



IPv6 クライアントのアドレス ラーニング

- [IPv6 クライアントアドレス ラーニングについて \(1 ページ\)](#)
- [IPv6 クライアントアドレス ラーニングの前提条件 \(5 ページ\)](#)
- [組み込みワイヤレスコントローラ インターフェイスでの IPv6 の設定 \(5 ページ\)](#)
- [ネイティブ IPv6 \(6 ページ\)](#)

IPv6 クライアント アドレス ラーニングについて

クライアント アドレス ラーニングは、ワイヤレスクライアントの IPv4 および IPv6 アドレスを学習し、アソシエーションおよびタイムアウト時に組み込みワイヤレスコントローラによって維持されるクライアント遷移状態を学習するために、組み込みワイヤレスコントローラで設定します。

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定 (SLAAC)
- ステートフル DHCPv6
- 静的設定

これらすべての方法において、IPv6 クライアントは常にネイバー送信要求 DAD (重複アドレス検出) 要求を送信して、ネットワークに重複する IP アドレスがないようにします。組み込みワイヤレスコントローラは、クライアントのネイバー探索プロトコル (NDP) および DHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習します。

SLAAC を使用したアドレス割り当て

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。

SLAAC は次のように設定されます。

- ホストは、ルータ送信要求メッセージを送信します。

- ホストは、ルータ アドバタイズメント メッセージを待機します。
- ホストは、ルータ アドバタイズメント メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、64 ビット EUI-64 アドレス（イーサネットの場合、MAC アドレスから作成）と組み合わせて、グローバルユニキャストメッセージを作成します。ホストは、デフォルトゲートウェイとして、ルータ アドバタイズメントメッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 選択されるランダムアドレスが他のクライアントと競合しないように、IPv6 クライアントによって重複アドレス検出が実行されます。

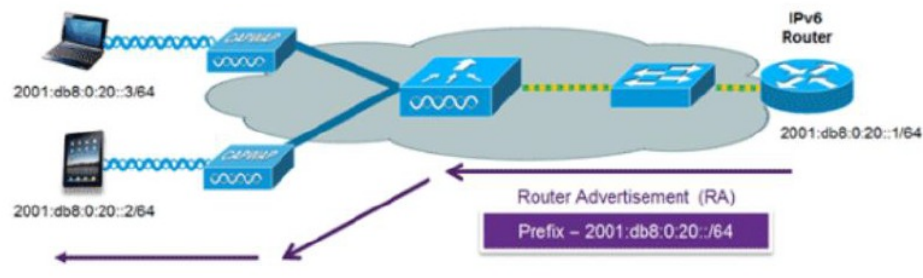


(注) アルゴリズムの選択はクライアントに依存し、多くの場合は設定できます。

IPv6 アドレスの最後の 64 ビットは、次のアルゴリズムに基づいて学習できます。

- インターフェ이스の MAC アドレスに基づく EUI-64
- ランダムに生成されるプライベートアドレス

図 1: SLAAC を使用したアドレス割り当て



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イネーブルにします。

```

ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end

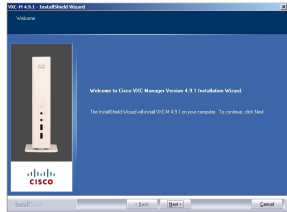
```

ステートフル DHCPv6 アドレス割り当て

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されますが、IPv6 アドレスは、SLAAC によってすでに提供されているため提供されません。情報には、DNS ドメイン名、DNS サーバー、その他の DHCP ベンダー固有のオプションが含まれます。

図 2: ステートフル DHCPv6 アドレス割り当て



このインターフェイス設定は、SLAAC を有効にしてステートレス DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

静的 IP アドレス割り当て

クライアントにスタティックに設定されたアドレス。

ルータ要求

ルータ送信要求メッセージは、コントローラがローカルルーティングに関する情報を入手できる、またはステートレス自動設定を設定できるルータアドバタイズメントを送信するようにローカルルータを促すために、ホストコントローラによって発行されます。ルータアドバタイズメントは定期的に送信され、起動時または再起動操作後などに、ホストはルータ送信要求を使用して即時ルータ アドバタイズメントを要求します。

ルータ アドバタイズメント

ルータ アドバタイズメント メッセージは、ルータから定期的に送信されるか、ホストからのルータ送信要求メッセージへの応答として送信されます。これらのメッセージに含まれる情報は、ホストでステートレス自動設定を実行し、ルーティングテーブルを変更するために使用されます。

ネイバー探索

IPv6 ネイバー ディスカバリとは、近隣のノード間の関係を決定するメッセージとプロセスのことです。ネイバー探索は、IPv4 で使用されていた Address Resolution Protocol (ARP)、Internet Control Message Protocol (ICMP) ルータ探索、および ICMP リダイレクトに代わるものです。

信頼できるバインディング テーブル データベースを構築するために、IPv6 ネイバー探索検査によってネイバー探索メッセージが分析され、準拠しない IPv6 ネイバー探索 パケットはドロップされます。内の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。クライアントは、ネイバーバインディング タイマーに従って、テーブルから消去されます。

ネイバー探索抑制

ワイヤレスクライアントの IPv6 アドレスは、deviceによってキャッシュされます。deviceが IPv6 アドレスを検索する NS マルチキャストを受信して、deviceによって特定された目的のアドレスがクライアントのいずれかに属している場合、deviceはクライアントに代わって NA メッセージで応答します。このプロセスの最後に IPv4 の ARP テーブルと同等のものが生成されますが、使用するメッセージが少ないため、より効率的です。



(注) deviceがプロキシのように動作し NA で応答するのは、`ipv6 nd suppress` コマンドが設定されている場合だけです。

deviceにワイヤレスクライアントの IPv6 アドレスがない場合、deviceは NA で応答せず、NS パケットをワイヤレス側に転送します。この問題を解決するために、NS マルチキャスト フォワーディング ノブが用意されています。このノブがイネーブルの場合、deviceは存在しない (キャッシュ欠落) IPv6 アドレスの NS パケットを取得し、ワイヤレス側に転送します。このパケットは、目的のワイヤレスクライアントに到達し、クライアントは NA で応答します。

このキャッシュミスシナリオが発生するのはまれで、完全な IPv6 スタックが実装されていないクライアントが、NDP 時にそれらの IPv6 アドレスをアドバタイズしない可能性はほとんどありません。

ルータ アドバタイズメント ガード

- フレームが受信されるポート
- IPv6 送信元アドレス
- プレフィックス リスト
- ルータ アドバタイズメント ガード メッセージを受信するための信頼できるポートまたは信頼できないポート
- ルータ アドバタイズメント 送信者の信頼できるまたは信頼できない送信元 IPv6 アドレス

- 信頼できる/信頼できないプレフィックス リストおよびプレフィックス範囲
- ルータプリファレンス

ルータ アドバタイズメント スロットリング

RA スロットリングを使用すると、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ます。RA スロットリングを有効にすると、多数の RA パケットを送信するルータを最小周波数に調整でき、IPv6 クライアントの接続も維持されます。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。この RA 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。

IPv6 クライアント アドレス ラーニングの前提条件

IPv6 クライアントアドレス ラーニングを設定する前に、IPv6 をサポートするように組み込みワイヤレスコントローラクライアントを設定します。

組み込みワイヤレスコントローラインターフェイスでの IPv6 の設定

インターフェイスで IPv6 を設定するには、次の手順に従います。

始める前に

クライアント上の IPv6 および有線インフラストラクチャ上の IPv6 サポートをイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： デバイス# configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	interface GigabitEthernet0 例： デバイス(config)# interface GigabitEthernet0	GigabitEthernet インターフェイスを作成し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	ip address fe80::1 link-local 例： デバイス(config-if)# ip address 198.51.100.1 255.255.255.0 デバイス(config-if)# ipv6 address fe80::1 link-local デバイス(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64 デバイス(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64	リンクローカルオプションを使用して、GigabitEthernet インターフェイスで IPv6 アドレスを設定します。
ステップ 5	ipv6 enable 例： デバイス(config)# ipv6 enable	(任意) GigabitEthernet インターフェイスで IPv6 を有効にします。
ステップ 6	end 例： デバイス(config)# end	インターフェイスモードを終了します。

ネイティブ IPv6

IPv6 について

IPv6 は、デジタル ネットワーク上のデータ、音声、およびビデオ トラフィックの交換に使用されるパケットベースのプロトコルです。IPv6 は IP に基づいていますがアドレス空間が大幅に拡大されており、メインヘッダーと拡張ヘッダーが簡素化されるなどの改善が行われています。IPv6 のアーキテクチャは、既存の IPv4 ユーザーがエンドツーエンドのセキュリティ、Quality Of Service (QoS)、およびグローバルに一意的なアドレスなどのサービスを引き続き利用しながら、簡単に IPv6 へ移行できるように設計されています。拡大された IPv6 アドレス空間により、ネットワークのスケラビリティが可能となり、グローバルな到達可能性が提供されます。



(注) IPv4 アドレスを使用して IPv4 ネットワークで動作する機能は、IPv6 アドレスを使用して IPv6 ネットワークでも動作します。

一般的な注意事項

- IPv6 機能を動作させるため、`ipv6 unicast-routing` コマンドを組み込みワイヤレスコントローラで設定する必要があります。
- ワイヤレス管理インターフェイスには、スタティック IPv6 アドレスを 1 つだけ設定する必要があります。
- ワイヤレス管理インターフェイスおよびクライアント VLAN でルータアドバタイズメントを抑制する必要があります (IPv6 がクライアント VLAN で設定されている場合)。
- 優先モードは、AP 接続プロファイルに含まれます。優先モードを IPv6 として設定すると、AP は最初に IPv6 を介した接続を試みます。無効にしなかった場合、AP は IPv4 にフォールバックします。
- AP およびクライアントの RA トレースには MAC アドレスを使用する必要があります。

サポートされない機能

- UDP Lite はサポートされていません。
- IPv6 を介した AP スニッファはサポートされていません。
- IPv6 は、HA ポート インターフェイスではサポートされていません。
- IPv6 を介した自動 RF グループ化はサポートされていません。静的 RF グループ化のみがサポートされます。

IPv6 アドレッシングの設定

IPv6 アドレッシングを設定するには、次の手順に従います。



- (注) IPv4 アドレスを使用して IPv4 ネットワークで動作する機能はすべて、IPv6 アドレスを使用して IPv6 ネットワークでも動作します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ipv6 unicast-routing 例： Device(config)# ipv6 unicast-routing	ユニキャスト用に IPv6 を設定します。

	コマンドまたはアクション	目的
ステップ 3	interface GigabitEthernet0 例 : デバイス(config)# interface GigabitEthernet0	GigabitEthernet インターフェイスを作成し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	ipv6 address ipv6-address 例 : Device(config-if)# ipv6 address FD09:9:2:49::53/64	グローバル IPv6 アドレスを指定します。
ステップ 5	ipv6 enable 例 : Device(config-if)# ipv6 enable	インターフェイス上で IPv6 をイネーブルにします。
ステップ 6	ipv6 nd ra suppress all 例 : Device(config-if)# ipv6 nd ra suppress all	インターフェイス上で IPv6 ルータ アドバタイズメントの送信を抑制します。
ステップ 7	exit 例 : Device(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	wireless management interface gigabitEthernet gigabitEthernet-interface-vlan 64 例 : Device(config)# wireless management interface gigabitEthernet vlan 64	ワイヤレス管理インターフェイスで、サポートされている AP に接続されているポートを設定します。
ステップ 9	ipv6 route ipv6-address 例 : Device(config)# ipv6 route ::/0 FD09:9:2:49::1	IPv6 スタティックルートを指定します。

AP 接続プロファイルの作成 (GUI)

手順

- ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。
- ステップ 2 [AP Join Profile] ウィンドウで [General] タブをクリックし、[Add] をクリックします。
- ステップ 3 [Name] フィールドに、AP 接続プロファイルの名前を入力します。

- ステップ4 (任意) AP 接続プロファイルの説明を入力します。
- ステップ5 [CAPWAP] > [Advanced] を選択します。
- ステップ6 [Advanced] タブの下にある [Preferred Mode] ドロップダウンリストから、[IPv6] を選択します。
AP の優先モードが IPv6 に設定されます。
- ステップ7 [Save & Apply to Device] をクリックします。

AP 接続プロファイルの作成 (CLI)

手順

	コマンドまたはアクション	目的
ステップ1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ2	ap profile <i>ap-profile</i> 例： Device(config)# ap profile xyz-ap-profile	AP プロファイルを設定し、AP プロファイル コンフィギュレーションモードを開始します。
ステップ3	description <i>ap-profile-name</i> 例： Device(config-ap-profile)# description "xyz ap profile"	AP プロファイルの説明を追加します。
ステップ4	preferred-mode ipv6 例： Device(config-ap-profile)# preferred-mode ipv6	AP の優先モードを IPv6 に設定します。

プライマリコントローラとバックアップ 組み込みワイヤレスコントローラの設定 (GUI)

始める前に

プライマリコントローラとバックアップ 組み込みワイヤレスコントローラを設定する前に、AP 接続プロファイルが設定済みであることを確認します。

手順

- ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。
- ステップ 2 [AP Join Profile] ウィンドウで、AP 接続プロファイル名をクリックします。
- ステップ 3 [Edit AP Join Profile] ウィンドウで [CAPWAP] タブをクリックします。
- ステップ 4 [Backup Controller Configuration] の [High Availability] タブで、[Enable Fallback] チェックボックスをオンにします。
- ステップ 5 プライマリ コントローラとセカンダリ コントローラの名前および IP アドレスを入力します。
- ステップ 6 [Update & Apply to Device] をクリックします。

プライマリ コントローラとバックアップコントローラの設定 (CLI)

選択した AP のプライマリおよびセカンダリコントローラを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ap profile profile-name 例： Device(config)# ap profile yy-ap-profile	APプロファイルを設定し、APプロファイル コンフィギュレーション モードを開始します。
ステップ 3	capwap backup primary primary-controller-name primary-controller-ip 例： Device(config)# capwap backup primary WLAN-Controller-A 2001:DB8:1::1	プライマリ バックアップ コントローラの名前を使用して APCAPWAP パラメータを設定します。 (注) capwap backup primary と capwap backup secondary を機能させるには、高速ハートビートを有効にする必要があります。 コントローラと AP 間のリンクの信頼性が低い場合に、高速ハートビートが有効になっていると、AP の切断が発生する可能性があります。

	コマンドまたはアクション	目的
ステップ 4	ap capwap backup secondary <i>secondary-controller-name</i> <i>secondary-controller-ip</i> 例 : Device(config)# capwap backup secondary WLAN-Controller-B 2001:DB8:1::1	セカンダリ バックアップ コントローラの名前を使用して APCAPWAP パラメータを設定します。
ステップ 5	syslog host ipaddress 例 : Device(config)# syslog host 2001:DB8:1::1	AP のシステムログの設定を設定します。
ステップ 6	tftp-downgrade tftp-server-ip imagename 例 : Device(config)# tftp-downgrade 2001:DB8:1::1 testimage	すべての AP の TFTP サーバーから AP イメージのダウングレードを開始します。

IPv6 設定の確認

次の **show** コマンドを使用して、IPv6 設定を確認します。

```
Device# show wireless interface summary
```

```
Interface Name   Interface Type  VLAN ID  IP Address   IP Netmask   NAT-IP Address  MAC
Address
-----
GigabitEthernet0 Management      0        0.0.0.0     255.255.255.0 0.0.0.0
d4c9.3ce6.b854
                                     fd09:9:2:49::54/64
```


翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。