CHAPTER 26

ダイナミック ARP インスペクションの設定

機能情報の確認

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ダイナミック ARP インスペクションの前提条件

- 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（Dynamic Address Resolution Protocol）インスペクション 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 アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

ダイナミック ARP インスペクションの制約事項

- この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

ダイナミック ARP インスペクションに関する情報

ダイナミック ARP インスペクション

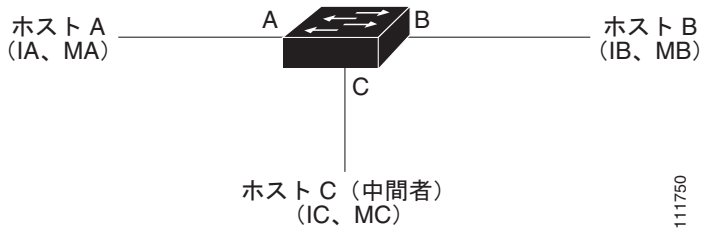
ダイナミック ARP インスペクション（DAI）により、同じ VLAN（仮想 LAN）内の他のポートの無効な ARP 要求や応答を信頼しないようにして、スイッチでの悪意のある攻撃を回避できます。

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 要求が受信されなった場合でも、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 26-1 は、ARP キャッシュ ポイズニングの例を示します。

図 26-1　　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。

DAI 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。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。

DAI を使用することで、有効な ARP 要求および応答だけが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。

DAI は信頼できるデータベースに保存された IP アドレスと MAC アドレスとの有効なバインディングに基づき、ARP パケットの有効性を判断します。このデータベースを、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースと呼びます。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。

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

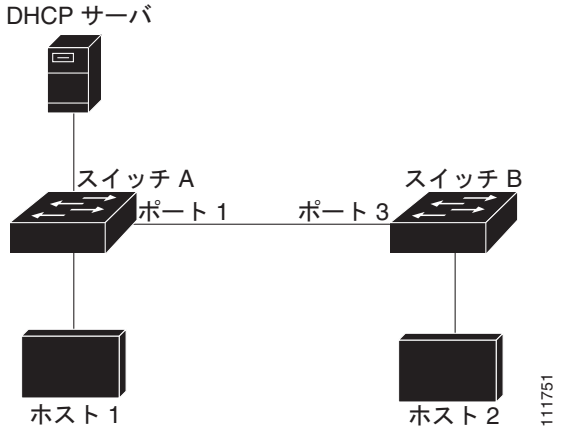
DAI は、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイス上で受信されたパケットは、DAI のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、DAI の有効性検査が行われます。

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 26-2 では、スイッチ A とスイッチ B の両方が VLAN に対して DAI を実行しているとします。この VLAN には、ホスト 1 とホスト 2 が含まれています。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 26-2　DAI をイネーブルにした VLAN での 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 DAI 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 DAI を実行している場合でも起こりえます。

DAI は、DAI を実行す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、ネットワークのその他のホストの 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、ネットワークのその他の場所にあるホストが、DAI 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可能性は防止できません。

VLAN のスイッチの一部が DAI を実行し、残りのスイッチは実行していない場合、これらの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、DAI 非対応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、DAI を実行するスイッチを設定します。バインディングが判断できない場合は、レイヤ 3 で、DAI スイッチを実行していないスイッチから、DAI を実行しているスイッチを分離します。

（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 によって DAI 違反チェックが実行されます。したがって、DoS 攻撃を防ぐために着信 ARP パケット数がレート制限されています。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）　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。

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

DAI では DHCP スヌーピング バインディング データベースを使用して、IP アドレスと MAC アドレスとの有効なバインディングのリストを維持します。

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 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 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。

1 つのログ バッファ エントリで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。このようなエントリが表示された場合は、ログ バッファ内のエントリ数を増やすか、またはログ レートを高くしてください。

ダイナミック ARP インスペクションのデフォルト設定

表 26-1　ダイナミック ARP インスペクションのデフォルト設定

機能	デフォルト設定
DAI	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	DAI をイネーブルにした場合は、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。 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 インスペクション設定時の注意事項

- DAI は入力セキュリティ機能であり、出力検査は行いません。
- DAI は、DAI 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にされていないスイッチに接続されているホストに対しては、効果がありません。man-in-the-middle 攻撃は 1 つのレイヤ 2 ブロードキャスト ドメインに限定されるため、DAI 検査が有効なドメインを、DAI 検査の行われないドメインから切り離します。これにより、DAI をイネーブルにしたドメイン内のホストの ARP キャッシュをセキュリティ保護できます。
- DAI では、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスとのバインディングを、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基づいて検証します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。コンフィギュレーションについては、第 25 章「DHCP 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。
- DAI 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ます。

（注）　RSPAN VLAN で DAI をイネーブルにしないでください。RSPAN VLAN で DAI をイネーブルにすると、DAI 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 チャネルに結合するには、この物理ポートとチャネル 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 チャネル内で中断状態のままとなります。ポート チャネルは、チャ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 チャネルで信頼状態を変更すると、スイッチは、チャ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。
- 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による累積値です。たとえば、ポート チャネルの ARP レート制限を 400 pps に設定すると、このチャ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 ポートで受信される ARP パケットのレートは、すべてのチャネル メンバーからの受信パケット レートの合計となります。EtherChannel ポートのレート制限は、各チャネル ポート メンバーが受信する 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 チャネルの設定に照合して検査されます。ポート チャネルのレート制限設定は、物理ポートの設定には依存しません。

  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 ポートは、各ポートのアグリゲーションを考慮し、DAI をイネーブルにした複数の VLAN でパケットを処理できるように、高い値に設定します。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 DAI 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 インスペクションの設定方法

DHCP 環境でのダイナミック ARP インスペクションの設定

2 つのスイッチがこの機能をサポートする場合の DAI の設定手順を示します。図 26-2（P.26-3）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。両方のスイッチは、これらのホストが置かれている VLAN 1 上で DAI 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。

はじめる前に

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	**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** vlan-range	VLAN 単位で DAI をイネーブルにします。デフォルトでは、すべての VLAN で DAI はディセーブルです。 *vlan-range*：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 ～ 4096 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る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	**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上の他のスイッチから受信した ARP パケットを確認せず、単純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、**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。
ステップ 6	**end**	特権 EXEC モードに戻ります。

非 DHCP 環境での ARP ACL の設定

ここでは、図 26-2（P.26-3）のように、スイッチ B が、DAI も DHCP スヌーピングもサポートしていない場合の DAI の設定方法を示します。

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 をセットアップして、これを 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。

	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 リストは定義されません。 **（注）** ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。
ステップ 3	**permit ip host** *sender-ip* **mac host** *sender-mac* [**log**]	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。 • *sender-ip*：ホスト 2 の IP アドレスを入力します。 • *sender-mac*：ホスト 2 の MAC アドレスを入力します。 • （任意）**log**：パケットがアクセス コントロール エントリ（ACE）に一致すると、ログ バッファにパケットを記録します。**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、「ログ バッファの設定」（P.26-12）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**]	VLAN に ARP ACL を適用します。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。 • *arp-acl-name*：ステップ 2 で作成した ACL の名前を指定します。 • *vlan-range*：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 ～ 4096 です。 • （任意）**static**：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。 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。 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。
ステップ 6	**interface** *interface-id*	スイッチ B に接続されたスイッチ A の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 の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は信頼できません。 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、**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。
ステップ 8	**end**	特権 EXEC モードに戻ります。

着信 ARP パケットのレート制限

	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*	レート制限される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。

	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 要求および ARP 応答のレートを制限します。 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。 • **rate** *pps*：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。 • （任意）**burst interval** *seconds*：高レートの 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。 • **rate none**：処理できる着信 ARP パケットのレートに上限を設定しません。
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）DAI 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、回復のインターバルは 300 秒です。 **interval** *interval*：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。

確認検査の実行

	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 パケットで特定の検査を実行します。デフォルトでは、検証は実行されません。 • **src-mac**：イーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信元 MAC アドレスと比較して検査します。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。 • **dst-mac**：イーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較して検査します。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。 • **ip**：ARP 本体を検査し、無効かつ予期されない IP アドレスの有無を確認します。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。 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 **src** および **dst mac** 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 番めのコマンドによって **src** および **dst mac** の検証が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。

ログ バッファの設定

	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*}	DAI のログ バッファを設定します。 デフォルトでは、DAI 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。 • **entries** *number*：バッファに記録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 • **logs** *number* **interval** *seconds*：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。 **logs** *number*：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。 **interval** *seconds*：指定できる範囲は 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。 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。 **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、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。
ステップ 3	**ip arp inspection vlan** *vlan-range* **logging** {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	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。* • *vlan-range*：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 ～ 4096 です。 • **acl-match matchlog**：ACE ロギング設定に基づいてログ パケットを指定します。このコマンドに **matchlog** キーワードを指定して、さらに **permit** または **deny** ARP アクセス リスト コンフィギュレーション コマンドに **log** 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。 • **acl-match none**：ACL と一致したパケットを記録しません。 • **dhcp-bindings all**：DHCP バインディングと一致したすべてのパケットが記録されます。 • **dhcp-bindings none**：DHCP バインディングと一致したパケットは記録されません。 • **dhcp-bindings permit**：DHCP バインディングによって許可されたパケットが記録されます。
ステップ 4	**exit**	特権 EXEC モードに戻ります。

ダイナミック ARP インスペクションのモニタリングおよびメンテナンス

コマンド	説明
clear ip arp inspection log	DAI のログ バッファを消去します。
clear ip arp inspection statistics	DAI 統計情報をクリアします。
show arp access-list [*acl-name*]	ARP ACL についての詳細情報を表示します。
show errdisable recovery	errdisable 回復タイマー情報を表示します。
show ip arp inspection interfaces [*interface-id*]	指定のインターフェイス、またはすべてのインターフェイスに対して、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 log	DAI ログ バッファの設定および内容を表示します。
show ip arp inspection vlan *vlan-range*	指定の VLAN に対し、DAI の設定内容および動作状態を表示します。VLAN を指定しない場合、または VLAN を範囲で指定した場合は、DAI がイネーブル（アクティブ）にされている VLAN だけの情報が表示されます。
show ip arp inspection statistics [**vlan** *vlan-range*]	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 を指定しない場合、または VLAN を範囲で指定した場合は、DAI がイネーブル（アクティブ）にされている VLAN だけの情報が表示されます。
show ip dhcp snooping binding	DHCP バインディングを確認します。

ダイナミック ARP インスペクションの設定例

DHCP 環境でのダイナミック ARP インスペクションの設定：例

次の例では、VLAN 1 のスイッチ A で DAI 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 gigabitethernet1/1
Switch(config-if)# ip arp inspection trust
```

非 DHCP 環境での ARP ACL の設定：例

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 gigabitethernet0/1
```

```
Switch(config-if)# no ip arp inspection trust
```

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IE 2000 コマンド	『*Cisco IE 2000 Switch Command Reference*, Release 15.0(1)EY』
Cisco IOS 基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
DHCP の設定	『Configuring DHCP on the IE 2000 Switch』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html