



## CHAPTER 23

# Dynamic ARP Inspection の設定

この章では、Catalyst 3750 スイッチにダイナミック 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 (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。特に明記しない限り、スイッチという用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。



(注)

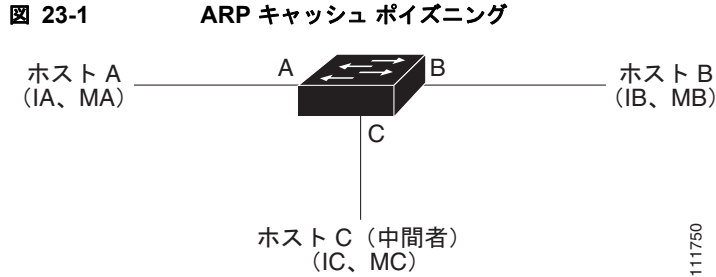
この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

- 「[ダイナミック ARP インспекションの概要](#)」 (P.23-1)
- 「[Dynamic ARP Inspection 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.23-16)

## 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 通信を実現します。たとえば、ホスト B はホスト A に情報を送信する必要がありますが、ARP キャッシュにホスト A の MAC アドレスを持っていないとします。ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャスト ドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロードキャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。しかし、ARP は、ARP 要求を受信されなかった場合でも、ホストからの余分な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ことがあります。攻撃が開始されると、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経由してルータ、スイッチ、またはホストに送信されるようになります。

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、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、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、およびルータを攻撃することができます。図 23-1 に、ARP キャッシュ ポイズニングの例を示します。



ホスト A、B、および C は、インターフェイス A、B、および C 上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。カッコ内に示されているのは、これらの IP アドレス、および MAC アドレスです。たとえば、ホスト A が使用する IP アドレスは IA、MAC アドレスは MA です。ホスト A が IP レイヤにあるホスト B と通信する必要がある場合、ホスト A は IP アドレス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。スイッチとホスト B は、この ARP 要求を受信すると、IP アドレスが IA で、MAC アドレスが MA のホストに対する ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は、MAC アドレス MA にバインドされています。ホスト B が応答すると、スイッチ、およびホスト A は、IP アドレスが IB で、MAC アドレスが MB のホストに対するバインディングを ARP に読み込みます。

ホスト C は、IP アドレスが IA (または IB) で、MAC アドレスが MC のホストに対する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により、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することができます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、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 がこの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 に関連付けられた本物の 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ます。おなじみの *中間者攻撃* です。

ダイナミック ARP インспекションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。この機能により、ネットワークをある種の中間者攻撃から保護することができます。

ダイナミック ARP インспекションにより、有効な ARP 要求と応答だけが確実にリレーされるようになります。スイッチが実行する機能は次のとおりです。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

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 データベースに格納されている有効な IP/MAC アドレス バインディングに基づいて、ARP パケットの正当性を判断します。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピングにより構築されます。信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、この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、スイッチはこのパケットが有効である場合だけ、この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 ごとにダイナミック ARP インспекションをイネーブルにすることができます。設定の詳細については、「[DHCP 環境でのダイナミック ARP インспекションの設定](#)」(P.23-8) 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、静的に設定された IP アドレスを持つホストに対するユーザ設定の ARP アクセス コントロール リスト (ACL) と照らし合わせて、ARP パケットの正当性を確認することができます。ARP ACL を定義するには、**arp access-list acl-name** グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「[非 DHCP 環境での ARP ACL の設定](#)」(P.23-10) 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ログに記録します。ログ バッファの詳細については、「[廃棄パケットのロギング](#)」(P.23-5) を参照してください。

パケットの IP アドレスが無効である場合、または ARP パケットの本文にある MAC アドレスが、イーサネット ヘッダーで指定されたアドレスと一致しない場合、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ションを設定することができます。このためには、**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、「[確認検査の実行](#)」(P.23-13) 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 インспекションは、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。信頼できるインターフェイスに到着するパケットは、ダイナミック ARP インспекションの確認検査をすべてバイパスし、信頼できないインターフェイスに到着するパケットには、ダイナミック ARP インспекションの検証プロセスを受けます。

一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチ ポートすべてを信頼できるものに設定します。この構成では、指定されたスイッチからネットワークに入ってくる ARP パケットはすべて、セキュリティ チェックをバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、**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。

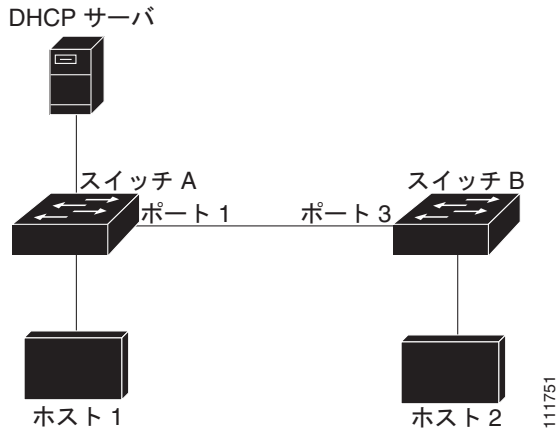


### 注意

信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

[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 でダイナミック ARP インспекションを実行しているとします。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 アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。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 によりドロップされます。こうして、ホスト 1 とホスト 2 の間の接続が失われます。

図 23-2 ダイナミック ARP インспекションのためにイネーブルにされた VLAN 上の ARP パケット検証



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、ネットワーク内にセキュリティホールが生じます。スイッチ A でダイナミック ARP インспекションが実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの間のリンクが信頼できるものとして設定されている場合はホスト 2）。この状況は、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る場合でも発生します。

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された（信頼できないインターフェイス上の）ホストが、そのネットワークにあるその他のホストの ARP キャッシュをポイズニングしていないことを保証します。しかし、ダイナミック ARP インспекションにより、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 インспекションを実行しているスイッチに接続されているホストのキャッシュをポイズニングできないようにすることはできません。

VLAN のスイッチの一部がダイナミック ARP インспекションを実行し、残りのスイッチは実行していない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定します。ただし、非ダイナミック ARP インспекションスイッチから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ションを実行するスイッチを設定します。このようなバインディングが判断できない場合は、レイヤ 3 で、ダイナミック ARP インспекションスイッチを実行していないスイッチから、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分離します。設定の詳細については、「非 DHCP 環境での ARP ACL の設定」(P.23-10) を参照してください。



(注) DHCP サーバとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

## 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ション確認検査を実行します。したがって、DoS 攻撃を阻止するために、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。この設定を変更するには、`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。

着信 ARP パケットのレートが設定された制限を超えると、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、ポートはこの状態を維持します。`errdisable recovery` グローバル コンフィギュレーション コマンドを使用すると、`errdisable` ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。



(注)

EtherChannel のレート制限は、スタックにある各スイッチに個別に適用されます。たとえば、EtherChannel で 20 pps の制限が設定されている場合、EtherChannel にあるポートの各スイッチでは、最大 20 pps まで実行できます。スイッチが制限を超過した場合、EtherChannel 全体が `errdisable` ステートになります。

設定の詳細については、「[着信 ARP パケットのレート制限](#)」(P.23-12) を参照してください。

## ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インスペクションでは、有効な IP/MAC アドレス バインディングのリストとして、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。

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、ARP ACL の方が優先されます。スイッチが ACL を使用するのには、ACL が `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作成されている場合だけです。スイッチは、まず、ARP パケットをユーザ設定の ARP ACL と比較します。DHCP スヌーピングによりデータが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ていても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

## 廃棄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と、ログ バッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。各ログ エントリには、受信側の 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 アドレスといったフロー情報が記録されます。

`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や、システム メッセージ生成までの指定のインターバルに必要とされるエントリ数を設定します。記録されるパケットの種類を指定するには、`ip arp inspection vlan logging` グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「[ログ バッファの設定](#)」(P.23-14) を参照してください。

## Dynamic ARP Inspection の設定

- 「[ダイナミック ARP インスペクションのデフォルト設定](#)」(P.23-6)
- 「[ダイナミック ARP インスペクション設定時の注意事項](#)」(P.23-6)
- 「[DHCP 環境でのダイナミック ARP インスペクションの設定](#)」(P.23-8) (DHCP 環境では必須)
- 「[非 DHCP 環境での ARP ACL の設定](#)」(P.23-10) (非 DHCP 環境では必須)
- 「[着信 ARP パケットのレート制限](#)」(P.23-12) (任意)
- 「[確認検査の実行](#)」(P.23-13) (任意)

- 「ログ バッファの設定」(P.23-14) (任意)

## ダイナミック ARP インспекションのデフォルト設定

表 23-1 に、ダイナミック ARP インспекションのデフォルト設定を示します。

表 23-1 ダイナミック ARP インспекションのデフォルト設定

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。
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 untrusted。
着信 ARP パケットのレート制限	1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチド ネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。  信頼できるすべてのインターフェイスでは、レート制限は行われません。  バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。
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化されると、拒否またはドロップされた ARP パケットはすべてが記録されます。  ログ内のエントリ数は 32 です。  システム メッセージ数は、毎秒 5 つに制限されます。  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 パケットが記録されます。

## ダイナミック ARP インспекション設定時の注意事項

ダイナミック ARP インспекション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ションは入力セキュリティ機能です。出力チェックはまったく行いません。
- 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、またはこの機能がイネーブルにされていないスイッチに接続されるホストに対しては有効ではありません。中間者攻撃は単一のレイヤ 2 ブロードキャスト ドメインに制限されているため、チェックされないドメインと、ダイナミック ARP インспекションによりチェックされるドメインは区別します。このアクションは、ダイナミック ARP インспекションのためにイネーブルにされているドメインでホストの ARP キャッシュを保護します。
- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インспекション 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依存します。IP アドレスを動的に割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。コンフィギュレーションについては、第 22 章「DHCP および IP ソース ガード機能の設定」を参照してください。

DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可または拒否を行います。

- 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 ポート上でサポートされています。



(注) RSPAN VLAN では、ダイナミック ARP インспекションをイネーブルにしないでください。RSPAN VLAN でダイナミック ARP インспекションをイネーブルにすると、ダイナミック ARP インспекション パケットが RSPAN 宛先ポートに届かない可能性があります。

- 物理ポートを EtherChannel ポート チャンネルに結合するには、この物理ポートとチャンネル ポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポート チャンネル内で中断状態のままとなります。ポート チャンネルは、チャンネルと結合された最初の物理ポートの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、チャンネルの信頼状態と一致する必要はありません。

逆に、ポート チャンネルで信頼状態を変更すると、スイッチは、チャンネルを構成するすべての物理ポート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別々に算出されます。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高い可能性があることを意味します。たとえば、レート制限が 30 pps に設定された EtherChannel で、スイッチ 1 に 1 つのポート、およびスイッチ 2 に 1 つのポートがある場合、EtherChannel が errdisable 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による累積値です。たとえば、ポート チャンネルの ARP レート制限を 400 pps に設定すると、このチャンネルに結合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。EtherChannel ポートのレート制限は、各チャンネル ポート メンバが受信する ARP パケットのレートを確認してから設定してください。

物理ポートで受信される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照合して検査されます。ポート チャンネル上のレート制限設定は、物理ポートの設定に依存しません。

EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャンネル（すべての物理ポートを含む）は errdisable ステートとなります。

- 着信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートの集約を反映し、複数のダイナミック ARP インспекションがイネーブルにされた VLAN にわたってパケットを処理するために、トランク ポートのレートをより高く設定します。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、レートを無制限に設定することもできます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。
- スイッチで、ダイナミック ARP インспекション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ように設定されたポリサーの有効性は失われます。この結果、すべての ARP トラフィックは CPU に送信されます。
- ダイナミック ARP インспекション スマート ロギングを設定する場合、ログ バッファ内にあるすべてのパケット（デフォルトでは、ドロップされたすべてのパケット）の内容が NetFlow 収集装置に送信されます。この機能を設定する場合は、スマート ロギングがグローバルにイネーブルになっていることを確認してください。スマート ロギングの詳細については、「[スマート ロギングの設定](#)」(P.31-14) を参照してください。

## DHCP 環境でのダイナミック ARP インспекションの設定

この手順では、2つのスイッチがダイナミック ARP インспекションをサポートしているときに、この機能を設定する方法を示します。図 23-2 (P.23-4) に示すとおり、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。スイッチは両方とも、ホストの配置されている 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 に接続されています。両方のホストは、同一の 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 はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。



(注)

着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インспекション 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依存します。IP アドレスを動的に割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。コンフィギュレーションについては、第 22 章「DHCP および IP ソース ガード機能の設定」を参照してください。

スイッチの 1 つだけ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の詳細については、「非 DHCP 環境での ARP ACL の設定」(P.23-10) 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実行します。この処理は、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	<b>show cdp neighbors</b>	スイッチ間の接続を確認します。
ステップ 2	<b>configure terminal</b>	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	<b>ip arp inspection vlan <i>vlan-range</i></b>	VLAN 単位で、ダイナミック ARP インспекションをイネーブルにします。デフォルトでは、すべての VLAN 上でダイナミック ARP インспекションはディセーブルになっています。  <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	<b>ip arp inspection smartlog</b>	(任意) 現在ロギングされているどのパケットもスマート ロギングされることを指定します。デフォルトでは、ドロップされたすべてのパケットが記録されます。
ステップ 5	<b>interface <i>interface-id</i></b>	もう 1 つのスイッチに接続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 6	<b>ip arp inspection trust</b>	スイッチ間の接続を、信頼できるものに設定します。  デフォルトでは、すべてのインターフェイスは信頼できません。スイッチは、信頼できるインターフェイスにあるもう 1 つのスイッチから受信した ARP パケットは確認しません。この場合、パケットはそのまま転送されます。  信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、 <b>ip arp inspection vlan logging</b> 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、「 <a href="#">ログ バッファの設定</a> 」(P.23-14) を参照してください。
ステップ 7	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show ip arp inspection interfaces</b> <b>show ip arp inspection vlan <i>vlan-range</i></b>	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 9	<b>show ip dhcp snooping binding</b>	DHCP バインディングを確認します。
ステップ 10	<b>show ip arp inspection statistics vlan <i>vlan-range</i></b>	ダイナミック ARP インспекション統計情報を確認します。
ステップ 11	<b>copy running-config startup-config</b>	(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。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。

次の例では、VLAN 1 のスイッチ A でダイナミック ARP インспекションを設定する方法を示します。スイッチ B でも同様の手順を実行します。

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip arp inspection trust
```

## 非 DHCP 環境での ARP ACL の設定

この手順は、[図 23-2 \(P.23-4\)](#) に示すスイッチ 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ときにダイナミック 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 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、スイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが作り出されます。これを阻止するには、スイッチ A のポート 1 を信頼できないもの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はない（スイッチ A で ACL 設定を適用することは不可能である）場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを使用してパケットをルートする必要があります。

スイッチ A 上で ARP ACL を設定するには、特権 EXEC モードで次の手順を実行します。この手順は、非 DHCP 環境では必須です。

	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 <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 リストは定義されません。  (注) ARP アクセス リストの末尾に暗黙的な <code>deny ip any mac any</code> コマンドが指定されています。
ステップ 3	<code>permit ip host <i>sender-ip</i> mac host <i>sender-mac</i> [log]</code>	指定されたホスト（ホスト 2）からの ARP パケットを許可します。  <ul style="list-style-type: none"> <li>• <i>sender-ip</i> には、ホスト 2 の IP アドレスを入力します。</li> <li>• <i>sender-mac</i> には、ホスト 2 の MAC アドレスを入力します。</li> <li>• (任意) パケットが Access Control Entry (ACE; アクセスコントロール エントリ) と一致するときに、ログ バッファにこのパケットをログするには、<code>log</code> を指定します。</li> </ul> <b>ip arp inspection vlan logging</b> グローバル コンフィギュレーション コマンドで <code>matchlog</code> キーワードを設定している場合も、一致したパケットがログ記録されます。詳細については、「 <a href="#">ログ バッファの設定</a> 」(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
<b>ステップ5</b> <code>ip arp inspection filter <i>arp-acl-name</i> vlan <i>vlan-range</i> [static]</code>	<p>ARP ACL を VLAN に適用します。デフォルトでは、定義済みの ARP ACL は、どのような VLAN にも適用されません。</p> <ul style="list-style-type: none"> <li>• <i>arp-acl-name</i> には、ステップ 2 で作成した ACL の名前を指定します。</li> <li>• <i>vlan-range</i> には、スイッチとホストが存在する VLAN を指定します。VLAN ID 番号で識別された 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。</li> <li>• (任意) <b>static</b> を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットは廃棄されます。DHCP バインディングは使用されません。</li> </ul> <p>このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。</p> <p>IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。パケットは、アクセスリストで許可された場合だけに許可されます。</p>
<b>ステップ6</b> <code>ip arp inspection smartlog</code>	<p>現在ロギングされているどのパケットもスマート ロギングされることを指定します。デフォルトでは、ドロップされたすべてのパケットが記録されます。</p>
<b>ステップ7</b> <code>interface <i>interface-id</i></code>	<p>スイッチ B に接続するスイッチ 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>
<b>ステップ8</b> <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ものとして設定します。</p> <p>デフォルトでは、すべてのインターフェイスは信頼できません。</p> <p>信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスとの有効なバインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、<b>ip arp inspection vlan logging</b> 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、「<a href="#">ログ バッファの設定</a>」(P.23-14) を参照してください。</p>
<b>ステップ9</b> <code>end</code>	<p>特権 EXEC モードに戻ります。</p>

	コマンド	目的
ステップ 10	<pre>show arp access-list [acl-name] show ip arp inspection vlan vlan-range show ip arp inspection interfaces</pre>	設定を確認します。
ステップ 11	<pre>copy running-config startup-config</pre>	(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 に接続された 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* を設定して、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、この ACL を VLAN 1 に適用してから、スイッチ A のポート 1 を信頼できないもの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ション確認検査を実行します。したがって、DoS 攻撃を阻止するために、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された制限を超えると、スイッチはポートを **errdisable** ステートにします。**errdisable** 回復をイネーブルにして、指定されたタイムアウト時間の後にポートがこのステートから自動的に抜け出すようになるまで、ポートはこのステートのままです。



(注)

インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、レート制限をその信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**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 ポートに対するレート制限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	<pre>configure terminal</pre>	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	<pre>interface interface-id</pre>	レート制限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。

	コマンド	目的
ステップ 3	<code>ip arp inspection limit {rate pps [burst interval seconds]   none}</code>	<p>インターフェイスでの着信 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 レートは、信頼できないインターフェイスでは 15 pps、信頼できる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。</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"> <li>• <b>rate pps</b> 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。有効な範囲は 0 ~ 2048 pps です。</li> <li>• (任意) <b>burst interval seconds</b> は、レートの高い ARP パケットの有無についてインターフェイスがモニタリングされる間隔 (秒) を指定します。指定できる範囲は 1 ~ 15 です。</li> <li>• <b>rate none</b> では、処理できる着信 ARP パケットのレートの上限を設定しません。</li> </ul>
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 インспекション <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>デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。</p> <p><b>interval interval</b> には、<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>	特権 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るには、`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。

## 確認検査の実行

ダイナミック ARP インспекションは、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。宛先 MAC アドレス、送信側および宛先の IP アドレス、および送信元 MAC アドレスで追加検証を実行するように、スイッチを設定できます。

着信 ARP パケットで特定の検証を実行するには、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	<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 パケットに対して特定の検証を実行します。デフォルトでは、検証は実行されません。</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"> <li>• <b>src-mac</b> では、イーサネット ヘッダーの送信元 MAC アドレスと ARP 本文の送信元 MAC アドレスが比較されます。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。</li> <li>• <b>dst-mac</b> では、イーサネット ヘッダーの宛先 MAC アドレスと ARP 本文の宛先 MAC アドレスが比較されます。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。</li> <li>• <b>ip</b> では、ARP 本文から、無効な IP アドレスや予期しない IP アドレスがないかを確認します。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。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。</li> </ul> <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。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが <b>src</b> および <b>dst mac</b> の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番目のコマンドによって <b>src</b> および <b>dst mac</b> の検証が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。

検証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。転送されたパケット、ドロップされたパケット、MAC および IP 検証に失敗したパケットの統計を表示するには、`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と、ログ バッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。各ログ エントリには、受信側の 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 アドレスといったフロー情報が記録されます。

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 ARP パラメータを使用して同じ VLAN 上で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組み合わせて 1 つのエントリとしてログ バッファに格納し、エントリとして 1 つのシステム メッセージを生成します。

ログバッファでオーバーフローが生じた場合は、1つのログイベントがログバッファ内に収まらなかったことを意味し、**show ip arp inspection log** 特権 EXEC コマンドによる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。このエントリに対しては、その他の統計情報は表示されません。出力にこのようなエントリが表示される場合、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。

ロギングバッファ コンフィギュレーションは、スイッチスタックの各スタックメンバに適用されます。各スタックメンバでは、**logs number** が指定されていて、設定されたレートでシステムメッセージを生成します。たとえば、インターバル（レート）が1秒ごとに1エントリの場合、5つのメンバスイッチスタックで、1秒ごとに最大5つまでのシステムメッセージが生成されます。

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 <b>configure terminal</b>	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 <b>ip arp inspection log-buffer {entries number   logs number interval seconds}</b>	<p>ダイナミック ARP インспекション ロ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 インспекションがイネーブル化されると、拒否またはドロップされた ARP パケットが記録されます。ログエントリ数は、32 です。システムメッセージ数は、毎秒5つに制限されます。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"> <li>• <b>entries number</b> は、バッファに記録されるエントリ数を表します。指定できる範囲は 0 ~ 1024 です</li> <li>• <b>logs number interval seconds</b> は、指定され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の数を表します。</li> </ul> <p><b>logs number</b> に指定できる範囲は 0 ~ 1024 です。0 は、エントリはログバッファ内に入力されますが、システムメッセージが生成されないことを意味します。</p> <p>指定できる <b>interval seconds</b> の範囲は 0 ~ 86400 秒 (1日) です。0 は、システムメッセージがただちに生成されることを意味します。この場合、ログバッファは常に空となります。</p> <p>インターバル値を 0 に設定すると、ログ値 0 は上書きされます。</p> <p><b>logs</b> および <b>interval</b> の設定は、相互に作用します。<b>logs number X</b> が <b>interval seconds Y</b> より大きい場合、X 割る Y (X/Y) 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 割る X (Y/X) 秒ごとに送信されます。</p>

## ■ ダイナミック ARP インспекション情報の表示

	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 単位で記録するパケットのタイプを制御します。デフォルトでは、拒否またはドロップされたパケットは、すべて記録されます。ログに記録されるという表現は、エントリがログ バッファに格納され、システム メッセージが生成されることを意味しています。</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"> <li>• <b>vlan-range</b> 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。</li> <li>• <b>acl-match matchlog</b> は、ACE ログ設定に基づいてパケットをログに記録します。このコマンドに <b>matchlog</b> キーワードを指定して、さらに <b>permit</b> または <b>deny</b> ARP アクセス リスト コンフィギュレーション コマンドに <b>log</b> キーワードを指定すると、ACL によって許可または拒否された ARP パケットが記録されます。</li> <li>• <b>acl-match none</b> では、ACL に一致するパケットは記録されません。</li> <li>• <b>dhcp-bindings all</b> では、DHCP バインディングに一致するパケットがすべて記録されます。</li> <li>• <b>dhcp-bindings none</b> では、DHCP バインディングに一致するパケットは記録されません。</li> <li>• <b>dhcp-bindings permit</b> では、DHCP バインディングが許可されたパケットが記録されます。</li> </ul>
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 バッファ設定に戻るには、`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 ログ設定に戻るには、`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 に記載された特権 EXEC コマンドを使用します。

表 23-2 ダイナミック ARP インспекション情報を表示するためのコマンド

コマンド	説明
<code>show arp access-list [<i>acl-name</i>]</code>	ARP ACL についての詳細情報を表示します。
<code>show ip arp inspection interfaces [<i>interface-id</i>]</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 <i>vlan-range</i></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 が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インспекションがイーネーブルにされた (アクティブ) VLAN だけの情報を表示します。



ダイナミック ARP インスペクションの統計をクリア、または表示するには、表 23-3 に記載された特権 EXEC コマンドを使用します。

表 23-3 ダイナミック ARP インスペクション統計をクリアまたは表示するためのコマンド

コマンド	説明
<code>clear ip arp inspection statistics</code>	ダイナミック ARP インスペクション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 において、転送されたパケット、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 によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インスペクションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。

`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 インスペクション ポート上の各 ARP 要求および応答パケットの転送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 インスペクションのログ情報をクリア、または表示するには、表 23-4 に記載された特権 EXEC コマンドを使用します。

表 23-4 ダイナミック ARP インスペクション ログ情報をクリアまたは表示するためのコマンド

コマンド	説明
<code>clear ip arp inspection log</code>	ダイナミック ARP インスペクション ログ バッファをクリアします。
<code>show ip arp inspection log</code>	ダイナミック ARP インスペクション ログ バッファの設定と内容を表示します。

このコマンドの詳細については、このリリースのコマンドリファレンスを参照してください。

