CHAPTER 22

# ダイナミック ARP 検査の設定

この章では、Catalyst 3750 Metro スイッチ上でダイナミック Address Resolution Protocol（ARP）検査を設定する方法を説明します。この機能により、不正な ARP 要求および応答は同一 VLAN（仮想 LAN）の他のポートにリレーしないことで、悪意のある攻撃を回避できるようにします。

（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。

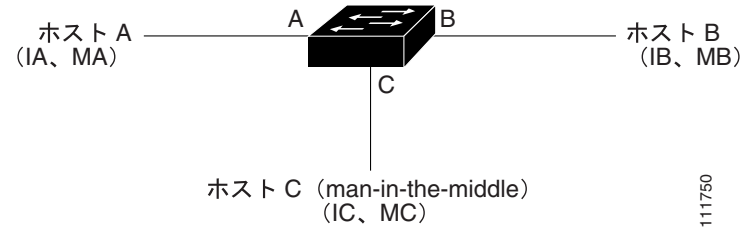
この章で説明する内容は、次のとおりです。

# ダイナミック ARP 検査の概要

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で、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を提供します。たとえば、ホスト B はホスト A に情報を送信したいのに、自身の ARP キャッシュにホスト A の MAC アドレスを持っていません。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てブロードキャスト メッセージを生成し、ホスト A の IP アドレスに関連する MAC アドレスを取得します。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 MAC アドレスを使用して応答します。ただし、ARP 要求を受信しなかった場合でも ARP は不当な応答を許可するため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生する可能性があります。攻撃後、攻撃にさらされたデバイスからのすべてのトラフィックが攻撃者のコンピュータを介して、ルータ、スイッチ、またはホストに流れます。

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したり、サブネット上の他のホストに宛てたトラフィックを代行受信したりして、レイヤ 2 ネットワークに接続したホスト、スイッチ、ルータを攻撃できます。図 22-1 に ARP キャッシュ ポイズニングの例を示します。

**図 22-1　ARP キャッシュ ポイズニング**




ホスト A、B および C はインターフェイス A、B および C 上のスイッチに接続され、すべて同じサブネット上にあります。これらの IP アドレスおよび MAC アドレスは、カッコ内に示してあります。たとえば、ホスト A は IP アドレス IA および MAC アドレス 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とき、ホスト A は IP アドレス IB に関連付けられた MAC アドレスに対して 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 を持つホストへの ARP バインディングを使用して ARP キャッシュを読み込みます。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 が応答すると、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 を持つホストへのバインディングを使用して ARP キャッシュを読み込みます。

ホスト C は、IP アドレス IA（または IB）および MAC アドレス MC を持つホストへのバインディングを使用して偽造した ARP 応答をブロードキャストすることで、スイッチ、ホスト A、およびホスト B をポイズニングできます。ポイズニングされた ARP キャッシュを持つホストは、IA または IB に宛てた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。ホスト C は、IA および IB に関連付けられた正当な MAC アドレスを知っているため、宛先として正しい MAC アドレスを使用して、代行受信され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、自身をホスト A からホスト B へのトラフィック ストリームに挿入し、典型的な *man-in-the-middle* 攻撃を行います。

ダイナミック ARP 検査は、ネットワークの ARP パケットを検証するセキュリティ機能です。この検査では、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信、ロギング、および廃棄します。この機能は、特定な 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リレーされるようにします。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上のすべての ARP 要求および応答を代行受信します。
- ローカル ARP キャッシュを更新する前、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が有効な IP/MAC アドレス バインディングを持っているかどうかを検証します。
- 無効な ARP パケットを廃棄します。

ダイナミック ARP 検査では、DHCP スヌーピング バインディング データベースなどの信頼性のある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いて、ARP パケットの妥当性を判別します。このデータベースは、DHCP スヌーピングが VLAN 上およびスイッチ上でイネーブルになっている場合、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上で受信された場合、スイッチはそのパケットを確認せずに転送します。信頼できないインターフェイス上では、スイッチはパケットが有効な場合のみ転送します。

ダイナミック ARP 検査は、VLAN ごとに **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イネーブルにします。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.22-7）を参照してください。

DHCP を使用しない環境では、ダイナミック ARP 検査は、スタティックに設定された IP アドレスを持つホストに対してユーザが設定した ARP Access Control List（ACL; アクセス コントロール リスト）と照合して ARP パケットを検証できます。ARP ACL は、**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定義します。設定の詳細については、「非 DHCP 環境の ARP ACL の設定」（p.22-9）を参照してください。スイッチは、廃棄されたパケットをロギングします。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.22-5）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 アドレスが無効な場合、または ARP パケット本体にある MAC アドレスがイーサネット ヘッダーで指定したアドレスに一致しない場合に、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行」（p.22-13）を参照してください。

## インターフェイスの信頼状態とネットワーク セキュリティ

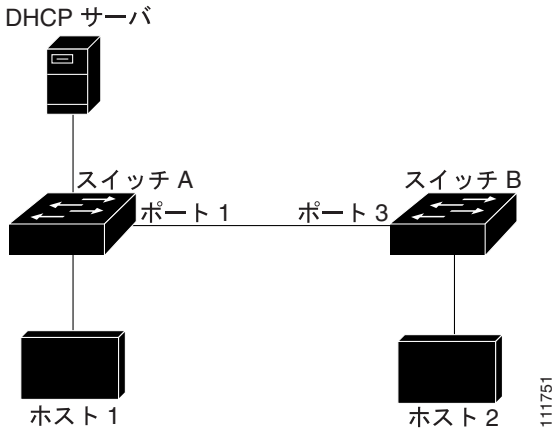
ダイナミック ARP 検査は、信頼状態とスイッチ上の各インターフェイスを対応付けます。信頼できるインターフェイスに到着したパケットは、すべてのダイナミック ARP 検査による検証確認を迂回し、信頼できないインターフェイスに到着したパケットには、ダイナミック ARP 検査による検証プロセスが実行されます。

標準的なネットワーク構成では、ホスト ポートに接続されたすべてのスイッチ ポートを信頼できないポートとして設定し、スイッチに接続されたすべてのスイッチ ポートは信頼できるポートとして設定します。この設定を使用して、指定されたスイッチからネットワークに入ってくるすべての ARP パケットは、セキュリティ チェックを迂回します。VLAN またはネットワークの他の場所では、それ以外の検証は必要ありません。信頼設定は、**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設定します。

**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のあるときに信頼できない状態に設定すると、接続が切断される結果になることがあります。

図 22-2 では、スイッチ A とスイッチ B の両方が、ホスト 1 およびホスト 2 を含む VLAN でダイナミック ARP 検査を実行していると想定しています。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 だけがホスト 1 の IP/MAC アドレスをバインドします。したがって、スイッチ A とスイッチ B と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、ホスト 1 とホスト 2 の間の接続は切断されます。

**図 22-2　ダイナミック ARP 検査がイネーブルになった VLAN 上での ARP パケットの検証**




実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワークにセキュリティ ホールを残すことになります。スイッチ A がダイナミック ARP 検査を実行していない場合、ホスト 1 は簡単にスイッチ B（およびスイッチ間のリンクが信頼できるリンク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。この条件は、スイッチ B がダイナミック ARP 検査を実行しているときにも発生することがあります。

ダイナミック ARP 検査では、ダイナミック ARP 検査を実行しているスイッチに接続された（信頼できないインターフェイスの）ホストが、ネットワークの他のホストの 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のホストがダイナミック ARP 検査を実行してい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のは回避しません。

VLAN の一部のスイッチがダイナミック ARP 検査を実行し、他のスイッチは実行していないような場合、そういったスイッチに接続しているインターフェイスは信頼できないインターフェイスとして設定します。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、ARP ACL を使用してダイナミック ARP 検査を実行しているスイッチを設定します。レイヤ 3 でそのようなバインディングを判別できないときは、ダイナミック ARP 検査を実行しているスイッチを、ダイナミック ARP 検査を実行していないスイッチから切り離します。設定の詳細については、「非 DHCP 環境の ARP ACL の設定」（p.22-9）を参照してください。

**（注）** DHCP サーバおよびネットワークのセットアップによっては、VLAN のすべてのスイッチ上では指定した 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 検査の妥当性チェックを実行します。したがって、着信 ARP パケットの数は、DoS 攻撃を回避するため、レートが制限されます。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、1 秒あたり 15 パケット（pps）です。信頼できるインターフェイスは、レート制限されません。この設定の変更は、**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。

着信 ARP パケットのレートが設定した制限値を超えると、スイッチはそのポートを errdisable ステートにします。変更しない限り、ポートはそのままの状態となります。指定したタイムアウト時間の経過後にポートが自動的にこの状態から抜け出すように、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。

設定の詳細については、「着信 ARP パケットのレート制限」（p.22-11）を参照してください。

## ARP ACL と DHCP スヌーピング エントリの相関プライオリティ

ダイナミック ARP 検査では、有効な IP/MAC アドレス バインディングのリストに対して DHCP スヌーピング バインディング データベースが使用されます。

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設定した場合のみ、ACL を使用します。スイッチは、まず ARP パケットとユーザ設定の ARP ACL を比較します。ARP ACL が ARP パケットを拒否する場合、DHCP スヌーピングが読み込んだデータベースに有効なバインディングが存在しても、スイッチも同様に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とき、エントリはログ バッファに保存され、レート制御ごとにシステム メッセージが生成されます。メッセージが生成されたあと、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、送信元と宛先の IP アドレス、および送信元と宛先の MAC アドレスといったフロー情報が含まれます。

バッファ内のエントリ数およびシステム メッセージの生成に必要な指定間隔内のエントリ数を設定するには、**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 コマンドを使用すると、ロギングされるパケットのタイプを指定できます。設定の詳細については、「ログ バッファの設定」（p.22-14）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、スイッチ上でダイナミック ARP 検査を設定する方法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（p.22-6）
- ダイナミック ARP 検査設定時の注意事項（p.22-6）
- DHCP 環境でのダイナミック ARP 検査の設定（p.22-7）（DHCP 環境では必須）
- 非 DHCP 環境の ARP ACL の設定（p.22-9）（非 DHCP 環境では必須）
- 着信 ARP パケットのレート制限（p.22-11）（任意）
- 妥当性チェックの実行（p.22-13）（任意）
- ログ バッファの設定（p.22-14）（任意）

## ダイナミック ARP 検査のデフォルト設定

表 22-1 に、デフォルトのダイナミック ARP 検査設定を示します。

**表 22-1　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 | 全 VLAN でディセーブル |
| インターフェイスの信頼状態 | 全インターフェイスが信頼できない |
| 着信 ARP パケットのレート制限 | ネットワークが 1 秒ごとに 15 個程度の新規ホストに接続しているホストを使用するスイッチド ネットワークであると想定した場合、レートは 15 pps。<br>すべての信頼できるインターフェイス上でレート制限なし。<br>バースト間隔は 1 秒です。 |
| 非 DHCP 環境の ARP ACL | ARP ACL は定義されていない。 |
| 妥当性チェック | チェックは実行されない。 |
| ログ バッファ | ダイナミック ARP 検査がイネーブルになっているとき、すべての拒否または廃棄された ARP パケットがロギングされる。<br>ログ内のエントリ数は 32。<br>システム メッセージ数は 5 秒ごとに制限される。<br>ロギング レートの間隔は 1 秒。 |
| VLAN ごとのロギング | 拒否または廃棄されたすべての ARP パケットがロギングされる。 |

## 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、入力側セキュリティ機能です。出力チェックは行いません。
- ダイナミック ARP 検査をサポートしていないスイッチ、またはこの機能がイネーブルになっていないスイッチに接続されたホストに対しては、ダイナミック ARP 検査は有効になりません。man-in-the-middle 攻撃は単一レイヤ 2 ブロードキャスト ドメインに限られているため、ダイナミック ARP 検査チェックが設定されたドメインを、チェックが設定されていないドメインから隔離します。このアクションにより、ダイナミック ARP 検査に対してイネーブルになっているドメインにあるホストの ARP キャッシュを保護します。

- 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したがって、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 バインディングを検証します。ダイナミックに IP アドレスが割り当てられた ARP パケットを許可するには、DHCP スヌーピングを必ずイネーブルにしてください。設定の詳細については、第 21 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か、非 DHCP 環境である場合、ARP ACL を使用してパケットを許可または拒否します。

- 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 ポート上でサポートされています。

- 物理ポートは、物理ポートとチャネル ポートの信頼状態が一致するときのみ EtherChannel ポート チャネルに加入できます。それ以外の場合、物理ポートはポート チャネルでサスペンドのままになります。ポート チャネルは、チャネルに加入した最初の物理ポートから信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、そのチャネルの信頼状態に一致する必要はありません。

  逆にポート チャネルの信頼状態を変更したときは、スイッチにより、チャネルを構成するすべての物理ポート上で新しい信頼状態が設定されます。

- レート制限は、スイッチ スタックの各スイッチごとに個別に計算されます。つまりクロス スタック EtherChannel では、実際のレート制限が設定値より高くなることがあります。たとえば、スイッチ 1 に 1 ポート、スイッチ 2 に 1 ポートの EtherChannel 上でのレート制限を 30 pps に設定した場合、EtherChannel が errdisable ステートにならずに、各ポートでパケットを 29 pps で受信できます。

- ポート チャネルの動作レートは、チャネル内のすべての物理ポートでの累積となります。たとえば、ARP レート制限を 400 pps でポート チャネルを設定した場合、チャネル上で組み合わされているすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポート上での着信 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と等しくなります。チャネル ポート メンバーでの着信 ARP パケットのレートを確認してから EtherChannel ポートのレート制限を設定するようにしてください。

  物理ポートの着信パケットのレートは、物理ポートの設定ではなく、ポート チャネルの設定と照合されます。ポート チャネルでのレート制限設定は、物理ポートでの設定とは無関係です。

  EtherChannel が設定されたレート以上の ARP パケットを受信する場合、チャネル（すべての物理ポートを含む）は errdisabled ステートになります。

- 着信トランク ポートで ARP パケットのレートを必ず制限してください。集約を反映させ、ダイナミック ARP 検査対応の複数の VLAN にわたるパケットを処理するには、トランク ポートに高めのレートを設定します。また、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 コマンドも使用できます。1 つの VLAN でレート制限を高くすると、ソフトウェアによってポートが errdisabled ステートになったときに他の VALN への DoS 攻撃を発生させる原因となることがあります。

## DHCP 環境でのダイナミック ARP 検査の設定

この手順では、2 つのスイッチがダイナミック ARP 検査をサポートする場合にこの機能を設定する方法を示します。図 22-2 にあるように、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。どちらのスイッチも、ホストが配置されている VLAN 1 上でダイナミック ARP 検査を実行しています。DHCP サーバは、スイッチ A に接続されています。どちらのホストも同じ DHCP サーバから IP アドレスを取得しています。したがって、スイッチ A にはホスト 1 とホスト 2 のバインディングがあり、スイッチ B にはホスト 2 のバインディングがあります。

（注）　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したがって、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 バインディングを検証します。ダイナミックに IP アドレスが割り当てられた ARP パケットを許可するには、DHCP スヌーピングを必ずイネーブルにしてください。設定の詳細については、第 21 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この機能をサポートしてい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、「非 DHCP 環境の ARP ACL の設定」（p.22-9）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、特権 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検証します。 |
| 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 ごとにダイナミック 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 検査はすべての VLAN 上でディセーブルになっています。<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 を指定します。指定できる範囲は 1 ～ 4094 です。<br><br>両方のスイッチで同じ VLAN ID を指定してください。 |
| 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信頼性のある接続として設定します。<br><br>デフォルトでは、すべてのインターフェイスが信頼されません。<br><br>スイッチは、信頼できるインターフェイス上の他のスイッチから受信する 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では、スイッチがすべての ARP 要求および応答を代行受信します。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、代行受信されたパケットが有効な IP/MAC アドレス バインディングを持っているかどうかが検証されます。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング コンフィギュレーションに従い、スイッチは無効なパケットを廃棄し、ログ バッファにロギングします。詳細については、「ログ バッファの設定」（p.22-14）を参照してください。 |
| ステップ 6 | **end** | 特権 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 検査の設定を検証します。 |
| ステップ 8 | **show ip dhcp snooping binding** | DHCP バインディングを検証します。 |
| ステップ 9 | **show ip arp inspection statistics vlan** *vlan-range* | ダイナミック ARP 検査の統計をチェックします。 |
| 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信頼できない状態に戻すには、**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、ダイナミック ARP 検査を VLAN 1 のスイッチ A に設定する例を示します。スイッチ B でも同様の手順を実行します。

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

## 非 DHCP 環境の ARP ACL の設定

ここでは、図 22-2 にあるスイッチ B がダイナミック ARP 検査または 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 検査を設定する手順を示します。

スイッチ A のポート 1 を信頼できるポートとして設定すると、スイッチ A およびホスト 1 が、スイッチ B またはホスト 2 のいずれかによって攻撃される可能性があるため、セキュリティ ホールができます。この可能性を避けるには、スイッチ A のポート 1 を信頼できないポート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 をセットアップして VLAN 1 に適用します。ホスト 2 の IP アドレスがスタティックでない場合（この場合、スイッチ A で ACL 設定を適用することはできません）、レイヤ 3 でスイッチ A をスイッチ B から切り離し、ルータを使用してスイッチ A と B の間で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、特権 EXEC モードで次の手順を実行します。この手順は、非 DHCP 環境では必須です。

| | 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。デフォルトでは、ARP アクセス リストは定義されていません。<br>（注）　ARP アクセス リストの最後には、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**] | 指定したホスト（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）Access Control Entry（ACE; アクセス コントロール エントリ）に一致する場合にパケットをログ バッファにロギングするには、**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 コマンドで **matchlog** キーワードも設定している場合、一致がロギングされます。詳細については、「ログ　バッファの設定」（p.22-14）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、VLAN のいずれにも、定義された ARP ACL は適用されていません。<br>• *arp-acl-name* には、ステップ 2 で作成した ACL の名前を指定します。<br>• *vlan-range*　には、スイッチおよびホストが存在している 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 での暗黙の拒否を明示的な拒否として扱い、ACL のそこまでのステートメントに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されません。<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 ACL に明示的な拒否が存在しないことになり、パケットが ACL のステートメントに一致しない場合には、パケットを許可するかまたは拒否するかを DHCP バインディングが判別することになります。<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 と照合して比較されます。パケットは、アクセス リストで許可されている場合のみ許可されます。 |
| 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、信頼できないインターフェイスとして設定します。<br>デフォルトでは、すべてのインターフェイスが信頼されません。<br>信頼できないインターフェイスでは、スイッチがすべての ARP 要求および応答を代行受信します。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、代行受信されたパケットが有効な IP/MAC アドレス バインディングを持っているかどうかが検証されます。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで指定されたロギング コンフィギュレーションに従い、スイッチは無効なパケットを廃棄し、ログ バッファにロギングします。詳細については、「ログ バッファの設定」（p.22-14）を参照してください。 |
| ステップ 8 | **end** | 特権 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 *host2* という名前の ARP ACL 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 でポート 1 を信頼されないように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 検査の妥当性チェックを実行します。したがって、着信 ARP パケットの数は、DoS 攻撃を回避するため、レートが制限されます。

着信 ARP パケットのレートが設定した制限値を超えると、スイッチはそのポートを errdisable ステートにします。指定したタイムアウト時間が経過したあとにポートが自動的にこの状態から抜け出すように、errdisable 回復をイネーブルにするまで、ポートはこの状態のままになります。

（注）　インターフェイスでレート制限を設定しない限り、インターフェイスの信頼状態を変更すると、レート制限もその信頼状態のデフォルト値に変更されます。レート制限を設定したあとは、信頼状態が変更されても、インターフェイスはそのレート制限のままとなります。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力した場合、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。

トランク ポートおよび EtherChannel ポートのレート制限の設定時の注意事項は、「ダイナミック ARP 検査設定時の注意事項」（p.22-6）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、特権 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**} | インターフェイス上での着信 ARP 要求および応答のレートを制限します。<br><br>信頼できないインターフェイスでのデフォルトのレートは 15 pps で、信頼できるインターフェイスでは無制限です。バースト間隔は 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* には、1 秒あたりに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 です。<br>• （任意）**burst interval** *seconds* では、高速の ARP パケットに対してインターフェイスがモニタされる、秒単位での連続インターバルを指定します。指定できる範囲は 1 ～ 15 です。<br>• **rate none** の場合、処理可能な着信 ARP パケットのレートを上限なしに指定します。 |

| | 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 ステートからの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で、回復インターバルは 300 秒になっています。<br>**interval** *interval* には、errdisable ステートからの回復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** | 特権 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行

ダイナミック ARP 検査では、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信、ロギング、および廃棄します。スイッチを設定して、宛先 MAC アドレス、送信者およびターゲット IP アドレス、および送信元 MAC アドレスの追加チェックを実行できます。

着信 ARP パケットで特定のチェックを実行するには、特権 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行します。デフォルトでは、チェックは実行されません。<br><br>キーワードの意味は次のとおりです。<br><br>• **src-mac** では、イーサネット ヘッダーの送信元 MAC アドレスが ARP 本体の送信者 MAC アドレスと照合されます。このチェックは、ARP 要求と ARP 応答の両方で実行されます。イネーブルになっている場合、異なる MAC アドレスを持つパケットは、無効なパケットとして分類され、廃棄されます。<br>• **dst-mac** では、イーサネット ヘッダーの宛先 MAC アドレスが ARP 本体のターゲット MAC アドレスと照合されます。このチェックは ARP 応答に対して実行されます。イネーブルになっている場合、異なる MAC アドレスを持つパケットは、無効なパケットとして分類され、廃棄されます。<br>• **ip** では、無効および予想外の IP アドレスの ARP 本体をチェックします。アドレスに 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。送信者 IP アドレスはすべての ARP 要求および応答でチェックされ、ターゲット 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、直前のコマンド設定を上書きします。つまり、あるコマンドが **src** および **dst mac** の検証をイネーブルにし、2 番めのコマンドが IP の検証のみをイネーブルにしている場合、2 番めのコマンドの結果として **src** および **dst mac** の検証がディセーブルになります。 |
| ステップ 3 | **exit** | 特権 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、廃棄されたパケット、MAC 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** 特権 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とき、エントリはログ バッファに保存され、レート制御ごとにシステム メッセージが生成されます。メッセージが生成されたあと、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、送信元と宛先の IP アドレス、および送信元と宛先の MAC アドレスといったフロー情報が含まれます。

ログ バッファのエントリは、複数のパケットを表すことができます。たとえば、同一 ARP パラメータを持つ同じ VLAN でインターフェイスが多くのパケットを受信した場合、スイッチはログ バッファ内でパケットを 1 つのエントリとして結合させ、エントリに対して 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 イベントはログ バッファに適合しないことになり、**show ip arp inspection log** 特権 EXEC コマンドの表示が影響を受けます。パケットのカウントと時刻を除き、すべてのデータ位置に -- が表示されます。そのエントリに対して、他の統計情報は提供されません。表示内にこのエントリが見つかった場合、ログ バッファのエントリ数を増やすか、ロギング レートを上げてください。

ログ バッファを設定するには、特権 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 検査のロギング バッファを設定します。<br><br>デフォルトでは、ダイナミック ARP 検査がイネーブルになっているとき、拒否または廃棄された ARP パケットがロギングされます。ログ エントリ数は 32 です。システム メッセージ数は 1 秒あたり 5 に制限されています。ロギング レートの間隔は 1 秒です。<br><br>キーワードの意味は次のとおりです。<br><br>• **entries** *number* には、バッファ内にロギングされ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* には、指定した間隔でシステム メッセージを生成するエントリ数を指定します。<br><br>**logs** *number* に対して、指定できる範囲は 0 ～ 1024 です。値を 0 にした場合、エントリはログ バッファに置かれますが、システム メッセージは生成されません。<br><br>**interval** *seconds* に対して、指定できる範囲は 0 ～ 86400 秒（1 日あたり）です。値を 0 にすると、システム メッセージが即座に生成されます（また、ログ バッファは常に空となります）。<br><br>間隔を 0 に設定すると、ログの 0 設定を上書きします。<br><br>**logs** 設定と **interval** 設定は相互作用します。**logs** *number* X が **interval** *seconds* Y より大きい場合、Y 分の X（X/Y）個のシステム メッセージが毎秒生成されます。それ以外の場合、X 分の Y（Y/X）秒ごとに 1 つのシステム メッセージが送信されます。 |

| | 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のタイプを制御します。デフォルトでは、すべての拒否または廃棄されたパケットがロギングされます。*ロギングされる*とは、エントリがログ バッファに置かれてシステム メッセージが生成され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 を指定します。指定できる範囲は 1 ～ 4094 です。<br>• **acl-match matchlog** では、ACE ロギング コンフィギュレーションに基づいてパケットがロギングされます。このコマンドで **matchlog** キーワードを、**permit** または **deny** ARP アクセス リスト コンフィギュレーション コマンドで **log** キーワードをそれぞれ指定した場合、ACL によって許可または拒否された ARP パケットがロギングされます。<br>• **acl-match none** では、ACL に一致したパケットはロギングされません。<br>• **dhcp-bindings all** では、DHCP バインディングに一致したパケットがすべてロギングされます。<br>• **dhcp-bindings none** では、DHCP バインディングに一致したパケットはロギングされません。<br>• **dhcp-bindings permit** では、DHCP バインディングで許可されたパケットがロギングされます。 |
| ステップ 4 | **exit** | 特権 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。 |

デフォルトのログ 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** 特権 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 22-2 で説明する特権 EXEC コマンドを使用します。

**表 22-2　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 についての詳細情報を表示します。 |
| **show ip arp inspection interfaces** [*interface-id*] | 指定し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* | 指定した VLAN のダイナミック ARP 検査の設定および動作状態を表示します。VLAN が指定されていないか範囲が指定されている場合、ダイナミック ARP 検査がイネーブル（アクティブ）になっている VLAN についての情報のみが表示されます。 |

ダイナミック ARP 検査の統計をクリアまたは表示するには、表 22-3 で説明する特権 EXEC コマンドを使用します。

**表 22-3　ダイナミック ARP 検査の統計情報をクリアまたは表示するコマンド**

| コマンド | 説明 |
|---|---|
| **clear ip arp inspection statistics** | ダイナミック ARP 検査の統計情報をクリアします。 |
| **show ip arp inspection statistics** [**vlan** *vlan-range*] | 指定した VLAN の転送、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL に許可されたおよび拒否されたパケット、および DHCP に許可されたおよび拒否されたパケットに関する統計情報を表示します。VLAN が指定されていないか範囲が指定されている場合、ダイナミック ARP 検査がイネーブル（アクティブ）になっている VLAN についての情報のみが表示されます。 |

**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 検査ポート上で各 ARP 要求および応答パケットに対して転送するパケット数を増加します。スイッチは、送信元 MAC、宛先 MAC、または IP チェックにより拒否された各パケットに対する ACL または DHCP 許可パケット数を増加させ、さらに適切な失敗カウントを増加します。

ダイナミック ARP 検査のロギング情報をクリアまたは表示するには、表 22-4 で説明する特権 EXEC コマンドを使用します。

**表 22-4　ダイナミック ARP 検査のロギング情報をクリアまたは表示するコマンド**

| コマンド | 説明 |
|---|---|
| **clear ip arp inspection log** | ダイナミック ARP 検査のログ バッファをクリアします。 |
| **show ip arp inspection log** | ダイナミック ARP 検査のログ 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。