CHAPTER 20

ダイナミック ARP 検査の設定

この章では、2960 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、無効な ARP 要求および応答を同じ VLAN 内の他のポートにリレーしないことで、スイッチへの悪質な攻撃を回避します。

（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。

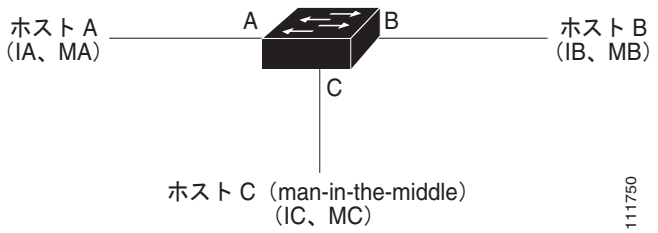
この章で説明する内容は、次のとおりです。

ダイナミック ARP 検査の概要

ARP は、IP アドレスを MAC アドレスにマッピングすることにより、レイヤ 2 ブロードキャスト ドメイン内で IP 通信を提供します。たとえば、ホスト B はホスト A に情報を送信したいが、ARP キャッシュにホスト 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 アドレスに対応付けられた 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 要求が受信されなかった場合も、ARP はホストからの gratuitous 応答を許可するため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生する可能性があります。攻撃のあと、攻撃を受けた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通過し、次にルータ、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たシステムの ARP キャッシュをポイズニングすることで、またサブネット上の他のホストに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たホスト、スイッチ、および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、および C は、インターフェイス A、B、および C 上のスイッチに接続されていて、すべてが同じサブネット上にあります。これらの IP および MAC アドレスをカッコ内に示します。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、IP レイヤでホスト B と通信する必要がある場合、IP アドレス IB に対応付けられた MAC アドレスを得るために 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 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 キャッシュに取り込みます（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 を持つホストのバインディングを ARP キャッシュに取り込みます。

ホスト C は、IP アドレス IA（または IB）と MAC アドレス MC が対応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、およびホスト 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 がトラフィックを代行受信することになります。ホスト C は IA および IB に対応付けられた真の 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こ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 ストリームに自身を割り込ませています。これは *man-in-the middle* 攻撃の典型的な例です。

ダイナミック ARP 検査は、ネットワーク内の ARP パケットを検証するセキュリティ機能です。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、ログに記録し、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 検査により、有効な ARP 要求と応答だけが確実にリレーされます。スイッチは次のアクティビティを実行します。

- untrusted 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、代行受信された各パケットに有効な IP/MAC アドレス バインディングが含まれていることを確認します。
- 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/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断します。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、このデータベースは DHCP スヌーピングによって構築されます。ARP パケットが trusted インターフェイスで受信された場合、スイッチはパケットをチェックなしで転送します。untrusted インターフェイスでは、スイッチは有効なパケットだけを転送します。

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.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）と照合して ARP パケットを検証できます。ARP ACL は、**arp access-list** *acl-name* グローバル コンフィギュレーション コマンドを使用して定義されます。設定情報については、「DHCP 以外の環境での 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グに記録します。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.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 ヘッダーに指定され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、「検証チェックの実行」（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

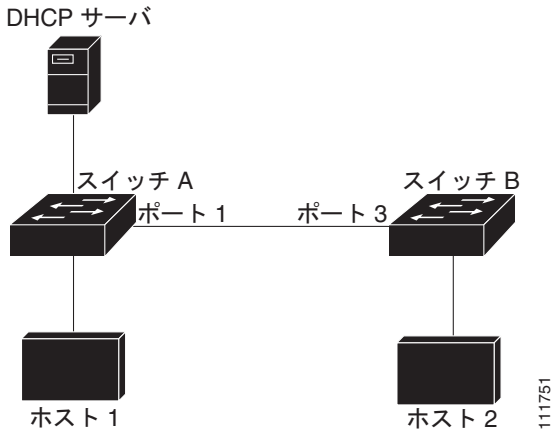
ダイナミック ARP 検査は、スイッチの各インターフェイスに信頼状態を関連付けます。trusted インターフェイスに着信するパケットは、ダイナミック ARP 検査の検証チェックをすべてバイパスしますが、untrusted インターフェイスに着信するパケットはダイナミック ARP 検査の検証を受けます。

一般的なネットワーク設定では、ホスト ポートに接続されたすべてのスイッチ ポートを untrusted に設定し、スイッチに接続されたすべてのスイッチ ポートを trusted に設定します。この設定では、指定したスイッチからネットワークに入るすべての ARP パケットがセキュリティ チェックをバイパスします。VLAN またはネットワーク内の他の場所で他の検証を行う必要はありません。**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、信頼設定を設定できます。

注意　信頼状態設定は慎重に使用してください。インターフェイスが信頼される必要がある場合に untrusted 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 とホスト 2 を含む VLAN 上でダイナミック ARP 検査を実行していると仮定します。ホスト 1 とホスト 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 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 とホスト 2 の間の接続は切断されます。

図 20-2　ダイナミック ARP 検査がイネーブルに設定された VLAN での ARP パケット検証



インターフェイスが実際には信頼できない場合に trusted として設定すると、ネットワークにセキュリティ ホールが残ります。スイッチ A がダイナミック ARP 検査を実行していない場合、ホスト 1 は容易にスイッチ B（スイッチの間のリンクが trusted 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。この状態は、スイッチ B がダイナミック ARP 検査を実行している場合でも発生します。

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された（untrusted 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にあるホストが、ダイナミック ARP 検査を実行す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ことは防止できません。

VLAN 内のスイッチの中に、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は、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は、ダイナミック ARP 検査を実行するスイッチを、ダイナミック ARP 検査を実行しないスイッチから分離します。設定情報については、「DHCP 以外の環境での 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設定によっては、VLAN 内のすべてのスイッチ上で特定の ARP パケットの検証を実行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 検査の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。デフォルトでは、untrusted インターフェイスのレートは 15 パケット/秒（pps）です。trusted 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。ユーザが介入するまで、ポートはこのステートのままです。**errdisable recovery** グローバル コンフィギュレーション コマンドを使用すれば、指定されたタイムアウト時間の経過後、ポートがこのステートから自動的に抜け出せるように errdisable 回復をイネーブルにできます。

設定情報については、「着信 ARP パケットのレート制限」（P.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 を設定する場合に限り、ACL を使用します。スイッチは最初に ARP パケットとユーザ設定の ARP ACL を比較します。ARP ACL が ARP パケットを拒否した場合、DHCP スヌーピングによって入力されたデータベースに有効なバインディングが存在したとしても、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

スイッチはパケットを廃棄する際に、ログ バッファにエントリを格納してから、レート制御ベースでシステム 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、および指定されたインターバルでのシステム メッセージ生成に必要な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 コマンドを使用して、ロギングされるパケットのタイプを指定します。設定情報については、「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、次の設定情報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

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	すべての VLAN でディセーブル
インターフェイス信頼状態	すべてのインターフェイスで untrusted
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と仮定した場合、レートは untrusted インターフェイスで 15 pps です。 すべての trusted 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 インターバルは 1 秒です。
DHCP 以外の環境の 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。

表 20-1　ダイナミック ARP 検査のデフォルト設定 （続き）

機能	デフォルト設定
ログ バッファ	ダイナミック ARP 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 パケットがログに記録されます。 ログのエントリ数は 32 です。 システム メッセージ数は 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 単位のロギング	拒否または廃棄されたすべての ARP パケットがログに記録されます。

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を次に示します。

- ダイナミック ARP 検査は入力セキュリティ機能であり、出力チェックは行いません。
- ダイナミック ARP 検査は、ダイナミック ARP 検査をサポートしないスイッチ、またはこの機能がイネーブルでないスイッチに接続されたホストに対しては効果がありません。man-in-the-middle 攻撃は単一のレイヤ 2 ブロードキャスト ドメインに限定されるため、ダイナミック ARP 検査チェックが行われるドメインとチェックなしのドメインを分離します。これにより、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。
- ダイナミック ARP 検査は、着信 ARP 要求および ARP 応答の IP/MAC アドレス バインディングを確認する 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ます。必ず DHCP スヌーピングをイネーブルにして、IP アドレスが動的に割り当てられた ARP パケットを許可してください。設定の詳細については、第 19 章「DHCP 機能および IP 送信元ガードの設定」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 DHCP 以外の環境では、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。

（注） RSPAN VLAN 上でダイナミック ARP 検査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 検査をイネーブルにすると、ダイナミック ARP 検査パケットが RSPAN 宛先ポートに到達しない場合があります。

- 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 チャネル内でサスペンドのままになります。ポート チャネルは、チャネルに加入する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チャ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に新しい信頼状態を設定します。

- 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での累積となります。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すべての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、すべてのチャネル メンバーからのパケットの着信レートの合計に等しくなります。チャネル ポート メンバーでの着信 ARP パケットのレートを調べてから、EtherChannel ポートのレート制限を設定するようにしてください。

  物理ポートの着信パケットのレートは、物理ポート設定ではなく、ポート チャネル設定と照合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、物理ポートの設定と無関係です。

  EtherChannel が設定されたレートよりも多くの ARP パケットを受信した場合、（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、ダイナミック ARP 検査に対応する複数の VLAN 全体でパケットを処理するには、より高いレートでトランク ポートを設定します。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することもできます。ある VLAN でレート制限が高いと、ソフトウェアがポートを errdisable ステートにしたときに、別の VLAN が DoS 攻撃を受けることがあります。

- スイッチでダイナミック ARP 検査をイネーブルにすると、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、すべての 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 検査の設定

この手順では、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。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.20-3）を参照）。両方のスイッチは、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 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、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する 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ます。必ず DHCP スヌーピングをイネーブルにして、IP アドレスが動的に割り当てられた ARP パケットを許可してください。設定の詳細については、第 19 章「DHCP 機能および IP 送信元ガードの設定」を参照してください。

1 つのスイッチだけがこの機能をサポートする場合にダイナミック ARP 検査を設定する方法については、「DHCP 以外の環境での 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、特権 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行う必要があります。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。

	コマンド	目的
ステップ 3	**ip arp inspection *vlan*** *vlan-range*	ダイナミック ARP 検査を VLAN 単位でイネーブルにします。デフォルトでは、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。 *vlan-range* には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、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。 両方のスイッチに同じ VLAN ID を指定します。
ステップ 4	**interface** *interface-id*	他のスイッチに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip arp inspection trust**	スイッチ間の接続を 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、trusted 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。単にパケットを転送するだけです。 untrusted インターフェイスの場合、スイッチはすべての ARP 要求と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、スイッチは代行受信されたパケットに有効な IP/MAC アドレス バインディングが含まれていることを確認します。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 コマンドで指定されたロギング設定にしたがって、無効なパケットを廃棄し、それらをログ 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.20-14）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** *vlan-range*	ダイナミック ARP 検査設定を確認します。
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** *vlan-range*	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	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ダイナミック ARP 検査をディセーブルにするには、**no ip arp inspection vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。インターフェイスを untrusted ステートに戻すには、**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、VLAN 1 のスイッチ A でダイナミック ARP 検査を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 gigabitethernet0/1
Switch(config-if)# ip arp inspection trust
```

DHCP 以外の環境での ARP ACL の設定

この手順では、図 20-2（P.20-3）に示すスイッチ 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について説明します。

スイッチ A のポート 1 を trusted に設定した場合、スイッチ A とホスト 1 の両方がスイッチ 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 ホールが作成されます。この可能性を防ぐには、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 アドレスがスタティックでない（スイッチ A の ACL 設定を適用できない）場合、レイヤ 3 でスイッチ A とスイッチ 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 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 DHCP 以外の環境で必須です。

	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 リストの末尾には、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* には、ホスト 2 の IP アドレスを入力します。 • *sender-mac* には、ホスト 2 の MAC アドレスを入力します。 • （任意）ログ バッファのパケットが Access Control Entry（ACE; アクセス コントロール エントリ）と一致した場合にそのパケットをログに記録するには、**log** を指定します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで **matchlog** キーワードを設定した場合にも、一致がログに記録されます。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。
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 を VLAN に適用します。デフォルトでは、定義された ARP ACL は VLAN に適用されません。 • *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ある VLAN を指定します。VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、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 内の暗黙の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、**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明示的な拒否が ACL にないことを意味します。また、パケットが ACL 内のどの句とも一致しない場合は 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/MAC アドレス 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。アクセス リストで許可された場合に限り、パケットは許可されます。
ステップ 6	**interface** *interface-id*	スイッチ B に接続されたスイッチ A インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**no ip arp inspection trust**	スイッチ B に接続されたスイッチ A インターフェイスを 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。 untrusted インターフェイスの場合、スイッチはすべての ARP 要求と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、スイッチは代行受信されたパケットに有効な IP/MAC アドレス バインディングが含まれていることを確認します。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 コマンドで指定されたロギング設定にしたがって、無効なパケットを廃棄し、それらをログ 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.20-14）を参照してください。
ステップ 8	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	**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 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ARP ACL を削除するには、**no arp access-list** グローバル コンフィギュレーション コマンドを使用します。VLAN に付加された ARP ACL を削除するには、**no ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチ A で ARP ACL（*host2*）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 のポート 1 を untrusted 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 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 検査の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超えた場合、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時間の経過後、ポートがこのステートから自動的に抜け出すように errdisable 回復をイネーブルにするまで、ポートは 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。レート制限を設定すると、信頼状態が変更されてもインターフェイスは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 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、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*	レートを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。

	コマンド	目的
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 要求と応答のレートを制限します。 デフォルトのレートは、untrusted インターフェイスでは 15 pps、trusted インターフェイスでは無制限です。バースト インターバルは 1 秒です。 キーワードの意味は次のとおりです。 • **rate** *pps* には、1 秒あたりに処理される着信パケット数の上限を指定します。指定できる範囲は 0 ～ 2048 pps です。 • （任意）**burst interval** *seconds* には、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連続したインターバルを秒単位で指定します。指定できる範囲は 1 ～ 15 です。 • **rate none** には、処理できる着信 ARP パケットのレートの上限を指定します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**errdisable recovery cause arp-inspection interval** *interval*	（任意）ダイナミック ARP 検査の errdisable ステートからのエラー回復をイネーブルにします。 デフォルトでは、回復はディセーブルで、回復インターバルは 300 秒です。 **interval** *interval* には、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 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。

検証チェックの実行

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、ログに記録し、廃棄します。宛先 MAC アドレス、送信側およびターゲット IP アドレス、送信元 MAC アドレスで追加チェックを実行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行するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	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。デフォルトでは、チェックは実行されません。 キーワードの意味は次のとおりです。 • **src-mac** では、イーサネット ヘッダーの送信元 MAC アドレスを、ARP 本体の送信側 MAC アドレスと照合します。このチェックは ARP 要求と応答の両方で実行されます。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、廃棄されます。 • **dst-mac** では、イーサネット ヘッダーの宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと照合します。このチェックは ARP 応答で実行されます。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、廃棄されます。 • **ip** では、ARP 本体をチェックして無効な予期しない IP アドレスが存在するかどうか調べます。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。送信側 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 応答でだけチェックされます。 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。つまり、あるコマンドが **src** および **dst mac** 検証をイネーブルにし、2 番めのコマンドが IP 検証だけをイネーブルにした場合、**src** および **dst mac** 検証は 2 番めのコマンドを受けて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、廃棄、MAC 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

スイッチはパケットを廃棄する際に、ログ バッファにエントリを格納してから、レート制御ベースでシステム 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 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 VLAN 上で同じ ARP パラメータを持つ多数のパケットを受信した場合、スイッチはこれらのパケットをログ バッファの 1 つのエントリとして結合し、このエントリに単一のシステム 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、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、**show ip arp inspection log** 特権 EXEC コマンドの表示に影響があります。パケット カウントと時間以外のすべてのデータの代わりに、-- が画面上に表示されます。他の統計情報はエントリに提供されません。このエントリが画面に表示された場合は、ログ バッファのエントリ数を増やすか、ロギング レートを高くしてください。

ログ バッファを設定するには、特権 EXEC モードで次の手順を実行します。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 log-buffer** {**entries** *number* | **logs** *number* **interval** *seconds*}	ダイナミック ARP 検査のログ バッファを設定します。 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 ARP パケットはログに記録されます。ログのエントリ数は 32 です。システム メッセージ数は 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。 キーワードの意味は次のとおりです。 • **entries** *number* には、バッファ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* には、指定したインターバルでシステム メッセージを生成するエントリ数を指定します。 **logs** *number* に指定できる範囲は、0 ～ 1024 です。0 の値は、ログ バッファにエントリは存在しますが、システム メッセージは生成されないことを意味します。 **interval** *seconds* では、指定できる範囲は 0 ～ 86400 秒（1 日）です。0 の値は、システム メッセージがただちに生成されること（およびログ バッファが常に空であること）を意味します。 インターバル設定の 0 は、ログ設定の 0 よりも優先されます。 **logs** および **interval** 設定は相互に作用します。**logs** *number* X が **interval** *seconds* Y よりも大きい場合、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。そうでない場合は、Y を X で除算した（Y/X）秒ごとに 1 つのシステム メッセージが送信されます。

	コマンド	目的
ステップ 3	**ip arp inspection vlan** *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	ログに記録されるパケットのタイプを VLAN 単位で制御します。デフォルトでは、拒否または廃棄されたすべてのパケットが記録されます。*logged* という用語は、エントリがログ バッファに存在し、システム メッセージが生成されてい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* には、VLAN ID で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、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。 • **acl-match matchlog** では、ACE ロギング設定に基づいて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すべてのパケットを記録します。 • **dhcp-bindings none** では、DHCP バインディングと一致するパケットを記録しません。 • **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 バッファを消去するには、**clear ip arp inspection log** 特権 EXEC コマンドを使用します。

ダイナミック ARP 検査情報の表示

ダイナミック ARP 検査情報を表示するには、表 20-2 に記載された特権 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
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*]	指定したインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。
show ip arp inspection vlan *vlan-range*	指定した VLAN のダイナミック ARP 検査の設定および動作状態を表示します。VLAN が指定されない場合、または範囲が指定された場合は、ダイナミック ARP 検査がイネーブル（アクティブ）である VLAN の情報だけを表示します。

ダイナミック ARP 検査統計情報を消去または表示するには、表 20-3 に記載された特権 EXEC コマンドを使用します。

表 20-3　ダイナミック ARP 検査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 検査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、廃棄、MAC 検証失敗、IP 検証失敗、ACL 許可および拒否、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 が指定されない場合、または範囲が指定された場合は、ダイナミック ARP 検査がイネーブル（アクティブ）である VLAN の情報だけを表示します。

show ip arp inspection statistics コマンドでは、スイッチは信頼性のあるダイナミック ARP 検査ポート上の各 ARP 要求および応答パケットに対して、転送パケットの数を増やします。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に対して、ACL または DHCP 許可パケットの数を増やし、また適切な失敗カウントを増やします。

ダイナミック ARP 検査ロギング情報を消去または表示するには、表 20-4 に記載された特権 EXEC コマンドを使用します。

表 20-4　ダイナミック ARP 検査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 検査のログ バッファを消去します。
show ip arp inspection log	ダイナミック ARP 検査ログ バッファの設定および内容を表示します。

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。