



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を説明します。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、スイッチ上の意図的な攻撃を回避します。



(注) ここ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。

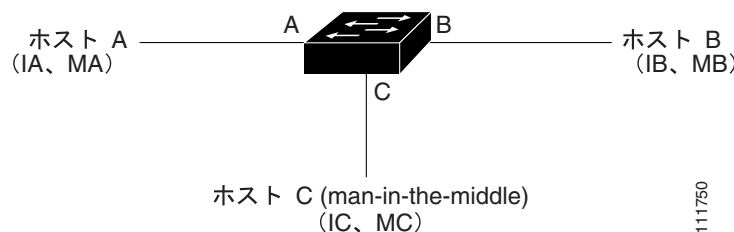
- [ダイナミック ARP 検査の概要 \(p.20-2\)](#)
- [ダイナミック ARP 検査の設定 \(p.20-6\)](#)
- [ダイナミック ARP 検査情報の表示 \(p.20-16\)](#)

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 に情報を送信するのに、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 要求を受信されなかった場合でも ARP はホストから不当な応答を許可するので、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向け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 20-1 に ARP キャッシュ ポイズニングの例を示します。

図 20-1 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、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 にバインドされず、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 を持った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 を持ったホスト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、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 キャッシュを持ったホストは、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。これはホスト C がトラフィックを代行受信することを意味します。ホスト C は、IA および IB に関連する正当な MAC アドレスを知っているので、宛先として正しい MAC アドレスを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、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った ARP パケットを代行受信、ロギング、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を確実にリレーします。スイッチは次のアクティビティを実行します。

- 信頼されないポート上のすべての ARP 要求と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に有効な IP/MAC アドレス バインディングがあるかどうかを確認します。
- 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でき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 パケットの有効性を判別します。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 単位で `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.20-7) 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 アドレスを持ったホストに対してユーザが設定した ARP Access Control List (ACL; アクセス制御リスト) と照合して ARP パケットを検証できます。`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、「[非 DHCP 環境の ARP ACL の設定](#)」(p.20-9) 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.20-5) を参照してください。

パケットの IP アドレスが無効な場合、または ARP パケット本体の 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と一致しない場合に、ARP パケットを廃棄するようダイナミック 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.20-13) 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着信するパケットは、すべてのダイナミック ARP 検査の妥当性チェックをバイパスします。信頼できないインターフェイスに着信するパケットでは、ダイナミック ARP 検査の検証プロセスが実行されます。

一般的なネットワーク構成では、ホスト ポートに接続されたスイッチ ポートすべてを信頼されない状態として設定し、スイッチに接続されたスイッチ ポートすべてを信頼される状態として設定します。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 チェックをバイパスします。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。`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。

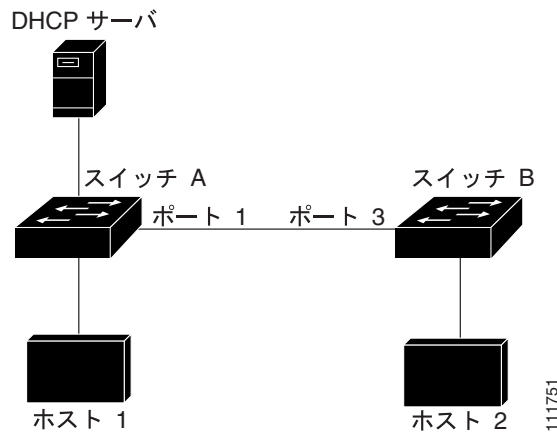


注意

信頼状態設定は、慎重に使用してください。インターフェイスを信頼する必要がある場合に信頼されない状態として設定すると、接続が切断されることがあります。

図 20-2 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 の間の接続が切断されます。

図 20-2 ダイナミック ARP 検査がイネーブルである 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します。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 (およびスイッチの間のリンクが信頼される状態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上の) 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 検査では、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を回避しません。

VLAN の一部のスイッチがダイナミック ARP 検査を実行し、他のスイッチが実行していない場合、そのスイッチに接続しているインターフェイスを信頼されない状態として設定します。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.20-9) 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、VLAN のすべてのスイッチ上で指定した 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、DoS 攻撃を回避するため着信 ARP パケット数は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した制限値を超えると、スイッチはそのポートをエラーディセーブル状態にします。変更しないかぎり、ポートはその状態のままです。指定したタイムアウト時間のあと、ポートが自動的にこの状態から抜け出せるようにエラーディセーブル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.20-11) 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/MAC アドレス バインディングのリストに 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 ACL を設定した場合のみ、ACL を使用します。まずスイッチは、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は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、エントリをログ バッファに格納してから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.20-14) 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 \(p.20-6\)](#)
- [ダイナミック ARP 検査設定時の注意事項 \(p.20-6\)](#)
- [DHCP 環境でのダイナミック ARP 検査の設定 \(p.20-7\)](#) (DHCP 環境で必須)
- [非 DHCP 環境の ARP ACL の設定 \(p.20-9\)](#) (非 DHCP 環境で必須)
- [着信 ARP パケットのレート制限 \(p.20-11\)](#) (任意)
- [妥当性チェックの実行 \(p.20-13\)](#) (任意)
- [ログバッファの設定 \(p.20-14\)](#) (任意)

ダイナミック ARP 検査のデフォルト設定

表 20-1 に、ダイナミック ARP 検査のデフォルト設定を示します。

表 20-1 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	すべてのインターフェイスは信頼されません。
着信 ARP パケットのレート制限	ネットワークが、1 秒間に 15 の新規ホストに接続するホストを持つスイッチドネットワークであると想定した場合、信頼されないインターフェイス上のレートは 15 pps です。 すべての信頼されるインターフェイス上ではレートは無制限です。 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。
妥当性チェック	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、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ます。 ログのエントリ数は 32 です。 システム メッセージ数は 5 秒単位で制限されます。 ロギングレートの間隔は 1 秒です。
VLAN 単位のロギング	拒否または廃棄された ARP パケットすべてがロギングされます。

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ではないスイッチに接続されたホストに対して、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ので、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であるドメインにあるホストの ARP キャッシュを保護します。

- ダイナミック ARP 検査は 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、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、必ず DHCP スヌーピングをイネーブルにしてください。設定の詳細については、第 19 章「DHCP 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である、または非 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、プライベート VLAN ポート上でサポートされます。
- 物理ポートは、物理ポートとチャンネル ポートの信頼状態が一致する場合のみ、EtherChannel ポート チャンネルに参加できます。それ以外の場合、物理ポートはポート チャンネルのままです。ポート チャンネルは、チャンネルに参加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、そのチャン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 チャンネルの信頼状態を変更した場合、スイッチはチャン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 では、実際のレート制限が設定値より高くなる場合があります。たとえば、スイッチ 1 に 1 個のポート、スイッチ 2 に 1 個のポートがある EtherChannel 上でレート制限を 30 pps に設定する場合、EtherChannel がエラーディセーブルにならずに、各ポートは 29 pps でパケットを受信できます。
- ポート チャンネルの動作レートは、チャン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、ポート チャンネルに 400 pps の ARP レート制限を設定した場合、チャンネル上で組み合わされた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、すべてのチャンネル 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。チャンネル 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 チャンネルの設定に対してチェックされます。ポート チャンネルのレート制限設定は、物理ポートの設定とは関係ありません。

EtherChannel が設定したレート以上の ARP パケットを受信する場合、チャンネル(すべての物理ポートを含む)はエラーディセーブル状態になります。

- 必ず、着信トランク ポートで ARP パケットのレートを制限してください。集約を反映し、複数のダイナミック ARP 検査対応 VLAN 上でパケットを処理するには、トランク ポートのレートを高く設定します。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 コマンドを使用できます。1 個の 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エラーディセーブル状態になった場合に他の VLAN へ DoS 攻撃を行うことがあります。

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。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 20-2 [p.20-4] を参照)。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) ダイナミック ARP 検査は DHCP スヌーピング バインディング データベースのエントリによって異なり、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、必ず DHCP スヌーピングをイネーブルにしてください。設定の詳細については、第 19 章「DHCP 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 検査をサポートする場合にこの機能を設定する方法については、「非 DHCP 環境の ARP ACL の設定」(p.20-9) 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実行します。この手順は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>	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 検査はすべての VLAN 上でディセーブルです。 <i>vlan-range</i> 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。 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て、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信頼される状態として設定します。 デフォルトでは、すべてのインターフェイスは信頼されません。 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。スイッチはただパケットを転送するだけです。 信頼され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に有効な IP/MAC アドレス バインディングがあるかどうかを確認します。 <code>ip arp inspection vlan logging</code> グローバル コンフィギュレーション コマンドで指定されたロギング設定に従い、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.20-14) 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。

	コマンド	目的
ステップ 9	<code>show ip arp inspection statistics vlan vlan-range</code>	ダイナミック ARP 検査の統計情報をチェックします。
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。インターフェイスを信頼され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 gigabitethernet 0/1
Switch(config-if)# ip arp inspection trust
```

非 DHCP 環境の ARP ACL の設定

次の手順では、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 (図 20-2 [p.20-4] を参照) 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 を信頼される状態として設定する場合、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ことがあるので、セキュリティ ホールが作成されます。これを避けるには、スイッチ A のポート 1 を信頼されない状態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、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 環境では必須です。

	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 acl-name</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、暗黙的な <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 sender-ip mac host sender-mac [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> には、ホスト 2 の IP アドレスを入力します。 <code>sender-mac</code> には、ホスト 2 の MAC アドレスを入力します。 (任意) パケットが Access Control Entry (ACE; アクセス制御 エントリ) と一致する場合にログ バッファにロギングするには、<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 コマンドで <code>matchlog</code> キーワードを設定する場合、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.20-14) を参照してください。

■ ダイナミック ARP 検査の設定

	コマンド	目的
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>ip arp inspection filter arp-acl-name vlan vlan-range [static]</code>	<p>ARP ACL を VLAN に適用します。デフォルトでは、どの VLAN にも定義された ARP ACL は適用されません。</p> <ul style="list-style-type: none"> <code>arp-acl-name</code> を指定する場合は、ステップ 2 で作成した ACL の名前を指定します。 <code>vlan-range</code> には、スイッチおよびホストが存在する 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。 (任意) ARP ACL での暗黙的な拒否を明示的な拒否として扱い、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 に明示的な拒否が存在せず、パケットが ACL の句と一致しない場合に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を意味します。</p> <p>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。</p>
ステップ 6	<code>interface interface-id</code>	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て、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	<code>no ip arp inspection trust</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信頼できない状態として設定します。</p> <p>デフォルトでは、すべてのインターフェイスは信頼されません。</p> <p>信頼され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に有効な IP/MAC アドレス バインディングがあるかどうかを確認します。<code>ip arp inspection vlan logging</code> グローバル コンフィギュレーション コマンドで指定されたロギング設定に従い、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.20-14) を参照してください。</p>
ステップ 8	<code>end</code>	イネーブル EXEC モードに戻ります。
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>	設定を確認します。
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。

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 を信頼されない状態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 gigabitethernet 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、DoS 攻撃を回避するため着信 ARP パケット数はレート制限されます。

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エラーディセーブル状態にします。指定したタイムアウト時間のあと、ポートが自動的にこの状態から抜け出せるようにエラーディセーブル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場合に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に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です。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については、「[ダイナミック ARP 検査設定時の注意事項](#)」(p.20-6) 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	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 <i>interface-id</i>	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。

■ ダイナミック ARP 検査の設定

	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で着信 ARP 要求および応答のレートを制限します。</p> <p>信頼できないインターフェイス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。</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"> • <code>rate pps</code> には、秒単位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。 • (任意) <code>burst interval seconds</code> には、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。 • <code>rate none</code> には、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。
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 検査のエラーディセーブル ステートからのエラー回復をイネーブルにします。</p> <p>デフォルトでは回復はディセーブルで、回復インターバルは 300 秒です。</p> <p><code>interval interval</code> には、エラーディセーブル 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。</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、不正な IP/MAC アドレス バインディングを持った ARP パケットを代行受信、ロギング、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、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、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。デフォルトでは、チェックは実行されません。</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"> <code>src-mac</code> 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 アドレスとチェックされます。このチェックは、ARP 要求と ARP 応答の両方で実行されます。イネーブルである場合、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。 <code>dst-mac</code> では、イーサネット ヘッダーの宛先 MAC アドレスと ARP 本体のターゲット MAC アドレスをチェックします。このチェックは ARP 応答に対して実行されます。イネーブルである場合、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。 <code>ip</code> の場合、無効で予想外の 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。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。 <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、直前のコマンドの設定を上書きします。つまり、あるコマンドが <code>src</code> および <code>dst mac</code> の検証をイネーブルにし、2 番目のコマンドが IP の検証のみをイネーブルにしている場合、<code>src</code> および <code>dst mac</code> の検証は 2 番目のコマンドの結果として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。転送および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` 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、エントリをログバッファに格納してから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、インターフェイスが同じ ARP パラメータを持った同じ 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、ログイベントはログバッファに適合しないことになり、`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。パケットのカウントと時刻以外のすべてのデータ位置に -- 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。表示内にこのエントリを見つけた場合、ログバッファのエントリ数を増やす、または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、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 log-buffer {entries number logs number interval seconds}</code>	<p>ダイナミック ARP 検査のロギング バッファを設定します。</p> <p>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すべての 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 個に制限されています。ロギングレートの間隔は 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"> <code>entries number</code> には、バッファにロギング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。 <code>logs number interval seconds</code> には、指定され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。 <p><code>logs number</code> の場合、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おかれませんがシステムメッセージは生成されません。</p> <p><code>interval seconds</code> の場合、指定できる範囲は 0 ~ 86400 秒 (1 日) です。値を 0 にすると、システムメッセージがただちに生成されます (ログバッファは常に空です)。</p> <p>間隔を 0 に設定すると、ログ設定に 0 を上書きします。</p> <p><code>logs</code> 設定と <code>interval</code> 設定は相互作用します。<code>logs number X</code> が <code>interval seconds Y</code> 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送信されます。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。</p>

	コマンド	目的
ステップ 3	<code>ip arp inspection vlan <i>vlan-range</i> logging {acl-match {matchlog none} dhcp-bindings {all none permit}}</code>	<p>VLAN 単位で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、拒否または廃棄されたパケットがすべてロギングされます。ロギングされるという用語は、エントリがログバッファにお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"> • <i>vlan-range</i> 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。 • <code>acl-match matchlog</code> には、ACE ロギング設定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 <code>matchlog</code> キーワードを、<code>permit</code> または <code>deny</code> ARP アクセスリスト コンフィギュレーション コマンドで <code>log</code> キーワードを指定する場合、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。 • <code>acl-match none</code> では、ACL と一致するパケットをロギングしないでください。 • <code>dhcp-bindings all</code> では、DHCP バインディングと一致するパケットすべてをロギングします。 • <code>dhcp-bindings none</code> では、DHCP バインディングと一致するパケットをロギングしないでください。 • <code>dhcp-bindings permit</code> では、DHCP バインディング許可パケットをロギングします。
ステップ 4	<code>exit</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show ip arp inspection log</code>	設定を確認します。
ステップ 6	<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 20-2 に示すイネーブル EXEC コマンドを使用します。

表 20-2 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
<code>show arp access-list [acl-name]</code>	ARP ACL についての詳細情報を表示します。
<code>show ip arp inspection interfaces [interface-id]</code>	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。
<code>show ip arp inspection vlan vlan-range</code>	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、または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) である VLAN に関する情報のみが表示されます。

ダイナミック ARP 検査の統計情報をクリアするには、表 20-3 に示すイネーブル EXEC コマンドを使用します。

表 20-3 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
<code>clear ip arp inspection statistics</code>	ダイナミック ARP 検査の統計情報をクリアします。
<code>show ip arp inspection statistics [vlan vlan-range]</code>	指定の VLAN の転送および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 許可および拒否パケット、DHCP 許可および拒否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、または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) である VLAN に関する情報のみが表示されます。

`show ip arp inspection statistics` コマンドの場合、スイッチは、信頼されるダイナミック 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 妥当性チェックによって拒否された各パケットに対し、ACL または DHCP 許可パケット数を増加し、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 20-4 に示すイネーブル EXEC コマンドを使用します。

表 20-4 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
<code>clear ip arp inspection log</code>	ダイナミック ARP 検査の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。