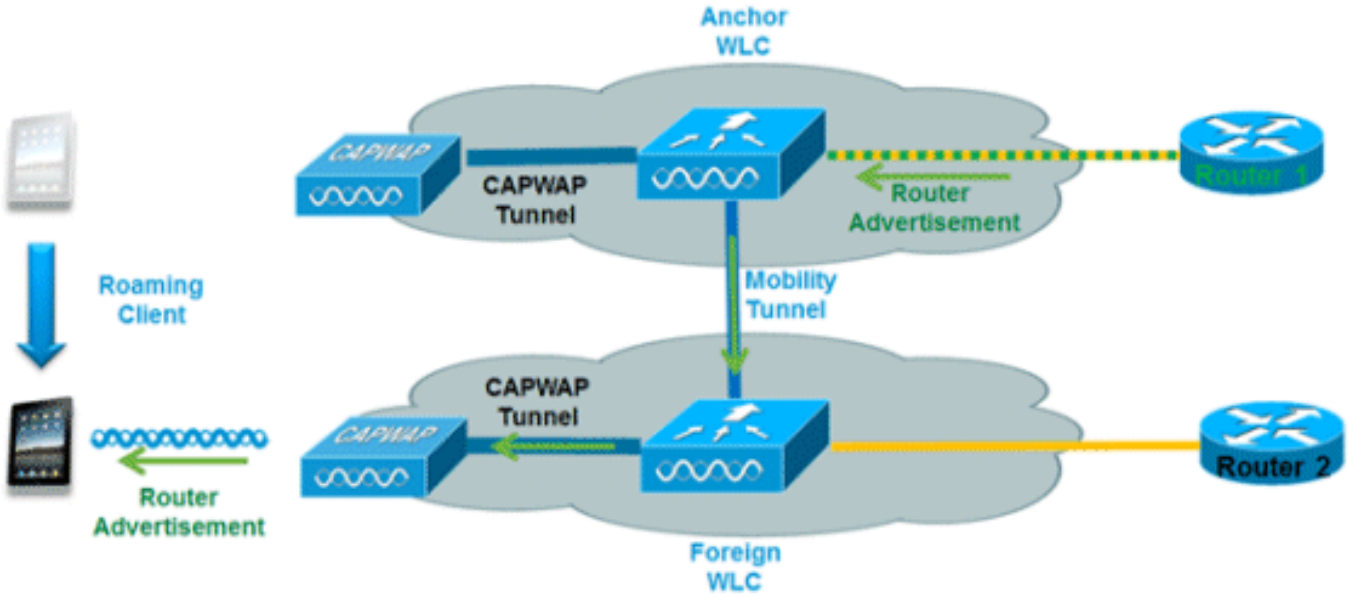
うに動作します。つまり固有のアドレスを、SLACC のとおりにアドレスの最後の 64 ビットを生成するクライアントではなく、それぞれのクライアントに割り当てます。このインターフェイス設定は、SLAAC をディセーブルにしてステートフル DHCPv6 を実装する Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
interface Vlan20
 description IPv6-DHCP-Stateful
 ip address 192.168.20.1 255.255.255.0
 ipv6 enable
 ipv6 address 2001:DB8:0:20::1/64
 ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:DB8:0:10::100
end
```

追加情報

デュアルスタックまたはトンネリングの接続方法を使用して完全な IPv6 キャンパス全体の接続用に有線ネットワークを設定する方法は、このドキュメントの対象範囲外です。詳細については、シスコの検証済み導入ガイド、『キャンパス ネットワークにおける IPv6 の導入』を参照してください。

IPv6 クライアント モビリティ



コントローラ間の IPv6 クライアントのローミングに対処するには、特にクライアントが同じレイヤ 3 ネットワーク上にとどまることを確実にするため、近隣要請（NS）、ネイバー アドバタイズメント（NA）、ルータ アドバタイズメント（RA）、およびルータ要請（RS）などの ICMPv6 メッセージに対処する必要があります。IPv6 モビリティの設定は、IPv4 モビリティの設定と同一であり、シームレスなローミングを実現するためにクライアント側で別個のソフトウェアを使用

する必要はありません。必要な設定は、コントローラが同じモビリティ グループまたはドメインに属している必要があることのみです。

コントローラ間の IPv6 クライアント モビリティのプロセスを次に示します。

1. 両方のコントローラにクライアントが配置された元の同じ VLAN へのアクセスがある場合、ローミングはクライアント レコードが新しいコントローラにコピーされる単純なレイヤ 2 のローミング イベントになり、アンカーのコントローラにトンネリングして戻されるトラフィックはありません。

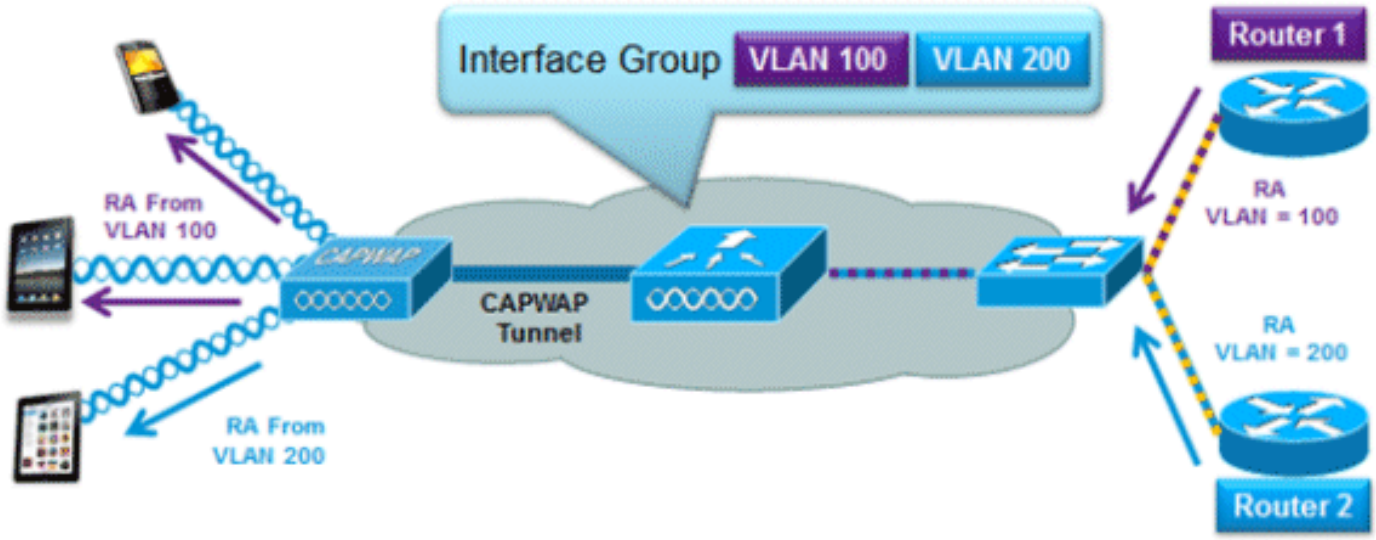
2. 2 つ目のコントローラにクライアントが配置された元の VLAN へのアクセスがない場合、レイヤ 3 のローミング イベントが発生します。これは、クライアントからのすべてのトラフィックがモビリティ トンネル（IP 上のイーサネット）経由でアンカー コントローラにトンネリングして戻される必要があることを意味します。

    a. クライアントが元の IPv6 アドレスを保持することを確実にするため、元の VLAN からの RA はアンカー コントローラによって外部コントローラに送信され、AP から L2 ユニキャストを使用してクライアントに配信されます。

    b. ローミングされたクライアントが DHCPv6 を介してアドレスを更新する、または SLAAC を介して新しいアドレスを生成すると、RS、NA、および NS パケットは元の VLAN に引き続きトンネリングされて、クライアントはその VLAN に適用できる IPv6 アドレスを受け取ります。

注：IPv6専用クライアントのモビリティは、VLAN情報に基づいています。これは、IPv6 専用クライアントのモビリティがタグなしの VLAN ではサポートされないことを意味します。

VLAN Select のサポート（インターフェイス グループ）

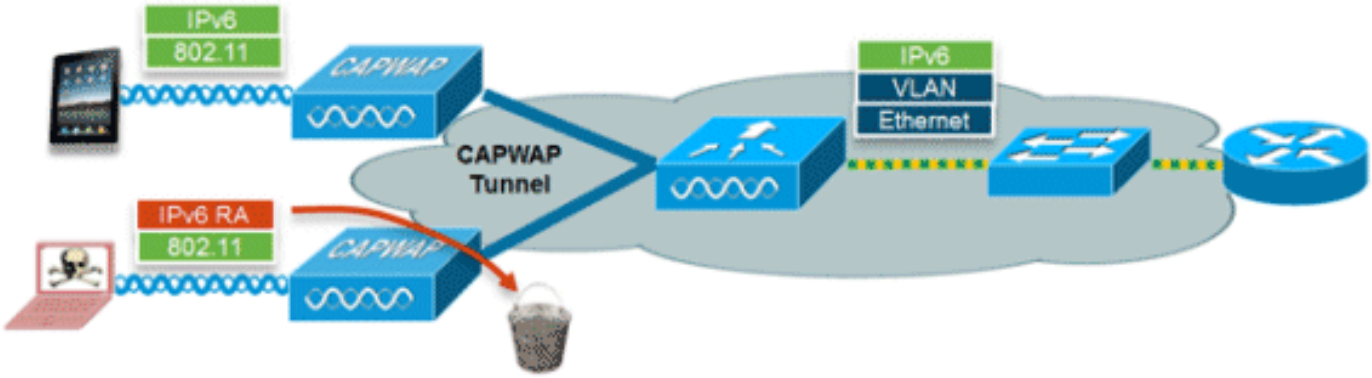


インターフェイス グループ機能は、組織がコントローラに複数の VLAN が設定された単一の WLAN を持てるようにし、これらの VLAN 全体でワイヤレス クライアントののロード バランシングを許可できるようにします。この機能は、グループ内の複数の VLAN 上の数千人のユーザに WLAN を拡張できるようにする一方で、IPv4 サブネット サイズを小さくするために使用されます。L2 ワイヤレス ユニキャスト経由で正しいクライアントに正しい RA がシステムによって自

動的に送信されるため、インターフェイス グループで IPv6 クライアントをサポートするための追加の設定は必要ありません。RA をユニキャストすることによって、別の VLAN にある、同じ WLAN 上のクライアントが間違った RA を受信することはありません。

IPv6 クライアントのファースト ホップ セキュリティ

ルータ アドバタイズメント ガード



RA ガード機能は、ワイヤレス クライアントから受信する RA をドロップすることによって IPv6 ネットワークのセキュリティを強化します。この機能がない場合、間違って設定された、または悪意のある IPv6 クライアントがネットワークのルータとして自分自身をアナウンスする可能性があります。このようなクライアントのほとんどは、有効な IPv6 ルータよりも優先される高い優先順位が設定されています。

デフォルトでは、RA ガードは AP で有効になり（ただし、AP で無効にすることも可能）、コントローラでは必ず有効になります。AP で RA をドロップすることは、よりスケーラブルなソリューションを実現し、機能拡張されたクライアントごとの RA ドロップ カウンタを提供するため推奨されます。いずれの場合も、悪意のある、または誤って設定された IPv6 クライアントから他のワイヤレス クライアントやアップストリームの有線ネットワークを保護するため、ある時点で IPv6 RA はドロップされます。

DHCPv6 サーバ ガード

DHCPv6 サーバ ガード機能は、ワイヤレス クライアントが他のワイヤレス クライアントやアップストリームの有線クライアントに IPv6 アドレスを配信しないようにします。DHCPv6 アドレスが配信されないようにするため、ワイヤレス クライアントからのすべての DHCPv6 アドバタイズ パケットはドロップされます。この機能はコントローラで動作し、設定を必要とせず、自動的に有効になります。

IPv6 ソース ガード

IPv6 ソース ガード機能は、ワイヤレス クライアントが他のクライアントの IPv6 アドレスをスプーフィングできないようにします。この機能は、IPv4 ソース ガードに似ています。IPv6 ソース ガードはデフォルトで有効になっていますが、CLI で無効にすることができます。

IPv6 アドレスのアカウンティング

RADIUS 認証とアカウンティングの場合、コントローラは [Framed-IP-address] 属性を使用して 1 つの IP アドレスを返信します。この場合は、IPv4 アドレスが使用されます。

[Calling-Station-ID] 属性は、コントローラの [Call Station ID Type] が [IP Address] に設定されている場合に IP アドレスを返信するため、このアルゴリズムを使用します。

1. IPv4 アドレス
2. グローバル ユニキャスト IPv6 アドレス
3. リンクローカル IPv6 アドレス

クライアント IPv6 アドレスは頻繁に変更されるため（一時的またはプライベート アドレス）、時間の経過とともにこれらを追跡することが重要です。Cisco NCS は、各クライアントで使用されているすべての IPv6 アドレスを記録し、クライアントがローミングされたり、新しいセッションが確立されたりするたびに、その履歴をログに記録します。これらのレコードは、NCS で最大 1 年間保持するように設定できます。

注：コントローラの「コールステーションIDタイプ」のデフォルト値は、バージョン7.2で「システムMACアドレス」に変更されました。アップグレードするときは、この値は MAC アドレスによるクライアントの一義的なトラッキングを可能にするため変更する必要があります。これは、[Calling-Station-ID] が IP アドレスに設定されている場合、IPv6 アドレスがセッション中に変更されてアカウンティングで問題が生じる可能性があるためです。

IPv6 アクセス コントロール リスト

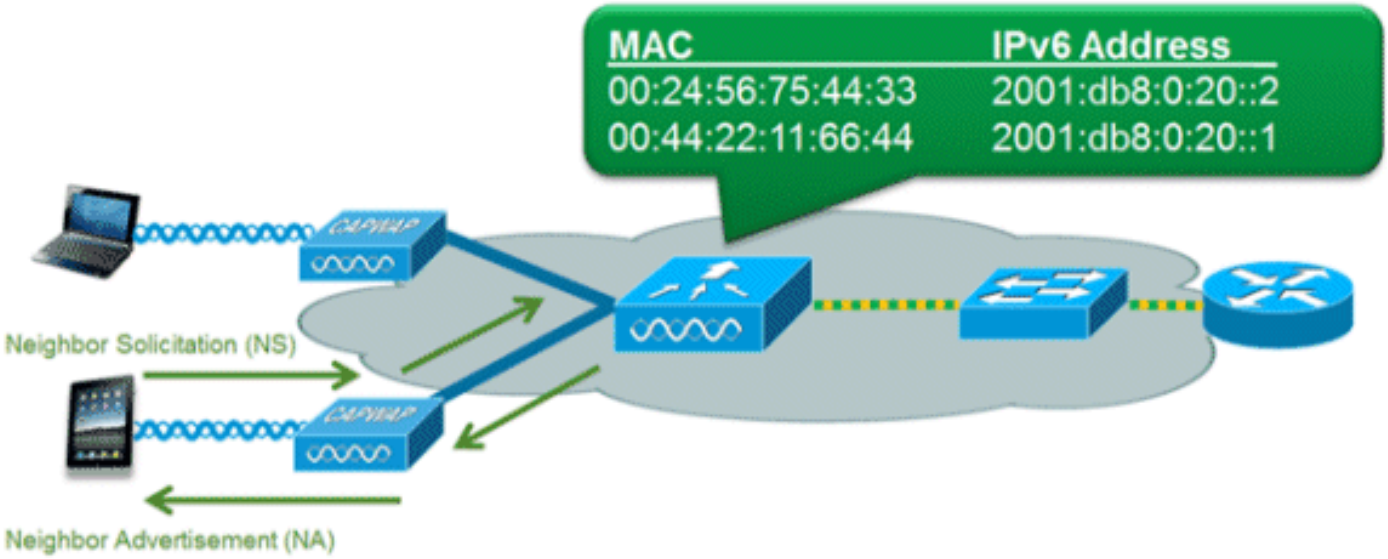
特定のアップストリームの有線リソースへのアクセスを制限したり、特定のアプリケーションをブロックしたりするために、IPv6 アクセス コントロール リスト（ACL）を使用してトラフィックを識別し、これを許可または拒否することができます。IPv6 ACL は、送信元、宛先、送信元ポート、および宛先ポートを含め IPv4 ACL と同じオプションがサポートされています（ポート範囲もサポートされています）。外部 Web サーバを使用した IPv6 ゲスト認証をサポートするために、事前認証 ACL もサポートされています。ワイヤレス コントローラは、それぞれ 64 個の固有ルールのある最大 64 個の固有 IPv6 ACL をサポートします。デュアルスタック クライアントの場合、ワイヤレス コントローラはそれぞれ 64 個の固有ルールのある最大 64 個の追加の固有 IPv4 ACL、合計 128 個の ACL をサポートします。

IPv6 ACL の AAA オーバーライド

Cisco Identity Services Engine（ISE）、ACS などの一元化された AAA サーバによるアクセス コントロールのサポートのために、AAA Override 属性を使用して毎クライアントについて IPv6 ACL をプロビジョニングできます。この機能を使用するには、IPv6 ACL をコントローラで設定し、AAA Override 機能を有効にして WLAN を設定する必要があります。IPv6 ACLの実際の名前付きAAA属性は、IPv4ベースのACLのプロビジョニングに使用されるAirespace-ACL-Name属性に似たAirespace-IPv6-ACL-Nameです。AAA 属性が返すコンテンツは、コントローラで設定された IPv6 ACL の名前に一致する文字列になるはずです。

IPv6 クライアントのパケット最適化

ネイバー探索キャッシング



IPv6 ネイバー探索プロトコル（NDP）は、アドレス解決プロトコル（ARP）の代わりに NA および NS パケットを利用し、IPv6 クライアントがネットワーク上の他のクライアントの MAC アドレスを解決できるようにします。NDPプロセスは、最初にマルチキャストアドレスを使用してアドレス解決を実行するため、通信が非常に多くなる可能性があります。これにより、マルチキャストパケットがネットワークセグメント上のすべてのクライアントに送信されるため、貴重なワイヤレス通信時間を消費する可能性があります。

NDP プロセスの効率を上げるため、ネイバー探索キャッシングはコントローラがプロキシとして機能し、解決できる NS クエリーに応答できるようにします。ネイバー探索キャッシングはコントローラに存在する、基盤となるネイバー バインディング テーブルによって可能になります。ネイバー バインディング テーブルでは、各 IPv6 アドレスと、アソシエートされた MAC アドレスが追跡されます。IPv6 クライアントが別のクライアントのリンク層アドレスを解決しようとすると、NS パケットは NA パケットで応答するコントローラによってインターセプトされます。

ルータ アドバタイズメント スロットリング

ルータ アドバタイズメント スロットリングは、コントローラがワイヤレス ネットワーク宛ての RA のレート制限を強制できるようにします。RA スロットリングを有効にすると、RA を頻繁（たとえば、3 秒ごと）に送信するように設定されたルータの周波数を、IPv6 クライアント接続を引き続き維持できる最小周波数に減らすことができます。これにより、送信されるマルチキャスト パケットの数を減らすことで通信時間を最適化することができます。いずれの場合も、クライアントが RS を送信すると、RA はコントローラを介して許可され、要求元クライアントにユニキャストで送信されます。これは、新しいクライアントまたはローミングされたクライアントが RA スロットリングによる悪影響を受けないことを確実にするためです。

IPv6 ゲスト アクセス

IPv4 クライアントの無線および有線のゲスト機能は、デュアルスタックと IPv6 専用クライアントで同じように動作します。ゲスト ユーザが関連付けられると、IPv4 または IPv6 キャプティブ ポータル経由でクライアントが認証されるまで「WEB_AUTH_REQ」の run 状態になります。コ

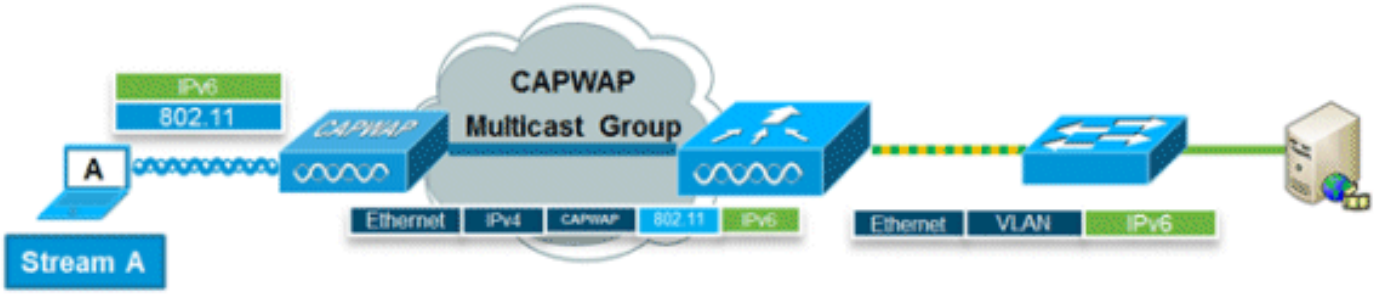
ントローラは、この状態の IPv4 と IPv6 の両方の HTTP/HTTPS トラフィックをインターセプトし、コントローラの仮想 IP アドレスにリダイレクトします。ユーザがキャプティブ ポータル経由で認証されると、その MAC アドレスが run 状態に遷移し、IPv4 と IPv6 の両方のトラフィックの通過が許可されます。外部 Web 認証の場合、事前認証 ACL は外部 Web サーバを使用できるようにします。

IPv6 専用クライアントのリダイレクションをサポートするために、コントローラは、コントローラに設定された IPv4 仮想アドレスに基づいて IPv6 仮想アドレスを自動的に作成します。仮想 IPv6アドレスは、`[::ffff:<virtual IPv4 address>]`の規則に従います。たとえば、仮想 IP アドレス 1.1.1.1 は、`[::ffff:1.1.1.1]` に変換されます。

ゲスト アクセス認証に信頼された SSL 証明書を使用する場合は、コントローラの IPv4 と IPv6 の両方の仮想アドレスが SSL 証明書のホスト名と一致するように DNS で定義されていることを確認します。これは、証明書がデバイスのホスト名と一致しないことを示すセキュリティ警告をクライアントが受信しないことを確実にします。

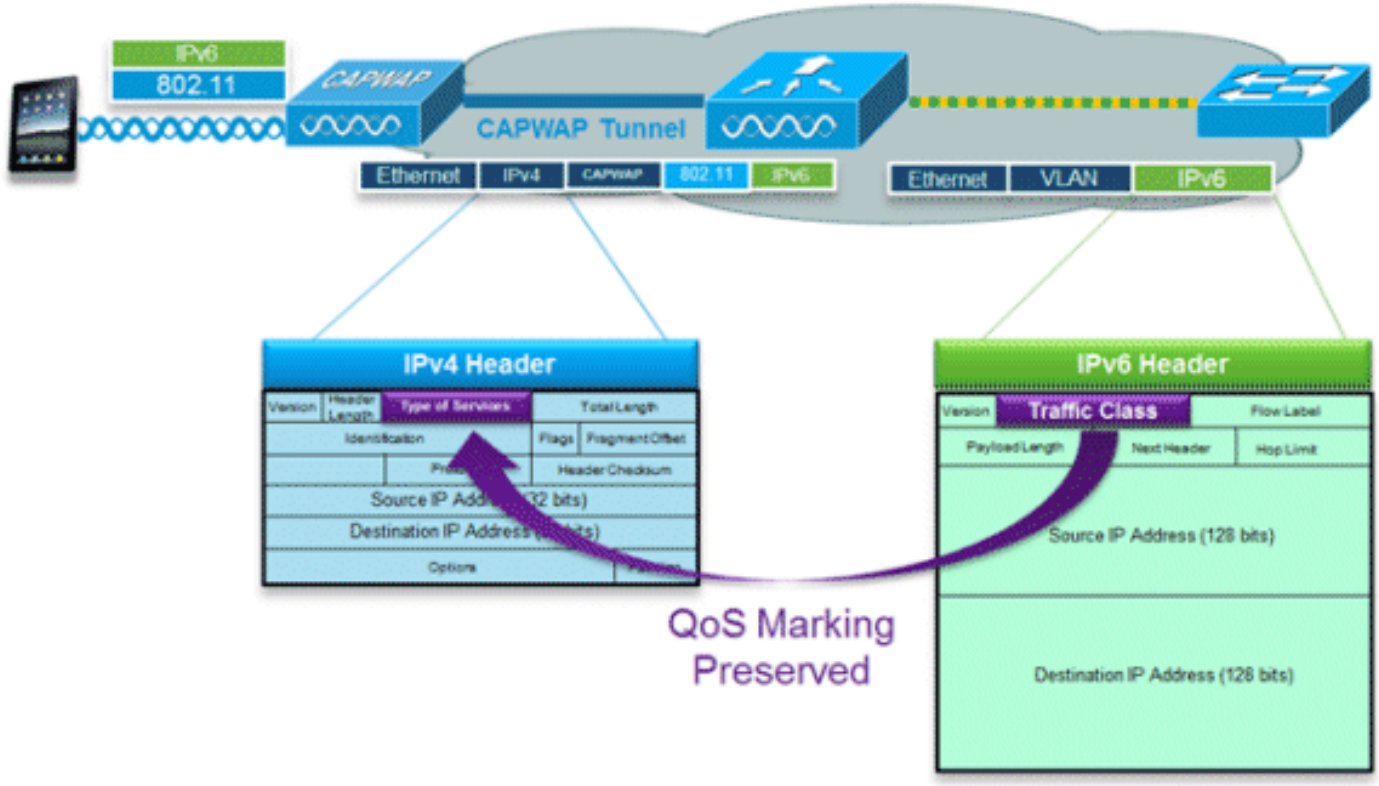
注：コントローラの自動生成されたSSL証明書にIPv6仮想アドレスが含まれていません。これにより、Web ブラウザにセキュリティ警告が表示される可能性があります。ゲスト アクセスに信頼された SSL 証明書を使用することを推奨します。

IPv6 VideoStream



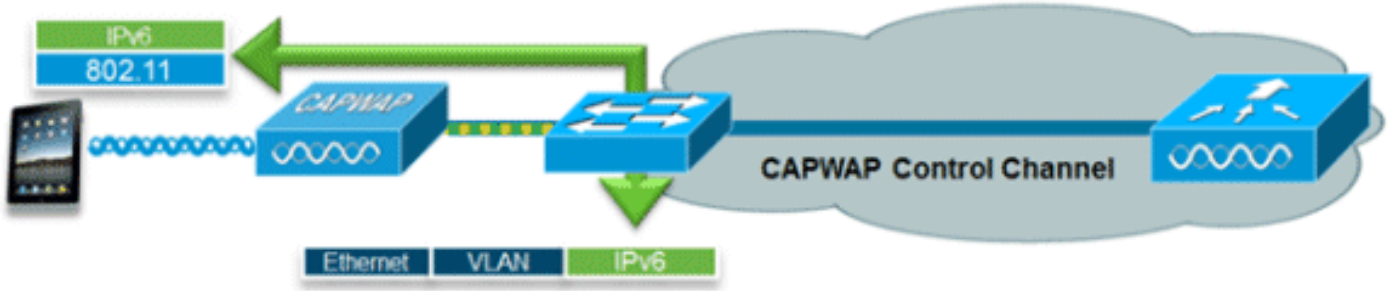
VideoStream は信頼性が高くスケーラブルなワイヤレス マルチキャスト ビデオ配信を可能にし、各クライアントにユニキャスト形式のストリームを送信します。実際のマルチキャストからユニキャストの変換（L2）は AP で実行されるため、スケーラブルなソリューションが提供されます。コントローラは IPv4 CAPWAP マルチキャスト トンネル内で IPv6 ビデオ トラフィックを送信し、AP に対する効率的なネットワーク分配を可能にします。

IPv6 QoS



IPv6 パケットは、IPv4 による DSCP 値の使用と同じようなマーキングを使用し、最大 64 個の異なるトラフィック クラス (0 ~ 63) をサポートします。有線ネットワークからのダウンストリーム パケットでは、エンドツーエンドの QoS が維持されることを確実にするため、IPv6 トラフィック クラス値は CAPWAP トンネルのヘッダーにコピーされます。アップストリーム方向では同様に、IPv6 トラフィック クラスでレイヤ 3 にマーキングされたクライアント トラフィックはコントローラに向かう CAPWAP パケットのマーキングによって承認されます。

IPv6 および FlexConnect



FlexConnect – ローカル スイッチング WLAN

ローカル スイッチング モードの FlexConnect は、IPv4 での動作と同じように、トラフィックをローカル VLAN とブリッジングすることによって IPv6 クライアントをサポートします。クライアント モビリティは、FlexConnect グループのレイヤ 2 ローミングでサポートされます。

FlexConnect ローカル スイッチング モードでは、次の IPv6 固有の機能がサポートされています。

- IPv6 RA ガード
- IPv6 ブリッジング
- IPv6 ゲスト認証 (コントローラでホストされます)

FlexConnect ローカル スイッチング モードでは、次の IPv6 固有の機能がサポートされていません。

- レイヤ 3 モビリティ
- IPv6 VideoStream
- IPv6 アクセス コントロール リスト
- IPv6 ソース ガード
- DHCPv6 サーバ ガード
- ネイバー探索キャッシング
- ルータ アドバタイズメント スロットリング

FlexConnect – 中央スイッチング WLAN

中央スイッチングを使用する FlexConnect モードの AP の場合 (コントローラにトラフィックをトンネリングして戻す)、コントローラの [AP Multicast Mode] に [Multicast - Unicast Mode] を設定する必要があります。FlexConnect AP はコントローラの CAPWAP マルチキャスト グループに参加しないため、コントローラでマルチキャスト パケットを複製し、各 AP に個別にユニキャストで送信する必要があります。この方法は、[Multicast - Multicast Mode] よりも非効率的で、コントローラに負荷を追加します。

FlexConnect 中央スイッチング モードでは、次の IPv6 固有の機能がサポートされていません。

- IPv6 VideoStream

注：IPv6を実行する中央でスイッチされるWLANは、Flex 7500シリーズコントローラではサポートされません。

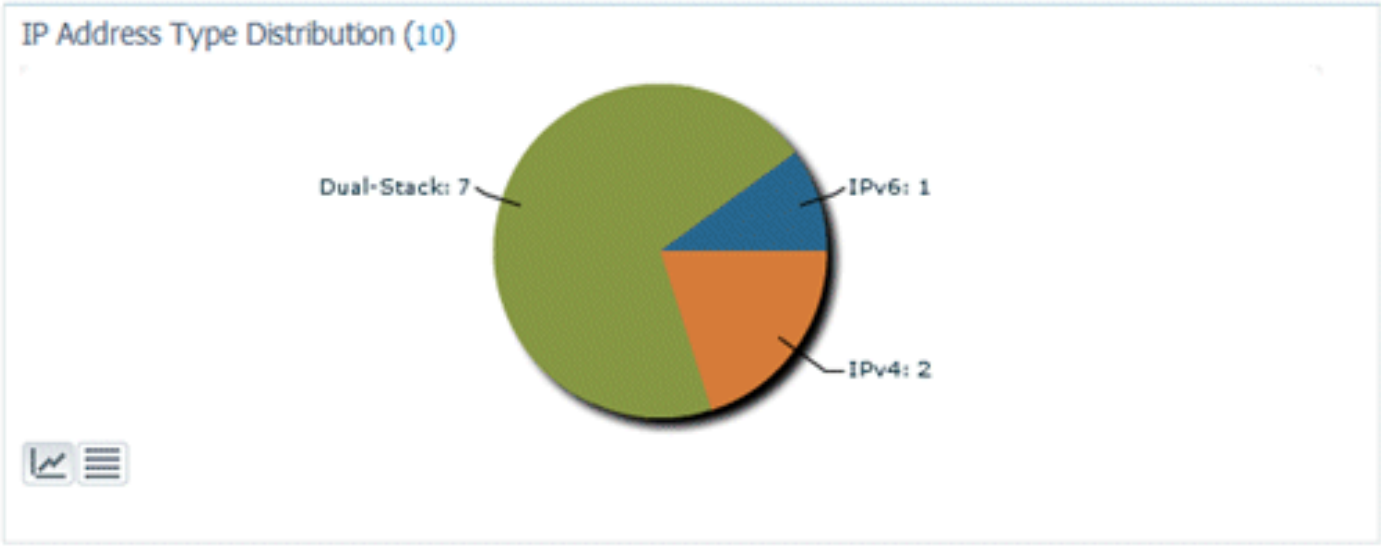
NCS での IPv6 クライアントの表示

NCS v1.1 のリリースでは、無線および有線ネットワークの両方にある IPv6 クライアントのネットワークを監視および管理するために、数多くの IPv6 固有の機能が追加されました。

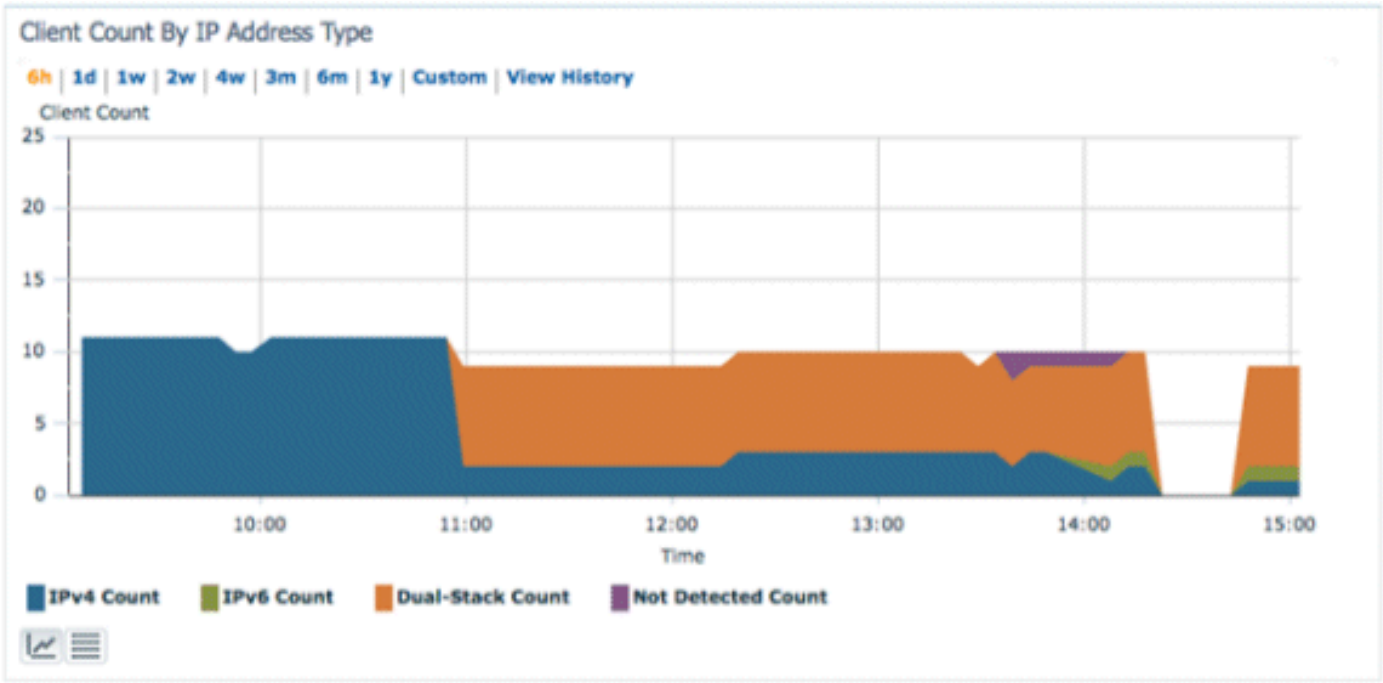
IPv6 ダッシュボード項目

どのようなタイプのクライアントがネットワークに存在するかを確認するには、NCS の「Dashlet」を使用できます。これは、IPv6 固有の統計情報を確認し、IPv6 クライアントをドリルダウンする機能を提供します。

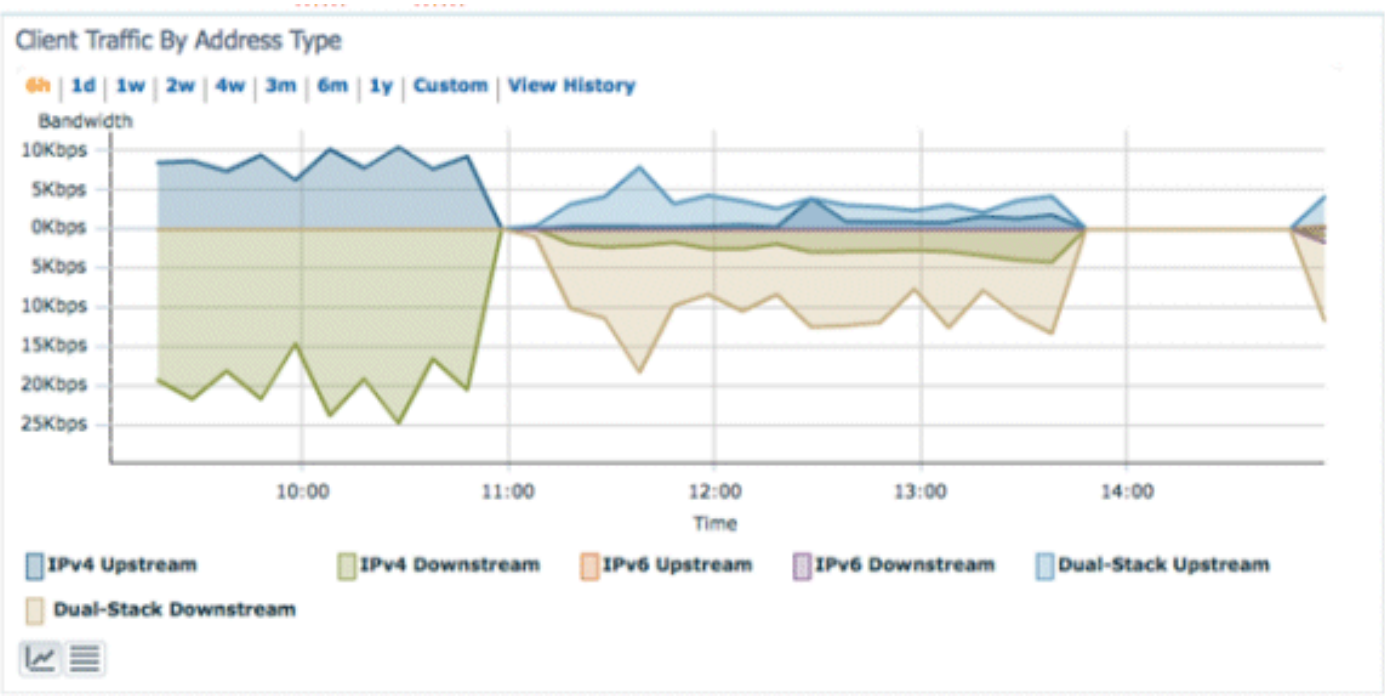
IP Address Type Dashlet：ネットワーク上の IP クライアントのタイプを表示します。



Client Count by IP Address Type：時間の経過とともに IP クライアントのタイプを表示します。



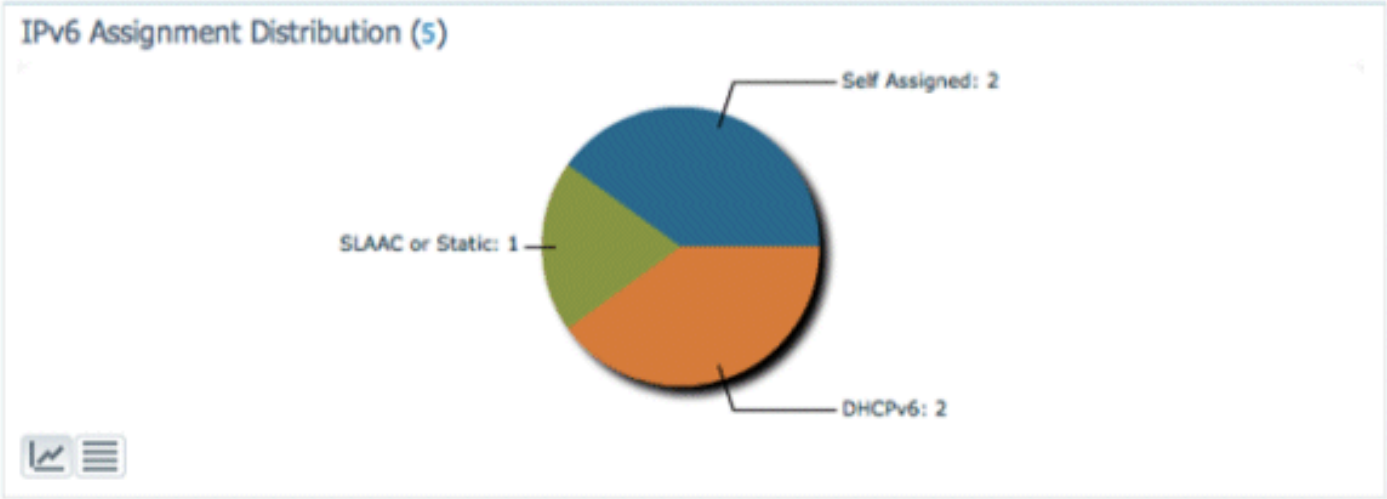
Client Traffic by IP Address Type：各タイプのクライアントからのトラフィックを表示します。デュアルスタックのカテゴリのクライアントは、IPv4 と IPv6 の両方のトラフィックを含んでいます。



IPv6 Address Assignment：各クライアントのアドレス割り当て方法を次の 4 種類のカテゴリのいずれかで表示します。

- DHCPv6：中央サーバによってアドレスが割り当てられるクライアント。このクライアントには、SLAAC アドレスもある場合があります。
- SLAAC or Static：ステートレス アドレス自動割り当てを使用するクライアント、または静的に設定されたアドレスを使用するクライアント。
- Unknown：場合によっては IPv6 アドレスの割り当てを検出できないことがあります。
    - この状態は、一部のスイッチが IPv6 のアドレス割り当て情報をスヌープしないため、NCS 有線クライアントでのみ発生します。
- Self-Assigned：完全に自動割り当てされるリンクローカル アドレスのみのクライアント。
    - このカテゴリのクライアントはグローバルな一意のアドレスまたはローカルな一意のアドレスを持たないため、IPv6 接続の問題が発生する場合があります。

円グラフの各セクションはクリック可能で、管理者はクライアントのリストをドリルダウンすることができます。



IPv6 クライアントの監視

IPv6 クライアント情報を監視および管理するために、[Clients and Users] ページに次の列が追加されました。

- IP Type：クライアント側から確認される IP アドレスに基づいたクライアントのタイプ。指定できるのは、IPv4、IPv6、またはデュアルスタック（IPv4 アドレスと IPv6 アドレスの両方があるクライアントを表す）です。
- IPv6 Assignment Type：アドレス割り当て方法は NCS によって SLAAC or Static、DHCPv6、Self-Assigned、または Unknown のいずれかとして検出されます。
- Global Unique：クライアントが使用する最新の IPv6 グローバル アドレス。列の内容にカーソルを合わせると、クライアントが使用する追加の IPv6 のグローバルな一意のアドレスが表示されます。
- Local Unique：クライアントが使用する最新の IPv6 のローカルな一意のアドレス。列の内容にカーソルを合わせると、クライアントが使用する追加の IPv6 のグローバルな一意のアドレスが表示されます。

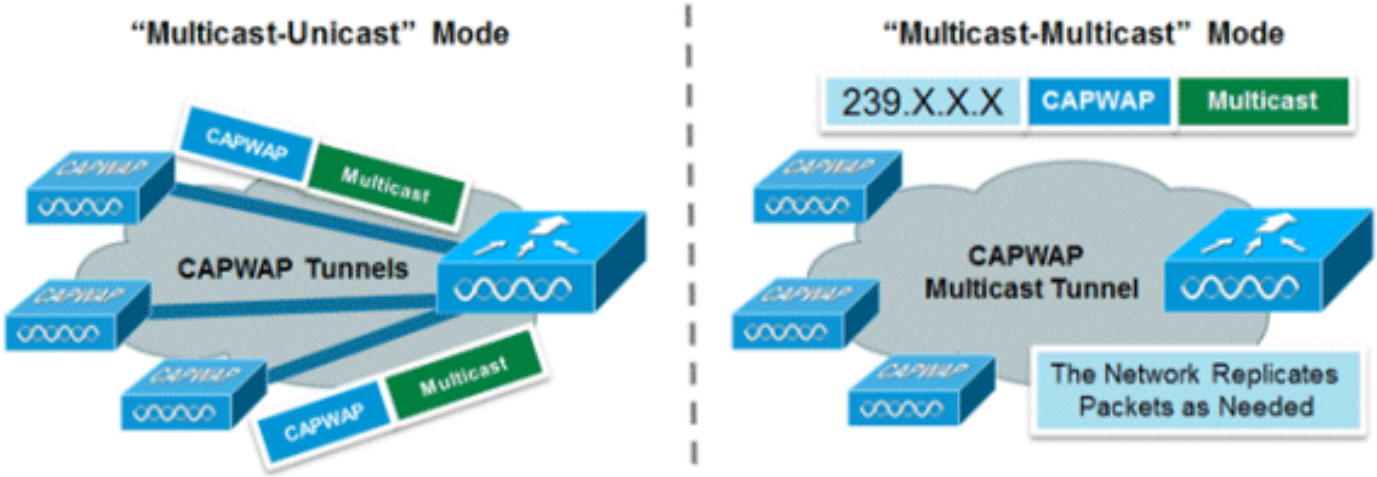
- Link Local：他の IPv6 アドレスが割り当てられる前に、セルフアサインされ、通信に使用されるクライアントの IPv6 アドレス。
- Router Advertisements Dropped：クライアントが送信し、AP でドロップされるルータ アドバタイズメントの数。この列を使用し、正しく設定されていないクライアント、または IPv6 ルータのように動作するように設定された悪意のあるクライアントを追跡できます。列を並べ替えて、問題のあるクライアントを簡単に特定することができます。

IPv6 固有の列の表示に加えて、[IP Address] 列には IPv4 アドレス（デュアルスタック クライアントの場合）または IPv6 のグローバルな一意のアドレス（IPv6 専用クライアントの場合）を最初に表示するプライオリティが設定されたクライアントの現在の IP アドレスが表示されます。

ワイヤレス IPv6 クライアント サポートの設定

AP へのマルチキャスト配信モード

Cisco Unified Wireless Network では、コントローラに関連付けられている AP へのマルチキャスト配信として 2 つの方法がサポートされています。両方のモードにおいて、有線ネットワークからの元のマルチキャスト パケットは、CAPWAP ユニキャストまたはマルチキャストのいずれかを介して AP に送信されたレイヤ 3 CAPWAP パケット内でカプセル化されます。トラフィックは CAPWAP カプセル化されるため、AP はクライアント トラフィックと同じ VLAN 上にある必要はありません。次にマルチキャスト配信の 2 つの方法を比較します。



	マルチキャスト ユニキャスト モード	マルチキャスト マルチキャスト モード

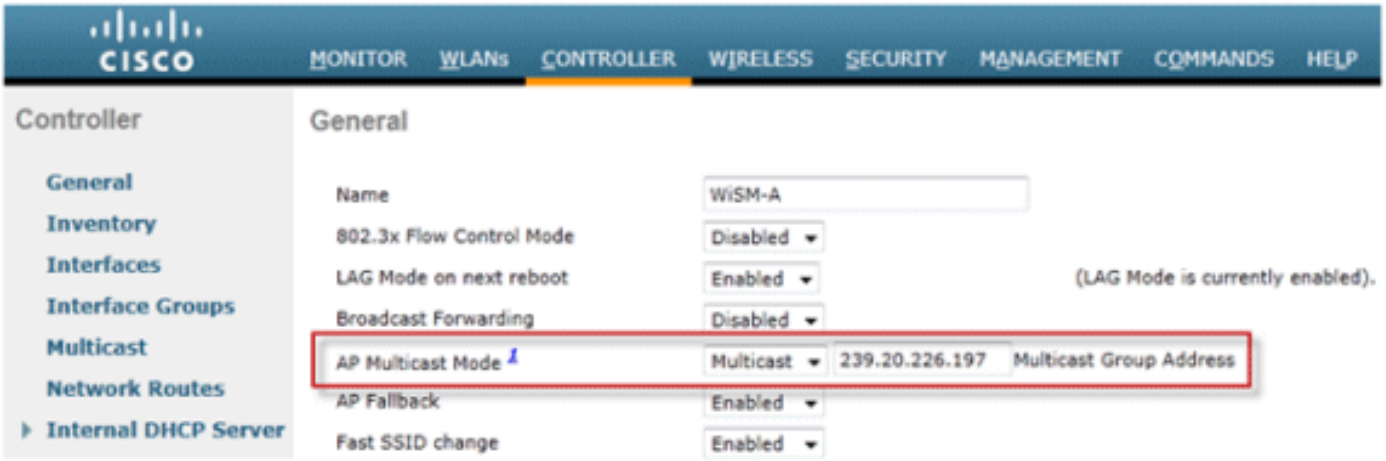
配信メカニズム	コントローラによってマルチキャスト パケットが複製されてユニキャスト CAPWAP トンネルの各 AP に送信されます。	コントローラによってマルチキャスト パケットの 1 つのコピーが送信されます。
サポートされる AP モード	FlexConnect およびローカル	ローカル モードのみ
有線ネットワーク上での L3 マルチキャスト ルーティングが必要	いいえ	Yes
コントローラの負荷	高	低い
有線ネットワークの負荷	高	低い

Multicast-Multicast 配信モードの設定

拡張性および有線帯域幅の効率化のために、マルチキャスト マルチキャスト モードのオプションが推奨されています。

注：この手順は2500シリーズワイヤレスコントローラでのみ必須ですが、より効率的なマルチキャスト送信が可能であり、すべてのコントローラプラットフォームに推奨されます。

[General] ページの [Controller] タブに移動して、[AP Multicast Mode] に [Multicast] モードの使用が設定されていて、有効なグループ アドレスが設定されていることを確認します。グループ アドレスは IPv4 マルチキャスト グループです。また、プライベート マルチキャスト アプリケーションの範囲である 239.X.X.X ~ 239.255.255.255 の範囲内であることが推奨されます。

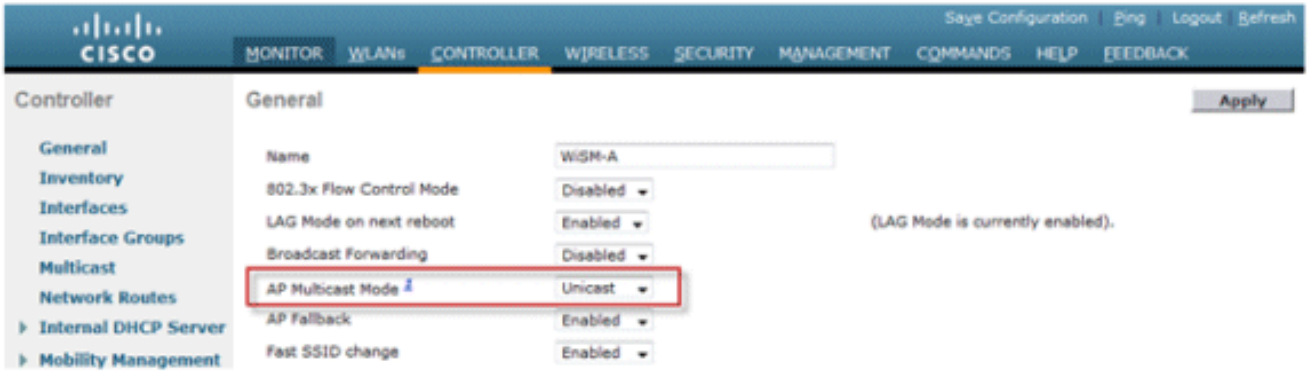


注：マルチキャストグループアドレスには、224.X.X.X、239.0.0.X、または239.128.0.Xのアドレス範囲を使用しないでください。これらの範囲のアドレスは、リンク ローカル MAC アドレスとオーバーラップし、IGMP スヌーピングが有効の場合でもすべてのスイッチ ポートにフラッディングします。

Multicast-Unicast 配信モードの設定

コントローラと AP または FlexConnect モード間に CAPWAP マルチキャストを配信するように有線ネットワークが適切に設定されてなく、IPv6 をサポートする中央でスイッチされる WLAN に AP が使用される場合は、ユニチキャスト モードが必要です。

1. [General] ページの [Controller] タブに移動して、[AP Multicast Mode] で [Unicast] モードの使用が設定されていることを確認します。



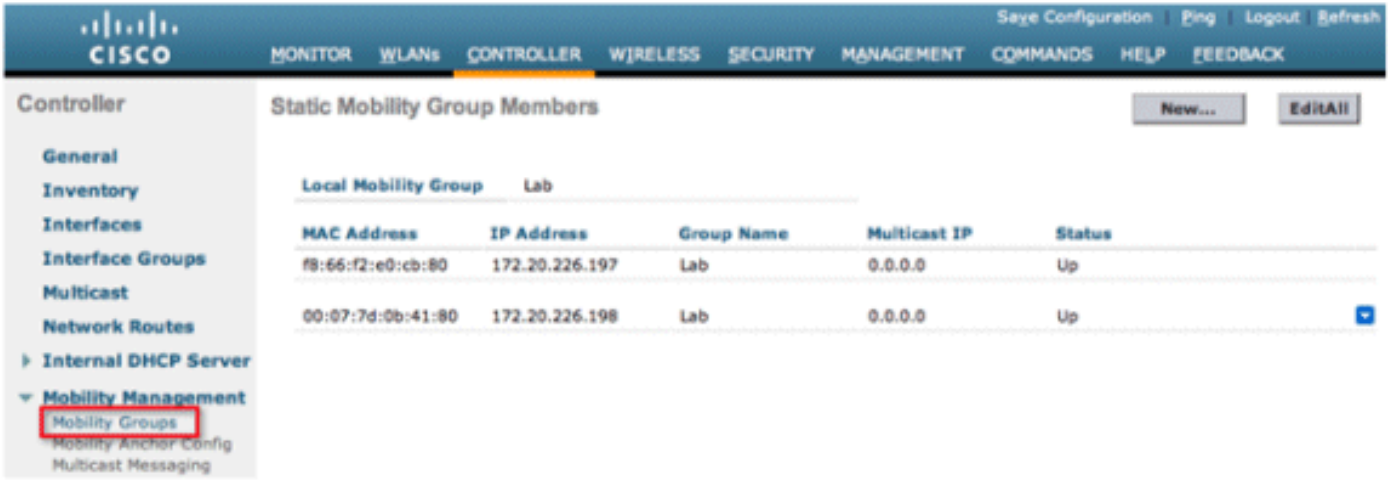
2. IPv6 対応クライアントをワイヤレス LAN に接続します。[Monitor] タブ、[Clients] メニューの順に移動して、クライアントが IPv6 アドレスを受信していること確認します。

IPv6 モビリティの設定

同じモビリティ グループまたは同じモビリティ ドメイン内にコントローラを配置することを除き、IPv6 モビリティのための特定の設定はありません。これは、合計で最大 72 個のコントローラ

がモビリティのドメインに参加できるようにし、最も大規模なキャンパスにもシームレスなモビリティを提供します。

[Controller] タブ > [Mobility Groups] の順に移動し、MAC アドレスおよび IP アドレスでグループに各コントローラを追加します。これは、モビリティ グループ内のすべてのコントローラで実行する必要があります。

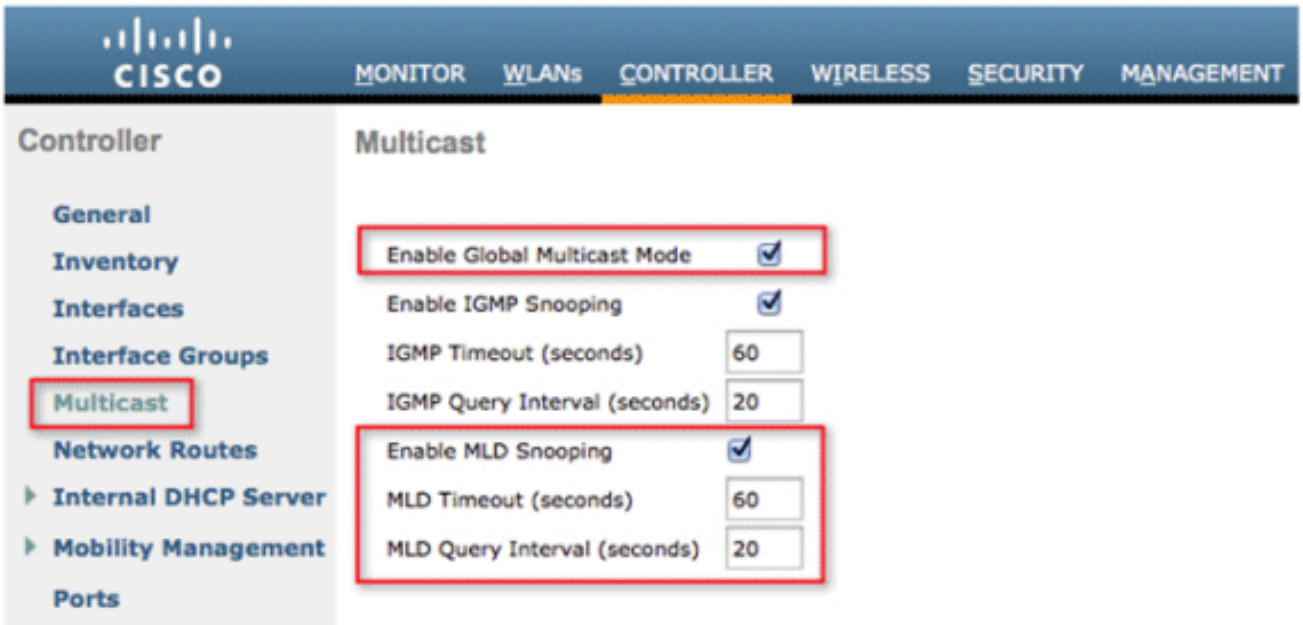


IPv6 マルチキャストの設定

コントローラはクライアントが要求するマルチキャスト フローをインテリジェントに追跡して配信できるようにする、IPv6 マルチキャスト用の MLDv1 スヌーピングをサポートしています。

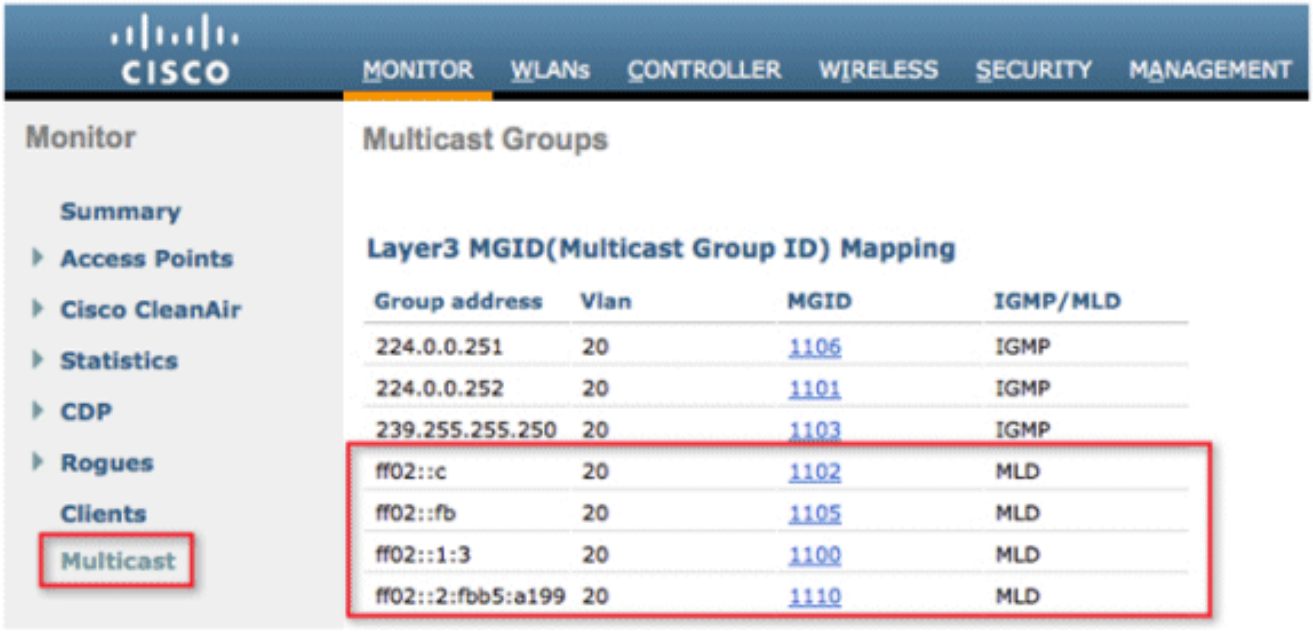
注：以前のバージョンのリリースとは異なり、IPv6ユニキャストトラフィックサポートでは、コントローラで「グローバルマルチキャストモード」を有効にする必要はありません。IPv6 ユニキャスト トラフィック サポートは、自動的に有効になります。

1. マルチキャスト IPv6 トラフィックをサポートするには、[Controller] タブ > [Multicast] ページ、および [Enable MLD Snooping] の順に移動します。IPv6 マルチキャストを有効にするには、コントローラの [Global Multicast Mode] も有効にする必要があります。



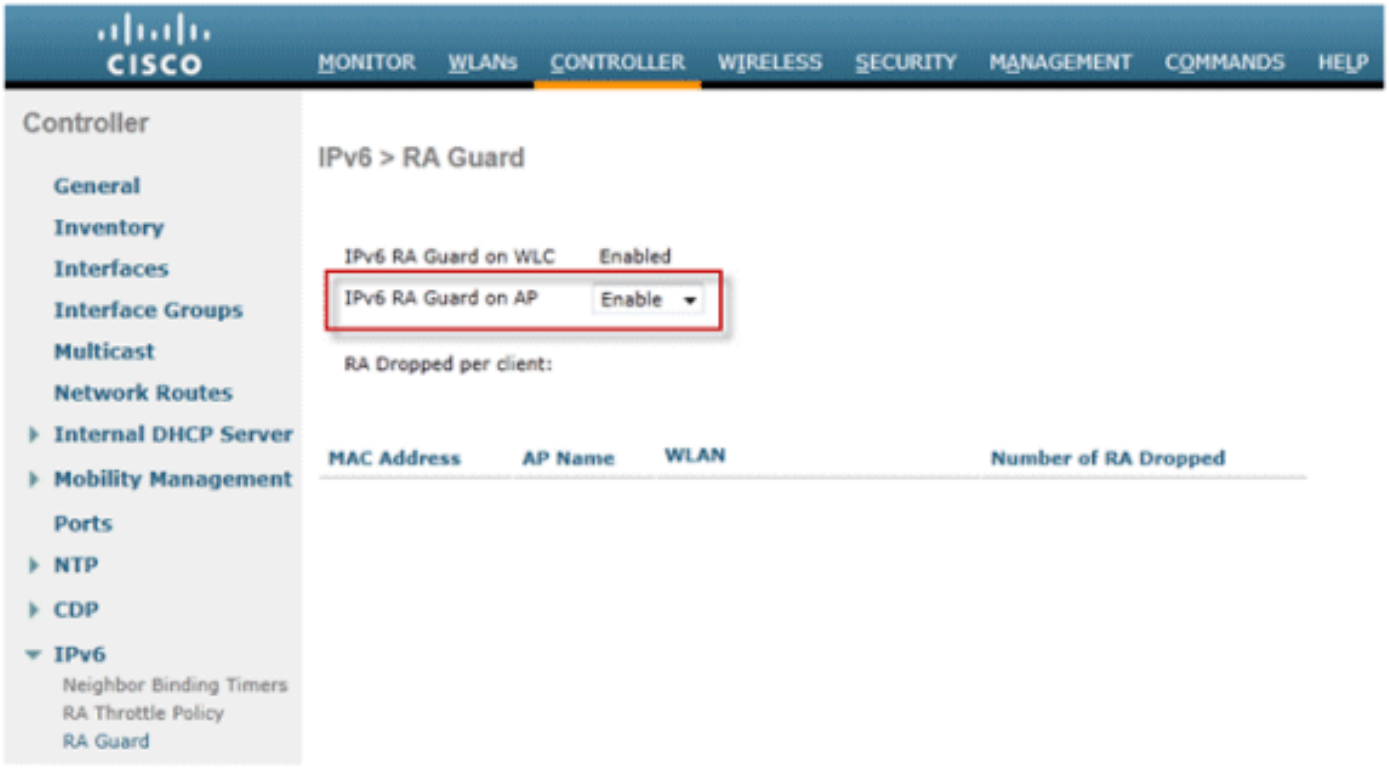
注：AppleのBonjourなどのピアツーピア検出アプリケーションが必要な場合は、グローバルマルチキャストモード、IGMP、およびMLDスヌーピングを有効にする必要があります。

2. IPv6 マルチキャスト トラフィックがスヌーピングされていることを確認するには、[Monitor] タブと [Multicast] ページに移動します。IPv4 (IGMP) と IPv6 (MLD) マルチキャスト グループの両方がリストされていることを確認します。MGID をクリックし、そのグループ アドレスに加入しているワイヤレス クライアントを表示します。



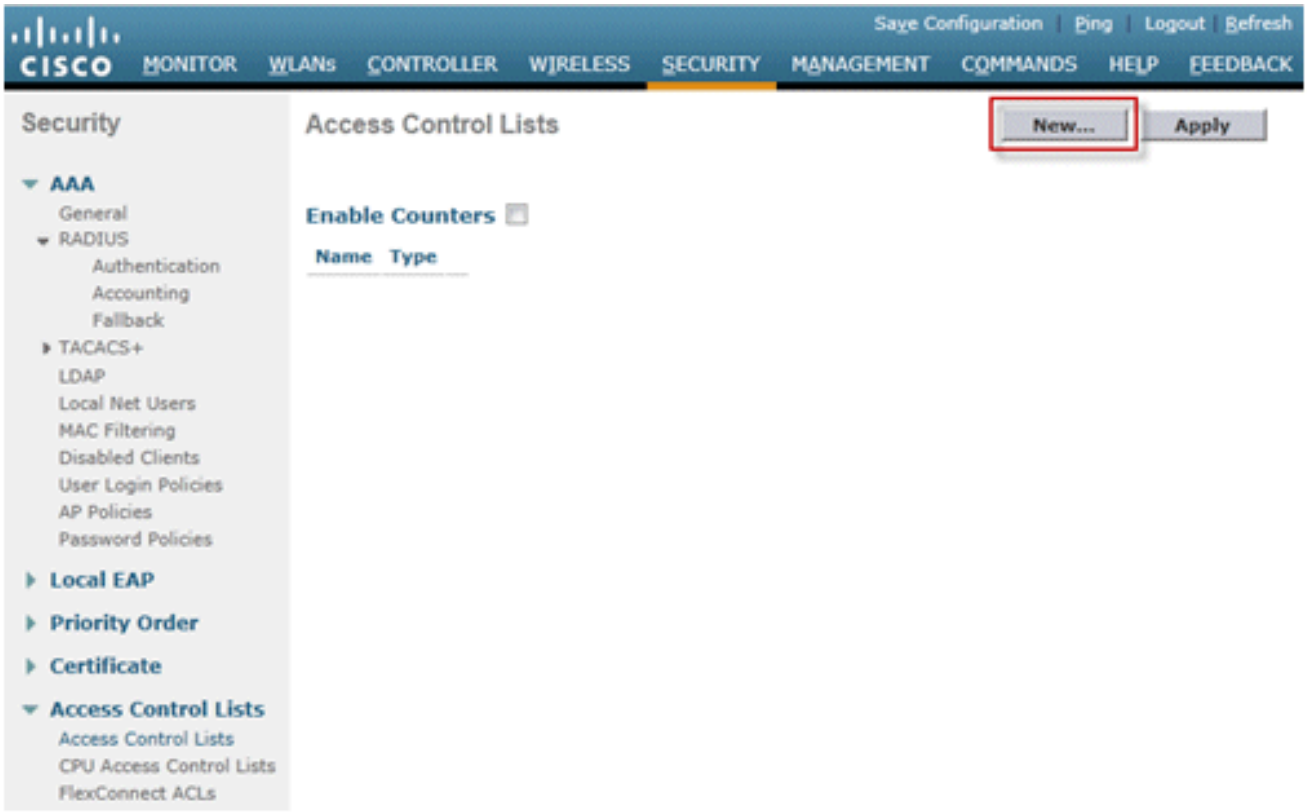
IPv6 RA ガードの設定

[Controller] タブに移動して、左側のメニューから [IPv6] > [RA Guard] に移動します。AP 上で IPv6 RA ガードを [Enable] にします。コントローラの RA ガードは無効にすることができません。RA ガードの設定に加えて、このページには RA の送信元として識別されたクライアントがすべて表示されます。



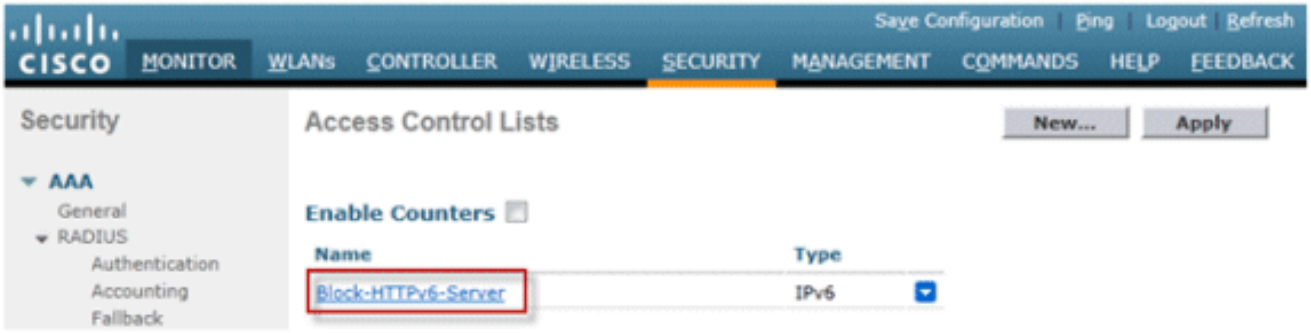
IPv6 アクセス コントロール リストの設定

1. [Security] タブに移動し、[Access Control Lists] を開き、[New] をクリックします。

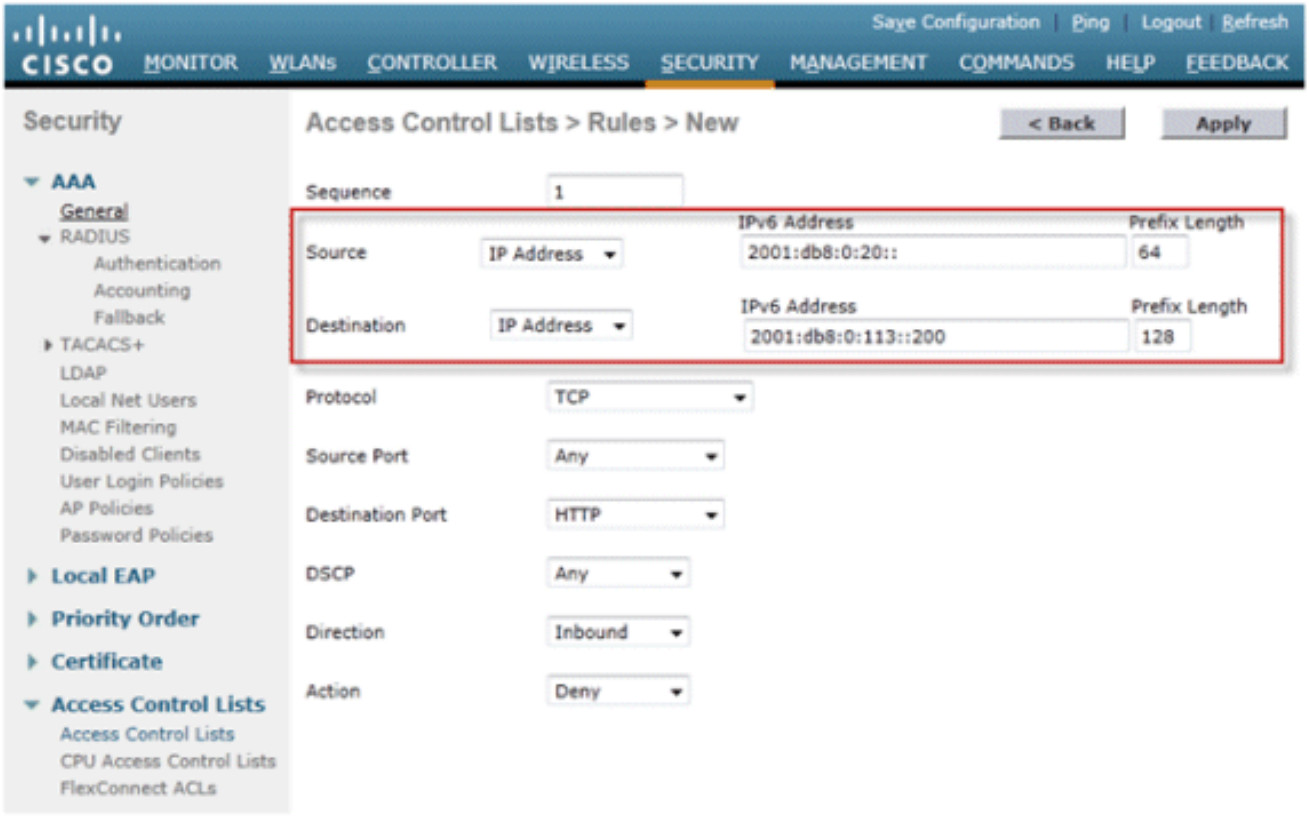


2. ACL の一意の名前を入力し、[ACL Type] を [IPv6] に変更し、[Apply]をクリックします。

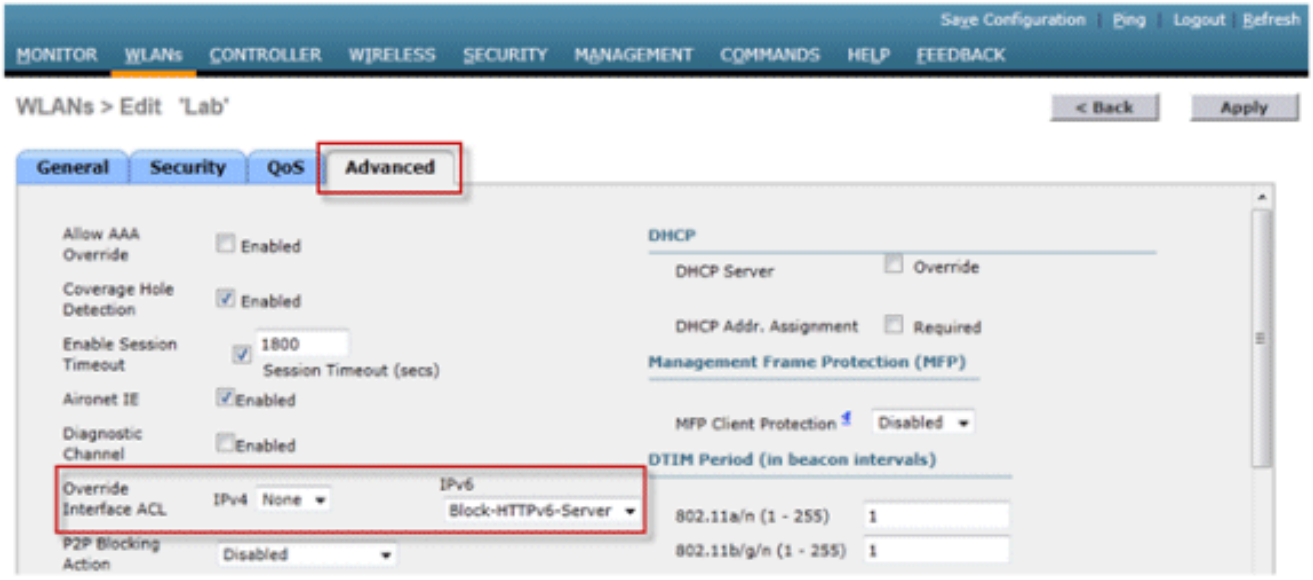
3. 上記の手順で作成した新しい ACL をクリックします。



4. [Add New Rule] をクリックし、ルールに必要なパラメータを入力し、[Apply] をクリックします。リストの最後にルールを配置するため、シーケンス番号は空白のままにします。[Inbound] の [Direction] オプションはワイヤレス ネットワークからのトラフィック、[Outbound] はワイヤレス クライアントに向かうトラフィックに使用します。ACL の最後のルールは、「すべてを暗黙的に拒否」であることに注意してください。IPv6 サブネット全体を照合するには 64 のプレフィックス長を使用し、個別のアドレスにアクセスを一義的に制限するには 128 のプレフィックス長を使用します。

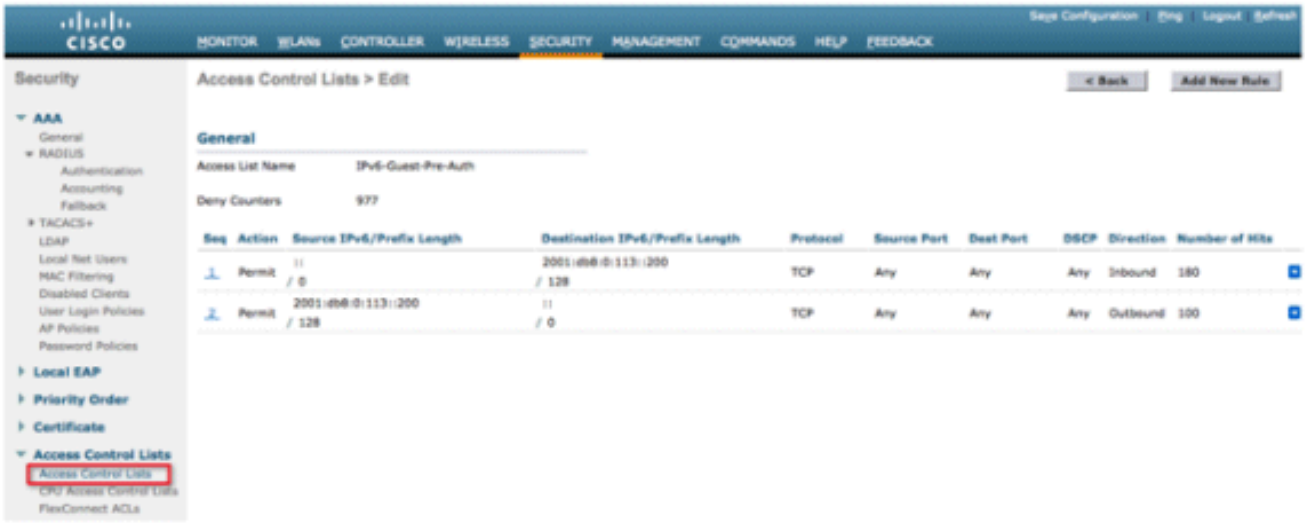


5. IPv6 ACL は WLAN/SSID 単位で適用され、複数の WLAN 上で同時に使用できます。[WLANs] タブに移動し、問題の [SSID] の [WLAN ID] をクリックし、IPv6 ACL を適用します。[Advanced] をクリックし、IPv6 の [Override Interface ACL] を ACL の名前に変更します。



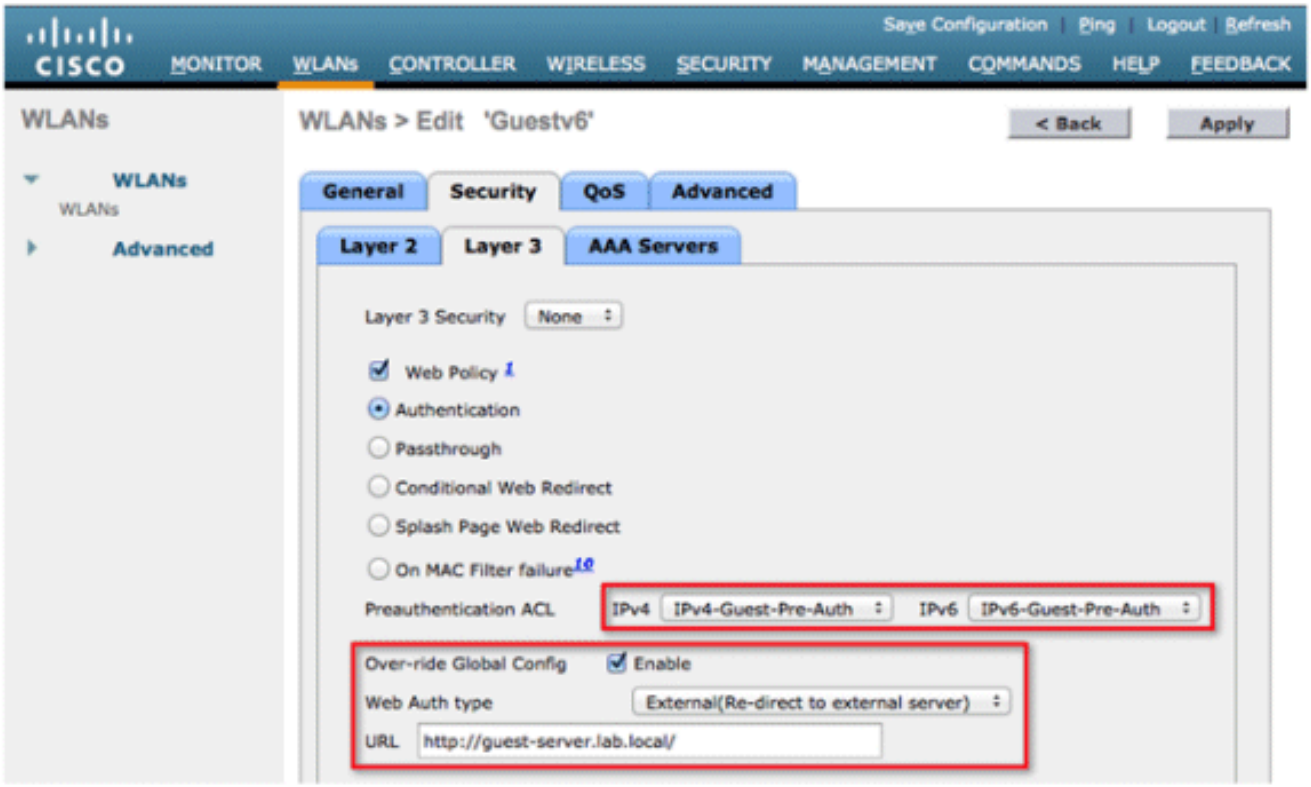
外部 Web 認証用の IPv6 ゲストアクセスの設定

1. Web サーバ用に IPv4 および IPv6 事前認証 ACL を設定します。これは、クライアントが完全に認証される前に外部サーバとの間のトラフィックの送受信を可能にします。



外部 Web アクセスの動作の詳細については、『ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例』を参照してください。

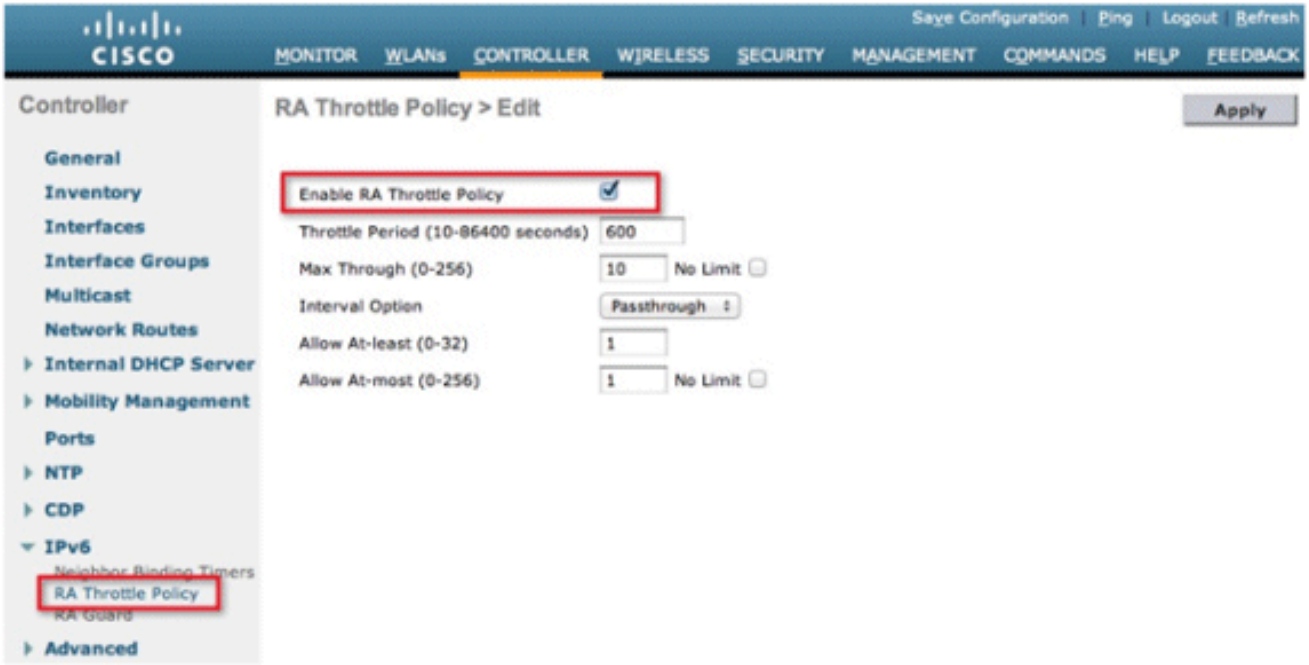
2. 上部の [WLANs] タブに移動し、ゲスト WLAN を設定します。ゲスト SSID を作成し、レイヤ 3 Web ポリシーを使用します。ステップ 1 で定義した事前認証 ACL が IPv4 および IPv6 に選択されています。[Over-ride Global Config] セクションにチェックマークを付け、[Web Auth type] ドロップダウン ボックスから [External] を選択します。Web サーバの URL を入力します。外部サーバのホスト名は、IPv4 および IPv6 DNS で解決可能である必要があります。



IPv6 RA スロットリングの設定

1. トップレベルの [Controller] メニューに移動して、左側の [IPv6] > [RA Throttle Policy] オプ

ションをクリックします。チェックボックスをクリックし、RA スロットリングを有効にします。



注：RAスロットリングが発生すると、最初のIPv6対応ルータのみが通過を許可されます。異なるルータでサービスされる複数の IPv6 プレフィックスがあるネットワークでは、RA にスロットリングを無効にする必要があります。

2. スロットル期間およびその他のオプションは、TAC からアドバイスされた場合にのみ調整します。ただし、ほとんどの導入ではデフォルト値が推奨されます。RA スロットリング ポリシーのさまざまな設定オプションは、次を考慮して設定する必要があります。

    - [Allow At-least] の数値は、[Max Through] よりも小さい [Allow At-most] 以下の数値にする必要があります。
    - RA スロットル ポリシーは、ほとんどの RA のデフォルトのライフタイムである 1800 秒以上のスロットル期間を使用すべきではありません。

RA スロットリングの各オプションは、次のとおりです。

- Throttle Period：スロットリングが実行される期間。RA スロットリングは、VLAN の [Max Through] 制限に到達した後にのみ有効になります。
- Max Through：これは、スロットリングが実行される前の VLAN ごとの RA の最大数です。[No Limit] オプションは、スロットリングを使用せずに、無制限の量の RA を許可します。
- Interval Option：間隔オプションは、IPv6 RA の RFC 3775 値セットに基づいてコントローラが異なる動作をするようにします。
    - Passthrough：この値は RFC3775 間隔オプションがある RA がスロットリングを使用せずに通過できるようにします。
    - Ignore：この値により、RA スロットルは間隔オプションがあるパケットを通常の RA

として処理し、有効な場合はスロットリングの対象とします。

- Throttle：この値により、間隔オプションがある RA は必ずレート制限の対象となります。

- Allow At-least：マルチキャストとして送信されるルータあたりの RA の最小数です。
- Allow At-most：スロットリングが実行される前にマルチキャストとして送信されるルータあたりの RA の最大数です。[No Limit] オプションは、そのルータに無制限の数の RA を許可します。

IPv6 ネイバー バインディング テーブルの設定

1. トップレベルの [Controller] メニューに移動して、左側のメニューで [IPv6] > [Neighbor Binding Timers] オプションをクリックします。

2. 必要に応じて、[Down Lifetime]、[Reachable Lifetime]、および [Stale Lifetime] を調整します。モバイル性の高いクライアントを使用する導入では、古いアドレス タイマーのタイマーを調整する必要があります。次に、推奨される値を示します。

   - Down Lifetime：30 秒
   - Reachable Lifetime：300 秒
   - State Lifetime：86400 秒

   各ライフタイムのタイマーは、IPv6 アドレスの状態を示します。

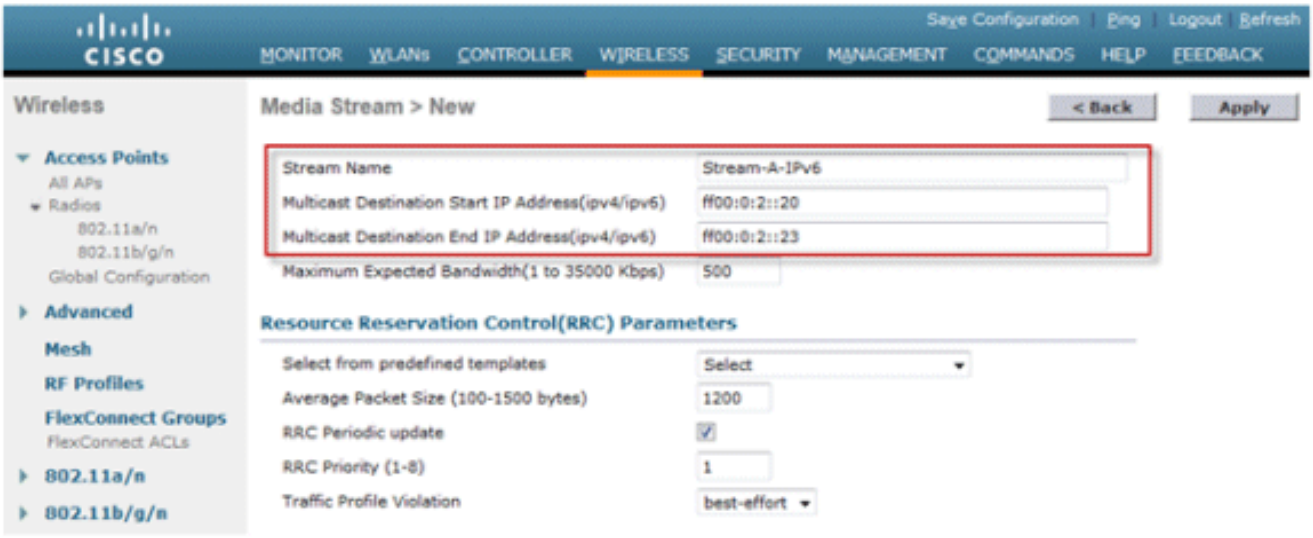
   - Down Lifetime：ダウン タイマーは、コントローラのアップリンク インターフェイスがダウンした場合に、IPv6 キャッシュ エントリを保持する期間を指定します。
   - Reachable Lifetime：このタイマーは、IPv6 アドレスがアクティブとしてマーキングされる期間を指定します。これは、このアドレスから最近トラフィックが受信されたことを意味します。このタイマーの期限が切れると、アドレスは「古い」状態に移行します。
   - Stale Lifetime：このタイマーは、[Reachable Lifetime] から表示されなくなった IPv6 アドレスをキャッシュに保持する期間を指定します。このライフタイムが終了すると、アドレスはバインディング テーブルから削除されます。

IPv6 VideoStream の設定

1. コントローラでグローバル VideoStream 機能が有効になっていることを確認します。802.11a/g/nネットワークおよびWLAN SSIDでVideoStreamを有効にする方法については、『Cisco Unified Wireless Networkソリューション：VideoStream導入ガイド』を参照してください。

2. コントローラの [Wireless] タブに移動し、[Media Stream] > [Streams] の順に選択します。[Add New] をクリックして新しいストリームを作成します。

3. ストリームに名前を付け、最初と最後の IPv6 アドレスを入力します。1 つのストリームのみを使用する場合、最初と最後のアドレスは同じです。アドレスの追加後、[Apply] をクリックしてストリームを作成します。



IPv6 クライアント接続のトラブルシューティング

特定のクライアントが IPv6 トラフィックを渡せない

一部のクライアント IPv6 ネットワーキング スタックの実装では、ネットワークにアクセスする際に自分自身を正しくアナウンスしないため、ネイバー バインディング テーブルで配置のためにコントローラによって適切にスヌープされません。ネイバー バインディング テーブルに存在しないアドレスはすべて、IPv6 ソース ガード機能によりブロックされます。これらのクライアントがトラフィックを渡すには、次のオプションを設定する必要があります。

1. CLI を介して IPv6 ソース ガード機能を無効にします。

```
<#root>

config network ip-mac-binding disable
```

2. CLI を介してマルチキャスト ネイバー要請の転送を有効にします。

```
<#root>

config ipv6 ns-mcast-fwd enable
```

IPv6 クライアントのレイヤ 3 ローミングに成功したことを確認する

アンカー コントローラと外部コントローラの両方で次の debug コマンドを発行します。

<#root>

debug client

<#root>

debug mobility handoff enable

<#root>

debug mobility packet enable

アンカー コントローラでの debug の結果：

<#root>

```
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Complete to
  Mobility-Incomplete
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Setting handles to 0x00000000
00:21:6a:a7:4f:ee pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE =
  0.
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Deleted mobile LWAPP rule on AP
  [04:fe:7f:49:03:30]
00:21:6a:a7:4f:ee Updated location for station old AP 04:fe:7f:49:03:30-1, new
  AP 00:00:00:00:00:00-0
00:21:6a:a7:4f:ee Stopping deletion of Mobile Station: (callerId: 42)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Incomplete to
  Mobility-Complete, mobility role=Anchor, client state=APF_MS_STATE_ASSOCIATED
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 4968
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Adding Fast Path rule type = Airespace AP
  Client on AP 00:00:00:00:00:00, slot 0, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IPv6 ACL ID = 255,
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP =
  0, TokenID = 7006  Local Bridging Vlan = 20, Local Bridging intf id = 13
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID
  255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee 0.0.0.0 Removed NPU entry.

00:21:6a:a7:4f:ee Set symmetric mobility tunnel for 00:21:6a:a7:4f:ee as in
  Anchor role

00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 1, dtlFlags 0x1

00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
```

```
00:21:6a:a7:4f:ee 0.0.0.0, VLAN Id 20 Not sending gratuitous ARP
00:21:6a:a7:4f:ee Copy AP LOCP - mode:0 slotId:0, apMac 0x0:0:0:0:0:0
00:21:6a:a7:4f:ee Copy WLAN LOCP EssIndex:3 aid:0 ssid:    Roam
00:21:6a:a7:4f:ee Copy Security LOCP ecypher:0x0 ptype:0x2, p:0x0, eaptype:0x6
  w:0x1 aalg:0x0, PMState:        RUN
00:21:6a:a7:4f:ee Copy 802.11 LOCP a:0x0 b:0x0 c:0x0 d:0x0 e:0x0 protocol2:0x5
  statuscode 0, reasoncode 99, status 3
00:21:6a:a7:4f:ee Copy CCX LOCP 4
00:21:6a:a7:4f:ee Copy e2e LOCP 0x1
00:21:6a:a7:4f:ee Copy MobilityData LOCP status:2, anchorip:0xac14e2c6
00:21:6a:a7:4f:ee Copy IPv6 LOCP: fe80::3057:534d:587d:73ae
```

外部コントローラでの debug の結果：

<#root>

```
00:21:6a:a7:4f:ee Adding mobile on LWAPP AP f0:25:72:3c:0f:20(1)
00:21:6a:a7:4f:ee Reassociation received from mobile on AP f0:25:72:3c:0f:20
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Changing IPv4 ACL 'none' (ACL ID 255) ===>
  'none' (ACL ID 255) --- (caller apf_policy.c:1697)
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Changing IPv6 ACL 'none' (ACL ID 255) ===>
  'none' (ACL ID 255) --- (caller apf_policy.c:1864)
00:21:6a:a7:4f:ee Applying site-specific Local Bridging override for station
  00:21:6a:a7:4f:ee - vapId 3, site 'default-group', interface 'client-b1'
00:21:6a:a7:4f:ee Applying Local Bridging Interface Policy for station
  00:21:6a:a7:4f:ee - vlan 25, interface id 12, interface 'client-b1'
00:21:6a:a7:4f:ee processSsidIE  statusCode is 0 and status is 0
00:21:6a:a7:4f:ee processSsidIE  ssid_done_flag is 0 finish_flag is 0
00:21:6a:a7:4f:ee STA - rates (8): 140 18 152 36 176 72 96 108 0 0 0 0 0 0 0 0
*apfMsConnTask_4: Jan 22 20:37:45.370: 00:21:6a:a7:4f:ee suppRates  statusCode
  is 0 and gotSuppRatesElement is 1
00:21:6a:a7:4f:ee Processing RSN IE type 48, length 22 for mobile
  00:21:6a:a7:4f:ee
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Initializing policy
00:21:6a:a7:4f:ee 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state
  AUTHCHECK (2)
00:21:6a:a7:4f:ee 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last
  state 8021X_REQD (3)
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) DHCP Not required on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3for this client
00:21:6a:a7:4f:ee Not Using WMM Compliance code qosCap 00
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rule on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3
00:21:6a:a7:4f:ee apfMsAssoStateInc
00:21:6a:a7:4f:ee apfPemAddUser2 (apf_policy.c:268) Changing state for mobile
  00:21:6a:a7:4f:ee on AP f0:25:72:3c:0f:20 from Idle to Associated
00:21:6a:a7:4f:ee Scheduling deletion of Mobile Station:  (callerId: 49) in 1800
  seconds
00:21:6a:a7:4f:ee Sending Assoc Response to station on BSSID f0:25:72:3c:0f:20
  (status 0) ApVapId 3 Slot 1
00:21:6a:a7:4f:ee apfProcessAssocReq (apf_80211.c:6290) Changing state for
  mobile 00:21:6a:a7:4f:ee on AP f0:25:72:3c:0f:20 from Associated to Associated
<…SNIP…>
00:21:6a:a7:4f:ee 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last
  state L2AUTHCOMPLETE (4)
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) DHCP Not required on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3for this client
00:21:6a:a7:4f:ee Not Using WMM Compliance code qosCap 00
```

```
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP
  f0:25:72:3c:0f:20 vapId 3 apVapId 3
00:21:6a:a7:4f:ee 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last
  state DHCP_REQD (7)
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 5253, Adding TMP rule
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP f0:25:72:3c:0f:20, slot 1, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IP
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0,
  DSCP = 0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id =
  12
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4
  ACL ID 255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee Stopping retransmission timer for mobile 00:21:6a:a7:4f:ee
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
00:21:6a:a7:4f:ee Sent an XID frame
00:21:6a:a7:4f:ee Username entry () already exists in name table, length = 253
00:21:6a:a7:4f:ee Username entry () created in mscb for mobile, length = 253
00:21:6a:a7:4f:ee Applying post-handoff policy for station 00:21:6a:a7:4f:ee -
  valid mask 0x1000
00:21:6a:a7:4f:ee QOS Level: -1, DSCP: -1, dot1p: -1, Data Avg: -1, realtime
  Avg: -1, Data Burst -1, Realtime Burst -1
00:21:6a:a7:4f:ee     Session: -1, User session: -1, User elapsed -1 Interface:
  N/A, IPv4 ACL: N/A, IPv6 ACL:
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Change state to DHCP_REQD (7) last state
  DHCP_REQD (7)
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) pemCreateMobilityState 6370, Adding TMP
  rule
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule type =
  Airespace AP - Learn IP address on AP f0:25:72:3c:0f:20, slot 1, interface =
  13, QOS = 0 IPv4 ACL ID = 255,
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0,
  DSCP = 0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id =
  12
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4
  ACL ID 255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee Scheduling deletion of Mobile Station:  (callerId: 55) in 1800
  seconds
00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee apfMsRunStateInc
00:21:6a:a7:4f:ee 0.0.0.0 DHCP_REQD (7) Change state to RUN (20) last state RUN
  (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 5776
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!

00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) State Update from Mobility-Incomplete to
  Mobility-Complete, mobility role=Foreign, client state=APF_MS_STATE_ASSOCIATED

00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Change state to RUN (20) last state RUN (20)
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Reached PLUMBFASTPATH: from line 4968
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Replacing Fast Path rule
  type = Airespace AP Client
  on AP f0:25:72:3c:0f:20, slot 1, interface = 13, QOS = 0
  IPv4 ACL ID = 255, IPv6 ACL ID = 25
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Fast Path rule (contd...) 802.1P = 0, DSCP =
  0, TokenID = 7006  Local Bridging Vlan = 25, Local Bridging intf id = 12
00:21:6a:a7:4f:ee 0.0.0.0 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID
  255, IPv6 ACL ID 255)
00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
```

```
00:21:6a:a7:4f:ee Set symmetric mobility tunnel for 00:21:6a:a7:4f:ee as in
  Foreign role

00:21:6a:a7:4f:ee 0.0.0.0 Added NPU entry of type 1, dtlFlags 0x1

00:21:6a:a7:4f:ee Pushing IPv6: fe80:0000:0000:0000: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!
00:21:6a:a7:4f:ee Pushing IPv6: 2001:0db8:0000:0020: 3057:534d:587d:73ae , and
  MAC: 00:21:6A:A7:4F:EE , Binding to Data Plane. SUCCESS !!

00:21:6a:a7:4f:ee Copy AP LOCP - mode:0 slotId:1, apMac 0xf0:25:72:3c:f:20
00:21:6a:a7:4f:ee Copy WLAN LOCP EssIndex:3 aid:1 ssid:    Roam
00:21:6a:a7:4f:ee Copy Security LOCP ecypher:0x0 ptype:0x2, p:0x0, eaptype:0x6
  w:0x1 aalg:0x0, PMState:        RUN
00:21:6a:a7:4f:ee Copy 802.11 LOCP a:0x0 b:0x0 c:0x0 d:0x0 e:0x0 protocol2:0x7
  statuscode 0, reasoncode 99, status 3
00:21:6a:a7:4f:ee Copy CCX LOCP 4
00:21:6a:a7:4f:ee Copy e2e LOCP 0x1
00:21:6a:a7:4f:ee Copy MobilityData LOCP status:3, anchorip:0xac14e2c5
00:21:6a:a7:4f:ee Copy IPv6 LOCP: fe80::3057:534d:587d:73ae
00:21:6a:a7:4f:ee Copy IPv6 LOCP: 2001:db8:0:20:3057:534d:587d:73ae
```

便利な IPv6 CLI コマンド

<#root>

```
Show ipv6 neighbor-binding summary
```

<#root>

```
Debug ipv6 neighbor-binding filter client


        enable
```

<#root>

```
Debug ipv6 neighbor-binding filter errors enable
```

よく寄せられる質問（FAQ）

Q：ブロードキャストドメインを制限するために最適なIPv6プレフィクスサイズは何ですか。

A: IPv6サブネットは/64以下に分割できますが、この設定ではSLAACが崩れ、クライアント接続の問題が発生します。ホストの数を減らすためにセグメンテーションが必要な場合は、インターフェイス グループ機能を使用し、それぞれが異なる IPv6 プレフィックスを使用する異なるバックエンド VLAN 間でクライアントをロード バランスすることができます。

Q: IPv6クライアントのサポートに関して、拡張性の制限はありますか。

A:IPv6クライアントのサポートに関する主な拡張性の制限は、すべてのワイヤレスクライアントのIPv6アドレスを追跡するネイバーバインディングテーブルです。このテーブルは、8 (クライアントあたりのアドレスの最大数) で乗算されたクライアントの最大数をサポートするためにコントローラ プラットフォームごとに拡張されます。IPv6 バインディング テーブルの追加は、プラットフォームによってはコントローラのメモリ使用量を全負荷の約 10 ~ 15% に増加させることがあります。

ワイヤレス コントローラ	クライアントの最大数	IPv6 ネイバー バインディング テーブルのサイズ
2500	500	4,000
5500	7,000	56,000
WiSM2	15,000	120,000

Q : コントローラのCPUとメモリに対するIPv6機能の影響は何ですか。

A:CPUにはコントロールプレーンを処理するための複数のコアがあるため、影響は最小限です。それぞれに 8 個の IPv6 アドレスがある、サポートされている最大数のクライアントでテストしたときの CPU 使用率は 30% 未満、メモリ使用率は 75% 未満でした。

Q: IPv6クライアントのサポートを無効にできますか。

A:ネットワークでIPv4のみを有効にしてIPv6をブロックしたいお客様は、deny-allトラフィックのIPv6 ACLを使用してWLANごとに適用できます。

Q:IPv4用とIPv6用にそれぞれ1つのWLANを設定することは可能ですか。

A:同じAPで動作する2つの異なるWLANに対して、同じSSID名とセキュリティタイプを設定することはできません。IPv6 クライアントからの IPv4 クライアントのセグメンテーションには、2 つの WLAN を作成する必要があります。各 WLAN は、すべての IPv4 または IPv6 トラフィックをそれぞれブロックする ACL で設定する必要があります。

Q : クライアントごとに複数のIPv6アドレスをサポートすることが重要なのはなぜですか。

A:クライアントは、インターフェイスごとに複数のIPv6アドレスを持つことができます。これらのアドレスは、常に自己割り当てのリンクローカルアドレスを持つことに加えて、スタティック、SLAAC、またはDHCPv6を割り当てることができます。クライアントは、異なる IPv6 プレフィックスを使用して追加アドレスを持つことができます。

Q: IPv6プライベートアドレスとは何ですか。また、追跡が重要なのはなぜですか。

A : プライベート (一時アドレスとも呼ばれます) アドレスは、SLAACアドレス割り当てが使用されるときにクライアントによってランダムに生成されます。これらのアドレスは通常、同じホストのポストフィックス (最後の 64 ビット) を常時使用することによるホストの追跡可能性を回避するために、1 日程度の頻度でローテーションされます。著作権の侵害のトレースなどの監視目的で、これらのプライベート アドレスを追跡することが重要です。Cisco NCS は、各クライ

アントで使用されているすべての IPv6 アドレスを記録し、クライアントがローミングされたり、新しいセッションが確立されたりするたびに、その履歴を口グに記録します。これらのレコードは、NCS で最大 1 年間保持するように設定できます。

関連情報

- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。