CHAPTER 23

ダイナミック ARP インスペクションの設定

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）インスペクションを設定する方法について説明します。この機能により、同じ VLAN 内の他のポートの無効な ARP 要求や応答を信頼しないようにして、スイッチでの悪意のある攻撃を回避できます。特に明記しない限り、*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。

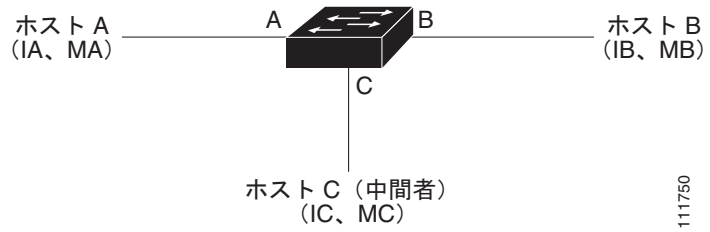
（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

ダイナミック ARP インスペクションの概要

ARP では、IP アドレスを MAC 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 通信を実現しています。たとえば、ホスト B がホスト A に情報を送信しようとしていて、ARP キャッシュ内にホスト A の MAC アドレスがないとします。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 アドレスで応答します。ただし、ARP 要求を受信しなくても ARP がホストからの余計な応答を許可するために、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。攻撃の後、攻撃下にあるデバイスからのすべてのトラフィックは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ていきます。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、サブネット上の他のホストへ向かうトラフィックを代行受信することで、ネットワーク上のレイヤ 2 ネットワークに接続されているホスト、スイッチ、ルータを攻撃します。図 23-1 は、ARP キャッシュ ポイズニングの例です。

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 上のスイッチに接続されていて、すべてが同じサブネット上にあります。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 と MAC アドレス MA を使用しています。ホスト A は、ホスト B と IP レイヤで通信を行う必要がある場合、ARP 要求をブロードキャストし、IP アドレス IB に関連する MAC アドレスを取得します。スイッチおよびホスト B は、ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を含むホストの ARP バインディングを ARP キャッシュに入力します（たとえば IP アドレス IA が MAC アドレス MA にバインドされる）。ホスト B が応答すると、スイッチとホスト A は、IP アドレス IB と MAC アドレス MB が関連付けられているホストの ARP バインディングを持つ 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）と MAC アドレス MC が関連付けられているホストのバインディングを持つ偽造 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、ホスト B の ARP キャッシュをポイズニングできます。ポイズニングされた ARP キャッシュのあるホストは、IA または IB 向けの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 がそのトラフィックを代行受信します。ホスト C は IA および IB に関連付けられた本当の 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それらのホストに転送できるのです。ホスト C は、ホスト A からホスト B へのトラフィック ストリームに割り込んで、一般的な*中間者*攻撃を行います。

ダイナミック ARP インスペクションは、ネットワーク内の ARP パケットを検査するセキュリティ機能です。このインスペクションでは、無効な IP と MAC アドレスのバインディングを持つ ARP パケットを代行受信し、記録して、廃棄します。この機能により、ある種の中間者攻撃からネットワークを保護できます。

ダイナミック ARP インスペクションにより、有効な ARP 要求および応答だけがリレーされることが保証されます。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 キャッシュの更新前、またはパケットが適切な宛先に転送される前に、代行受信された各パケットに有効な IP と MAC アドレスのバインディングがあるかを確認します。
- 無効な ARP パケットをドロップします。

ダイナミック ARP インスペクションは、信頼できるデータベースである 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ている、有効な IP と MAC アドレスのバインディングに基づいて、ARP パケットの有効性を判断します。このデータベースは、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に、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る場合、スイッチはチェックなしに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、スイッチは有効な場合だけパケットを転送します。

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 インスペクションをイネーブルにできます。設定手順については、「DHCP 環境でのダイナミック ARP インスペクションの設定」（P.23-7）を参照してください。

非 DHCP 環境では、ダイナミック ARP インスペクションは、スタティックに設定された IP アドレスを持つホストのユーザ設定 ARP Access Control List（ACL; アクセス コントロール リスト）に対して、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されます。設定手順については、「非 DHCP 環境の ARP ACL の設定」（P.23-9）を参照してください。スイッチは、ドロップ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、「ドロップされたパケットのロギング」（P.23-5）を参照してください。

パケット内の IP アドレスが無効か、または ARP パケットの本体にある MAC アドレスがイーサネット ヘッダーで指定されているアドレスと一致しない場合に、ARP パケットをドロップするようにダイナミック ARP インスペクションを設定できます。**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.23-12）を参照してください。

インターフェイス信頼状態およびネットワーク セキュリティ

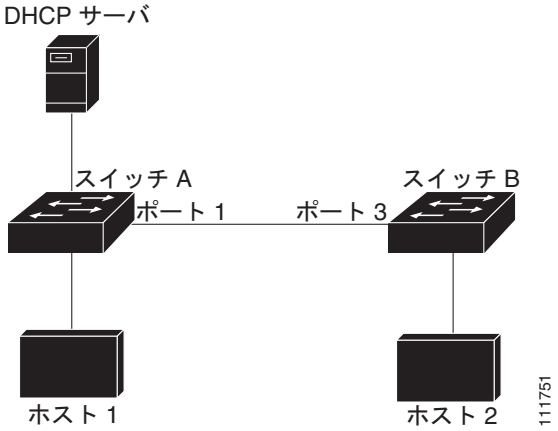
ダイナミック ARP インスペクションは、信頼状態とスイッチ上の各インターフェイスとを関連付けます。信頼できるインターフェイスに着信したパケットは、すべてのダイナミック ARP インスペクションの検証チェックを迂回し、信頼できないインターフェイスに着信したパケットはダイナミック ARP インスペクションの検証プロセスで処理されます。

一般的なネットワーク設定では、ホスト ポートに接続するすべてのスイッチ ポートを untrusted に設定し、スイッチに接続しているすべてのスイッチ ポートを trusted に設定します。このような設定では、指定したスイッチからネットワークに入ったすべての ARP パケットがセキュリティ チェックを迂回します。VLAN またはネットワーク内のその他の場所でその他の検証を行う必要はありません。信頼設定を **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　信頼状態は慎重に設定してください。インターフェイスを信頼すべきときに untrusted と設定すると、接続が切断される可能性があります。

図 23-2 では、スイッチ A およびスイッチ B の両方が、ホスト 1 およびホスト 2 のそれぞれを含む VLAN でダイナミック ARP インスペクションを実行しているとします。ホスト 1 およびホスト 2 がスイッチ A に接続している DHCP サーバから IP アドレスを取得すると、スイッチ A だけがホスト 1 の IP アドレスと MAC アドレスのペアをバインドします。このため、スイッチ A およびスイッチ 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 によってドロップされます。ホスト 1 およびホスト 2 の間の接続は失われます。

図 23-2　ダイナミック ARP インスペクションがイネーブルな VLAN での ARP パケット インスペクション



実際にインターフェイスを信頼できない場合にインターフェイスを信頼できるように設定してしまうと、ネットワークにセキュリティ ホールが残ってしまいます。スイッチ A でダイナミック ARP インスペクションが動作していない場合、ホスト 1 は簡単にホスト B の ARP キャッシュをポイズニングできます（スイッチ間のリンクが trusted に設定されている場合はホスト 2 も可能）。この状態は、スイッチ B がダイナミック ARP インスペクションを実行していても発生します。

ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションを実行しているスイッチに接続している（信頼できないインターフェイス上の）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ないようにするものです。ただし、ダイナミック ARP インスペクションでは、ネットワークの他の部分にあるホストでは、ダイナミック ARP インスペクションを実行しているスイッチに接続しているホストのキャッシュに対するポイズニングは回避されません。

VLAN 内にあるスイッチの中で、ダイナミック ARP インスペクションを実行しているものとしていないものがある場合、そのようなスイッチに接続しているインターフェイスを untrusted に設定します。ただし、ダイナミック ARP インスペクションを実行していない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 インスペクションを実行するようにスイッチを設定します。そのようなバインディングをレイヤ 3 で判別できない場合、ダイナミック ARP インスペクションを実行しているスイッチを、ダイナミック ARP インスペクションを実行していないスイッチから分離します。設定手順については、「非 DHCP 環境の 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り、VLAN 内のすべてのスイッチにある指定した ARP パケットを検査できない場合があります。

ARP パケットのレート制限

スイッチの CPU はダイナミック ARP インスペクション検証チェックを実行するので、着信 ARP パケットの数は、DoS 攻撃を受けないようにレート制限されています。デフォルトで、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。**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た場合、スイッチはポートを errdisable ステートにします。ユーザが介入するまでポートは errdisable ステートのままになります。**errdisable recovery** グローバル コンフィギュレーション コマンドを使用して、指定したタイムアウト期間の経過後ポートがこのステートから自動的に回復するように errdisable 回復をイネーブルにできます。

（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。

設定手順については、「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 と 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 インスペクションでは、有効な IP と MAC アドレスのバインディングのリスト用に 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 データベース内のエントリよりも優先度が高くなります。**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 を設定した場合、スイッチは ACL だけを使用します。スイッチは最初に ARP パケットとユーザ定義の 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読み込まれたデータベースに有効なバインディングがあっても、スイッチもパケットを拒否します。

ドロップされたパケットのロギング

スイッチがパケットをドロップする際に、ログ バッファにエントリを配置してレート制限ベースにシステム メッセージを生成します。メッセージの生成後、スイッチはエントリをログ バッファから削除します。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ています。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数、およびシステム メッセージを生成するのに指定した間隔で必要となるエントリ数を設定します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用してロギングされるパケットのタイプを指定できます。設定手順については、「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 インスペクションの設定

デフォルトのダイナミック ARP インスペクションの設定

表 23-1 に、デフォルトのダイナミック ARP インスペクションの設定を示します。

表 23-1　デフォルトのダイナミック ARP インスペクションの設定

機能	デフォルト設定
ダイナミック ARP インスペクション	すべての VLAN でディセーブルです。
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。 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。 バースト間隔は 1 秒です。

表 23-1　デフォルトのダイナミック ARP インスペクションの設定 （続き）

機能	デフォルト設定
非 DHCP 環境の ARP ACL	ARP ACL は定義されません。
検証チェック	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 インスペクションがイネーブルの場合、すべての拒否またはドロップ ARP パケットがログされます。 ログ内のエントリ数は 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。 ロギングレート間隔は 1 秒です。
VLAN 単位ロギング	拒否またはドロップされたすべての ARP パケットがログされます。

ダイナミック ARP インスペクションの設定時の注意事項

ダイナミック ARP インスペクションの設定時の注意事項は次のとおりです。

- ダイナミック ARP インスペクションは着信セキュリティ機能で、発信チェックは実行しません。
- ダイナミック ARP インスペクションは、ダイナミック ARP インスペクションをサポートしていないスイッチや、この機能をイネーブルにしていないスイッチに接続されたホストでは有効ではありません。中間者攻撃が単一のレイヤ 2 ブロードキャスト ドメインに限定されているため、ダイナミック ARP インスペクション チェックのあるドメインとチェックのないドメインとを分離します。この処置により、ダイナミック ARP インスペクションをイネーブルにしたドメイン内のホストの ARP キャッシュが保護されます。
- 着信 ARP 要求と ARP 応答内の IP と MAC アドレスのバインディングを確認する場合、ダイナミック ARP インスペクションは DHCP スヌーピング バインディング データベース内のエントリに依存します。IP アドレスがダイナミックに割り当てられている ARP パケットを許可するために、DHCP スヌーピングをイネーブルにしてい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 ガード機能の設定」を参照してください。

  DHCP スヌーピングがディセーブルの場合または非 DHCP 環境では、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 インスペクションは、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 ポートでサポートされています。

（注） RSPAN VLAN 上でダイナミック ARP インスペクションをイネーブルにしないでください。RSPAN VLAN 上でダイナミック ARP インスペクションをイネーブルにすると、ダイナミック ARP インスペクション パケットが RSPAN 宛先ポートに到達しないことがあります。

- 物理ポートとチャネル ポートの信頼状態が一致した場合に限り、物理ポートは EtherChannel ポート チャネルに加入できます。そうでない場合、物理ポートはポート チャネル内で停止したままになります。ポート チャネルは、チャネルに最初に参加した物理ポートの信頼状態を継承します。その結果、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がありません。

  逆にいえば、ポート チャネルの信頼状態を変更した場合、スイッチはチャネルを構成するすべての物理ポートの信頼状態を新規に設定します。

- 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、チャネル内のすべての物理ポートを累積したものです。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定した場合、チャネル上に集約される全インターフェイスで合計 400 pps を受信します。EtherChannel ポートの着信 ARP パケットのレートは、全チャネル メンバーからのパケットの着信レートを合計したものです。チャネルポート メンバーの着信 ARP パケットのレートを検査した後に、EtherChannel ポートのレート制限を設定します。

  物理ポート上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、物理ポートの設定からは独立しています。

  EtherChannel が設定レートよりも多くの ARP パケットを受信する場合、（すべての物理ポートを含む）チャネルは errdisable ステートになります。
- 着信トランク ポート上の ARP パケットのレートを制限していることを確認します。集約を反映して、複数のダイナミック ARP インスペクション対応 VLAN でパケットを処理するために、トランク ポートを高めのレートに設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用してレートを無制限にできます。1 つの VLAN でレート制限が高いと、ソフトウェアがポートを errdisable ステートにするときに、他の VLAN が DoS 攻撃を受ける可能性があります。
- ダイナミック ARP インスペクションをスイッチでイネーブルにする際に、ARP トラフィックをポリシングするために設定されたポリシーは無効となります。その結果、すべての ARP トラフィックが CPU に送信されます。
- ダイナミック ARP インスペクション スマート ロギングを設定すると、ログ バッファ内のすべてのパケット（デフォルトでは、ドロップされたすべてのパケット）の内容が NetFlow 収集装置に送信されます。この機能を設定する場合は、スマート ロギングがグローバルでイネーブルになっていることを確認してください。スマート ロギングの詳細については、「スマート ロギングの設定」（P.31-14）を参照してください。

DHCP 環境でのダイナミック ARP インスペクションの設定

この手順は、2 つのスイッチがこの機能をサポートしている場合にダイナミック ARP インスペクションを設定する方法について説明します。図 23-2（P.23-3）で示しているように、ホスト 1 はスイッチ A に接続していて、ホスト 2 はスイッチ B に接続しています。両方のスイッチが、ホストが位置する VLAN 1 でダイナミック ARP インスペクションを実行しています。DHCP サーバはスイッチ A に接続されています。両方のホストは、同じ DHCP サーバから IP アドレスを取得します。したがって、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）　着信 ARP 要求と ARP 応答内の IP と MAC アドレスのバインディングを確認する場合、ダイナミック ARP インスペクションは DHCP スヌーピング バインディング データベース内のエントリに依存します。IP アドレスがダイナミックに割り当てられている ARP パケットを許可するために、DHCP スヌーピングをイネーブルにしてい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 ガード機能の設定」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 インスペクションをサポートしている場合の、この機能の設定の詳細については、「非 DHCP 環境の ARP ACL の設定」（P.23-9）を参照してください。

ダイナミック ARP インスペクションを設定するには、特権 EXEC モードで次の手順を行います。この手順を両方のスイッチで実行する必要があります。この手順は必須です。

	コマンド	目的
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*	ダイナミック ARP インスペクションを VLAN 単位でイネーブルにします。デフォルトで、ダイナミック ARP インスペクションはすべての VLAN でディセーブルに設定されています。 *vlan-range* では、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。 両方のスイッチに同じ VLAN ID を指定します。
ステップ 4	**ip arp inspection smartlog**	（任意）現在ロギングされているすべてのパケットのスマートロギングも行われるよう指定します。デフォルトでは、ドロップされたすべてのパケットがロギングされます。
ステップ 5	**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 6	**ip arp inspection trust**	スイッチ間の接続を trusted に設定します。 デフォルトでは、すべてのインターフェイスが untrusted です。 スイッチは、信頼できるインターフェイス上にある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。単純にパケットを転送するだけです。 信頼できないインターフェイスの場合、スイッチはすべての ARP 要求および応答を代行受信します。ローカル キャッシュの更新前、およびパケットが適切な宛先に転送される前に、代行受信された各パケットに有効な IP アドレスと MAC アドレスのバインディングがあるかを確認します。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 コマンドによって指定されたロギング設定に従って、無効なパケットをドロップしてログ 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 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip arp inspection interfaces** **show ip arp inspection vlan** *vlan-range*	ダイナミック ARP インスペクションの設定を確認します。
ステップ 9	**show ip dhcp snooping binding**	DHCP バインディングを確認します。
ステップ 10	**show ip arp inspection statistics vlan** *vlan-range*	ダイナミック ARP インスペクションの設定をチェックします。
ステップ 11	**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 インスペクション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。ポートを untrusted の状態に戻すには、**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。

以下は、VLAN 1 のスイッチ A でダイナミック ARP インスペクションを設定する方法の例です。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

この手順は、図 23-2（P.23-3）で示すスイッチ B がダイナミック ARP インスペクションまたは DHCP スヌーピングをサポートしていない場合に、ダイナミック ARP インスペクションを設定する方法を示しています。

スイッチ A のポート 1 を trusted に設定すると、スイッチ A およびホスト 1 はスイッチ B またはホスト 2 から攻撃される可能性があるため、セキュリティ ホールができてしまいます。この可能性をなくすため、スイッチ A のポート 1 を untrusted に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 を設定して VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスが静的でなく、スイッチ A で ACL 設定を適用できない場合は、レイヤ 3 でスイッチ B とスイッチ A を分離し、ルータを使用してその間でパケットをルーティングする必要があります。

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 環境で必須です。

	コマンド	目的
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。 **（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。 • *sender-ip* に対して、ホスト 2 の IP アドレスを入力します。 • *sender-mac* に対して、ホスト 2 の MAC アドレスを入力します。 • （任意）Access Control Entry（ACE; アクセス コントロール エントリ）が一致した場合にログ バッファ内のパケットをログするために **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 コマンドを **matchlog** キーワードとともに設定した場合、一致も記録されます。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	目的
ステップ 5	**ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]	ARP ACL に VLAN を適用します。デフォルトで、どの VLAN にも ARP ACL が定義されていません。 • *arp-acl-name* には、ステップ 2 で作成した ACL 名を指定します。 • *vlan-range* には、スイッチおよびホストが含まれる VLAN を指定します。VLAN ID 番号によって識別される単一の VLAN を指定したり、ハイフンで区切って VLAN の範囲を指定したり、カンマで区切って一連の VLAN を指定したりできます。指定できる範囲は 1 ～ 4094 です。 • （任意）ARP ACL 内の暗黙の拒否を明示的な拒否として処理し、ACL の前の句と一致しないパケットをドロップするには、**static** を指定します。DHCP バインディングは使用されません。 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 に暗黙拒否がないことを意味し、パケットが ACL 内のどの句とも一致しない場合に DHCP バインディングがパケットを許可するか拒否するかを判断します。 IP および MAC アドレスのバインディングのみを含む ARP パケットが ACL と比較されます。パケットは、アクセス リストが許可した場合に限り許可されます。
ステップ 6	**ip arp inspection smartlog**	現在ロギングされているすべてのパケットのスマートロギングも行われるよう指定します。デフォルトでは、ドロップされたすべてのパケットがロギングされます。
ステップ 7	**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 8	**no ip arp inspection trust**	スイッチ B に接続しているスイッチ A インターフェイスを untrusted として設定します。 デフォルトでは、すべてのインターフェイスが untrusted です。 信頼できないインターフェイスの場合、スイッチはすべての ARP 要求および応答を代行受信します。ローカル キャッシュの更新前、およびパケットが適切な宛先に転送される前に、代行受信された各パケットに有効な IP アドレスと MAC アドレスのバインディングがあるかを確認します。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 コマンドによって指定されたロギング設定に従って、無効なパケットをドロップしてログ 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 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show arp access-list** [*acl-name*] **show ip arp inspection vlan** *vlan-range* **show ip arp inspection interfaces**	設定を確認します。
ステップ 11	**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 に添付されている 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、*host2* という ARP ACL を設定し、ホスト 2（IP アドレスが 1.1.1.1 で MAC アドレスが 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 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

スイッチの CPU はダイナミック ARP インスペクション検証チェックを実行するので、着信 ARP パケットの数は、DoS 攻撃を受けないようにレート制限されています。

着信 ARP パケットのレートが設定された制限を越えた場合、スイッチはポートを errdisable ステートにします。指定したタイムアウト期間の経過後、ポートがこのステートから自動的に回復するように errdisable 回復をイネーブルにしないと、ポートは errdisable ステートのままになります。

（注） インターフェイスに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の変更によって、レート制限が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後、信頼状態が変更される際にインターフェイスはレート制限を保存します。**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 のレート制限の設定時の注意事項については、「ダイナミック ARP インスペクションの設定時の注意事項」（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、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	目的
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*	レート制限を設定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の着信 ARP 要求および応答のレートを制限します。 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 15 pps、信頼できるインターフェイスで無制限です。バースト間隔は 1 秒です。 キーワードの意味は次のとおりです。 • **rate** *pps* では、1 秒あたりに処理される着信パケットの上限数を指定します。指定できる範囲は 0 ～ 2048 pps です。 • （任意）**burst interval** *seconds* では、高いレートの ARP パケットについてインターフェイスがモニタされる累積期間を秒単位で指定します。範囲は 1 ～ 15 です。 • **rate none** では、処理可能な着信 ARP パケットの上限を指定しません。

	コマンド	目的
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 インスペクションの errdisable ステートからのエラー回復をイネーブルにします。 デフォルトで、回復はディセーブルで、回復間隔は 300 秒です。 **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**	特権 EXEC モードに戻ります。
ステップ 7	**show ip arp inspection interfaces** **show errdisable recovery**	設定値を確認します。
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 インスペクション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 インスペクションでは、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、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	目的
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、チェックは実行しません。 キーワードの意味は次のとおりです。 • **src-mac** では、ARP ボディ内の発信者 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、ドロップされます。 • **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、ドロップされます。 • **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。 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、別のコマンドが IP 検証だけをイネーブルにした場合、別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**	特権 EXEC モードに戻ります。
ステップ 4	**show ip arp inspection vlan** *vlan-range*	設定値を確認します。
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、ドロップ、MAC 検証失敗、および IP 検証失敗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ドロップする際に、ログ バッファにエントリを配置してレート制限ベースにシステム メッセージを生成します。メッセージの生成後、スイッチはエントリをログ バッファから削除します。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ています。

ログバッファ エントリは、複数のパケットを表示できます。たとえば、インターフェイスが同じ ARP パラメータを持つ VLAN 上で多くのパケットを受信する場合、スイッチはパケットをログ バッファ内の 1 つのエントリに結合して、エントリの単一のシステム 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、つまり、ログ イベントがログ バッファに収まらない場合、**show ip arp inspection log** 特権 EXEC コマンドの表示が影響を受けます。表示内の「--」は、パケット カウントと時間を除く、すべてのデータの代わりに表示されます。他の統計情報はエントリ用に提供されます。このエントリを表示で見る場合、ログ バッファ内のエントリ数を増やすか、ロギング レートを増やします。

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、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	目的
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 インスペクション ロギング バッファを設定します。 デフォルトで、ダイナミック ARP インスペクションがイネーブルの場合、拒否パケットまたはドロップ ARP パケットがログされます。ログ エントリの数は 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。ロギングレート間隔は 1 秒です。 キーワードの意味は次のとおりです。 • **entries** *number* では、バッファ内に記録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。 • **logs** *number* **interval** *seconds* では、指定した間隔でシステム メッセージを生成するためのエントリ数を指定します。 **logs** *number* に指定できる範囲は 0 ～ 1024 です。値を 0 にすると、エントリはログ バッファに配置されますが、システム メッセージは生成されません。 **interval** *seconds* に指定できる範囲は 0 ～ 86400 秒（1 日）です。0 値は、システム メッセージが即座に生成されます（またログ バッファは常に空です）。 0 の間隔設定は、ログ設定 0 を上書きします。 **logs** および **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、X を Y で除算した（X/Y）数のシステム メッセージが毎秒送信されます。そうでない場合、1 つのシステム メッセージが Y を X で除算した（Y/X）秒ごとに送信されます。

	コマンド	目的
ステップ 3	**ip arp inspection vlan** *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	記録されるパケットのタイプを VLAN 単位で制御します。デフォルトで、すべての拒否パケットおよびドロップ パケットが記録されます。用語 *logged* は、エントリはログ 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。 キーワードの意味は次のとおりです。 • *vlan-range* では、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。 • **acl-match matchlog** では、ACR ロギング設定に基づいたパケットを記録します。このコマンドで **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 コマンドで **log** キーワードを指定した場合、ACL で許可または拒否された ARP パケットが記録されます。 • **acl-match none** では、ACL と一致するパケットを記録しません。 • **dhcp-bindings all** では、DHCP バインディングと一致するパケットがすべて記録されます。 • **dhcp-bindings none** では、DHCP バインディングと一致するパケットが記録されません。 • **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**	特権 EXEC モードに戻ります。
ステップ 5	**show ip arp inspection log**	設定値を確認します。
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 バッファをクリアするには、**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 インスペクション情報の表示

ダイナミック ARP インスペクション情報を表示するには、表 23-2 で説明している特権 EXEC コマンドを使用します。

表 23-2　ダイナミック ARP インスペクション情報のコマンド

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 インスペクションの設定および動作状態を表示します。VLAN を指定しない場合、または範囲を指定しない場合は、ダイナミック ARP インスペクションがイネーブル（アクティブ）である VLAN の情報だけが表示されます。

ダイナミック ARP インスペクション統計情報を消去または表示するには、表 23-3 で説明している特権 EXEC コマンドを使用します。

表 23-3　ダイナミック ARP インスペクションの統計情報を消去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 インスペクションの統計情報を消去します。
show ip arp inspection statistics [**vlan** *vlan-range*]	指定した VLAN の転送パケット、ドロップ パケット、MAC 確認エラー パケット、IP 確認エラー パケット、ACL の許可および拒否パケット、DHCP 許可および拒否パケットの統計情報が表示されます。VLAN を指定しない場合、または範囲を指定しない場合は、ダイナミック ARP インスペクションがイネーブル（アクティブ）である VLAN の情報だけが表示されます。

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 インスペクション ポート上の各 ARP 要求および応答パケットの転送パケット数を増やします。スイッチは、各パケットに対して、送信元 MAC、宛先 MAC、または IP 検証チェックで拒否された ACL または DHCP 許可パケット数を増加させ、スイッチは該当する失敗カウントを増加させます。

ダイナミック ARP インスペクション ロギング情報を消去または表示するには、表 23-4 で説明している特権 EXEC コマンドを使用します。

表 23-4　ダイナミック ARP インスペクションのロギング情報を消去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 インスペクション 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 インスペクション ログ バッファの設定と内容を表示します。

こ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。