IPv6

IPv6 モビリティについて

インターネットプロトコルバージョン6（IPv6）は、プロトコルのTCP/IPスイートのバージョン4（IPv4）の後継となることを意図された次世代のネットワーク層インターネットプロトコルです。この新しいバージョンでは、一意なグローバルIPアドレスを必要とするユーザとアプリケーションを収容するためのインターネット グローバル アドレス空間が拡張されています。IPv6は、128ビットの送信元アドレスおよび宛先アドレスを組み込むことにより、32ビットのIPv4アドレスよりも格段に多くのアドレスを提供します。

コントローラをまたいだIPv6クライアントをサポートするには、IPv6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ように、ICMPv6メッセージを特別に処理する必要があります。コントローラは、ICMPv6メッセージを代行受信することでIPv6クライアントを追跡し、シームレスなモビリティを提供して、ネットワーク攻撃からネットワークを保護します。ICMPv6パケットは、マルチキャストからユニキャストに変換され、クライアントごとに個別に配信されます。このプロセスによって、より詳細な制御が可能になります。特定のクライアントは、特定のネイバーディスカバリ パケットおよびルータ アドバタイズメント パケットを受信することでIPv6アドレス指定が適切であることを確認し、不要なマルチキャスト トラフィックを回避します。

IPv6モビリティの設定は、IPv4モビリティと同一であり、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。コントローラは、同じモビリティ グループに属している必要があります。IPv4とIPv6の両クライアント モビリティが、デフォルトで有効になります。

IPv6 モビリティを設定するための前提条件

- クライアントごとに最大 8 個のクライアント アドレスを追跡できます。
- ステートフル DHCPv6 IP アドレス指定を正常に動作させるには、DHCPv6 サーバとして機能するように設定された、DHCP for IPv6 機能をサポートするスイッチまたはルータを設置する必要があります。または、組み込みの DHCPv6 サーバを備えた、Windows 2008 サーバなどの専用サーバが必要です。

シームレスな IPv6 モビリティをサポートするには、次の設定が必要になる場合があります。

- IPv6 クライアントのための RA ガードの設定
- IPv6 クライアントのための RA スロットリングの設定
- IPv6 ネイバー ディスカバリ キャッシングの設定

IPv6 モビリティの設定の制約事項

- クライアントは、スタティック ステートレス自動設定（Windows XP クライアントなど）またはステートフル DHCPv6 IP アドレス指定（Windows Vista クライアントなど）のいずれかで IPv6 をサポートする必要があります。

（注） 現在、Windows Vista では、スタティック ステートレス自動設定機能を提供していません。したがって、シームレスなローミングには DHCPv6 が必要です。DHCPv6 を使用しない場合、VLAN を変更するたびにこれらのクライアントを手動で更新する必要があります。

（注） IPv6 のダイナミック VLAN 機能はサポートされていません。

- タグなしインターフェイスにマッピングされている WLAN に関連付けられた IPv6 クライアントが、タグなしインターフェイスにマッピングされている別の WLAN にローミングすることはサポートされていません。
- 7.4 リリースでは、同じモビリティ グループ、同じ VLAN ID、および異なる IPv4 および IPv6 サブネットがある WLC は、それぞれの IPv6 ルータ アドバタイズメントを生成します。これらの WLC の WLAN は、すべてのコントローラで同じ VLAN ID を持つ同じ動的インターフェイスに割り当てられます。クライアントは正しい IPv4 アドレスを受信します。ただし他の WLC に到達する別のサブネットからルータ アドバタイズメントを受信します。クライアントに最初に渡された IPv6 アドレスが IPv4 アドレスのサブネットに一致

しないため、クライアントからのトラフィックがないという問題が生じる可能性があります。これを解決するために、異なるモビリティ グループの WLC を設定できます。

（注） IPv6 モビリティ ピアの追加または削除時に、トラフィックをバイパスするための SSH ルールが 16666 ポートおよびモビリティ ピアの IP ペアに適用されます。

- Flex ローカル スイッチングを備えた WLAN で AAA Override が有効になっている場合、クライアントは、AAA サーバから返された IPv6 アドレスを VLAN から受け取る必要があります。これは、ローカル スイッチングと AAA オーバーライドの両方が有効になっている WLAN が VLAN X にマッピングされ、 AAA サーバが VLAN Y を返す場合は、クライアントが VLAN Y からアドレスを受信する必要があることを意味します。ただし、このコントローラ リリースではサポートされません。

（注） クライアントが管理サブネット上にある場合、Cisco WLC からクライアントへの IPv6 ping はサポートされていません。

- Cisco WLC は、ホストが同じサブネットにある場合でも、すべてのアプリケーションの IPv6 トラフィックをゲートウェイに送信します。ゲートウェイは、同じサブネットにあるホストにトラフィックを転送します。ゲートウェイが Cisco ASA で、トラフィックを同じサブネットに送信する必要がある場合、デフォルトでは、Cisco ASA は Cisco WLC からゲートウェイに送信されたトラフィックをドロップします。これは、トラフィックの入力と出力のインターフェイスが同じためです。Cisco ASA にこのトラフィックの転送を許可させるには、Cisco ASA で **same-security-traffic permit intra-interface** コマンドを使用します。詳細については、https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/vpn/asa-vpn-cli/vpn-params.html#56144を参照してください。

IPv6 のグローバルな設定

グローバル IPv6 の制約事項

- IPv6 アドレスを設定する前に、インターフェイスに IPv4 アドレスを設定する必要があります。

IPv6 のグローバルな設定（GUI）

手順

ステップ 1 **[Controller]** > **[General]** を選択します。
ステップ 2 [Global IPv6 Config] ドロップダウン リストから、[Enabled] または [Disabled] を選択します。
ステップ 3 [Apply] をクリックします。
ステップ 4 [Save Configuration] をクリックします。

IPv6 のグローバルな設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	次のコマンドを入力して、IPv6 をグローバルに有効または無効にします。	**config ipv6** {**enable** | **disable**}

IPv6 クライアントのための RA ガードの設定

RA ガードについて

IPv6 クライアントは、IPv6 アドレスを設定し、IPv6 ルータ アドバタイズメント（RA）パケットに基づいてルータ テーブルにデータを入力します。RA ガード機能は、有線ネットワークの RA ガード機能に類似しています。RA ガードは、ワイヤレス クライアントから発信される不要な、または不正な RA パケット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。この機能が設定されていないと、悪意のある IPv6 クライアントが、それ自体をネットワークのルータとして通知する可能性があり、そのため、正規の IPv6 ルータよりも優先されることになります。

RA ガードは、コントローラで実行されます。アクセス ポイントまたはコントローラで RA メッセージをドロップするように、コントローラを設定できます。デフォルトでは、RA ガードはアクセスポイントで設定され、コントローラでも有効になります。すべての IPv6 RA メッセージがドロップされ、それによって他のワイヤレスクライアントおよびアップストリーム有線ネットワークが悪意のある IPv6 クライアントから保護されます。

（注）
- IPv6 RA ガード機能が動作するのはワイヤレス クライアントのみです。この機能は、有線ゲスト アクセス（GA ）では動作しません。
- RA ガードは、FlexConnect ローカル スイッチング モードでもサポートしています。

RA ガードの設定（GUI）

手順

ステップ 1 [Controller] > [IPv6] > [RA Guard] を選択して、[IPv6 RA Guard] ページを開きます。デフォルトでは、[IPv6 RA Guard on AP] が有効になります。

ステップ 2 RA ガードを無効にするには、ドロップダウン リストから、[Disable] を選択します。コントローラは、RA パケットの送信側として識別されたクライアントも表示します。

ステップ 3 [Apply] をクリックして、変更を確定します。

ステップ 4 [Save Configuration] をクリックして、変更を保存します。

RA ガードの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	このコマンドを入力して、RA ガードを設定します。	**config ipv6 ra-guard ap** {**enable** | **disable**}

IPv6 クライアントのための RA スロットリングの設定

RA スロットリングについて

RA 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 パケットを強制的に制限できるようにします。RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。クライアントが RS パケットを送信すると、RA がクライアントに返送されます。これは、コントローラを通過でき、クライアントにユニキャストされます。このプロセスによって、新しいクライアントやローミング クライアントが RA スロットリングの影響を受けないようにすることができます。

RA スロットリングの設定（GUI）

手順

ステップ 1 [Controll] > [IPv6] > [RA Throttle Policy] ページを選択します。デフォルトでは、[IPv6 RA Throttle Policy] が無効になります。このチェックボックスをオフにして、RA スロットリング ポリシーを無効にします。

ステップ 2 次のパラメータを設定します。

- [Throttle period]：スロットリングの期間。RA スロットリングは、VLAN に対する [Max Through] 制限に達した後、または特定のルータに対する [Allow At-Most] 値に達した後にのみ実行されます。範囲は 10 ～ 86400 秒です。デフォルトは 600 秒です。
- [Max Through]：スロットリングが実行される前に送信可能な、VLAN 上の RA パケットの最大数。[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 RA パケット数を許可します。範囲は 0 ～ 256 RA パケットです。デフォルトは 10 RA パケットです。
- [Interval Option]：このオプションは、IPv6 RA パケットに設定された RFC 3775 値に基づいた、さまざまなコントローラの動作を許可します。
  - [Passthrough]：RFC 3775 インターバル オプションが指定された RA メッセージが、スロットリングなしで通過することを許可します。
  - [Ignore]：RA スロットルが、インターバル オプションの指定されたパケットを通常の RA として処理し、有効である場合はスロットリングが適用されるようにします。
  - [Throttle]：インターバル オプションが指定された RA パケットに、常にレート制限が適用されるようにします。
- [Allow At-least]：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できる、ルータごとの RA パケットの最小数。範囲は 0 ～ 32 RA パケットです。
- [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できる、ルータごとの RA パケットの最大数。[No Limit] オプションは、ルータの通過する無制限の RA パケット数を許可します。範囲は 0 ～ 256 RA パケットです。

  （注） RA スロットリングが実行されると、最初の IPv6 対応ルータのみの通過が許可されます。異なるルータが複数の IPv6 プレフィックスを処理しているネットワークについては、RA スロットリングを無効にしてください。

ステップ 3 設定を保存します。

RA スロットル ポリシーの設定（CLI）

手順

次のコマンドを入力して、RA スロットル ポリシーを設定します。

config ipv6 neigbhor-binding ra-throttle {**allow at-least** *at-least-value* | **enable** | **disable** | **interval-option** { **ignore** | **passthrough** | **throttle**} | **max-through** {**max-through-value** | **no-limit**}}