IPv4 の設定

この章は、次の項で構成されています。

IPv4インターフェイス

IPv4 インターフェイスのアドレスは、ユーザーが手動で割り当てるか、または、DHCP サーバーから自動的に割り当てられます。このセクションでは、デバイスの IPv4 アドレスを手動で、またはデバイスを DHCP クライアントにして定義することについて説明します。デバイス管理用の IP アドレスを設定するには、[IPv4 Interface] ページを使用します。この IP アドレスは、ポート、LAG、VLAN、ループバック インターフェイス、またはアウトオブバンド インターフェイスに設定できます。デバイスに複数の IP アドレス（インターフェイス）を設定できます。これにより、さまざまなインターフェイス間のトラフィック ルーティングと、リモート ネットワークへのトラフィック ルーティングがサポートされます。一般に（デフォルトでは）ルーティング機能はハードウェアにより実行されます。ハードウェアリソースを使い尽くした場合、またはハードウェアでルーティングテーブルのオーバーフローが発生した場合は、IP ルーティングはソフトウェアにより実行されます。

（注） デバイス ソフトウェアは、ポートまたは LAG に設定されている IP アドレスごとに 1 つの VLAN ID（VID）を使用します。4094 以降で未使用の VID のうち最初のものが採用されます。

IPv4 アドレスを設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [IPv4 Interface] をクリックします。

次のフィールドに入力します。

- [IP v 4ルーティング]： IPv4 ルーティングを有効にするには、[有効] ボックスをオンにします（デフォルトで有効になっています）。

ステップ 2 [Apply] をクリックします。パラメータが実行コンフィギュレーション ファイルに保存されます。

次のフィールドが IPv4 インターフェイス テーブルに表示されます。

- [Interface]：IPアドレスが定義されているインターフェイス。これは、アウトオブバンドポートにすることもできます。
- [IP Address Type]：使用可能なオプションを以下に示します。
  - [DHCP]：DHCP サーバーから受信したもの。
  - [Static]：手動で入力したもの。スタティック インターフェイスは、ユーザが作成した DHCP 以外のインターフェイスです。
  - デフォルト（Default）：設定が行われる前にデフォルトでデバイスに存在するデフォルトのアドレス。
- [IP Address]：インターフェイスに設定されている IP アドレス。
- マスク（Mask）：設定された IP アドレス マスク。
- 状態（Status）：IP アドレスの重複チェックの結果。
  - [Tentative]：IP アドレス重複チェックの最終結果はありません。
  - 有効（Valid）：IPアドレス衝突チェックが完了し、IPアドレスの衝突が検出されませんでした。
  - 有効（重複あり）（Valid-Duplicated）：IP アドレス重複チェックが完了し、重複する IP アドレスが検出されました。
  - 重複（Duplicated）：デフォルト IP アドレスの重複 IP アドレスが検出されました。
  - 遅延（Delayed）：DHCP クライアントが起動時に有効化される場合、DHCP アドレスを検出する時間を確保するために、IP アドレスの割り当てが 60 秒遅延します。
  - [Not Received]：DHCP アドレスに関するステータスです。DHCP クライアントが検出プロセスを開始すると、実際のアドレスが取得される前に、ダミーの IP アドレス 0.0.0.0 が割り当てられます。このダミー アドレスの状態は、「未受信」です。

ステップ 3 [Add] をクリックします。

ステップ 4 インターフェイスを選択します。この IP 設定に関連するインターフェイスとしてポート、LAG、VLAN、またはループバックを選択し、関連リストからインターフェイスを選択します。

ステップ 5 IP アドレスタイプを選択します。次のいずれかのオプションを選択してください。

- [ダイナミック IP アドレス]：IP アドレスを DHCP サーバーから受け取ります。
- [スタティックIPアドレス]：IP アドレスを入力し、[マスク] フィールドに入力します。
  - [Network Mask]：このアドレスの IP マスク。
  - [Prefix Length]：IPv4 プレフィックスの長さ。
- [Renew IP Address Now]：[Enable] チェックボックスをオンにして有効にします。
- [Auto Configuration via DHCP]：ステータス（[Disabled] または [Enabled]）が表示されます。

ステップ 6 [Apply] をクリックします。IPv4 アドレス設定が実行コンフィギュレーション ファイルに書き込まれます。

注意 システムが、スタンバイ アクティブ ユニットの存在するスタッキングモードのいずれか 1 つである場合は、IP アドレスをスタティックアドレスとして設定することにより、アクティブ スタッキング ユニットのスイッチオーバー時にネットワークから切断しないようにすることをお勧めします。スタンバイ アクティブ ユニットがスタックを制御するようになると、DHCP を使用する場合には、スタックの元のアクティブ対応ユニットで受信したものとは異なる IP アドレスを受信する可能性があります。

アウトオブバンド インターフェイスの設定

アウトオブバンド管理により、ネットワークオペレータは、管理機能にアクセスする際に信頼境界を確立し、それをネットワークリソースに適用することができます。ここでは、アウトオブバンド（OOB）インターフェイスで IPv4 アドレスを設定する方法について説明します。

ステップ 1 スイッチの Web ベースユーティリティにログインし、[IPv4 Configuration] > [IPv4 Interface] の順に選択します。

[IPv4 Interface] ページの [IPv4 Interface] テーブルには、次の情報が含まれています。

- [Interface]：IP アドレスが定義されているユニットまたはインターフェイス。これはループバックインターフェイスの場合もあります。
- [IP Address Type]：使用可能なオプションは次のとおりです。
  - [DHCP]：Dynamic Host Configuration Protocol（DHCP）サーバーから受信されたもの。
  - [Static]：手動で入力したもの。スタティック インターフェイスはユーザーが作成した非 DHCP インターフェイスです。
  - [Default]：設定が行われる前にデフォルトでデバイスに存在するデフォルトのアドレス。
- [IP Address]：インターフェイスに設定されている IP アドレス。
- [Mask]：設定されている IP アドレスマスク。

- [Status]：IP アドレス重複チェックの結果。
  - [Tentative]：IP アドレス重複チェックの最終結果はありません。
  - [Valid]：IP アドレスのコリジョンチェックが完了しており、IP アドレスのコリジョンは検出されませんでした。
  - [Valid-Duplicated]：IP アドレス重複チェックが完了しており、IP アドレスの重複が検出されました。
  - [Duplicated]：デフォルト IP アドレスの、IP アドレスの重複が検出されました。
  - [Delayed]：DHCP クライアントが始動時に有効なら、DHCP アドレス検出のための時間を取るため、IP アドレスの割り当ては 60 秒間遅延されます。
  - [Not Received]：DHCP アドレスのみに関するステータスです。DHCP クライアントが検出プロセスを開始すると、実際のアドレスが取得される前に、ダミーの IP アドレス 0.0.0.0 が割り当てられます。このダミーアドレスのステータスは [Not Received] です。

ステップ 2 [Add] をクリックして、静的 IP アドレスを手動で割り当てます。

ステップ 3 [Interface] エリアから [Out of Band] を選択します。

ステップ 4 [IP Address Type] エリアから [Static IP Address] を選択します。

ステップ 5 [IP Address] フィールドにアウトオブバンド インターフェイスの IP アドレスを入力します。

ステップ 6 [Mask] エリアのオプションボタンをクリックし、対応するサブネットマスクを入力します。次のオプションがあります。

- [Network Mask]：このアドレスの IP マスク。
- [Prefix Length]：IPv4 プレフィックスの長さ。

ステップ 7 [Apply] をクリックして [Close] をクリックします。

セッションが自動的に終了し、スイッチへの接続は失われます。これは、アウトオブバンドポートに新しい管理 IP アドレスを適用するためです。

以上で、スイッチに IPv4 管理インターフェイスアドレスが正常に設定されます。

IPv4スタティックルート

このページでは、デバイスの IPv4 スタティック ルートを設定および表示できます。トラフィックをルーティングするときに、ネクスト ホップは最長プレフィックス照合（LPM アルゴリズム）に従って決定されます。宛先 IPv4 アドレスは、IPv4 スタティック ルート テーブルの複数のルートに一致する可能性があります。デバイスは、最も高いサブネットマスク、つまり最長プレフィックス照合を持つ一致したルートを使用します。複数のデフォルト ゲートウェイが同じメトリック値で定義されている場合は、すべての設定済みデフォルト ゲートウェイの中から最も低い IPv4 アドレスが使用されます。

IP スタティックルートを定義するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [IPv4 Static Routes] をクリックします。

IPv4 スタティック ルート テーブルが表示されます。各エントリについて、次のフィールドが表示されます。

- [Destination IP Prefix]：宛先 IP アドレスプレフィックス。
- [Prefix Length]：宛先 IP の IP ルートプレフィックス。
- [Route Type]：ルートは拒否ルート、リモートルートのうちどれか。
- [Next Hop Router IP Address]：ルート上のネクストホップ IP アドレスまたは IP エイリアス。
- [Metric]：このホップのコスト（低い値が推奨されます）。
- [Outgoing Interface]：このルートの送信インターフェイス。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドの値を入力します。

- [Destination IP Prefix]：宛先 IP アドレスプレフィックスを入力します。
- [Mask]：次のフィールドを選択して値を入力します。
  - [Network Mask]：マスク形式の、宛先 IP の IP ルートプレフィックス（ルートネットワークアドレス内のビット数）。
  - [Prefix Length]：IP アドレス形式の、宛先 IP の IP ルートプレフィックス。
- [Route Type]：ルートタイプを選択します。
  - [Reject]：ルートを拒否し、すべてのゲートウェイを通じた宛先ネットワークへのルーティングを停止します。これにより、このルートの宛先 IP が指定されたフレームが着信した場合、ドロップされます。この値を選択すると、ネクストホップ IP アドレス、メトリック、および IP SLA トラックの各コントロールが無効になります。
  - [Remote]：このルートがリモートパスであることを示します。
- [Next Hop Router IP Address]：ルート上のネクストホップルータ IP アドレスまたは IP エイリアスを入力します。

  （注） デバイスが DHCP サーバーから IP アドレスを取得する、直接接続された IP サブネットを介してスタティックルートを設定することはできません。

- [メトリック]：次のいずれかを選択します。
  - [デフォルトを使用]：デフォルトのメトリックを使用する場合に選択します。
  - [ユーザー定義]：ネクスト ホップへの管理距離を入力します。範囲は 1 ～ 255 です。

ステップ 4 [Apply] をクリックします。IP スタティック ルートが実行コンフィギュレーション ファイルに保存されます。

IPv4転送テーブル

IPv4 転送テーブルを表示するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [IPv4 Forwarding Table] の順にクリックします。

IPv4 転送ルート テーブルが表示されます。各エントリについて、次のフィールドが表示されます。

- 宛先 IP プレフィックス（Destination IP Prefix）：宛先 IP アドレスのプレフィックス。
- プレフィックス長（Prefix Length）：宛先 IP の IP ルート プレフィックス。
- ルート タイプ（Route Type）：ルートがローカル、拒否、またはリモート ルートかどうか。
- ネクスト ホップ ルータ IP アドレス（Next Hop Router IP Address）：ネクスト ホップ IP アドレス。
- [Route Owner]：次のいずれかのオプションを選択できます。
  - [デフォルト]：デフォルト システム コンフィギュレーションによって設定されたルート。
  - [スタティック]：手動で作成されたルート。
  - [ダイナミック]：IP ルーティング プロトコルによって作成されたルート。
  - [DHCP]：DHCP サーバーから受け取ったルート。
  - [直接接続]：デバイスが接続されるサブネット。
  - [Rejected]：ルートは拒否されました。
- メトリック（Metric）：このホップのコスト（より低い値が優先）。
- アドミニストレーティブ ディスタンス（Administrative Distance）：ネクスト ホップまでのアドミニストレーティブ ディスタンス（より低い値が優先）。これは、スタティックルートには関係ありません。
- 発信インターフェイス（Outgoing Interface）：このルートの発信インターフェイス。

ステップ 2 [Refresh] アイコンをクリックしてデータを更新します。

RIPv2

このセクションでは、Routing Information Protocol（RIP）バージョン 2 の機能について説明します。

Note この機能は、ファームウェア 3.1 以降でのみサポートされます。

Routing Information Protocol（RIP）は、ローカルエリア ネットワークおよびワイドエリア ネットワーク向けのディスタンスベクタープロトコルの実装です。ルータをアクティブまたはパッシブ（サイレント）のいずれかとして分類します。アクティブ ルータは、それらのルートを他のルータにアドバタイズします。パッシブ ルータはアドバタイズメントに基づいて、それらのルートをリッスンして更新しますが、アドバタイズはしません。通常、ルータはアクティブ モードで RIP を実行しますが、ホストはパッシブ モードを使用します。

デフォルト ゲートウェイはスタティック ルートであり、設定によって有効な場合は、他のすべてのスタティック ルータと同じ方法で RIP によってアドバタイズされます。IP ルーティングを有効にすると、RIP が完全に機能します。IP ルーティングを無効にすると、RIP はパッシブ モードで稼動します。つまり、受信した RIP メッセージからルートを学習するだけで、それらを送信しません。

Note IP ルーティングを有効にするには、IPv4 インターフェイスページに移動します。デバイスは RIP バージョン 2 をサポートします。以下の標準規格に基づいています。

- RFC2453 RIP バージョン 2、1998 年 11 月
- RFC2082 RIP-2 MD5 認証、1997 年 1 月
- RFC1724 RIP バージョン 2 拡張 MIB

受信した RIPv1 パケットはドロップされます。

RIP のイネーブル化

- RIP は、グローバルに、インターフェイスごとに有効にする必要があります。
- RIP は、有効になっている場合にのみ設定できます。
- RIP をグローバルに無効にすると、システムの RIP 設定が削除されます。
- インターフェイス上の RIP を無効にすると、指定したインターフェイスの RIP 設定が削除されます。
- IP ルーティングを無効にすると、RIP メッセージは送信されませんが、RIP メッセージを受信した場合、それらはルーティング テーブル情報を更新するために使用されます。

Note RIP は、手動で設定されている IP インターフェイスでのみ定義できます。つまり、IP アドレスを DHCP サーバから受信したインターフェイス、または IP アドレスがデフォルトの IP アドレスであるインターフェイスでは RIP を定義できません。

RIPv2プロパティ

デバイスで RIPv2 を有効化または無効化するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [RIPv2] > [RIPv2 Properties] の順にクリックします。

ステップ 2 必要に応じて、次のオプションを選択します。

- [RIP]：次のオプションを使用できます。
  - [Enable]：RIP を有効にします。
  - [Disable]：RIP を無効にします。RIP を無効にすると、システムの RIP 設定は削除されます。
  - シャットダウン（Shutdown）：シャットダウンするための RIP のグローバルな状態を設定します。
- RIP アドバタイズメント（RIP Advertisement）：選択すると、すべての RIP IP インターフェイスでルーティング アップデートの送信が有効になります。
- デフォルト ルートのアドバタイズメント（Default Route Advertisement）：選択すると、RIP ドメインへのデフォルト ルートの送信が有効になります。このルートは、デフォルト ルートして機能します。
- [Default Metric]：デフォルトメトリックの値を入力します。

ステップ 3 [Redistribute Static Route]：手動で定義した（リモート）ルートを有効にする場合に選択します。

ステップ 4 [Redistribute Static Route] が有効な場合、[Redistribute Static Metric] フィールドのオプションを選択します。次のオプションを使用できます。

- [Default Metric]：RIP では、伝播するスタティックルートの設定にデフォルトメトリック値が使用されるようになります。
- [Transparent]：RIP では、ルーティング テーブル メトリックが RIP メトリックとして使用されるようになります。
  - スタティック ルートのメトリック値が 15 以下の場合、この値は、このスタティック ルートをアドバタイズするときに RIP プロトコルで使用されます。
  - スタティック ルートのメトリック値が 15 より大きい場合は、スタティック ルートは RIP を使用して他のルータにアドバタイズされません。
- ユーザ定義メトリック（User Defined Metric）：メトリックの値を入力します。

ステップ 5 [Redistribute Connected Route]：RIP が有効になっていない定義済みの IP インターフェイス（ローカルに定義されている）に対応する RIP ルートを有効にする場合に選択します。

ステップ 6 [Redistribute Connected Route] が有効な場合、[Redistribute Connected Metric] フィールドのオプションを選択します。次のオプションを使用できます。

- [Default Metric]：RIP では、伝播するスタティックルートの設定にデフォルトメトリック値が使用されるようになります。
- 透過型（Transparent）：RIP が、伝播されたスタティック ルート設定の RIP メトリックとして、ルーティング テーブル メトリックをを使用するようにします。この結果、次のように動作します。
  - スタティック ルートのメトリック値が 15 以下の場合、この値は、このスタティック ルートをアドバタイズするときに RIP プロトコルで使用されます。
  - スタティック ルートのメトリック値が 15 より大きい場合は、スタティック ルートは RIP を使用して他のルータにアドバタイズされません。
- ユーザ定義メトリック（User Defined Metric）：メトリックの値を入力します。

ステップ 7 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

RIPv2設定

IP インターフェイス上で RIP を設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [RIPv2] > [RIPv2 Settings] の順にクリックします。

ステップ 2 RIP パラメータは、IP インターフェイスごとに表示されます。新しい IP インターフェイスを追加するには、[Add] をクリックして、次のフィールドを入力します。

- IP アドレス（IP Address）：レイヤ 2 インターフェイスで定義されている IP インターフェイスを選択します。
- シャットダウン（Shutdown）：インターフェイスで RIP 構成を保持するが、インターフェイスを非アクティブに設定します。
- パッシブ（Passive）：指定した IP インターフェイスで RIP ルート更新メッセージの送信を許可するかどうかを指定します。このフィールドが有効になっていない場合は、RIP アップデートが送信されません（パッシブ）。
- オフセット（Offset）：指定した IP インターフェイスのメトリック数値を指定します。これには、インターフェイスの速度に基づいて、このインターフェイスを使用するための追加コストが反映されます。
- [Default Route Advertisement]：このオプションは、RIPv2プロパティ （8 ページ）ページでグローバルに定義されます。グローバルな定義を使用することもできれば、特定のインターフェイスに対してこのフィールドを定義することもできます。次のオプションを使用できます。

- [Global]：[RIPv2 Properties] に定義されているグローバル設定を使用します。画面
- [Disable]：この RIP インターフェイス上でデフォルトルートをアドバタイズしません。
- 有効化（Enable）：この RIP インターフェイス上でデフォルト ルートをアドバタイズします。

- デフォルト ルート アドバタイズメントのメトリック（Default Route Advertisement Metric）：このインターフェイスのデフォルト ルートのメトリックを入力します。
- 認証モード（Authentication Mode）：指定した IP インターフェイスの RIP 認証状態（有効/無効）。次のオプションを使用できます。
  - [None]：認証が実行されません。
  - テキスト（Text）：以下に入力されたキー パスワードが認証に使用されます。
  - MD5：以下で選択したキー チェーンの MD5 ダイジェストが認証に使用されます。
- キー パスワード（Key Password）：認証タイプとして [Text] を選択した場合は、使用するパスワードを入力します。
- キー チェーン（Key Chain）：認証モードとして [MD5] を選択した場合は、ダイジェスト対象のキーチェーンを入力します。このキーチェーンは、この項に記載されているように作成されます。
- [Distribute-list In]：[Access List Name] で指定した 1 つ以上の IP アドレスに対して RIP 着信ルートのフィルタリングを設定する場合に選択します。このフィールドが有効な場合は、次の [Access List Name] を選択します。
- [Access List Name]：指定した IP インターフェイスに割り当てる RIP 着信ルートフィルタリングのアクセスリスト名（IP アドレスの一覧を含む）を選択します。
- [Distribute-list Out]：[Access List Name] で指定した 1 つ以上の IP アドレスに対して RIP 発信ルートのフィルタリングを設定する場合に選択します。このフィールドが有効な場合は、次の [Access List Name] を選択します。
- [Access List Name]：指定した IP インターフェイスに割り当てる RIP 発信ルートフィルタリングのアクセスリスト名（IP アドレスの一覧を含む）を選択します。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

RIPv2統計情報

IP アドレスごとの RIP 統計情報カウンタを表示するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [RIPv2] > [RIPv2 Statistics] の順にクリックします。

次のフィールドが表示されます。

- IP インターフェイス（IP Interface）：レイヤ 2 インターフェイスで定義されている IP インターフェイス。
- 受信済み不良パケット（Bad Packets Received）：IP インターフェイスで RIP によって識別された不良パケットの数を指定します。
- 受信済み不正ルート（Bad Routes Received）：IP インターフェイスで RIP によって受信および識別された不正ルートの数を指定します。不正なルートとは、ルート パラメータが正しくないことを意味します。たとえば、IP 宛先がブロードキャストアドレスになっていたり、メトリックが 0 または 16 を超えていたりした場合です。
- 送信の更新（Update Sent）：IP インターフェイスで RIP によって送信されたパケットの数を指定します。

ステップ 2 すべてのインターフェイス カウンタをクリアするには、[Clear All Interface Counters] をクリックします。

RIPv2ピアルータ データベース

RIP ピアルータデータベースを表示するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [RIPv2] > [RIPv2 Peer Router Database] の順にクリックします。

ピア ルータ データベースに関する次のフィールドが表示されます。

- ルータの IP アドレス（Router IP Address）： レイヤ 2 インターフェイスで定義されている IP インターフェイス。
- 受信済み不良パケット（Bad Packets Received）：IP インターフェイスで RIP によって識別された不良パケットの数を指定します。
- 受信済み不正ルート（Bad Routes Received）：IP インターフェイスで RIP によって受信および識別された不正ルートの数を指定します。不正なルートとは、ルート パラメータが正しくないことを意味します。たとえば、IP 宛先がブロードキャストになっていたり、メトリックが 0 または 16 を超えていたりした場合です。
- 最終更新時間（Last Updated）：RIP がリモート IP アドレスから RIP ルートを最後に受信した時間を示します。

ステップ 2 すべてのカウンタをクリアするには、[Clear All Interface Counters] をクリックします。

アクセス リスト

アクセスリストは、デバイス上のトラフィックをフィルタ処理する permit および deny ステートメントで構成されます。これらのステートメントはトップダウン方式で実行されます。つま

り、トラフィックをアクセスリストで照合する際、アクセスリストは上から下に解析され、一致が検索されます。最初に一致したステートメントにより、トラフィックが許可されるか拒否されるかが決定されます。そのため、アクセスリストのステートメントの順序は非常に重要です。アクセスリストでは、限定性の最も高いものから最も低いものへとステートメントを順に並べる必要があります。これにより、意図しない一致が最小限に抑えられます。一致するものがない場合は、アクセスリストのすべてのステートメントの後には「すべて拒否」が暗黙的に存在します。

アクセスリストはスイッチが動作するために必要であり、セキュリティにとって不可欠です。

アクセスリスト設定

アクセスリストのグローバル設定を設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [Access List] > [Access List Settings] の順にクリックします。

ステップ 2 新しいアクセスリストを追加するには、[Add] をクリックして [Add Access List] ページを開き、次のフィールドを入力します。

- [Name]：アクセスリストの名前を定義します。
- [Source IPv4 Address]：送信元 IPv4 アドレスを入力します。次のオプションを使用できます。
  - 任意（Any）：すべての IP アドレスを含めます。
  - [User defined]：IP アドレスを入力します。
- [Source IPv4 Mask]：送信元 IPv4 アドレスマスクのタイプと値を入力します。次のオプションを使用できます。
  - [Network mask]：ネットワークマスクを入力します。
  - [Prefix length]：プレフィックス長を入力します。
- アクション（Action）：アクセスリストのアクションを選択します。次のオプションを使用できます。
  - [Permit]：アクセスリスト内の 1 つ以上の IP アドレスからのパケットのエントリを許可します。
  - [Deny]：アクセスリスト内の 1 つ以上の IP アドレスからのパケットのエントリを拒否します。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

送信元IPv4アドレスリスト

IP アドレスを使用してアクセスリストに入力するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [Access List] > [Source IPv4 Address List] の順にクリックします。

ステップ 2 アクセス リストのパラメータを変更するには、[Add] をクリックし、次のフィールドのいずれかを変更します。

- [Access List Name]：アクセスリストの名前。
- [Source IPv4 Address]：送信元 IPv4 アドレス。次のオプションを使用できます。
  - 任意（Any）：すべての IP アドレスを含めます。
  - [User defined]：IP アドレスを入力します。
- 送信元 IPv4 マスク（Source IPv4 Mask）：送信元 IPv4 アドレスのマスクのタイプと値。次のオプションを使用できます。
  - [ネットワークマスク]：ネットワーク マスク（255.255.0.0 など）を入力します。
  - [Prefix length]：プレフィックス長を入力します。
- [Action]：アクセスリストに対するアクション。次のオプションを使用できます。
  - [Permit]：アクセスリスト内の 1 つ以上の IP アドレスからのパケットのエントリを許可します。
  - [Deny]：アクセスリスト内の 1 つ以上の IP アドレスからのパケットのエントリを拒否します。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

ARP

デバイスは、直接接続されている IP サブネットに存在するすべての既知のデバイス用の ARP（Address Resolution Protocol）テーブルを保持します。直接接続されている IP サブネットとは、デバイスの IPv4 インターフェイスが接続されているサブネットのことです。デバイスがローカル デバイスにパケットを送信またはルーティングする必要がある場合、ARP テーブルを検索してデバイスの MAC アドレスを取得します。ARP テーブルには、スタティック アドレスとダイナミック アドレスの両方が含まれています。スタティックアドレスは手動で設定され、エージアウトしません。デバイスは、受信する ARP パケットからダイナミック アドレスを作成します。ダイナミック アドレスは、設定された時間が過ぎるとエージ アウトします。

（注） マッピング情報は、ルーティングと生成されたトラフィックの転送に使用されます。

ARP テーブルを定義するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [ARP] の順にクリックします。

ステップ 2 パラメータを入力します。

- [ARP エントリのエージングアウト] : ARP テーブル内でダイナミック アドレスを保 持する期間（単位：秒）を入力します。テーブルに登録されている期間が [ARP Entry Age Out] の時間を超えると、そのダイナミックアドレスはエージアウトします。ダイナミックアドレスは、エージアウトするとテーブルから削除され、再度学習された場合のみテーブルに戻されます。
- [ARP テーブルエントリのクリア] : システムから削除する ARP エントリのタイプを 選択します。
  - [All] : すべてのスタティックアドレスとダイナミックアドレスをただちに削除します。
  - [Dynamic] : すべてのダイナミックアドレスをただちに削除します。
  - [Static] : すべてのスタティックアドレスをただちに削除します。
  - 通常のエージ アウト（Normal Age Out）：設定されている ARP エントリ エージ アウト時間に基づいてダイナミック アドレスを削除します。

ステップ 3 [Apply] をクリックします。ARP グローバル設定が実行コンフィギュレーション ファイルに書き込まれます。

ARP テーブルには以下のフィールドが表示されます。

- [Interface] : IP デバイスが存在する、直接接続されている IP サブネットの IPv4 インターフェイス。
- [IP アドレス] : IP デバイスの IP アドレス。
- [MAC アドレス] : IP デバイスの MAC アドレス。
- [ステータス] : エントリのタイプ（手動で入力されたか、動的に学習されたか）。

ステップ 4 [Add] をクリックします。

ステップ 5 パラメータを入力します。

- [IP バージョン] : このホストでサポートされている IP アドレス形式。IPv4 だけがサポートされます。
- [Interface] : IPv4 インターフェイスをポート、LAG、または VLAN 上に設定できます。デバイスに設定されている IPv4 インターフェイスの一覧から、目的のインターフェイスを選択します。
- [IP アドレス] : ローカル デバイスの IP アドレスを入力します。
- [MAC アドレス] : ローカル デバイスの MAC アドレスを入力します。

ステップ 6 [Apply] をクリックします。ARP エントリが実行コンフィギュレーション ファイルに保存されます。

ARP プロキシ

プロキシ ARP 手法は、ネットワーク上にないネットワークアドレスに対する ARP クエリに応答するために、特定の IP サブネット上のデバイスによって使用されます。

（注） ARP プロキシ機能は、デバイスが L3 モードのときにのみ使用できます。

ARP プロキシはトラフィックの宛先を認識し、返信で別の MAC アドレスを提供します。別のホストの ARP プロキシとして機能することで、LAN トラフィックの宛先をホストに効果的に指示できます。キャプチャされたトラフィックは通常、別のインターフェイスを使用するか、またはトンネルを使用して、プロキシによって目的の宛先にルーティングされます。プロキシ目的で、異なる IP アドレスの ARP クエリ要求を受け、ノードが自身の MAC アドレスで応答するプロセスを、パブリッシングということがあります。

すべての IP インターフェイスで ARP プロキシを有効にするには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [ARP Proxy] の順にクリックします。

ステップ 2 [ARP Proxy] を選択して、デバイスがリモート ノードに関する ARP 要求にデバイス MAC アドレスで応答できるようにします。

ステップ 3 [Apply] をクリックします。ARP プロキシが有効になり、実行コンフィギュレーション ファイルが更新されます。

UDPリレー/IPヘルパー

一般的にスイッチは、IP サブネット間の IP ブロードキャストパケットのルーティングを行いません。ただし、この機能を使用すると、デバイスは、その IPv4 インターフェイスから受信した特定の UDP ブロードキャスト パケットを特定の宛先 IP アドレスにリレーできます。

特定の IPv4 インターフェイスから受信した UDP パケットの特定の宛先ポートへのリレーを設定するには、UDP リレーを追加します。

ステップ 1 [IPv4 Configuration] > [UDP Relay/IP Helper] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 設定されている UDP 宛先ポートに基づいてデバイスがリレーする UDP ブロードキャスト パケットの送信元となる [Source IP Interface] を選択します。このインターフェイスは、デバイスに設定されている IPv4 インターフェイスのいずれかである必要があります。

ステップ 4 デバイスがリレーするパケットの [UDP Destination Port] 番号を入力します。ドロップダウンメニューから既知のポートを選択するか、またはポート オプション ボタンをクリックして番号を手動で入力します。

ステップ 5 リレーする UDP パケットを受信する [Destination IP Address] を入力します。このフィールドが 0.0.0.0 である場合、UDP パケットは破棄されます。このフィールドが 255.255.255.255 である場合、UDP パケットはすべての IP インターフェイスにフラッディングされます。

ステップ 6 [Apply] をクリックします。UDP リレー設定が実行コンフィギュレーション ファイルに書き込まれます。

DHCP スヌーピング/リレー

ここでは、Dynamic Host Configuration Protocol（DHCP）スヌーピング/リレーについて説明します。DHCP リレー エージェントとは、クライアントとサーバー間で DHCP パケットを転送するホストです。リレー エージェントは、同一の物理サブネット上にないクライアントとサーバー間で要求および応答を転送するために使用されます。リレーエージェント転送は、IP ルータの通常の転送とは異なります。通常の転送では、IP データグラムがネットワーク間である程度透過的にスイッチングされます。これとは対照的に、リレーエージェントは DHCP メッセージを受信すると、DHCP メッセージを新たに生成して他のインターフェイスから送信します。

DHCP スヌーピングは、対応ネットワークスイッチのオペレーティングシステムに組み込まれたレイヤ 2 のセキュリティ技術であり、許容できないと判断した DHCP トラフィックをドロップします。DHCP スヌーピングは通常、不正な DHCP サーバーによる DHCP クライアントへの IP アドレスの提供を防止するために使用されます。

プロパティ

DHCP リレーは、DHCP パケットを DHCP サーバーに転送します。

DHCP スヌーピング/リレーのプロパティを設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Snooping/Relay] > [Properties] の順にクリックします。

ステップ 2 次のフィールドを設定します。

- [DHCP Relay]：DHCP リレーを有効にする場合に選択します。
- [DHCPスヌーピングステータス]：DHCP スヌーピングを有効にする場合に選択します。
- Option 82 パス スルー（Option 82 Pass Through）：選択すると、パケットを転送する際に異種の Option 82 情報をそのままにします。
- MAC アドレスの確認（Verify MAC Address）：選択すると、レイヤ 2 ヘッダーの送信元 MAC アドレスが、DHCP で信頼できるポートの DHCP ヘッダー（ペイロードの一部）に表示されるクライアント ハードウェア アドレスに一致することを確認します。
- データベースのバックアップ（Backup Database）：選択すると、デバイスのフラッシュ メモリに DHCP スヌーピング バインディング データベースをバックアップします。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

ステップ 4 DHCP サーバを定義するには、**[Add]** をクリックします。[DHCPサーバーを追加] ダイアログが表示されます。IP バージョンが示されています。

ステップ 5 DHCP サーバの IP アドレスを入力し、**[Apply]** をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

オプション82の設定

Option 82（DHCP リレーエージェント情報オプション）は、ポートおよびエージェント情報を中央 DHCP サーバに渡して、割り当てられた IP アドレスがネットワークに物理的に接続されている場所を示します。オプション 82 の主な目的は、DHCP サーバが IP アドレスを取得する最適な IP サブネット（ネットワーク プール）を選択できるようにすることです。

オプション 82（有効になっている場合）は、DHCP スヌーピングおよび IP アドレスが設定されている DHCP リレーインターフェイスに適用されます。オプション 82 が有効になっていない場合でも、IP アドレスのない VLAN で DCHP リレーが有効になっていれば、この VLAN で受信された DHCP パケットにはオプション 82 情報が挿入されます。

DHCP メッセージ内のオプション 82 データのフォーマットとデバイスのステータスを設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Snooping /Relay] > [Option 82 Settings] の順にクリックします。

次のフィールドに入力します。

- [オプション82挿入]：[有効] チェックボックスをオンにすると、オプション 82 情報がパケット内に挿入されます。
- [Numeric Token Format]：必要に応じて [Hexadecimal] または [Ascii] を選択します。このパラメータによって、次のトークンに使用するフォーマットが定義されます。
  - $int-ifindex$
  - $int-portid$
  - $switch-moduleid$
  - $vlan-id$

    たとえば、VLAN ID が 35 の $vlan-id$ トークンがあるとします。VLAN ID 35 は、16 進バイト 0x23 または ASCII 表現の値 0x3335 のどちらかで送信できます。下記の表に、各種トークンの詳細情報を示しています。

ステップ 2 [回線IDテンプレート] に入力します。デフォルトの回線 ID を使用する場合は [デフォルトを使用] を選択します。回線 ID を設定する場合は [ユーザー定義] を選択します。テキスト ボックスを使用して回線 ID テンプレートに入力します。テンプレートは、自由形式のテキストと事前定義済みトークンから成る文字列です（下記表を参照）。トークンを入力するには、手動で入力する方法と、ドロップダウンを使用して利用可能トークンリストからトークンを選択し、矢印ボタンをクリックして回線 ID テキストに追加する方法があります。実際のサブオプション バイトの内容と、選択されたサブオプションのテキスト表現を確認するには、[プレビュー] ボタンを使用します。

ステップ 3 [リモートIDテンプレート] に入力します。該当するテキスト ボックスとドロップダウン リストを使用して、回線 ID テンプレートと同じ要領で入力します

（注） [サブオプションペイロードの合計] には、両サブオプションの予約済みバイト数が動的に更新されて表示されます。ペイロードは247以下である必要があります。バイト数は、サブオプションに含まれるトークンの予約済みの長さと、サブオプションで使用される自由形式テキストの文字数を加算した値に基づいています。

ステップ 4 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

ドロップダウンボックスから利用できるトークンを下記の表に示します。

オプション	説明	予約済みバイト数	16 進数フォーマットでの使用バイト数
$int-ifindex$	DHCP クライアント リクエストが受信されたインターフェイスの ifIndex。 値は ifTable MIB エントリの ifIndex フィールドから取得されます。	4	2
$int-portid$	個々のユニット（スタンドアロンユニットまたはスタッキング ユニット）に関連するインターフェイス番号。 物理インターフェイスの場合、この値の先頭は、個々のユニットの第 1 ポートでは 1、そのユニットの第 2 ポートでは2、そのユニットの最終ポートではN となります。 LAG インターフェイスの場合、この値は、LAG ID に基づいてグローバルに決定されます（個々のユニットには基づきません）。例：1,2,3…	2	1
$int-name$	DHCP クライアント リクエストが受信されたインターフェイスのフル ネーム。 この名前は、このインターフェイスの情報を設定または表示する際に CLI が使用するインターフェイス フル ネーム フォーマットに基づいています。	32	該当なし
$int-abrvname$	DHCP クライアント リクエストが受信されたインターフェイスの略称。 このパラメータは、このインターフェイスの情報を設定または表示する際に CLI が使用するインターフェイス略称フォーマットに基づいています。	8	該当なし

オプション	説明	予約済みバイト数	16 進数フォーマットでの使用バイト数
$int-desc-16$	DHCP クライアントパケットが受信されたインターフェイスに関するインターフェイス記述。最大で（先頭の）16 バイトまで。 この変数の値は、インターフェイス レベルの「description」コマンドを使用してユーザーがインターフェイスに追加した記述から取得されます。 記述の長さが 16 バイトを超える場合でも、使用できる最大バイト数は（先頭の）16 バイトです。 ユーザーによって定義された記述のないインターフェイスの場合は、インターフェイス略称フォーマットが使用されます。	16	該当なし
$int-desc-32$	DHCP クライアントパケットが受信されたインターフェイスに関するインターフェイス記述。最大で（先頭の）32 バイトまで。 この変数の値は、インターフェイス レベルの「description」コマンドを使用してユーザーがインターフェイスに追加した記述から取得されます。 記述の長さが 32 バイトを超える場合でも、使用できる最大バイト数は（先頭の）32 バイトです。 ユーザーによって定義された記述のないインターフェイスの場合は、インターフェイス略称フォーマットが使用されます。	32	該当なし
$int-desc-64$	DHCP クライアントパケットが受信されたインターフェイスに関するインターフェイス記述の全部分（最大で 64 バイトまで）。 この変数の値は、インターフェイス レベルの「description」コマンドを使用してユーザーがインターフェイスに追加した記述から取得されます。 ユーザーによって定義された記述のないインターフェイスの場合は、インターフェイス略称フォーマットが使用されます。	64	該当なし

オプション	説明	予約済みバイト数	16 進数フォーマットでの使用バイト数
$int-mac$	DHCP クライアント リクエストが受信された物理インターフェイスの MAC アドレス。 このフィールドの形式は常に 16 進数フォーマットとなり、区切り文字はありません（例：000000112205）。	6	6
$switch-mac$	オプション 82（リレー エージェント）を挿入するデバイスのベース MAC アドレス このフィールドの形式は常に 16 進数フォーマットとなり、区切り文字はありません（例：000000112200）。	6	6
$switch-hostname-16$	デバイスのホスト名の先頭バイト。最大 16 バイトまで。	16	該当なし
$switch-hostname-32$	デバイスのホスト名の先頭バイト。最大 32 バイトまで。	32	該当なし
$switch-hostname-58$	デバイスのホストのフル ネーム。	58	該当なし
$switch-module-id$	DHCP クライアント リクエストが受信されたユニットのユニット ID。 スタンドアロン システムの場合、ID は常に 1。	2	1
$vlan-id$	DHCP クライアントリクエストが受信された VLAN の VLAN ID。 値：1 ～ 4094	4	2
$vlan-name-16$	DHCP クライアント パケットが受信された VLAN に関する、VLAN 名の先頭バイト。最大 16 バイトまで。 指定された VLAN に名前が設定されていない場合は、ifTable MIB エントリの当該 VLAN ifDescr MIB フィールドから値が取得されます。	16	該当なし
$vlan-name-32$	DHCP クライアント リクエストが受信された VLAN のフル ネーム。 指定された VLAN に名前が設定されている場合は、ifTable MIB エントリの当該 ifDescr MIB フィールドから値が取得されます。	32	該当なし

（注） 両サブオプションのペイロードの予約済みバイト数の合計が247バイトを超えることはできません。バイト数は動的に更新されず、画面下部に表示されます。バイト数は、サブオプションに含まれるトークンの予約済みの長さ（上記参照）と、サブオプションで使用される自由形式テキストの文字数を、加算した値に基づいています。

インターフェイスの設定

すべてのインターフェイスまたは VLAN で DHCP リレーおよびスヌーピングを有効化できます。DHCP リレーが機能するには、VLAN またはインターフェイスに IP アドレスを設定する必要があります。

DHCPv4 リレーの概要

DHCP リレーは、DHCP サーバに DHCP パケットをリレーします。デバイスは、IP アドレスを持たない VLAN から受信した DHCP メッセージをリレーできます。IP アドレスのない VLAN で DHCP リレーを有効にすると、Option 82 が自動的に挿入されます。この挿入は特定の VLAN 内のものであり、Option 82 の挿入のグローバル管理状態には影響しません。

DHCPv4 スヌーピングの概要

DHCP スヌーピングは、偽の DHCP 応答パケットの受信を防止し、DHCP アドレスをログに記録するためのセキュリティメカニズムを提供します。これを行うために、DHCP スヌーピングではデバイスのポートは信頼できるポートまたは信頼できないポートのいずれかとして扱われます。信頼できるポートは、DHCP サーバに接続しており、DHCP アドレスの割り当てが許可されているポートです。信頼できるポートで受信した DHCP メッセージは、デバイスをパススルーできます。信頼できないポートは、DHCP アドレスの割り当てが許可されていないポートです。デフォルトでは、すべてのポートは、ユーザが（[Interface Settings] ページで）信頼できると宣言するまで、信頼できないポートであると見なされます。

特定のインターフェイス上で DHCP スヌーピング/リレーを有効にするには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Snooping/Relay] > [Interface Settings] の順にクリックします。

ステップ 2 インターフェイス上で DHCP リレーまたは DHCP スヌーピングを有効にするには、[追加] をクリックします。

ステップ 3 有効にするインターフェイスと機能（**DHCP リレー**、**DHCP ヌーピング**、または両方）を選択します。

（注） DHCP スヌーピング設定は、選択したインターフェイスに IP アドレスが設定されている場合にのみ使用できます。

ステップ 4 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

DHCPスヌーピングで信頼されたインターフェイス

信頼できないポート/LAG からのパケットは DHCP スヌーピング バインディング データベースに照らしてチェックされます（DHCP スヌーピング バインディング データベース （22 ページ）を参照）。デフォルトでは、インターフェイスは信頼されていません。インターフェイスを信頼できるものとして指定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Snooping/Relay] > [DHCP Snooping Trusted Interfaces] の順にクリックします。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

ステップ 3 [Trusted Interface] （信頼できる場合は [Yes]、信頼できない場合は [No]）を選択します。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

DHCP スヌーピング バインディング データベース

DHCP スヌーピング バインディング データベースのメンテナンスについては、次の点に注意してください。

- ステーションが別のインターフェイスに移っても、デバイスは DHCP スヌーピング バインディング データベースを更新しません。
- ポートがダウンしても、そのポートのエントリは削除されません。
- VLAN の DHCP スヌーピングが無効になると、その VLAN 用に収集されたバインド エントリが削除されます。
- データベースが一杯になった場合、DHCP スヌーピングはパケットの転送を続行しますが、新しいエントリは作成されません。IP ソースガードや ARP インスペクションの機能がアクティブの場合、DHCP スヌーピング バインディング データベースに書き込まれていないクライアントは、ネットワークに接続できません。

DHCP スヌーピング バインディング データベースにエントリを追加するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Snooping/Relay] > [DHCP Snooping Binding Database] の順にクリックします。

DHCP スヌーピング バインディング データベース内の IP ソースガードに関するフィールドが表示されます。

- Status
  - [アクティブ] : デバイス上で IP ソース ガードがアクティブです。
  - [Inactive] : デバイス上で IP ソースガードがアクティブではありません。
- 理由

- 問題なし（No Problem）
- リソースなし（No Resource）
- スヌープ VLAN なし（No Snoop VLAN）
- ポートを信頼（Trust Port）

ステップ 2 エントリを追加するには、[Add] をクリックします。サポートされるアドレス タイプは IPv4 です。

ステップ 3 次のフィールドに入力します。

- [VLAN ID]：パケットを受信すると予想される VLAN。
- [MAC Address]：パケットの MAC アドレス。
- [IP Address]：パケットの IP アドレス。
- インターフェイス（Interface）：パケットを受信するユニット/スロット/インターフェイス。
- [Type]：フィールドで可能な値は、次のとおりです。
  - [ダイナミック]：エントリのリース時間は制限されています。
  - [スタティック]：エントリは静的に設定されています。
- リース時間（Lease Time）：エントリがダイナミックの場合は、DHCP データベースでエントリがアクティブである時間を入力します。リース時間がない場合、[Infinite] をチェックします。

ステップ 4 [Apply] をクリックします。設定が定義され、デバイスが更新されます。

ステップ 5 設定を削除するには、[Clear Dynamic] をクリックします。

DHCP サーバ

DHCP サーバー機能により、デバイスを DHCPv4 サーバーとして設定できます。DHCPv4 サーバーは、IPv4 アドレスやその他の情報を別のデバイス（DHCP クライアント）に割り当てるために使用されます。DHCPv4 サーバーは、IPv4 アドレスを、IPv4 アドレスのユーザー定義プールから割り当てます。

これらのモードは、次のいずれかになります。

- スタティック割り当て（Static Allocation）：ホストのハードウェア アドレスまたはクライアント ID が手動で IP アドレスにマッピングされます。
- ダイナミック割り当て（Dynamic Allocation）：クライアントはリースされた IP アドレスを指定された期間（無限に設定可能）にわたって取得します。DHCP クライアントが割り当てられた IP アドレスを更新しない場合は、この期間の終了時に IP アドレスが無効になり、クライアントは別の IP アドレスを要求する必要があります。

DHCP サーバーのプロパティ

デバイスを DHCPv4 サーバーとして設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [Properties] の順にクリックして、[Properties] ページを表示します。

ステップ 2 DHCP サーバとしてデバイスを設定するには、[Enable] を選択します。

ステップ 3 [Apply]をクリックします。デバイスは、直ちにDHCPサーバとして機能します。ただし、プールを作成するまでクライアントに IP アドレスを割り当てません。

ネットワーク プール

デバイスが DHCP サーバーとして機能している場合は、1 つ以上の IP アドレスのプールを定義する必要があります。デバイスはそれらのプールから、DHCP クライアントに IP アドレスを割り当てます。各ネットワーク プールには、特定のサブネットに属しているアドレスの範囲が含まれています。これらのアドレスは、そのサブネット内のさまざまなクライアントに割り当てられます。

クライアントが IP アドレスを要求すると、DHCP サーバとしてのデバイスは、次に従って IP アドレスを割り当てます。

- [Directly Attached Client]：デバイスは、DHCP 要求の受信元であるデバイスの IP インターフェイスで設定されているサブネットと一致するサブネットを持つネットワークプールのアドレスを割り当てます。

  メッセージが（DHCP リレー経由ではなく）直接到着した場合、プールはローカル プールであり、入力レイヤ 2 インターフェイスに定義されている IP サブネットのいずれかに属しています。この場合、プールの IP マスクは、IP インターフェイスの IP マスク、および IP サブネットに属しているプールの最小 IP アドレスと最大 IP アドレスと等しくなります。

- リモート クライアント ：デバイスは、DHCP リレー エージェントの IP アドレスに一致する IP サブネットに属しているネットワーク プールから IP アドレスを取得します。

  メッセージが DHCP リレー経由で到着した場合、使用されるアドレスは、プールの最小 IP アドレスと IP マスクで指定された IP サブネットに属します。このプールはリモート プールです。

最大 16 個のネットワーク プールを定義できます。

IP アドレスのプールを作成し、リース期間を定義するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [Network Pools] の順にクリックします。

定義済みのネットワークプールが表示されます。これらのフィールドについては、次の [Add] ページで説明されています。次のフィールドが表示されます（[Add] ページには表示されません）。

- リースされたアドレスの数（Number of Leased Addresses）：プール内の割り当て（リース）済みのアドレスの数。

ステップ 2 [Add] をクリックして、新しいネットワーク プールを定義します。サブネット IP アドレスとマスク、またはマスク、アドレス プール開始、およびアドレス プール終了のいずれかを入力することに注意してください。

ステップ 3 次のフィールドに入力します。

- [Pool Name]：プール名を入力します。
- サブネット IP アドレス（Subnet IP Address）：ネットワーク プールが存在するサブネットを入力します。
- [Mask]：次のいずれかを入力します。
  - ネットワーク マスク（Network Mask）：プールのネットワーク マスクを確認し、入力します。
  - プレフィックス長（Prefix Length）：アドレス プレフィックスを構成するビットの数を確認し、入力します。
- アドレス プールの開始（Address Pool Start）：ネットワーク プールの範囲の最初の IP アドレスを入力します。
- アドレス プールの開始（Address Pool End）：ネットワーク プールの範囲の最後の IP アドレスを入力します。
- リース期間（Lease Duration）：DHCP クライアントがこのプールから IP アドレスを使用できる時間を入力します。最大 49,710 日のリース期間または無制限の期間を設定できます。
  - 無制限（Infinite）：リースの期間に制限はありません。
  - [Days]：リースの期間（日数）。範囲は 0 ～ 49,710 日です。
  - [Hours]：リースの時間数。時間数の値を追加する前に、日数の値を指定する必要があります。
  - [Minutes]：リースの分数。分数の値を追加する前に、日数の値と時間数の値を指定する必要があります。
- [Default Router IP Address (Option 3)]：DHCP クライアントのデフォルトルータを入力します。
- [Domain Name Server IP Address（Option 6)]：デバイス DNS サーバー（設定済みの場合）の 1 つを選択するか、または [Other] を選択して DHCP クライアントが利用可能な DNS サーバーの IP アドレスを入力します。
- ドメイン名（オプション 15）（Domain Name (Option 15)）：DHCP クライアントのドメイン名を入力します。
- [NetBIOS WINS Server IP Address (Option 44)]：DHCP クライアントが利用可能な NetBIOS WINS ネームネーバを入力します。
- NetBIOS ノード タイプ（オプション 46）（NetBIOS Node Type (Option 46)）：NetBIOS 名を解決する方法を選択します。有効なノード タイプは次のとおりです。

- ハイブリッド（Hybrid）：b ノードと p ノードのハイブリッドな組み合せが使用されます。h ノードを使用するように設定した場合、コンピュータは常に p ノードを最初に試行し、p ノードが失敗した場合にのみ、b ノードを使用します。これはデフォルトです。
- 混合（Mixed）：b ノードと p ノードの通信の組み合わせを、NetBIOS 名を登録して解決するために使用します。M ノードは最初に b ノードを使用し、その後必要に応じて、p ノードを使用します。M ノードでは、b ノードが優先されるため、通常は大規模なネットワークにとって最適な選択肢ではありません。ブロードキャストによってネットワークトラフィックが増加します。
- ピア ツー ピア（Peer-to-Peer）：NetBIOS ネーム サーバとのポイントツー ポイント通信が、コンピュータ名を IP アドレスに登録して解決するために使用されます。
- ブロードキャスト（Broadcast）：IP ブロードキャスト メッセージは、NetBIOS 名を IP アドレスに登録して解決するために使用されます。

- [SNTP Server IP Address (Option 4)]：デバイスの SNTP サーバー（設定済みの場合）の 1 つを選択するか、または [Other] を選択して DHCP クライアントのタイムサーバーの IP アドレスを入力します。
- ファイル サーバの IP アドレス（siaddr）（File Server IP Address (siaddr)）：設定ファイルのダウンロード元である TFTP/SCP サーバの IP アドレスを入力します。
- ファイル サーバのホスト名（sname/オプション 66）（File Server Host Name (sname/Option 66)）：TFTP/SCP サーバの名前を入力します。
- 設定ファイル名（file/オプション 67）（Configuration File Name (file/Option 67)）：設定ファイルとして使用されるファイルの名前を入力します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

除外されるアドレス

デフォルトでは、DHCP サーバは、プール内のすべてのプール アドレスをクライアントに割り当てることができると仮定します。1 つの IP アドレスまたは IP アドレスの範囲を除外することができます。除外アドレスは、すべての DHCP プールから除外されます。

除外されるアドレス範囲を定義するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [Excluded Addresses] の順にクリックします。

定義済みの除外される IP アドレスが表示されます。

ステップ 2 除外する IP アドレスの範囲を追加するには、[Add] をクリックし、次のフィールドに入力します。

- 開始 IP アドレス（Start IP Address）：除外 IP アドレスの範囲の最初の IP アドレス。
- 終了 IP アドレス（End IP Address）：除外 IP アドレスの範囲の最後の IP アドレス。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

スタティックホスト

一部の DHCP クライアントに、変化しないを永続的な IP アドレスを割り当てることができます。このようなクライアントは、スタティック ホストと呼ばれます。スタティック ホストは、最大 120 個定義できます。

特定のクライアントに固定 IP アドレスを手動で割り当てるには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [Static Hosts] の順にクリックします。

スタティック ホストが表示されます。表示されるフィールドについては、次のフィールドを除いて [Add] ページで説明されています。

- MACアドレス/クライアント識別子

ステップ 2 スタティック ホストを追加するには、[Add] をクリックし、次のフィールドに入力します。

IP アドレス	ホストに静的に割り当てられた IP アドレスを入力します。
ホスト名	ホスト名を入力します。ホスト名には、シンボルの文字列と整数を指定できます。
Mask	スタティックホストのネットワークマスクを入力します。 • ネットワーク マスク（Network Mask）：スタティック ホストのネットワーク マスクを確認し、入力します。 • プレフィックス長（Prefix Length）：アドレス プレフィックスを構成するビットの数を確認し、入力します。
識別子タイプ	特定のスタティックホストを識別する方法を設定します。 • クライアント識別子（Client Identifier）：16 進数の表記法で指定されたクライアントの一意の ID を入力します（例：01b60819681172）。 または： • [MAC Address]：クライアントの MAC アドレスを入力します。 選択したタイプに従って、クライアント識別子または MAC アドレスを入力します。
Client Name	標準の ASCII 文字セットを使用して、スタティックホストの名前を入力します。クライアント名にはドメイン名を含めることはできません。

デフォルトルータIPアドレス(オプション3)	スタティックホストのデフォルトルータを入力します。
ドメインネームサーバーIPアドレス(オプション6)	デバイス DNS サーバー（設定済みの場合）の 1 つを選択するか、または [Other] を選択して DHCP クライアントが利用可能な DNS サーバーの IP アドレスを入力します。
ドメイン名(オプション15)	スタティックホストのドメイン名を入力します。
NetBIOS WINSサーバーIPアドレス(オプション44)	スタティックホストで使用可能な NetBIOS WINS ネームサーバーを入力します。
NetBIOSノードタイプ(オプション46)	NetBIOS 名の解決方法を選択します。有効なノードタイプは次のとおりです。 • ハイブリッド（Hybrid）：b ノードと p ノードのハイブリッドな組み合せが使用されます。h ノードを使用するように設定した場合、コンピュータは常に p ノードを最初に試行し、p ノードが失敗した場合にのみ、b ノードを使用します。これはデフォルトです。 • 混合（Mixed）：b ノードと p ノードの通信の組み合わせを、NetBIOS 名を登録して解決するために使用します。M ノードは最初に b ノードを使用し、その後必要に応じて、p ノードを使用します。M ノードでは、b ノードが優先されるため、通常は大規模なネットワークにとって最適な選択肢ではありません。ブロードキャストによってネットワークトラフィックが増加します。 • ピア ツー ピア（Peer-to-Peer）：NetBIOS ネーム サーバとのポイントツーポイント通信が、コンピュータ名を IP アドレスに登録して解決するために使用されます。 • ブロードキャスト（Broadcast）：IP ブロードキャスト メッセージは、NetBIOS 名を IP アドレスに登録して解決するために使用されます。
SNTPサーバーIPアドレス(オプション4)	デバイスの SNTP サーバー（設定済みの場合）の 1 つを選択するか、または [Other] を選択して DHCP クライアントのタイムサーバーの IP アドレスを入力します。
ファイルサーバーIPアドレス(siaddr)	設定ファイルのダウンロード元 TFTP/SCP サーバーの IP アドレスを入力します。
ファイルサーバーホスト名(sname/オプション66)	TFTP/SCP サーバーの名前を入力します。
コンフィギュレーションファイル名(file/オプション67)	設定ファイルとして使用されるファイルの名前を入力します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

DHCP オプション

デバイスが DHCP サーバとして動作している場合は、16 進数オプションを使用して DHCP オプションを設定できます。これらのオプションの説明は、RFC2131 で確認できます。これらのオプションの設定により、設定された DHCP オプションの要求（オプション 55 を使用）が含まれているパケットを持つ DHCP クライアントに送信される応答が決定されます。例：DHCP オプション 66 は、[DHCP Options] ページで TFTP サーバの名前を指定して設定します。オプション 66 が含まれているクライアント DHCP パケットを受信すると、TFTP サーバがオプション 66 の値として返されます。

1 つ以上の DHCP オプションを設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [DHCP Options] の順にクリックします。

それまでに設定された DHCP のオプションが表示されます。

ステップ 2 設定されていないオプションを設定するには、次のフィールドに入力します。

- [DHCP Server Pool Name equals to]：ネットワーク プール （24 ページ）で定義されているネットワークアドレスのプールの 1 つを選択し、[Go] をクリックして、そのネットワークアドレスのプールを基準にしたフィルタ処理を行います。

ステップ 3 [Add] をクリックして、次のフィールドに入力します。

- プール名（Pool Name）：定義されているコードの対象となるプール名が表示されます。
- コード（Code）：DHCP オプション コードを入力します。
- タイプ（Type）：DHCP オプションのパラメータのタイプに応じて、このフィールドのオプション ボタンを変更します。次のいずれかのコードを選択し、DHCP オプションパラメータの値を入力します。
  - 16 進（Hex）：DHCP オプションのパラメータの 16 進数値を入力するかどうかを選択します。16 進数値は、他のタイプの値の代わりに指定できます。たとえば、IP アドレス自体ではなく、IP アドレスの 16 進値を指定できます。

    16 進数値の検証は行われません。そのため、不正な値を表す 16 進数値を入力した場合は、エラーが提供されず、クライアントはサーバからの DHCP パケットを処理できない可能性があります。
  - IP ：これが選択した DHCPオプションに関連する場合は、IP アドレスを入力するかどうかを選択します。
  - [IP List]：複数の IP アドレスをカンマで区切ったリストを入力します。
  - 整数（Integer）：選択した DHCP オプションのパラメータの整数値を入力するかどうかを選択します。
  - ブール（Boolean）：選択した DHCPオプションのパラメータがブール値かどうかを選択します。

- ブール値（Boolean Value）：タイプがブール値である場合は、返される値（True または False）を選択します。
- [Value]：タイプがブーリアンでない場合に、このコードについて送信する値を入力します。
- 説明（Description）：ドキュメンテーションの目的でテキストの説明を入力します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

アドレスバインディング

[Address Binding] ページを使用して、デバイスによって割り当てられた IP アドレスと対応する MAC アドレスを表示および削除します。

アドレスバインディングを表示または削除するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [Address Binding] の順にクリックします。

アドレス バインドに関する次のフィールドが表示されます。

- [IP Address]：DHCP クライアントの IP アドレス。
- [Address Type]：DHCP クライアントのアドレスが MAC アドレスとして表示されるか、クライアント識別子を使用して表示されるかを示します。
- [MACアドレス/クライアント識別子]：MACアドレスとして、または16進表記（例：01b60819681172）として指定される、クライアントの固有識別子。
- リースの有効期限（Lease Expiration）：ホストの IP アドレスのリースの有効期日および時刻。
- タイプ（Type）：IP アドレスがクライアントに割り当てられた方法。オプションは次のいずれかです。
  - スタティック（Static）：ホストのハードウェア アドレスが IP アドレスにマッピングされています。
  - [Dynamic]：デバイスから動的に取得される IP アドレスが、指定された期間クライアントによって所有されている場合。指定された期間が終了すると IP アドレスは無効になり、クライアントは別の IP アドレスを要求する必要があります。
- [State]：次のオプションがあります。
  - 割り当て済み（Allocated）：IP アドレスが割り当てられています。スタティック ホストが設定されている場合は、その状態は割り当て済みです。
  - [Allocated]：IP アドレスは提供されているが受け入れられなかったため、割り当てられていません。
  - 期限切れ（Expired）：IP アドレスのリースの有効期限が切れています。

- [Pre-Allocated]：エントリは、提供されたときから、クライアントから DHCP ACK が送信されるまでの間、事前割り当て済み状態になります。その後、割り当て済みになります。

ステップ 2 [Delete] をクリックします。実行コンフィギュレーション ファイルが更新されます。

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。