



ダイナミック ARP インспекションの設定

この章では、スイッチ上でダイナミック アドレス解決プロトコル インспекション (ダイナミック ARP インспекション) を設定する方法を説明します。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。特に記述がない限り、スイッチという用語はスタンドアロンスイッチとスイッチ スタックを意味しています。



(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。

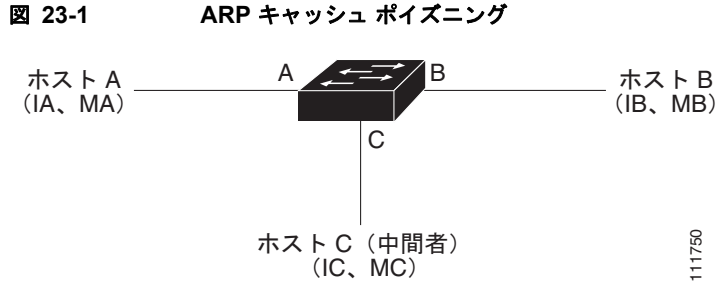
この章で説明する内容は、次のとおりです。

- 「[ダイナミック ARP インспекションの概要](#)」 (P.23-1)
- 「[ダイナミック ARP インспекションの設定](#)」 (P.23-5)
- 「[ダイナミック ARP インспекション情報の表示](#)」 (P.23-15)

ダイナミック ARP インспек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向けのブロードキャスト メッセージを生成して、ホスト A の IP アドレスに関連付けられた 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、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。



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 が IP レイヤでホスト B と通信する必要がある場合は、IP アドレス B に関連付けられている MAC アドレスの ARP 要求をブロードキャストします。スイッチとホスト B が ARP 要求を受信するときには、IP アドレス IA と MAC アドレス MA を持つホストの ARP バインディングで ARP キャッシュを入力します。たとえば、IP アドレス IA は MAC アドレス MA に向けられます。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 キャッシュを持つホストは、MAC アドレス MC を、IA または IB に向けられたトラフィックの宛先 MAC アドレスとして使用します。これは、ホスト C がその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ます。ホスト C は、ホスト A からホスト B へのトラフィック ストリームに割り込んで、一般的な *中間者攻撃* を行います。

ダイナミック ARP インспек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спек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 キャッシュのアップデート前、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спек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спекション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 インспек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спек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。設定情報については、「[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спек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、「[検証チェックの実行](#)」(P.23-13) 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спек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спек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спек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。

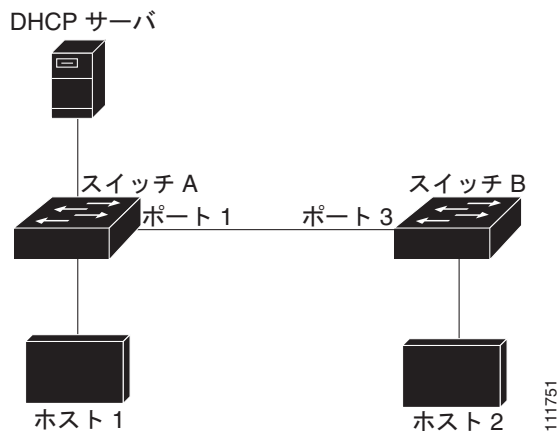


注意

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 とスイッチ B の両方がホスト 1 とホスト 2 を含む VLAN 上でダイナミック ARP インспекションを実行していると想定します。ホスト 1 とホスト 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場合は、スイッチ A だけがホスト 1 の IP と 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 の間のインターフェイスを信頼できない場合は、スイッチ B でホスト 1 からの ARP パケットがドロップされます。ホスト 1 とホスト 2 の間の接続は失われます。

図 23-2 ダイナミック ARP インспекションがイネーブルな 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 インспек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спек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спекションは、ダイナミック ARP インспек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спекションでは、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 インспек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спек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спек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спек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спекションを実行しているスイッチを、ダイナミック ARP インспекション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.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спекション検証チェックを実行するため、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、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された制限を超えた場合、スイッチはポートを **errdisable** ステートにします。介入しない限り、ポートはそのままの状態となります。**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、スタックの各スイッチに個別に適用されます。たとえば、20 pps の上限が EtherChannel で設定されている場合は、EtherChannel のポートを持つ各スイッチが最大 20 pps で伝送を行います。スイッチがこの制限を超えると、EtherChannel は **errdisable** ステートになります。

設定情報については、「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спек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。設定情報については、「[ログ バッファの設定](#)」(P.23-14) を参照してください。

ダイナミック ARP インспекションの設定

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 インспекションの設定](#)」(P.23-5)
- 「[ダイナミック ARP インспекションの設定時の注意事項](#)」(P.23-6)
- 「[DHCP 環境でのダイナミック ARP インспекションの設定](#)」(P.23-7) (DHCP 環境で必須)
- 「[非 DHCP 環境の ARP ACL の設定](#)」(P.23-9) (非 DHCP 環境で必須)
- 「[着信 ARP パケットのレート制限](#)」(P.23-11) (任意)
- 「[検証チェックの実行](#)」(P.23-13) (任意)
- 「[ログ バッファの設定](#)」(P.23-14) (任意)

デフォルトのダイナミック ARP インспек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спек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спекションの設定

機能	デフォルト設定
ダイナミック ARP インспек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	このレートは、信頼できないインターフェイス上で 15 pps に設定されています。ただし、1 台のホストが 1 秒間に 15 台の新規ホストに接続できるスイッチドネットワークであると仮定しています。 信頼できるすべてのインターフェイスでは、レートは無制限です。 バースト インターバルは 1 秒に設定されています。
非 DHCP 環境の ARP ACL	ARP ACL は定義されません。
検証チェック	どの検証も実行されません。

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

機能	デフォルト設定
ログ バッファ	ダイナミック ARP インспек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 メッセージの数は 1 秒あたり 5 つに制限されています。 ロギングレート インターバルは、1 秒です。
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спекションの設定時の注意事項

ダイナミック ARP インспек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спек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спекションは、ダイナミック ARP インспек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спек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を分離します。この処置により、ダイナミック ARP インспек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спек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「Dynamic Host Configuration Protocol \(DHCP\) 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 インспек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。
- 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だけ、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 チャネル内で一時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ごとに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、ポートチャンネルの ARP レート制限を 400 pps に設定した場合、チャン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、全チャン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。チャン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ンネル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) チャンネルは `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спек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спек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サーは無効となります。その結果、全ての ARP トラフィックが CPU に送信されます。

DHCP 環境でのダイナミック ARP インспек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спек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спекションを実行しています。DHCP サーバはスイッチ A に接続しています。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спек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「Dynamic Host Configuration Protocol (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 つのスイッチだけがダイナミック ARP インспек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спек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。

■ ダイナミック ARP インспекションの設定

	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 <i>vlan-range</i>	ダイナミック ARP インспек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спек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。 <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	interface <i>interface-id</i>	他のスイッチに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	ip arp inspection trust	スイッチ間の接続を trusted 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 要求と ARP 応答を代行受信します。ローカル キャッシュのアップデート前、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、無効なパケットをドロップし、 ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ 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.23-14) 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 show ip arp inspection vlan <i>vlan-range</i>	ダイナミック ARP インспекションの設定を確認します。
ステップ 8	show ip dhcp snooping binding	DHCP バインディングを確認します。
ステップ 9	show ip arp inspection statistics vlan <i>vlan-range</i>	ダイナミック ARP インспекションの設定をチェックします。
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 インспек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。

この例では、VLAN 1 のスイッチ A のダイナミック ARP インспекションを設定する方法を示します。スイッチ B で同様の手順を実行することもあります。

```
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спек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спек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 を信頼できるポートとして設定する場合には、スイッチ A とホスト 1 がスイッチ B またはホスト 2 によって攻撃される可能性があるため、セキュリティ ホールが生じます。この可能性を防止するには、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はない（スイッチ A に ACL 設定を適用できない）場合は、スイッチ A とレイヤ 3 のスイッチ B を分離し、ルータを使用してスイッチ間の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 の 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 環境で必要です。

	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"> • <i>sender-ip</i> に対して、ホスト 2 の IP アドレスを入力します。 • <i>sender-mac</i> 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。 <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 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.23-14) 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"> • <i>arp-acl-name</i> には、ステップ 2 で作成した ACL 名を指定します。 • <i>vlan-range</i> には、スイッチとホストがある VLAN を指定します。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 • (任意) ARP ACL 内の暗黙の拒否を明示的な拒否として取り扱い、ACL 内の前の句に一致しないパケットをドロップするために、static 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は、パケットを拒否する明示的な拒否が ACL 内にないことを意味し、パケットが ACL 内の句に一致しないと DHCP バインディングがパケットの許可または拒否を決定します。</p> <p>IP および MAC アドレスのバインディングだけを含む 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だけ許可されます。</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 untrusted 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 untrusted 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 要求と ARP 応答を代行受信します。ローカル キャッシュのアップデート前、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、無効なパケットをドロップし、ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ 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.23-14) を参照してください。</p>
ステップ 8	<code>end</code>	<p>特権 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 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спекション検証チェックを実行するため、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超えた場合、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。レート制限を設定すると、インターフェイスはその信頼状態が変更された場合でも設定されたレート制限を維持します。**no ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

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спек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}	<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。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 インターバルは 1 秒に設定されています。</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"> 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。

■ ダイナミック ARP インспекションの設定

	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 detect cause arp-inspection および errdisable recovery cause arp-inspection および errdisable recovery interval interval	(任意) ダイナミック ARP インспекション errdisable ステートからのエラー回復をイネーブルにし、ダイナミック ARP インспекション回復メカニズム変数を設定します。 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спек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。

検証チェックの実行

ダイナミック ARP インспек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 アドレスおよびターゲット 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	<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</code> <code>{[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。この検証は、ARP 要求と ARP 応答に両方に対して実行されます。このチェックがイネーブルの場合、異なる MAC アドレスを持つ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。この検証は、ARP 応答に対して実行されます。このチェックがイネーブルの場合、異なる MAC アドレスを持つ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。0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスがこれに該当します。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、ターゲット IP アドレスは ARP 応答でだけチェックされます。 <p>少なくとも 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 検証だけ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>	特権 EXEC モードに戻ります。
ステップ 4	<code>show ip arp inspection vlan</code> <code>vlan-range</code>	設定値を確認します。
ステップ 5	<code>copy running-config</code> <code>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、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する場合は、ログイベントがログバッファに収まらないことを意味しており、**show ip arp inspection log** 特権 EXEC コマンドの出力が影響を受けます。パケット数および時間以外のすべてのデータの代わりに「--」が表示されます。このエントリに関してそれ以外の統計情報は表示されません。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** エントリがあり、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、間隔（レート）が毎秒 1 つのエントリである場合は、5 つのメンバーから構成されるスイッチスタックで、最大 5 つのシステムメッセージが毎秒生成されます。

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 }	<p>ダイナミック ARP インспекション 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 インспекションがイネーブルの場合、拒否またはドロップ ARP パケットがログされます。ログエントリ数は、32 です。システムメッセージの数は 1 秒あたり 5 つに制限されています。ロギングレート インターバルは、1 秒です。</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 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 に設定すると、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が生成されません。</p> <p>指定できる interval seconds の範囲は 0 ~ 86400 秒（1 日）です。値を 0 に設定すると、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になります）。</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 の設定は、相互に作用します。logs number X が interval seconds Y より大きい場合は、X を Y で割って (X/Y) 求められたシステムメッセージ数が 1 秒間に送信されます。それ以外の場合は、Y を X で割って (Y/X) 求められた間隔（秒）で 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 vlan-range logging {acl-match {matchlog none} dhcp-bindings {all none permit}}</code>	<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ドロップ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、ACE ロ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	<code>exit</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip arp inspection log</code>	設定値を確認します。
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спекション情報の表示

ダイナミック ARP インспек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спекション情報のコマンド

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に関して信頼状態と ARP パケットの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 のダイナミック ARP インспекションの設定および動作ステータスを表示します。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спек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спекション統計情報を消去する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спек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спек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спек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、スイッチは信頼されたダイナミック ARP インспекションポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

ダイナミック ARP インспек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спек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спекション ログ バッファを消去します。
show ip arp inspection log	ダイナミック ARP インспек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。