CHAPTER 23

# ダイナミック ARP 検査の設定

この章では、Catalyst 3750 スイッチにダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）検査を設定する方法について説明します。この機能により、無効な ARP 要求および応答を同じ VLAN（仮想 LAN）内の他のポートにリレーしないことで、スイッチでの悪質な攻撃を排除します。特に明記しないかぎり、*スイッチ*という用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

（注） この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

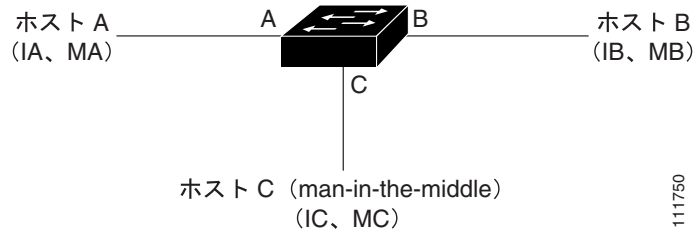
この章で説明する内容は、次のとおりです。

# ダイナミック ARP 検査の設定

ARP は、IP アドレスを MAC（メディア アクセス制御）アドレスにマッピングすることにより、レイヤ 2 ブロードキャスト ドメイン内で IP 通信を提供します。たとえば、ホスト B がホスト A に情報を送信したいが、ARP キャッシュのホスト A に MAC アドレスがないと想定します。ホスト A の IP アドレスに対応付けられた MAC アドレスを取得するため、ホスト B はブロードキャスト ドメイン内のすべてのホストに対しブロードキャスト メッセージを生成します。ブロードキャスト ドメイン内のすべてのホストは ARP 要求を受信し、ホスト A は取得した MAC アドレスで応答します。ただし、ARP 要求が受信されなかった場合も、ARP はホストから Gratuitous 応答を許可するので、ARP スプーフィング攻撃および ARP キャッシュのポイズニングが発生します。攻撃のあと、攻撃にさらされたデバイスからのトラフィックすべては、攻撃者のコンピュータを通過し、続いてルータ、スイッチ、ホストを通過します。

悪意のあるユーザは、サブネットに接続されたシステムの ARP キャッシュをポイズニングすることで、またサブネット上の他のホストへのトラフィックを代行受信することで、レイヤ 2 ネットワークに接続されたホスト、スイッチ、ルータを攻撃できます。図 23-1 に、ARP キャッシュ ポイズニングの例を示します。

**図 23-1　ARP キャッシュ ポイズニング**




ホスト A、B、C はインターフェイス A、B、C に接続され、すべてが同じサブネット上に存在します。これらの IP および MAC アドレスをカッコ内に示します。たとえば、ホスト A は IP アドレスの IA および MAC アドレスの MA を使用します。ホスト A が IP レイヤでホスト B と通信する必要がある場合、ホスト A は、IP アドレス IB に対応付けられた MAC アドレスに対し、ARP 要求をブロードキャストします。スイッチおよびホスト B が ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持ったホストへの ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は MAC アドレス MA にバインドされます。ホスト B が応答したとき、スイッチおよびホスト A は、IP アドレス IB および MAC アドレス MB へのホストのバインディングを ARP キャッシュに読み込みます。

ホスト C は、IP アドレス IA（または IB）および MAC アドレス MC を保持するホストに、バインディングを持つ偽造 ARP 要求をブロードキャストすることにより、スイッチ A、ホスト A、ホスト B の ARP キャッシュをポイズニングする可能性があります。ポイズニングされた ARP キャッシュがあるホストでは、IA または IB 向けトラフィックの宛先 MAC アドレスとして、MAC アドレス MC を使用します。つまり、ホスト C がトラフィックを代行受信することになります。ホスト C は IA および IB に対応付けられた真の MAC アドレスを知っているので、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は、ホスト A からホスト B へのトラフィック ストリーム、すなわち典型的な *man-in-the-middle* 攻撃に自ら入り込んでいます。

ダイナミック ARP 検査は、ネットワーク内の ARP パケットを検証するセキュリティ機能です。ダイナミック ARP 検査は、無効な IP/MAC アドレス バインディングのある ARP パケットを代行受信し、記録し、廃棄します。この機能は特定の man-in-the-middle 攻撃からネットワークを保護します。

ダイナミック ARP 検査では、有効な ARP 要求および応答のみが確実にリレーされます。スイッチは次のアクティビティを実行します。

- 信頼できないポートで ARP 要求および応答すべてを代行受信します。
- ローカル ARP キャッシュを更新する、またはパケットを適切な宛先に転送する前に、代行受信されたパケットそれぞれに有効な IP/MAC アドレス バインディングが含まれていることを確認します。
- 無効な ARP パケットを廃棄します。

ダイナミック ARP 検査は、信頼できるデータベースである Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースに保存された、有効な IP/MAC アドレス バインディングに基づき、ARP パケットの妥当性を決定します。DHCP スヌーピングが VLAN およびスイッチでイネーブルの場合、このデータベースは DHCP スヌーピングによって構築されます。ARP パケットが信頼できるインターフェイスで受信された場合、スイッチはチェックしないでパケットを転送します。信頼できないインターフェイスでは、スイッチは有効なパケットのみを転送します。

**ip arp inspection vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用して、VLAN 単位でダイナミック ARP 検査をイネーブルにできます。設定の詳細については、「DHCP 環境でのダイナミック ARP 検査の設定」（p.23-7）を参照してください。

DHCP 以外の環境では、ダイナミック ARP 検査は、スタティックに設定された IP アドレスのあるホストのユーザ設定 ARP Access Control List（ACL; アクセス制御リスト）に対して、ARP パケットを有効にできます。**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用して、ARP ACL を定義できます。設定の詳細については、「DHCP 以外の環境での ARP ACL の設定」（p.23-9）を参照してください。スイッチは廃棄されたパケットを記録します。ログ バッファの詳細については、「廃棄されたパケットのロギング」（p.23-5）を参照してください。

ダイナミック ARP 検査を設定して、パケットの IP アドレスが無効である、または ARP パケット形式の MAC アドレスがイーサネット ヘッダーで指定されたアドレスと一致しない場合に ARP パケットを廃棄できます。**ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} グローバル コンフィギュレーション コマンドを使用します。詳細については、「妥当性チェックの実施」（p.23-12）を参照してください。

## インターフェイスの信頼状態およびネットワーク セキュリティ

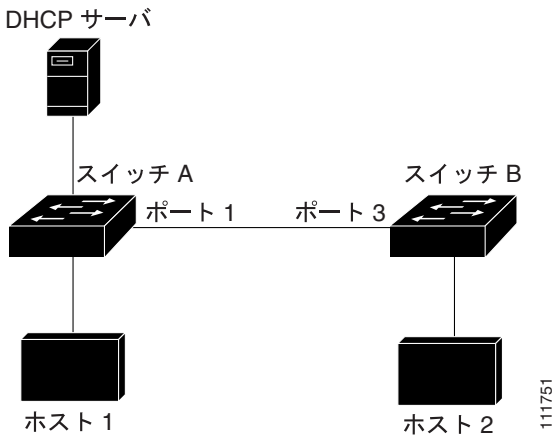
ダイナミック ARP 検査は、信頼状態とスイッチの各インターフェイスとを関連付けます。信頼できるインターフェイスに着信するパケットはダイナミック ARP 検査妥当性チェックをすべてバイパスします。信頼できないインターフェイスに着信するパケットはダイナミック ARP 検査妥当性チェックを受けます。

一般的なネットワーク設定では、ホスト ポートに接続されたスイッチすべてを untrusted として、スイッチに接続されたスイッチ ポートすべてを trusted として設定します。この設定では、所定のスイッチからネットワークに入力する ARP パケットすべてはセキュリティ チェックをバイパスします。VLAN またはネットワーク内の他の場所で検証を実行する必要はありません。**ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用して、信頼設定を設定できます。

**注意**　信頼状態設定は慎重に使用してください。インターフェイスが信頼される必要があるときに untrusted として設定すると、接続が切断されます。

図 23-2 では、スイッチ A およびスイッチ B 両方が、ホスト 1 およびホスト 2 を含む VLAN 上でダイナミック ARP 検査を実行していると想定します。ホスト 1 およびホスト 2 が、スイッチ A に接続された DHCP サーバから IP アドレスを取得した場合、スイッチ A のみがホスト 1 の IP/MAC アドレスをバインドします。従って、スイッチ A とスイッチ B の間のインターフェイスが信頼できない場合、ホスト 1 からの ARP パケットはスイッチ B によって廃棄されます。ホスト 1 およびホスト 2 の間の接続は切断されます。

**図 23-2　ダイナミック ARP 検査用にイネーブルにされた VLAN 上での ARP パケット検証**




インターフェイスが実際に信頼できない場合に信頼できるように設定すると、ネットワークにセキュリティ ホールが残ります。スイッチ A でダイナミック ARP 検査が稼働していない場合、ホスト 1 は容易にスイッチ B（スイッチの間のリンクが trusted として設定されている場合はホスト 2）の ARP キャッシュをポイズニングできます。スイッチ B でダイナミック ARP 検査を稼働しているときでも、これは発生します。

ダイナミック ARP 検査は、ダイナミック ARP 検査を稼働しているスイッチに接続された（untrusted インターフェイスの）ホストが、ネットワーク内の他のホストの ARP キャッシュをポイズニングしていないことを確認します。ただし、ダイナミック ARP 検査はネットワークの他の部分にいるホストが、ダイナミック ARP 検査を実行するスイッチに接続されたホストのキャッシュをポイズニングすることを禁止できません。

VLAN の一部のスイッチではダイナミック ARP 検査が実行され、他のスイッチでは実行されない場合、untrusted であるスイッチと接続するようにインターフェイスを設定します。ただし、非ダイナミック ARP 検査スイッチからのパケットのバインディングを検証するには、ダイナミック ARP 検査を実行するスイッチを ARP ACL で設定します。レイヤ 3 でバインディングを決定できない場合、ダイナミック ARP 検査を実行するスイッチとダイナミック ARP 検査を実行しないスイッチを切り離します。設定の詳細については、「DHCP 以外の環境での ARP ACL の設定」（p.23-9）を参照してください。

**（注）** DHCP サーバおよびネットワークの設定によって、VLAN 内のすべてのスイッチの特定の ARP パケットを検証できないことがあります。

## ARP パケットのレート制限

スイッチ CPU はダイナミック ARP 検査妥当性チェックを実施するので、DoS 攻撃を防ぐため着信 ARP パケット数がレート制限されます。デフォルトでは、信頼できないインターフェイスのレートは 15 パケット / 秒（pps）です。信頼できるインターフェイスはレート制限を受けません。**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用して、この設定を変更できます。

着信 ARP パケットのレートが設定された制限を越えると、スイッチはポートを errdisable ステートにします。調整するまで、ポートはこのステートのままです。指定されたタイムアウト時間が経過したあと、ポートがこのステートから自動的に抜け出せるように、errdisable 回復をイネーブルにするには、**errdisable recovery** グローバル コンフィギュレーション コマンドを使用します。

（注）　EtherChannel のレート制限は、スタック内の各スイッチに別々に適用されます。たとえば、EtherChannel で 20 pps の制限が設定されている場合、EtherChannel にポートを持つ各スイッチは最大 20 pps を搬送できます。スイッチの 1 つが制限を超えると、EtherChannel 全体が errdisable ステートになります。

設定の詳細については、「着信 ARP パケットのレート制限」（p.23-11）を参照してください。

## ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP 検査は、有効な IP/MAC アドレス バインディングのリスト用 DHCP スヌーピング バインディング データベースを使用します。

ARP ACL は DHCP スヌーピング バインディング データベースのエントリよりも優先されます。スイッチは、**ip arp inspection filter vlan** グローバル コンフィギュレーション コマンドを使用して ACL を設定する場合にのみ、ACL を使用します。スイッチは始めに ARP パケットとユーザ設定された ARP ACL を比較します。ARP ACL が ARP パケットを拒否した場合、DHCP スヌーピングによって実装されたデータベースに有効なバインディングが存在したとしても、スイッチもパケットを拒否します。

## 廃棄されたパケットのロギング

スイッチがパケットを廃棄する場合、スイッチはエントリをログ バッファに置き、レート制御ごとにシステム メッセージを生成します。メッセージが生成されたら、スイッチはログ バッファからエントリを消去します。各ログ エントリには、受信 VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスなどのフロー情報が含まれます。

バッファのエントリ数、指定されたインターバルでのシステム メッセージ生成に必要なエントリ数を指定するには、**ip arp inspection log-buffer** グローバル コンフィギュレーション コマンドを使用します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用して、ロギングされているパケット タイプを指定します。設定の詳細については、「ログ バッファの設定」（p.23-13）を参照してください。

# ダイナミック ARP 検査の設定

ここでは、次の設定について説明します。



## ダイナミック ARP 検査のデフォルト設定

表 23-1 に、ダイナミック ARP 検査のデフォルト設定を示します。

**表 23-1　ダイナミック ARP 検査のデフォルト設定**

| 機能 | デフォルト設定 |
|---|---|
| ダイナミック ARP 検査 | すべての VLAN でディセーブルになっています。 |
| インターフェイス信頼状態 | すべてのインターフェイスが信頼できません。 |
| 着信 ARP パケットのレート制限 | ネットワークがスイッチド ネットワークでホストが 1 秒あたり 15 の新しいホストと接続することを想定した場合、レートは信頼できないインターフェイスで 15 pps です。<br>信頼できるすべてのインターフェイス上ではレートは制限されません。<br>バースト間隔は 1 秒です。 |
| DHCP 以外の環境の ARP ACL | ARP ACL は定義されません。 |
| 妥当性チェック | 妥当性チェックは実行されません。 |
| ログ バッファ | ダイナミック ARP 検査がイネーブルの場合、拒否または廃棄された ARP パケットすべてが記録されます。<br>ログのエントリ数は 32 です。<br>システム メッセージ数は 5 個 / 秒に制限されています。<br>ロギングレート インターバルは 1 秒です。 |
| VLAN 単位のロギング | 拒否または廃棄された ARP パケットすべてが記録されます。 |

## ダイナミック ARP 検査設定時の注意事項

ダイナミック ARP 検査設定時の注意事項は次のとおりです。

- ダイナミック ARP 検査は入力セキュリティ機能で、出力チェックは行いません。
- ダイナミック ARP 検査は、ダイナミック ARP 検査をサポートしないスイッチ、またはこの機能がイネーブルでないスイッチに接続されたホストに対し、有効ではありません。man-in-the-middle 攻撃は単一のレイヤ 2 ブロードキャスト ドメインに制限されているので、ダイナミック ARP 検査チェックのあるドメインをチェックなしドメインから切り離します。このアクションにより、ダイナミック ARP 検査用にイネーブルされたドメイン内のホストの ARP キャッシュを保護します。

- ダイナミック ARP 検査は、着信 ARP 要求および ARP 応答の IP/MAC アドレス バインディングを確認する DHCP スヌーピング バインディング データベースのエントリによって異なります。DHCP スヌーピングをイネーブルにして、動的に IP アドレスを割り当てた ARP パケットを許可できることを確認します。設定の詳細については、第 22 章「DHCP 機能および IP ソース ガードの設定」を参照してください。

  DHCP スヌーピングがディセーブルである、または DHCP 以外の環境にいる場合、ARP ACL を使用してパケットを許可または拒否できます。
- ダイナミック ARP 検査はアクセス ポート、トランク ポート、EtherChannel ポート、およびプライベート VLAN でサポートされます。
- 物理ポートとチャネル　ポートの信頼状態が一致する場合にのみ、物理ポートは　EtherChannel ポート チャネルに参加できます。そうでない場合、物理ポートは、ポート チャネルで一時停止のままです。ポート チャネルは、チャネルに参加する最初の物理ポートからの信頼状態を継承します。従って、最初の物理ポートの信頼状態はチャネルの信頼状態と一致する必要はありません。

  反対に、ポート チャネルの信頼状態を変更する場合、スイッチはチャネルを構成する物理ポートすべてに新しい信頼状態を設定します。
- レート制限はスイッチ スタックの各スイッチで個別に計算されます。クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも大きいことを意味します。たとえば、スイッチ 1 にポートが 1 つ、スイッチ 2 にポートが 1 つある EtherChannel 上でレート制限を 30 pps に設定した場合、EtherChannel を errdisable にせずに、各ポートは 29 pps でパケットを受信できます。
- ポート チャネルの動作レートは、チャネル内の物理ポートすべてにわたって累積されたものです。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定する場合、チャネル上の組み合わされたインターフェイスすべてで 400 pps のレートで受信します。EtherChannel ポート上の着信 ARP パケットのレートは、すべてのチャネル メンバーからのパケットの着信レートの合計に等しくなります。チャネル ポート メンバー上の着信 ARP パケットのレートを調べたあとでのみ、EtherChannel ポートのレート制限を設定します。

  物理ポートの着信パケットのレートは、物理ポート設定ではなく、ポート チャネル設定に対してチェックされます。ポート チャネルのレート制限設定は、物理ポートの設定に依存しません。

  EtherChannel が設定されたレートよりも多い ARP パケットを受信した場合、チャネル（すべての物理ポートを含む）は errdisable ステートになります。
- 着信トランク ポートの ARP パケットのレート制限を確認します。集約を反映させ、複数のダイナミック ARP 検査対応 VLAN でパケットを処理するには、より高いレートでトランク ポートを設定します。レートを無制限にするには、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用します。ある VLAN でレート制限が高いと、ソフトウェアがポートを errdisable ステートにしたときに、他の VLAN が DoS 攻撃にさらされます。

## DHCP 環境でのダイナミック ARP 検査の設定

次の手順では、2 つのスイッチがダイナミック ARP 検査機能をサポートする場合にダイナミック ARP 検査を設定する方法を示します。ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B に接続されています（図 23-2 [p.23-4] を参照）。両方のスイッチとも、ホストが置かれている VLAN 1 でダイナミック ARP 検査を実行します。DHCP サーバはスイッチ A に接続されています。両方のホストとも同じ DHCP サーバから IP アドレスを取得します。従って、スイッチ A にはホスト 1 およびホスト 2 のバインディングが、スイッチ B にはホスト 2 のバインディングが含まれます。

（注）　ダイナミック ARP 検査は、着信 ARP 要求および ARP 応答の IP/MAC アドレス バインディングを確認する DHCP スヌーピング バインディング データベースのエントリによって異なります。DHCP スヌーピングをイネーブルにして、動的に IP アドレスを割り当てた ARP パケットを許可できることを確認します。設定の詳細については、第 22 章「DHCP 機能および IP ソース ガードの設定」を参照してください。

1 つのスイッチのみがダイナミック ARP 検査機能をサポートする場合にダイナミック ARP 検査を設定する方法については、「DHCP 以外の環境での ARP ACL の設定」（p.23-9）を参照してください。

ダイナミック ARP 検査を設定するには、イネーブル EXEC モードで次の手順を行います。この手順は両方のスイッチで行う必要があります。この手順は必須です。

| | コマンド | 説明 |
|---|---|---|
| ステップ 1 | **show cdp neighbors** | スイッチ間の接続を確認します。 |
| ステップ 2 | **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 3 | **ip arp inspection *vlan*** *vlan-range* | VLAN 単位でダイナミック ARP 検査をイネーブルにします。デフォルトでは、ダイナミック ARP 検査は VLAN すべてでディセーブルに設定されています。<br><br>*vlan-range* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。<br><br>両方のスイッチに同じ VLAN ID を指定します。 |
| ステップ 4 | **interface** *interface-id* | 他のスイッチに接続されたインターフェイスを指定し、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 5 | **ip arp inspection trust** | スイッチ間の接続を trusted として設定します。<br><br>デフォルトでは、すべてのインターフェイスは untrusted に設定されています。<br><br>スイッチは、信頼できるインターフェイスの他のスイッチから受信した ARP パケットをチェックしません。単にパケットを転送するだけです。<br><br>信頼できないインターフェイスの場合、スイッチは ARP 要求および応答をすべて代行受信します。ローカル キャッシュを更新する前、およびパケットを適切な宛先に転送する前に、スイッチは代行受信されたパケットに有効な IP/MAC アドレス バインディングが含まれていることを確認します。スイッチは、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従って、無効なパケットを廃棄し、それらをバッファに記録します。詳細については、「ログ バッファの設定」（p.23-13）を参照してください。 |
| ステップ 6 | **end** | イネーブル EXEC モードに戻ります。 |
| ステップ 7 | **show ip arp inspection interfaces**<br><br>**show ip arp inspection vlan** *vlan-range* | ダイナミック ARP 検査設定を確認します。 |
| ステップ 8 | **show ip dhcp snooping binding** | DHCP バインディングを確認します。 |
| ステップ 9 | **show ip arp inspection statistics vlan** *vlan-range* | ダイナミック ARP 検査統計情報をチェックします。 |
| ステップ 10 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ダイナミック ARP 検査をディセーブルにするには、**no ip arp inspection vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。インターフェイスを untrusted ステートに戻すには、**no ip arp inspection trust** インターフェイス コンフィギュレーション コマンドを使用します。

次に、VLAN 1 のスイッチ A でダイナミック ARP 検査を設定する方法を示します。スイッチ B でも同様の手順を実施します。

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip arp inspection trust
```

## DHCP 以外の環境での ARP ACL の設定

次の手順では、スイッチ B（図 23-2 [p.23-4] を参照）がダイナミック ARP 検査機能、または DHCP スヌーピングをサポートしない場合にダイナミック ARP 検査を設定する方法を示します。

スイッチ A のポート 1 を trusted として設定する場合、スイッチ A およびホスト 1 の両方ともスイッチ B またはホスト 2 による攻撃を受けるので、セキュリティ ホールが作成されます。この攻撃を防ぐには、スイッチ A のポート 1 を untrusted として設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL を設定し、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックでない（スイッチ A の ACL 設定を適用できない）場合、レイヤ 3 でスイッチ A とスイッチ B を切り離し、ルータを使用してスイッチの間のパケットをルーティングします。

スイッチ A で ARP ACL を設定するには、イネーブル EXEC モードで次の手順を実行します。この手順は DHCP 以外の環境で必要です。

| | コマンド | 説明 |
|---|---|---|
| ステップ 1 | **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 | **arp access-list** *acl-name* | ARP ACL を定義し、ARP アクセスリスト コンフィギュレーション モードを開始します。デフォルトで、ARP アクセス リストは定義されていません。<br><br>（注）　ARP アクセス リストの最後に、暗黙の **deny ip any mac any** コマンドがあります。 |
| ステップ 3 | **permit ip host** *sender-ip* **mac host** *sender-mac* [**log**] | 指定されたホスト（ホスト 2）からの ARP パケットを許可します。<br>• *sender-ip* には、ホスト 2 の IP アドレスを入力します。<br>• *sender-mac* には、ホスト 2 の MAC アドレスを入力します。<br>• （任意）ログ バッファのパケットが Access Control Entry（ACE; アクセス制御エントリ）と一致する場合、そのパケットを記録するには、**log** を指定します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドの **matchlog** キーワードを設定しても、一致が記録されます。詳細については、「ログ バッファの設定」（p.23-13）を参照してください。 |
| ステップ 4 | **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。 |

| | コマンド | 説明 |
|---|---|---|
| ステップ 5 | **ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**] | ARP ACL を VLAN に適用します。デフォルトでは、定義された ARP ACL は VLAN に適用されません。<br>• *arp-acl-name* には、ステップ 2 で作成した ACL 名を指定します。<br>• *vlan-range* には、スイッチおよびホストがある VLAN を指定します。VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。<br>• （任意）ARP ACL の暗黙の拒否を明示的な拒否として扱い、ACL の前のステートメントと一致しないパケットを廃棄するには、**static** を指定します。DHCP バインディングは使用しません。<br>このキーワードを指定しない場合、パケットを拒否する明示的な拒否が ACL にないことを意味します。また、パケットが ACL のステートメントと一致しない場合に、DHCP バインディングがパケットを許可または拒否するかどうかを決定することを意味します。<br>IP/MAC アドレス バインディングのみを含む ARP パケットは、ACL に対して比較されます。アクセス リストが許可した場合にのみ、パケットは許可されます。 |
| ステップ 6 | **interface** *interface-id* | スイッチ B に接続されたスイッチ A インターフェイスを指定し、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 7 | **no ip arp inspection trust** | スイッチ B に接続されたスイッチ A インターフェイスを untrusted として設定します。<br>デフォルトでは、すべてのインターフェイスは untrusted に設定されています。<br>信頼できないインターフェイスの場合、スイッチは ARP 要求および応答をすべて代行受信します。ローカル キャッシュを更新する、またはパケットを適切な宛先に転送する前に、スイッチは代行受信されたパケットに有効な IP/MAC アドレス バインディングが含まれていることを確認します。スイッチは、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング設定に従って、無効なパケットを廃棄し、それらをバッファに記録します。詳細については、「ログ バッファの設定」（p.23-13）を参照してください。 |
| ステップ 8 | **end** | イネーブル EXEC モードに戻ります。 |
| ステップ 9 | **show arp access-list** [*acl-name*]<br>**show ip arp inspection vlan** *vlan-range*<br>**show ip arp inspection interfaces** | 設定を確認します。 |
| ステップ 10 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

ARP ACL を削除するには、**no arp access-list** グローバル コンフィギュレーション コマンドを使用します。VLAN に付加された ARP ACL を削除するには、**no ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチ A で ARP ACL（*host2*）を設定し、ホスト 2（IP アドレス 1.1.1.1 および MAC アドレス 0001.0001.0001）からの ARP パケットを許可し、ACL を VLAN 1 に適用し、スイッチ A のポート 1 を untrusted として設定する例を示します。

```
Switch(config)# arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter host2 vlan 1
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no ip arp inspection trust
```

## 着信 ARP パケットのレート制限

スイッチ CPU はダイナミック ARP 検査妥当性チェックを実施するので、DoS 攻撃を防ぐため着信 ARP パケット数がレート制限されます。

着信 ARP パケットのレートが設定された制限を越えると、スイッチはポートを errdisable ステートにします。指定されたタイムアウト時間が経過したあと、ポートがこのステートから自動的に抜け出せるように、errdisable 回復をイネーブルにするまで、ポートは errdisable ステートのままです。

**（注）** インターフェイスでレート制限を設定しない場合、インターフェイスの信頼状態を変更すると、レート制限を信頼状態のデフォルト設定に変更します。レート制限を設定したあと、信頼状態が変更されるまでインターフェイスはこのレート制限を保持します。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

レート制限トランク ポートおよび EtherChannel ポートの設定時の注意事項については、「ダイナミック ARP 検査設定時の注意事項」（p.23-6）を参照してください。

着信 ARP パケットのレートを制限するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 説明 |
|---|---|---|
| ステップ 1 | **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 | **interface** *interface-id* | レートを制限するインターフェイスを指定し、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 3 | **ip arp inspection limit** {**rate** *pps* [**burst interval** *seconds*] \| **none**} | インターフェイスで、着信 ARP 要求および応答のレートを制限します。<br><br>デフォルトのレートは信頼できないインターフェイスでは 15 pps で、信頼できるインターフェイスでは無制限です。バースト インターバルは 1 秒です。<br><br>キーワードの意味は次のとおりです。<br><br>• **rate** *pps* では、秒あたりで処理される着信パケット数の上限を指定します。指定できる範囲は 0 ～ 2048 pps です。<br>• （任意）**burst interval** *seconds* では、秒単位の連続したインターバルを指定します。このインターバルでは ARP パケットのレートが大きい場合にインターフェイスをモニタします。指定できる範囲は 1 ～ 15 です。<br>• **rate none** では、処理できる着信 ARP パケットのレートの上限を指定します。 |

| | コマンド | 説明 |
|---|---|---|
| ステップ 4 | **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 5 | **errdisable recovery cause arp-inspection interval** *interval* | （任意）ダイナミック ARP 検査 errdisable ステートからエラー回復をイネーブルにします。<br>デフォルトでは、回復はディセーブルに設定されており、回復インターバルは 300 秒です。<br>**interval** *interval* では、errdisable ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ～ 86400 です。 |
| ステップ 6 | **exit** | イネーブル EXEC モードに戻ります。 |
| ステップ 7 | **show ip arp inspection interfaces**<br>**show errdisable recovery** | 設定を確認します。 |
| ステップ 8 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

デフォルトのレート制限設定に戻すには、**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。ダイナミック ARP 検査のエラー メッセージ回復をディセーブルにするには、**no errdisable recovery cause arp-inspection** グローバル コンフィギュレーション コマンドを使用します。

## 妥当性チェックの実施

ダイナミック ARP 検査は、無効な IP/MAC アドレス バインディングのある ARP パケットを代行受信し、記録し、廃棄します。宛先 MAC アドレス、発信者 IP アドレスおよび対象 IP アドレス、送信元 MAC アドレスで追加チェックを実施するようにスイッチを設定できます。

着信 ARP パケットで特定のチェックを実施するには、イネーブル EXEC モードで次の手順を実行します。この手順は任意です。

| | コマンド | 説明 |
|---|---|---|
| ステップ 1 | **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 | **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} | 着信 ARP パケットで特定のチェックを実施します。デフォルトでは、チェックは実施されません。<br><br>キーワードの意味は次のとおりです。<br><br>• **src-mac** では、ARP 形式の発信者 MAC アドレスに対して、イーサネット ヘッダーの送信元 MAC アドレスをチェックします。チェックは ARP 要求および応答の両方で実施されます。イネーブルの場合、異なる MAC アドレスのあるパケットは無効として分類され、廃棄されます。<br>• **dst-mac** では、ARP 形式の対象 MAC アドレスに対して、イーサネット ヘッダーの宛先 MAC アドレスを検査します。この検査は ARP 応答で実施されます。イネーブルの場合、異なる MAC アドレスのあるパケットは無効として分類され、廃棄されます。<br>• **ip** では、無効で予期しない IP アドレスの ARP 形式をチェックします。アドレスには、0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。発信者 IP アドレスは ARP 要求および応答すべてでチェックされ、対象 IP アドレスは ARP 応答でのみチェックされます。<br><br>最低 1 つのキーワードを指定する必要があります。各コマンドは前のコマンドの設定を上書きします。たとえば、あるコマンドが **src** および **dst mac** 検証をイネーブルにし、2 番めのコマンドが IP 検証のみをイネーブルにした場合、2 番めのコマンドによって **src** および **dst mac** 検証はディセーブルになります。 |
| ステップ 3 | **exit** | イネーブル EXEC モードに戻ります。 |
| ステップ 4 | **show ip arp inspection vlan** *vlan-range* | 設定を確認します。 |
| ステップ 5 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

チェックをディセーブルにするには、**no ip arp inspection validate** [**src-mac**] [**dst-mac**] [**ip**] グローバル コンフィギュレーション コマンドを使用します。転送されたパケット、廃棄されたパケット、MAC 検証が失敗したパケット、および IP 検証が失敗したパケットの統計情報を表示するには、**show ip arp inspection statistics** イネーブル EXEC コマンドを使用します。

## ログ バッファの設定

スイッチがパケットを廃棄する場合、スイッチはエントリをログ バッファに置き、レート制御ごとにシステム メッセージを生成します。メッセージが生成されたら、スイッチはログ バッファからエントリを消去します。各ログ エントリには、受信 VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスなどのフロー情報が含まれます。

ログバッファ エントリでは、複数のパケットを表します。インターフェイスが、たとえば、同じ ARP パラメータを持った同じ VLAN で多くのパケットを受信した場合、スイッチはパケットをログ バッファの 1 つのエントリとして結合し、エントリに対し 1 つのシステム メッセージを生成します。

ログ バッファがオーバーフローした場合、ログ イベントがログ バッファに適合していないことを意味します。また、**show ip arp inspection log** イネーブル EXEC コマンドの表示が影響を受けたことを意味します。パケット カウントおよび時間以外のすべてのデータの代わりに、-- が表示されます。他の統計情報はエントリに提供されません。このエントリ表示を見ると、ログ バッファのエントリ数またはロギング レートが増加しています。

ログ バッファ設定は、スイッチ スタックの各スタック メンバーに適用されます。各スタック メンバーには指定された **logs** *number* エントリが含まれ、設定されたレートでシステム メッセージを生成します。たとえば、インターバル（レート）が 1 エントリ / 秒の場合、最大 5 つのシステム メッセージが 5 メンバー スイッチ スタック内で秒ごとに生成されます。

ログ バッファを設定するには、イネーブル EXEC モードで次の手順を行います。この手順は任意です。

| | コマンド | 説明 |
|---|---|---|
| ステップ 1 | **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 | **ip arp inspection log-buffer** {**entries** *number* \| **logs** *number* **interval** *seconds*} | ダイナミック ARP 検査ロギング バッファを設定します。<br>デフォルトでは、ダイナミック ARP 検査がイネーブルの場合、拒否または廃棄された ARP パケットが記録されます。ログ エントリ数は 32 です。システム メッセージ数は 5 個 / 秒に制限されています。ロギング レート インターバルは 1 秒です。<br>キーワードの意味は次のとおりです。<br>• **entries** *number* では、バッファに記録するエントリ数を指定します。指定できる範囲は 0 ～ 1024 です。<br>• **logs** *number* **interval** *seconds* では、指定されたインターバルでシステム メッセージを生成するエントリ数を指定します。<br>**logs** *number* では、指定できる範囲は 0 ～ 1024 です。0 はエントリがログ バッファ内にありますが、システム メッセージが生成されないことを意味します。<br>**interval** *seconds* では、指定できる範囲は 0 ～ 86400 秒（1 日）です。0 はシステム メッセージをただちに生成すること（およびログ バッファが常に空であること）を意味します。<br>0 のインターバル設定は 0 のログ設定を上書きします。<br>**logs** 設定および **interval** 設定は相互に作用します。**logs** *number* X が **interval** *seconds* Y より大きい場合、Y によって割られた X（X/Y）個のシステム メッセージが毎秒送信されます。その他に、あるシステム メッセージは、X によって割られた Y（Y/X）秒ごとに送信されます。 |

| | コマンド | 説明 |
|---|---|---|
| ステップ 3 | **ip arp inspection vlan** *vlan-range* **logging** {**acl-match** {**matchlog** \| **none**} \| **dhcp-bindings** {**all** \| **none** \| **permit**}} | VLAN ごとにロギングされるパケット タイプを制御します。デフォルトでは、拒否または廃棄された ARP パケットすべてが記録されます。*logged* という用語は、エントリがログ バッファにあり、システム メッセージが生成されていることを意味します。<br><br>キーワードの意味は次のとおりです。<br><br>• *vlan-range* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。<br>• **acl-match matchlog** では、ACE ロギング設定に基づきパケットを記録します。このコマンドに **matchlog** キーワードを指定し、**permit** または **deny** ARP アクセス リスト コンフィギュレーション コマンドに **log** キーワードを指定すると、ACL によって許可または拒否された ARP パケットが記録されます。<br>• **acl-match none** では、ACL と一致するパケットを記録しません。<br>• **dhcp-bindings all** では、DHCP バインディングと一致するパケットをすべて記録します。<br>• **dhcp-bindings none** では、DHCP バインディングと一致するパケットを記録しません。<br>• **dhcp-bindings permit** では、DHCP バインディング許可パケットを記録します。 |
| ステップ 4 | **exit** | イネーブル EXEC モードに戻ります。 |
| ステップ 5 | **show ip arp inspection log** | 設定を確認します。 |
| ステップ 6 | **copy running-config startup-config** | （任意）コンフィギュレーション ファイルに設定を保存します。 |

デフォルト ログ バッファ設定に戻すには、**no ip arp inspection log-buffer** {**entries** | **logs**} グローバル コンフィギュレーション コマンドを使用します。デフォルトの VLAN ログ設定に戻すには、**no ip arp inspection vlan** *vlan-range* **logging** {**acl-match** | **dhcp-bindings**} グローバル コンフィギュレーション コマンドを使用します。ログ バッファを消去するには、**clear ip arp inspection log** イネーブル EXEC コマンドを使用します。

# ダイナミック ARP 検査情報の表示

ダイナミック ARP 検査情報を表示するには、表 23-2 に記載されたイネーブル EXEC コマンドを使用します。

**表 23-2　ダイナミック ARP 検査情報を表示するコマンド**

| コマンド | 説明 |
|---|---|
| **show arp access-list** [*acl-name*] | ARP ACL の詳細情報を表示します。 |
| **show ip arp inspection interfaces** [*interface-id*] | 指定されたインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。 |
| **show ip arp inspection vlan** *vlan-range* | 指定された VLAN に対するダイナミック ARP 検査の設定および動作状態を表示します。VLAN が指定されない場合、または範囲が指定された場合、ダイナミック ARP 検査がイネーブルな（アクティブな）VLAN の情報のみを表示します。 |

ダイナミック ARP 検査統計情報をクリアするには、表 23-3 に記載されたイネーブル EXEC コマンドを使用します。

**表 23-3　ダイナミック ARP 検査統計情報をクリアおよび表示するコマンド**

| コマンド | 説明 |
|---|---|
| **clear ip arp inspection statistics** | ダイナミック ARP 検査統計情報をクリアします。 |
| **show ip arp inspection statistics** [**vlan** *vlan-range*] | 指定された VLAN の転送されたパケット、廃棄されたパケット、MAC 検証を失敗したパケット、IP 検証を失敗したパケット、ACL で許可または拒否されたパケット、DHCP で許可または拒否されたパケットの統計情報を表示します。VLAN が指定されない場合、または範囲が指定された場合、ダイナミック ARP 検査がイネーブルな（アクティブな）VLAN の情報のみを表示します。 |

**show ip arp inspection statistics** コマンドでは、スイッチは信頼できるダイナミック ARP 検査ポート上の各 ARP 要求および応答パケット用に転送されたパケット数を増やします。スイッチは、送信元 MAC、宛先 MAC、または IP 妥当性チェックによって拒否された各パケットの ACL または DHCP 許可パケットの数を増やし、また適切な障害カウントを増やします。

ダイナミック ARP 検査ロギング情報をクリアするには、表 23-4 に記載されたイネーブル EXEC コマンドを使用します。

**表 23-4　ダイナミック ARP 検査ロギング情報をクリアおよび表示するコマンド**

| コマンド | 説明 |
|---|---|
| **clear ip arp inspection log** | ダイナミック ARP 検査ログ バッファをクリアします。 |
| **show ip arp inspection log** | ダイナミック ARP 検査ログ バッファの設定および内容を表示します。 |

これらのコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。