



ダイナミック ARP 検査の設定

この章では、Catalyst 3560 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、同じ VLAN (仮想 LAN) 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。



(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。

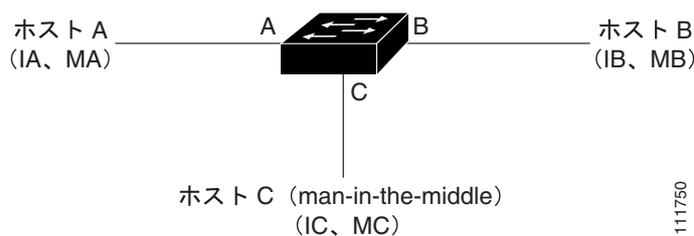
- [ダイナミック ARP 検査の概要 \(p.22-2\)](#)
- [ダイナミック ARP 検査の設定 \(p.22-6\)](#)
- [ダイナミック ARP 検査情報の表示 \(p.22-16\)](#)

ダイナミック ARP 検査の概要

ARP では、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。攻撃のあと、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 22-1 は、ARP キャッシュ ポイズニングの例です。

図 22-1 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 アドレスは括弧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ため、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 *man-in-the-middle* 攻撃を行います。

ダイナミック ARP 検査は、ネットワーク内の ARP パケットを検査するセキュリティ機能です。この検査では、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 *man-in-the-middle* 攻撃からネットワークを保護できます。

ダイナミック ARP 検査により、有効な ARP 要求および応答のみ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 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のみ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 検査をイネーブルにできます。設定情報については、「[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。

非 DHCP 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。設定情報については、「[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.22-5) 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 パケットを廃棄するようにダイナミック ARP 検査を設定できます。**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.22-12) 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 検査は、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 検査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 検査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。

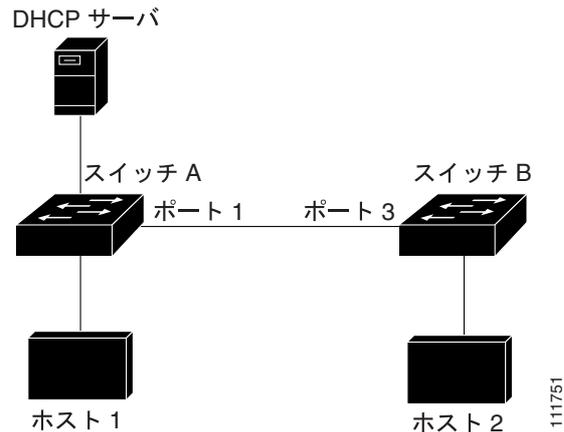


注意

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 22-2 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 検査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 のみがホスト 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 によって廃棄されます。ホスト 1 およびホスト 2 の間の接続は失われます。

図 22-2 ダイナミック ARP 検査がイネーブルな VLAN での ARP パケット検証



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 検査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 検査を実行していても発生します。

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 検査では、ネットワークのほかの部分にあるホストでは、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 検査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 検査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 検査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 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分離します。設定情報については、「[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 検査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** ステータスにします。ユーザが介入するまでポートは **errdisable** ステータスのままになります。**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タス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。

設定手順については、「[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 エントリの相対的なプライオリティ

ダイナミック ARP 検査では、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 のみを使用します。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。

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。設定情報については、「[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、次の設定情報について説明します。

- デフォルトのダイナミック ARP 検査の設定 (p.22-6)
- ダイナミック ARP 検査の設定時の注意事項 (p.22-6)
- DHCP 環境でのダイナミック ARP 検査の設定 (p.22-7) (DHCP 環境で必須)
- 非 DHCP 環境の ARP ACL の設定 (p.22-9) (非 DHCP 環境で必須)
- 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.22-12) (任意)
- ログバッファの設定 (p.22-14) (任意)

デフォルトのダイナミック ARP 検査の設定

表 22-1 に、デフォルトのダイナミック ARP 検査の設定を示します。

表 22-1 デフォルトのダイナミック ARP 検査の設定

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。
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 検査がイネーブルの場合、すべての拒否または廃棄 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。 ログングレート間隔は 1 秒です。
VLAN 単位ログング	拒否または廃棄されたすべての ARP パケットがログされます。

ダイナミック ARP 検査の設定時の注意事項

ダイナミック ARP 検査の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 検査は、ダイナミック ARP 検査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。man-in-the-middle 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 検査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 検査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 検査は 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 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 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 ポートでサポートされています。
- 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のみ、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。

- 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あとに、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 検査対応 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 ステートにするとときに、他の VLAN が DoS 攻撃を受ける可能性があります。

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 検査を設定する方法について説明します。図 22-2 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 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。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 検査は 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 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。

■ ダイナミック ARP 検査の設定

1つのスイッチのみがダイナミック ARP 検査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.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、イネーブル 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	<code>show cdp neighbors</code>	スイッチ間の接続を確認します。
ステップ 2	<code>configure terminal</code>	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	<code>ip arp inspection vlan vlan-range</code>	ダイナミック ARP 検査を 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 検査はすべての VLAN でディセーブルに設定されています。 <i>vlan-range</i> 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	<code>interface interface-id</code>	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	<code>ip arp inspection trust</code>	スイッチ間の接続を <code>trusted</code> 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 <code>untrusted</code> 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、 <code>ip arp inspection vlan logging</code> 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、無効なパケットを廃棄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.22-14)を参照してください。
ステップ 6	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show ip arp inspection interfaces</code> <code>show ip arp inspection vlan vlan-range</code>	ダイナミック ARP 検査の設定を確認します。
ステップ 8	<code>show ip dhcp snooping binding</code>	DHCP バインディングを確認します。
ステップ 9	<code>show ip arp inspection statistics vlan vlan-range</code>	ダイナミック ARP 検査の設定をチェックします。
ステップ 10	<code>copy running-config startup-config</code>	(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。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 検査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 gigabitethernet0/1
Switch(config-if)# ip arp inspection trust
```

非 DHCP 環境の ARP ACL の設定

この手順は、[図 22-2](#) で示すスイッチ 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ていない場合に、ダイナミック ARP 検査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、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、非 DHCP 環境で必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>arp access-list <i>acl-name</i></code>	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 <code>deny ip any mac any</code> コマンドがあります。
ステップ 3	<code>permit ip host <i>sender-ip</i> mac host <i>sender-mac</i> [log]</code>	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。 <ul style="list-style-type: none"><code>sender-ip</code> に対して、ホスト 2 の IP アドレスを入力します。<code>sender-mac</code> 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; アクセス制御エントリ) 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 <code>log</code> を指定します。<code>ip arp inspection vlan logging</code> グローバル コンフィギュレーション コマンドを <code>matchlog</code> 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.22-14) を参照してください。
ステップ 4	<code>exit</code>	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	<code>ip arp inspection filter arp-acl-name vlan vlan-range [static]</code>	<p>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。</p> <ul style="list-style-type: none"> • <code>arp-acl-name</code> には、ステップ 2 で作成した ACL 名を指定します。 • <code>vlan-range</code> 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廃棄するには、<code>static</code> を指定します。DHCP バインディングは使用されません。 <p>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。</p> <p>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のみ許可されます。</p>
ステップ 6	<code>interface interface-id</code>	<p>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。</p>
ステップ 7	<code>no ip arp inspection trust</code>	<p>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 <code>untrusted</code> として設定します。</p> <p>デフォルトでは、すべてのインターフェイスが <code>untrusted</code> です。</p> <p>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、<code>ip arp inspection vlan logging</code> 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、無効なパケットを廃棄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.22-14) を参照してください。</p>
ステップ 8	<code>end</code>	<p>イネーブル EXEC モードに戻ります。</p>
ステップ 9	<code>show arp access-list [acl-name]</code> <code>show ip arp inspection vlan vlan-range</code> <code>show ip arp inspection interfaces</code>	<p>設定を確認します。</p>
ステップ 10	<code>copy running-config startup-config</code>	<p>(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。</p>

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 gigabitethernet0/1
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 検査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* ステータスにします。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タス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* ステータスのままになります。



(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あと、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 検査の設定時の注意事項](#)」(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、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	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	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。

	コマンド	目的
ステップ 3	<code>ip arp inspection limit {rate pps [burst interval seconds] none}</code>	<p>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。</p> <p>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。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • 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。
ステップ 4	<code>exit</code>	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	<code>errdisable recovery cause arp-inspection interval interval</code>	<p>(任意) ダイナミック ARP 検査の <code>errdisable</code> ステートからのエラー回復をイネーブルにします。</p> <p>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。</p> <p>interval interval では、<code>errdisable</code> 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。</p>
ステップ 6	<code>exit</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show ip arp inspection interfaces</code> <code>show errdisable recovery</code>	設定値を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(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、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	目的
ステップ 1	<code>configure terminal</code>	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	<code>ip arp inspection validate {[src-mac] [dst-mac] [ip]}</code>	<p>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。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • 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、廃棄されます。 • 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、廃棄されます。 • 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。 <p>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 番目のコマンドが IP 検証のみをイネーブルにした場合、2 番目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。</p>
ステップ 3	<code>exit</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show ip arp inspection vlan <i>vlan-range</i></code>	設定値を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(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、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` 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** イネーブル 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える場合、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	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}	<p>ダイナミック ARP 検査ロギングバッファを設定します。</p> <p>デフォルトで、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 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の数は、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。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>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)。</p> <p>0 の間隔設定は、ログ設定 0 を上書きします。</p> <p>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) 秒毎に送信されます。</p>

	コマンド	目的
ステップ 3	ip arp inspection vlan <i>vlan-range</i> logging {acl-match {matchlog none} dhcp-bindings {all none permit}}	<p>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、すべての拒否および廃棄パケットが記録されます。用語 <i>logged</i> 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。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • 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	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** 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 22-2 で説明しているイネーブル EXEC コマンドを使用します。

表 22-2 ダイナミック ARP 検査情報のコマンド

コマンド	説明
<code>show arp access-list [acl-name]</code>	ARP ACL の詳細情報を表示します。
<code>show ip arp inspection interfaces [interface-id]</code>	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。
<code>show ip arp inspection vlan vlan-range</code>	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 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 検査がイネーブル（アクティブ）である VLAN の情報のみが表示されます。

ダイナミック ARP 検査統計情報を消去するには、表 22-3 で説明しているイネーブル EXEC コマンドを使用します。

表 22-3 ダイナミック ARP 検査の統計情報を消去または表示するコマンド

コマンド	説明
<code>clear ip arp inspection statistics</code>	ダイナミック ARP 検査の統計情報を消去します。
<code>show ip arp inspection statistics [vlan vlan-range]</code>	指定した VLAN の転送パケット、廃棄パケット、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 検査がイネーブル（アクティブ）である VLAN 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 検査ロギング情報を消去するには、表 22-4 で説明しているイネーブル 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消去または表示するコマンド

コマンド	説明
<code>clear ip arp inspection log</code>	ダイナミック ARP 検査ログ バッファをクリアします。
<code>show ip arp inspection log</code>	ダイナミック ARP 検査ログ 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。

■ ダイナミック ARP 検査情報の表示