グローバル トラフィックの転送の設定

IPv6 ネイバー ディスカバリについて

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 ディスカバリは、IPv4 で使用されていた ARP、ICMP ルータ探索、および ICMP リダイレクトに代わるものです。

常に、クライアントあたり 8 つの IPv6 アドレスしかサポートされません。9 番目の IPv6 アドレスが検出されると、コントローラは最も古いエントリーを削除して、最新のエントリーを受け入れます。

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 ディスカバリ検査によってネイバー ディスカバリ メッセージが分析され、準拠しない IPv6 ネイバー ディスカバリ パケットはドロップされます。コントローラ内のネイバー 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 バインディングの設定（GUI）

手順

ステップ 1 [Controller] > [IPv6] > [Neighbor Binding] ページを選択します。

ステップ 2 次を設定します。

- [Down–Lifetime]：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時間を指定します。範囲は 0 ～ 86400 秒です。
- [Reachable–Lifetime]：IPv6 アドレスがアクティブである時間を指定します。範囲は 0 ～ 86400 秒です。
- [Stale–Lifetime]：IPv6 アドレスをキャッシュに保持する時間を指定します。範囲は 0 ～ 86400 秒です。

ステップ 3 [Unknown Address Multicast NS Forwarding] を有効または無効にします。

ステップ 4 [NA Multicast Forwarding] を有効または無効にします。

[NA Multicast Forwarding] を有効にすると、有線/無線からのすべての未承認マルチキャスト NA は無線に転送されません。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

ネイバー バインディングの設定（CLI）

手順

- 次のコマンドを入力して、ネイバー バインディング パラメータを設定します。

  config ipv6 neighbor-binding timers {down-lifetime | reachable-lifetime | stale-lifetime} {enable | disable}

- 次のコマンドを入力して、不明なアドレス マルチキャスト NS の転送を設定します。

  config ipv6 ns-mcast-fwd {enable | disable}

- 次のコマンドを入力して、NA マルチキャストの転送を設定します。

  config ipv6 na-mcast-fwd {enable | disable}

  [NA Multicast Forwarding] を有効にすると、有線/無線からのすべての未承認マルチキャスト NA は無線に転送されません。

- 次のコマンドを入力して、コントローラで設定されているネイバー バインディング データを表示します。

  show ipv6 neighbor-binding summary

802.3 ブリッジの設定について

コントローラでは、802.3 のフレームおよびそれらを使用するアプリケーションをサポートしています。このようなアプリケーションには、キャッシュ レジスタやキャッシュ レジスタ サー

バなどがあります。ただし、これらのアプリケーションをコントローラとともに使用するには、802.3 のフレームがコントローラ上でブリッジされている必要があります。

Cisco Prime Network Control System を使用して 802.3 ブリッジを設定することもできます。手順については、『*Cisco Prime Network Control System Configuration Guide*』を参照してください。

802.3 ブリッジの制限

- 未加工の 802.3 フレームのサポートにより、コントローラを、IP 上で実行していないアプリケーション用の IP 以外のフレームにブリッジできるようになります。

  802.3 Raw フレームには、宛先 MAC アドレス、送信元 MAC アドレス、総パケット長、およびペイロードが含まれます。

- デフォルトでは、Cisco WLC では、すべての非 IPv4 パケット（AppleTalk、IPv6 など）がブリッジされます。ACL を使用してこれらのプロトコルのブリッジングをブロックすることもできます。

802.3 ブリッジの設定（GUI）

手順

ステップ 1 [Controller] > [General] の順に選択して、[General] ページを開きます。

ステップ 2 802.3 ブリッジをコントローラ上で有効にする場合は、[802.3 Bridging] ドロップダウン リストから [Enabled] を選択し、無効にする場合は [Disabled] を選択します。デフォルト値は [Disabled] です。

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。

802.3 ブリッジの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、すべての WLAN の 802.3 ブリッジの現在のステータスを表示します。

show network

ステップ 2 次のコマンドを入力して、すべての WLAN でグローバルに 802.3 ブリッジを有効または無効にします。

config network 802.3-bridging {**enable** | **disable**}

デフォルト値は [disabled] です。

ステップ 3 次のコマンドを入力して、変更を保存します。

save config

802.3X のフロー制御の有効化

802.3X のフロー制御は、デフォルトでは無効にされています。有効にするには、**config switchconfig flowcontrol enable** コマンドを入力します。

リンク ローカル トラフィックのブリッジングの設定

リンク ローカル トラフィックのブリッジングの設定（GUI）

次の手順に従って、ローカル サイトでリンク ローカル トラフィックのブリッジングを設定します。

手順

ステップ 1 **[Controller]** > **[General]** を選択します。

ステップ 2 [Link Local Bridging] 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。

リンク ローカル トラフィックのブリッジングの設定（CLI）

手順

- 次のコマンドを使用して、ローカル サイトでリンク ローカル トラフィックのブリッジングを設定します。

  config network link-local-bridging {**enable** | **disable**}

高速 SSID 変更（Fast SSID Change）

高速 SSID 変更の設定について

controllerで Fast SSID Change が有効になっている場合、クライアントは SSID 間で移動することができます。高速 SSID が有効になっている場合、クライアント エントリがクリアされず、遅延は適用されません。

高速 SSID 変更が無効になっている場合、controllerは一定の遅延時間が経過した後でクライアントに新しい SSID への移動を許可します。高速 SSID が無効になっており、クライアントが異なる SSID の新しいアソシエーションを送信すると、controllerの接続テーブルのクライアント エントリがクリアされてから、新しい SSID にクライアントが追加されます。

高速 SSID 変更の設定（GUI）

手順

ステップ 1 [Controller] を選択して [General] ページを開きます。

ステップ 2 この機能を有効にするには、[Fast SSID Change] ドロップダウン リストから [Enabled] を選択します。無効にするには、[Disabled] を選択します。デフォルト値は [disabled] です。

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。

高速 SSID 変更の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、高速 SSID 変更を有効または無効にします。

config network fast-ssid-change {enable | disable}

ステップ 2 次のコマンドを入力して、変更を保存します。

save config

IP-MAC アドレス バインディング

IP-MAC アドレス バインディングの設定について

Cisco WLC では、クライアント パケットの厳密な IP アドレスと MAC アドレス間のバインディングが適用されます。コントローラは、パケット内の IP アドレスおよび MAC アドレスを確認し、これらのアドレスとコントローラに登録されているアドレスを比較します。パケットは、両方が一致した場合に限り転送されます。以前のリリースでは、クライアントの MAC アドレスだけが確認され、IP アドレスは無視されていました。

アクセス ポイントが Cisco 2504 WLC、5508 WLC、またはコントローラ ネットワーク モジュールと関連付けられている場合は、IP-MAC アドレス バインディングを無効にして、そのアクセス ポイントをスニファ モードで使用する必要があります。IP-MAC アドレス バインディングを無効にするには、**config network ip-mac-binding disable** を入力します。

アクセス ポイントが Cisco 2504 WLC、5508 WLC、またはコントローラ ネットワーク モジュールと関連付けられている場合は、WLAN を有効にして、そのアクセスポイントをスニファ モードで使用する必要があります。WLAN が無効の場合は、アクセス ポイントはパケットを送信できません。

（注） パケットの IP アドレスまたは MAC アドレスがスプーフィングされている場合は検査不合格となり、パケットは破棄されます。スプーフィングされたパケットがコントローラを通過できるのは、IP アドレスと MAC アドレスの両方がスプーフィングされて、同じコントローラ上の別の有効なクライアントのものに変更されている場合だけです。

IP-MAC アドレス バインディングの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、IP-MAC アドレス バインディングを有効または無効にします。

config network ip-mac-binding {**enable** | **disable**}

デフォルト値はイネーブルです。

（注） Workgroup Bridge（WGB）の背後にルーテッド ネットワークが存在する場合は、このバインディング チェックを無効にすることを推奨します。

（注） アクセス ポイントが Cisco 5508 WLC に join している場合に、そのアクセス ポイントをスニファ モードで使用するためには、このバインディング チェックを無効にする必要があります。

ステップ 2 次のコマンドを入力して、変更を保存します。

save config

ステップ 3 次のコマンドを入力して、IP-MAC アドレス バインディングのステータスを表示します。

show network summary

以下に類似した情報が表示されます。

```
RF-Network Name.............................. ctrl4404
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
...
```

IP/MAC Addr Binding Check ..... Enabled

```
...<?Line-Break?><?HardReturn?>
```

AP TCP MSS 調整

TCP MSS の設定について

トランスミッション コントロール プロトコル（TCP）スリーウェイ ハンドシェイクにおけるクライアントの最大セグメントサイズ（MSS）が、最大伝送単位で処理できるサイズよりも大きい場合、スループットの低下およびパケットのフラグメンテーションが発生する場合があります。コントローラ ソフトウェア リリース 6.0 以降のリリースでこの問題を回避するには、コントローラに join しているすべてのアクセス ポイントまたは特定のアクセス ポイントに MSS を指定します。

この機能を有効にすると、アクセス ポイントがデータ パスのワイヤレス クライアントと送受信する TCP パケットの MSS を選択します。これらのパケットの MSS が設定した値または CAPWAP トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、設定された新しい値に変更します。

TCP MSS の設定（GUI）

手順

ステップ 1 **[Wireless]** > **[Access Points]** > **[Global Configuration]** の順に選択して、[Global Configuration] ページを開きます。

ステップ 2 [TCP MSS] の下にある [Global TCP Adjust MSS] チェックボックスをオンして、コントローラに関連付けられているすべての AP の MSS を設定します。

有効な範囲は次のとおりです。

- IPv4 の場合、TCP は 536 ～ 1363 バイトの範囲内である必要があります。
- IPv6 の場合、TCP は 1220 ～ 1331 バイトの範囲内である必要があります。

（注） L3 およびゲスト アンカー モビリティの導入の場合、高いスループット レートを得るために、アンカーとフォーリン コントローラの TCP MSS は 1250 バイトに設定する必要があります。

CAPWAPv6 AP に対しては、1220 未満または 1331 より大きい TCP MSS 値は有効ではありません。

TCP MSS の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、特定のアクセス ポイントまたはすべてのアクセス ポイントの TCP MSS を有効または無効にします。

config ap tcp-mss-adjust {**enable**|**disable**} {*Cisco_AP* | *all*} *size*

size パラメータの値は、IP□4 の場合は 536 ～ 1363 バイト、IPv6 の場合は 1220 ～ 1331 バイトです。デフォルト値はクライアントにより異なります。

有効な範囲は次のとおりです。

- IPv4 の場合、TCP は 536 ～ 1363 バイトの範囲内である必要があります。
- IPv6 の場合、TCP は 1220 ～ 1331 バイトの範囲内である必要があります。

（注） L3 およびゲスト アンカー モビリティの導入の場合、高いスループット レートを得るために、アンカーとフォーリン コントローラの TCP MSS は 1250 バイトに設定する必要があります。

CAPWAPv6 AP に対しては、1220 未満または 1331 より大きい TCP MSS 値は有効ではありません。

ステップ 2 次のコマンドを入力して、変更を保存します。

save config

ステップ 3 次のコマンドを入力して、特定のアクセス ポイントまたはすべてのアクセス ポイントの現在の TCP MSS 設定を表示します。

show ap tcp-mss-adjust {*Cisco_AP* | **all**}

以下に類似した情報が表示されます。

```
AP Name              TCP State  MSS Size
------------------   --------   -------
AP58AC.78DC.A810     disabled   -
APa89d.21b2.2688     enabled    1250
AP00FE.C82D.DE80     disabled   -
```