ダイナミック ARP インスペクションの設定

この章の内容は、次のとおりです。

DAI の概要

ARP

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 がホスト A に情報を送信しようとして、ホスト B の ARP キャッシュにホスト A の MAC アドレスがないという場合、ARP の用語では、ホスト B が送信者、ホスト A はターゲットになります。

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。

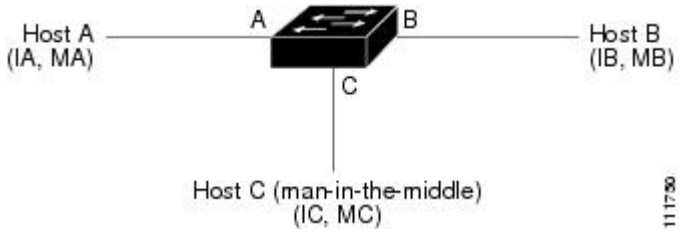
ARP スプーフィング攻撃

ARP では、たとえ ARP 要求を受信していなくても、ホストからの応答が可能なので、ARP スプーフィング攻撃と ARP キャッシュ ポイズニングが発生する可能性があります。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。

ARP スプーフィング攻撃は、サブネットに接続されているデバイスの ARP キャッシュに偽りの情報を送信することにより、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、ルータに影響を及ぼす可能性があります。ARP キャッシュに偽りの情報を送信することを ARP キャッシュ ポイズニングといいます。スプーフ攻撃では、サブネット上の他のホストに対するトラフィックの代行受信も可能です。

次の図に、ARP キャッシュ ポイズニングの例を示します。

図 *1*：*ARP* キャッシュ ポイズニング



ホスト A、B、C は、それぞれインターフェイス A、B、C を介してデバイスに接続されています。これらのインターフェイスは同一サブネットに属します。カッコ内は、各ホストの IP および MAC アドレスを示します。たとえば、ホスト A は IP アドレス IA、および MAC アドレス MA を使用します。ホスト A がホスト B に IP データを送信する必要がある場合、ホスト A は IP アドレス IB に関連付けられた MAC アドレスを求める ARP 要求をブロードキャストします。デバイスとホスト B はこの ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持つホストの ARP バインディングを、それぞれの ARP キャッシュ内に書き込みます。たとえば、IP アドレス IA は MAC アドレス MA にバインドされます。ホスト B が応答すると、デバイスとホスト A は、IP アドレス IB および MAC アドレス MB を持つホストのバインディングを、それぞれの ARP キャッシュ内に書き込みます。

ホスト C は、バインディングを伴う 2 つの偽造 ARP 応答をブロードキャストすることにより、デバイス、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。偽造 ARP 応答の 1 つは、IP アドレス IA と MAC アドレス MC を持つホストの応答、もう 1 つは IP アドレス IB と MAC アドレス MC を持つホストの応答です。これにより、ホスト B とデバイスは、IA を宛先とする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 がこのトラフィックを代行受信することになります。同様に、ホスト A とデバイスは、IB を宛先とする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。

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。このトポロジでは、ホスト C は、ホスト A からホスト B へのトラフィック ストリーム内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。

DAI および ARP スプーフィング攻撃

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。DAI がイネーブルになり適切に設定されている場合、Cisco Nexus デバイス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 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た有効な IP アドレスと 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、VLAN とデバイス上で DHCP スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。また、このデータベースにはユーザが作成するスタティック エントリも保存できます。ARP パケットを信頼できるインターフェイス上で受信した場合は、デバイスはこのパケットを検査せずに転送します。信頼できないインターフェイス上では、デバイスは有効性を確認できたパケットだけを転送します。

DAI では、パケット内の IP アドレスが無効な場合に ARP パケットをドロップするのか、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 パケットをドロップするのかを設定できます。

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、デバイス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、次のガイドラインに従ってインターフェイスの信頼状態を設定します。

信頼できない

ホストに接続されているインターフェイス

信頼できる

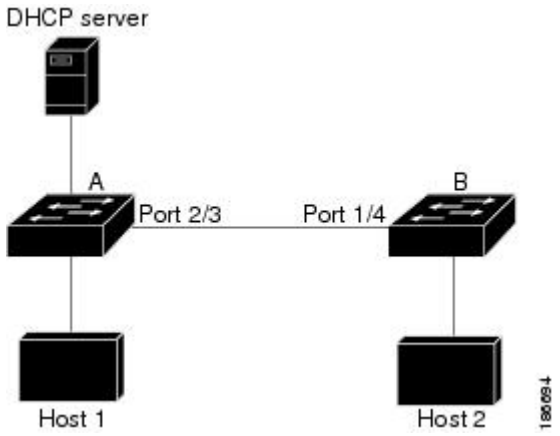
デバイスに接続されているインターフェイス

この設定では、デバイスからネットワークに送信されるARPパケットはすべて、セキュリティ検査をバイパスします。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。

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。

次の図では、デバイス A およびデバイス B の両方が、ホスト 1 およびホスト 2 を収容する VLAN 上で DAI を実行していると仮定します。ホスト 1 およびホスト 2 が、デバイス A に接続されている DHCP サーバから IP アドレスを取得すると、デバイス A だけがホスト 1 の IP/MAC アドレスをバインドします。デバイス A とデバイス B 間のインターフェイスが信頼できない場合は、ホスト 1 からの ARP パケットはデバイス B ではドロップされ、ホスト 1 およびホスト 2 の間の接続は切断されます。

図 *2*：*DAI* をイネーブルにした *VLAN* での *ARP* パケット検証



信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワークにセキュリティ ホールが生じる可能性があります。デバイス A が DAI を実行していなければ、ホスト 1 はデバイス B の ARP キャッシュを簡単にポイズニングできます（デバイス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 も同様）。この状況は、デバイス B が DAI を実行している場合でも起こりえます。

DAI は、DAI が稼働するデバイスに接続されているホスト（信頼できないインターフェイス上）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保証します。ただし、DAI が稼働するデバイスに接続されているホストのキャッシュがネットワークの他の部分のホストによってポイズニングされるのを防ぐことはできません。

VLAN 内の一部のデバイスで DAI が稼働し、他のデバイスでは稼働していない場合は、DAI が稼働しているデバイス上のインターフェイスの信頼状態を次のガイドラインに従って設定します。

信頼できない

ホスト、または DAI を実行していないデバイスに接続されているインターフェイス

信頼できる

DAI が稼働しているデバイスに接続されているインターフェイス

DAI が稼働していないデバイスからのパケットのバインディングを検証するには、DAI が稼働しているデバイスに ARP ACL を設定します。バインディングの有効性を判断できない場合は、DAI が稼働しているデバイスを DAI が稼働していないデバイスからレイヤ 3 で隔離します。

（注） ネットワークの設定によっては、VLAN 内の一部のデバイスで ARP パケットを検証できない場合もあります。

ARP ACL および DHCP スヌーピング エントリのプライオリティ

デフォルトでは、DAI は DAI パケットを、DHCP スヌーピング データベース内の IP-MAC アドレス バインディングと照合することにより、DAI トラフィックをフィルタリングします。

DAI が適用されると、ARP ACL と VACL より優先されます。デバイスは、ユーザ設定の ARP ACL または VACL に関係なく、有効な IP-MAC バインディングが DHCP スヌーピング データベースに存在するかどうかに基づいてパケットを拒否または許可します。

MAC ACL と ARP ACL に関連付けられた VACL を VLAN へ適用すると、VACL は、ARP トラフィックで動作するように設定されている VACL に関係なく ARP ACL よりも優先されます。VACL に一致するエントリがないと、トラフィックは VACL の暗黙の deny エントリによって廃棄される場合があります。

PACL は ARP ACL よりも優先されます。

DAI パケットのロギング

Cisco NX-OS は処理された DAI パケットについてのログ エントリのバッファを維持しています。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。

ログに記録するパケットのタイプを指定することもできます。デフォルトでは、Cisco Nexus デバイスは DAI がドロップしたパケットだけを記録します。

ログ バッファがあふれると、デバイスは最も古い DAI ログ エントリを新しいエントリで上書きします。バッファ内の最大エントリ数を設定できます。

（注） Cisco NX-OS は、ログに記録される DAI パケットに関するシステム メッセージを生成しません。

DAI のライセンス要件

次の表に、DAI のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	DAI にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

DAI の前提条件

- DHCP を設定するには、その前に DAI 機能をイネーブルにする必要があります。

DAI の注意事項と制約事項

DAI に関する注意事項と制約事項は次のとおりです。

- 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 をサポートしないデバイス、またはこの機能がイネーブルにされていないデバイス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 が有効なドメインを、DAI が実行されないドメインから切り離す必要があります。これにより、DAI が有効な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。DAI が ARP パケットの有効性を判断するのにスタティック IP-MAC アドレス バインディングを使用するように設定する場合、DHCP スヌーピングの設定はイネーブルにするだけで済みます。DAI が ARP パケットの有効性を判断するのにダイナミック IP-MAC アドレス バインディングを使用するように設定する場合は、DAI を設定した VLAN と同じ VLAN に DHCP スヌーピングを設定する必要があります。
- **feature dhcp** コマンドを使用して DHCP 機能をイネーブルにすると、I/O モジュールが DHCP を受信する前、または DAI の設定前に約 30 秒の遅延が発生します。この遅延は、DHCP 機能がディセーブルになった設定から、DHCP 機能がイネーブルになった設定に変更するために使用する方式には関係なく発生します。たとえば、ロールバック機能を使用して、DHCP

機能をイネーブルにする設定に戻した場合、ロールバックを完了してから約 30 秒後に I/O モジュールが DHCP と DAI 設定を受信します。

- DAI は、アクセス ポート、トランク ポート、ポート チャネル 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。
- ポート チャネルに対する DAI の信頼設定によって、そのポート チャネルに割り当てたすべての物理ポートの信頼状態が決まります。たとえば、ある物理ポートを信頼できるインターフェイスとして設定し、信頼できないインターフェイスであるポート チャネルにその物理ポートを追加した場合、その物理ポートは信頼できない状態になります。
- ポート チャネルから物理ポートを削除した場合、その物理ポートはポート チャネルの DAI 信頼状態の設定を保持しません。
- ポートチャネルの信頼状態を変更すると、デバイスはそのチャネルを構成するすべての物理ポートに対し、新しい信頼状態を設定します。
- ARP パケットが有効かどうかを判定するために DAI でスタティック IP-MAC アドレス バインディングを使用するように設定する場合は、DHCP スヌーピングがイネーブルになっていること、およびスタティック IP-MAC アドレス バインディングを設定していることを確認します。
- ARP パケットが有効かどうかを判定するために DAI でダイナミック IP-MAC アドレス バインディングを使用するように設定する場合は、DHCP スヌーピングがイネーブルになっていることを確認します。
- ARP ACL を使用して ACL で SPAN を実行できます。
- ARP ACL は、QoS ポリシーに関する ACL ベースの分類に使用できますが、FEX にオフロードされるポリシーには使用できません。
- DAI は VACL および ARP ACL に優先され、VACL は ARP ACL に優先されます。
- ARP ACL の一致基準の最大数は、VACL リージョン用の TCAM の空き領域によって制限されます。Cisco Nexus デバイスの各一致基準は、1 つのエントリを持ちます。

DAI のデフォルト設定

次の表に、DAI パラメータのデフォルト設定を示します。

表 *1*：デフォルトの *DAI* パラメータ

パラメータ	デフォルト
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。
有効性検査	検査は実行されません。

パラメータ	デフォルト
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。

DAI の設定

VLAN での DAI のイネーブル化とディセーブル化

VLAN に対して DAI をイネーブルまたはディセーブルにすることができます。デフォルトでは、DAI はすべての VLAN でディセーブルです。

はじめる前に

DAI をイネーブルにする場合は、次の点を確認してください。

- DHCP 機能がイネーブルになっていることを確認します。
- DAI をイネーブルにする VLAN が設定されている。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	[**no**] **ip arp inspection vlan***list* 例： `switch(config)# ip arp inspection vlan 13`	VLAN の特定のリストに対して DAI をイネーブルにします。**no** オプションを使用すると、指定した VLAN の DAI がディセーブルになります。

	コマンドまたはアクション	目的
ステップ 3	**showip arp inspection vlan***list* 例： `switch(config)# show ip arp inspection vlan 13`	（任意） VLAN の特定リストの DAI ステータスを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ 2 インターフェイスの DAI 信頼状態の設定

レイヤ 2 インターフェイスの DAI インターフェイス信頼状態を設定できます。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。

デバイスは、信頼できるレイヤ 2 インターフェイス上で受信した ARP パケットを転送しますが、検査は行いません。

信頼できないインターフェイス上では、デバイスはすべての ARP 要求および ARP 応答を代行受信します。デバイスは、ローカル キャッシュをアップデートして、代行受信したパケットを適切な宛先に転送する前に、そのパケットの IP-MAC アドレス バインディングが有効かどうかを検証します。そのパケットのバインディングが無効であると判断すると、デバイスはそのパケットをドロップし、ロギングの設定に従ってログに記録します。

はじめる前に

DAI をイネーブルにする場合は、DHCP 機能がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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***typenumber/slot*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		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。

	コマンドまたはアクション	目的
ステップ 3	**[no] ip arp inspection trust** 例： `switch(config-if)# ip arp inspection trust`	インターフェイスを、信頼できる ARP インターフェイスとして設定します。**no** オプションを使用すると、そのインターフェイスは信頼できない ARP インターフェイスとして設定されます。
ステップ 4	**show ip arp inspection interface** *type number/slot* 例： `switch(config-if)# show ip arp inspection interface ethernet 2/1`	（任意） 特定のインターフェイスの信頼状態および ARP パケット レートを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI フィルタリングを目的とした ARP ACL の VLAN への適用

1 つまたは複数の VLAN に ARP ACL を適用できます。デバイスがパケットを許可するのは、ACL がそのパケットを許可する場合だけです。デフォルトでは、どの VLAN にも ARP ACL は適用されません。

はじめる前に

適用する ARP ACL が正しく設定されていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**[no] ip arp inspection filter** *acl-name* **vlan** *list* 例： `switch(config)# ip arp inspection filter arp-acl-01 vlan 100`	ARP ACL を VLAN のリストに適用します。あるいは、**no** オプションを使用している場合は、ARP ACL を VLAN のリストから削除します。

	コマンドまたはアクション	目的
ステップ 3	**showip arp inspection vlan***list* 例： `switch(config)# show ip arp inspection vlan 100`	（任意） 特定の VLAN リストの DAI ステータスを表示します（ARP ACL が適用されているかどうかも含む）。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

追加検証のイネーブル化またはディセーブル化

ARP パケットの追加検証をイネーブルまたはディセーブルにできます。デフォルトでは、ARP パケットの追加検証はイネーブルになりません。追加検証が設定されていない場合、送信元 MAC アドレス、ARP パケットの IP/MAC バインディング エントリと照合する送信元 IP アドレスのチェックは、イーサネット送信元 MAC アドレス（ARP 送信者の MAC アドレスではない）と ARP 送信者の IP アドレスを使用して実行されます。

DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、記録、および廃棄します。宛先 MAC アドレス、送信元および宛先 IP アドレス、送信元 MAC アドレスに対し、追加検証をイネーブルにすることができます。

追加検証を実装するには、**ip arp inspection validate** コマンドで次のキーワードを使用します。

dst-mac

ARP 応答のイーサネット 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。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 本文をチェックして、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。

src-mac

ARP 要求と応答のイーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信者 MAC アドレスと比較して検査します。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。

追加検証をイネーブルにする場合は、次の点に注意してください。

- 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。指定するキーワードは、1つでも、2 つでも、3 つすべてでもかまいません。
- 各 **ip arp inspection validate** コマンドにより、それまでに指定したコマンドの設定が置き換えられます。**ip arp inspection validate** コマンドによって src -mac および dst-mac 検証をイネーブルにし、2 つ目の **ip arp inspection validate** コマンドで IP 検証をイネーブルにした場合は、2 つ目のコマンドを入力した時点で src-mac と dst-mac の検証がディセーブルになります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	[**no**] **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} 例： `switch(config)# ip arp inspection validate src-mac dst-mac ip`	追加の DAI 検証をイネーブルにします。あるいは、**no** オプションを使用して、追加の DAI 検証をディセーブルにします。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI のログ バッファ サイズの設定

DAI のログ バッファ サイズを設定できます。デフォルトのバッファ サイズは 32 メッセージです。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	[**no**] **ip arp inspection log-buffer entries***number* 例： `switch(config)# ip arp inspection log-buffer entries 64`	DAI のログ バッファ サイズを設定します。**no** オプションを使用すると、デフォルトのバッファ サイズ（32 メッセージ）に戻ります。設定できるバッファ サイズは、1 ～ 1024 メッセージです。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI のログ フィルタリングの設定

DAI パケットを記録するかどうかをデバイスが判断する方法を設定できます。デフォルトでは、デバイスはドロップされる DAI パケットをログに記録します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	次のいずれかのコマンドを入力します。 • **ip arp inspection vlan***vlan-list***loggingdhcp-bindings all**	次のようにして、DAI ログ フィルタリングを設定します。**no** オプションを使用すると、DAI ログ フィルタリングが削除されます。 • DHCP バインディングに一致するすべてのパケットを記録します。

	コマンドまたはアクション	目的
	• **ip arp inspection vlan***vlan-list***loggingdhcp-bindings none** • **ip arp inspection vlan***vlan-list***loggingdhcp-bindingspermit** • **no ip arp inspection vlan***vlan-list***loggingdhcp-bindings** {**all** | **none** | **permit**} 例： `switch(config)# ip arp inspection vlan 100 dhcp-bindings permit`	• DHCPバインディングに一致するパケットを記録しません。 • DHCP バインディングによって許可されるパケットを記録します。 • DAI ログ フィルタリングを削除します。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI の設定の確認

DAI の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip arp inspection	DAI のステータスを表示します。
show ip arp inspection interface ethernet	信頼状態を表示します。
show ip arp inspection vlan	特定の VLAN の DAI 設定を表示します。
show arp access-lists	ARP ACL を表示します。
show ip arp inspection log	DAI のログ設定を表示します。

DAI の統計情報のモニタリングとクリア

DAI の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドを使用します。これらのコマンドの詳細については、Cisco Nexus デバイスの『*Security Command Reference*』を参照してください。

コマンド	目的
show ip arp inspection statistics	DAI の統計情報を表示します。
clear ip arp inspection statistics vlan <id>	DAI 統計情報をクリアします。

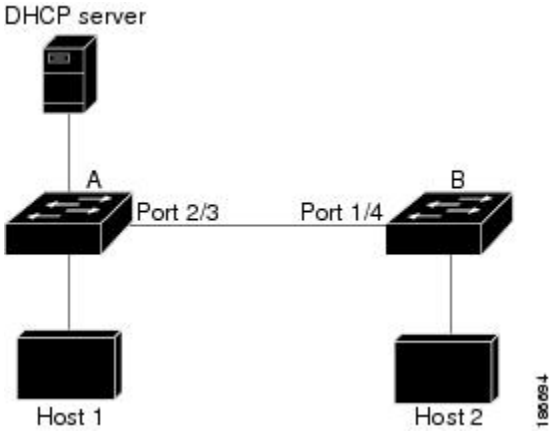
DAI の設定例

例 1：2 つのデバイスが DAI をサポートする場合

2 つのデバイスが DAI をサポートする場合の DAI の設定手順を次に示します。

次の図に、この例のネットワーク構成を示します。ホスト 1 はデバイス A に、ホスト 2 はデバイス B にそれぞれ接続されています。デバイスは両方とも、ホストが配置されている VLAN 1 で DAI を実行しています。DHCP サーバはデバイス 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。デバイス A はホスト 1 およびホスト 2 のバインディングを持ち、デバイス B はホスト 2 のバインディングを持ちます。デバイス A のイーサネット インターフェイス 2/3 は、デバイス B のイーサネット インターフェイス 1/4 に接続されています。

図 *3*：*DAI* をサポートする *2* つのデバイス



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。

- この構成は、DHCP サーバがデバイス A から別の場所に移動されると機能しません。
- この構成によってセキュリティが損なわれないようにするには、デバイス A のイーサネット インターフェイス 2/3、およびデバイス B のイーサネット インターフェイス 1/4 を、信頼できるインターフェイスとして設定します。

デバイス A の設定

デバイス A で DAI をイネーブルにし、イーサネット インターフェイス 2/3 を信頼できるインターフェイスとして設定するには、次の作業を行います。

手順

ステップ 1 デバイス A にログインして、デバイス A とデバイス B の間の接続を確認します。

```
switchA# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchB                Ethernet2/3     177     R S I    WS-C2960-24TC Ethernet1/4
switchA#
```

ステップ 2 VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
switchA# config t
switchA(config)# ip arp inspection vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchA(config)#
```

ステップ 3 イーサネット インターフェイス 2/3 を、信頼できるインターフェイスとして設定します。

```
switchA(config)# interface ethernet 2/3
switchA(config-if)# ip arp inspection trust
switchA(config-if)# exit
switchA(config)# exit
switchA# show ip arp inspection interface ethernet 2/3
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
```

```
 Ethernet2/3      Trusted           15             5
```

ステップ 4 バインディングを確認します。

```
switchA# show ip dhcp snooping binding
MacAddress         IpAddress        LeaseSec  Type           VLAN  Interface
-----------------  ---------------  --------  -------------  ----  -------------
00:60:0b:00:12:89  10.0.0.1         0         dhcp-snooping  1     Ethernet2/3
switchA#
```

ステップ 5 DAI がパケットを処理する前、およびあとの統計情報を調べます。

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

ホスト 1 が IP アドレス 10.0.0.1 および MAC アドレス 0002.0002.0002 を持つ 2 つの ARP 要求を送信すると、両方の要求が許可されます。これは、次の統計情報で確認できます。

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

ホスト 1 が、IP アドレス 10.0.0.3 を持つ ARP 要求を送信しようとすると、このパケットはドロップされ、エラー メッセージがログに記録されます。

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Ethernet2/3, vlan
1.([0002.0002.0002/10.0.0.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Fri Jul 13 2008])
```

この場合に表示される統計情報は次のようになります。

```
switchA# show ip arp inspection statistics vlan 1
switchA#
```

```
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 2
ARP Res Dropped    = 0
DHCP Drops         = 2
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

デバイス B の設定

デバイス B で DAI をイネーブルにし、イーサネット インターフェイス 1/4 を信頼できるインターフェイスとして設定するには、次の作業を行います。

手順

ステップ 1 デバイス B にログインして、デバイス B とデバイス A の間の接続を確認します。

```
switchB# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchA                Ethernet1/4     120     R S I    WS-C2960-24TC Ethernet2/3
switchB#
```

ステップ 2 VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
switchB# config t
switchB(config)# ip arp inspection vlan 1
switchB(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchB(config)#
```

ステップ 3 イーサネット インターフェイス 1/4 を、信頼できるインターフェイスとして設定します。

```
switchB(config)# interface ethernet 1/4
switchB(config-if)# ip arp inspection trust
```

```
switchB(config-if)# exit
switchB(config)# exit
switchB# show ip arp inspection interface ethernet 1/4
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet1/4      Trusted           15             5
switchB#
```

ステップ 4 DHCP スヌーピング バインディングのリストを確認します。

```
switchB# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type           VLAN  Interface
------------------  ---------------  --------  -------------  ----  -------------
00:01:00:01:00:01  10.0.0.2         4995      dhcp-snooping  1     Ethernet1/4
switchB#
```

ステップ 5 DAI がパケットを処理する前、およびあとの統計情報を調べます。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

ホスト 2 が、IP アドレス 10.0.0.2 および MAC アドレス 0001.0001.0001 を持つ ARP 要求を送信すると、このパケットは転送され、統計情報が更新されます。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

ホスト 2 が IP アドレス 10.0.0.1 を持つ ARP 要求を送信しようとすると、この要求はドロップされ、システム メッセージがログに記録されます。

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Ethernet1/4, vlan
1.([0001.0001.0001/10.0.0.1/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri Jun 13 2008])
```

この場合に表示される統計情報は次のようになります。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 1
ARP Res Dropped    = 0
DHCP Drops         = 1
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

ARP ACL の設定

ARP ACL の作成

デバイスに ARP ACL を作成し、これにルールを追加できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**arpaccess-list***name*
	
	例：
	`switch(config)# arp access-list arp-acl-01`
	`switch(config-arp-acl)#`
		ARP ACL を作成し、ARP ACL コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	[*sequence-number*] {**permit** | **deny**} **ip** {**any** | **host***sender-IP* | *sender-IPsender-IP-mask*} **mac** {**any** | **host***sender-MAC* | *sender-MAC sender-MAC-mask*} 例： `switch(config-arp-acl)# permit ip 192.168.2.0 255.2555.255.0 mac 00C0.4F00.0000 ffff.ff00.0000`	メッセージ送信者の IP アドレスおよび MAC アドレスに基づいて、ARP メッセージを許可または拒否するルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。
ステップ 4	[*sequence-number*] {**permit** | **deny**} **requestip** {**any** | **host***sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host***sender-MAC*|*sender-MACsender-MAC-mask*} 例： `switch(config-arp-acl)# permit request ip 192.168.102.0 0.0.0.255 mac any`	メッセージ送信者の IP アドレスおよび MAC アドレスに基づいて、ARP 要求メッセージを許可または拒否するルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。
ステップ 5	[*sequence-number*] {**permit** | **deny**} **responseip** {**any** | **host***sender-IP* | *sender-IP sender-IP-mask*} [**any** | **host***target-IP*|*target-IP target-IP-mask*]] **mac** {**any** | **host***sender-MAC* | *sender-MACsender-MAC-mask*} [**any** | **host***target-MAC* | *target-MAC target-MAC-mask*] 例： `switch(config-arp-acl)# permit response ip host 192.168.202.32 any mac host 00C0.4FA9.BCF3 any`	メッセージの送信者およびターゲットの IPv4 アドレスおよび MAC アドレスに基づいて、ARP 応答メッセージを許可または拒否するルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。
ステップ 6	**show arp access-lists***acl-name* 例： `switch(config-arp-acl)# show arp access-lists arp-acl-01`	（任意） ARP ACL の設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config-arp-acl)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ARP ACL の変更

既存の ARP ACL のルールの変更および削除を実行できます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**arpaccess-list***name*
	
	例：
	`switch(config)# arp access-list arp-acl-01`
	`switch(config-acl)#`
		名前を指定する ACL の ARP ACL 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	[*sequence-number*] {**permit** | **deny**} [**request** | **response**] **ip***IP-data***mac***MAC-data* 例： `switch(config-arp-acl)# 100 permit request ip 192.168.132.0 255.2555.255.0 mac any`	（任意） ルールを作成します。 シーケンス番号を指定すると、ACL内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールはACLの末尾に追加されます。
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**}[**request** | **response**] **ip***IP-data***mac***MAC-data* 例： `switch(config-arp-acl)# no 80`	（任意） 指定したルールを ARP ACL から削除します。
ステップ 5	**showarpaccess-lists** 例： `switch(config-arp-acl)# show arp access-lists`	ARP ACL の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-arp-acl)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ARP ACL の削除

ARP ACL をデバイスから削除できます。

はじめる前に

その ACL が VLAN に適用されているかどうかを確認します。削除できるのは、現在適用されている ACL です。ACL を削除しても、その ACL が適用されている VLAN の設定には影響しません。デバイスは削除された ACL を空であると見なします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**noarpaccess-list***name* 例： `switch(config)# no arp access-list arp-acl-01`	名前を指定した ARP ACL を実行コンフィギュレーションから削除します。
ステップ 3	**showarpaccess-lists** 例： `switch(config)# show arp access-lists`	ARP ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ARP ACL のシーケンス番号の変更

ARP ACL 内のルールに割り当てられているすべてのシーケンス番号を変更できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**resequencearp access-list** *name starting-sequence-numberincrement*
	
	例：
	`switch(config)# resequence arp access-list arp-acl-01 100 10`
	`switch(config)#`
		ACL内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。

ステップ 3	**showarpaccess-lists** *name* 例： `switch(config)# show arp access-lists arp-acl-01`	*name* に名前を指定した ACL の ARP ACL 設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ARP ACL の設定の確認

ARP ACL の設定情報を表示するには、次の表に示すコマンドを使用します。

コマンド	目的
show arp access-lists	ARP ACL の設定を表示します。
show running-config aclmgr	実行コンフィギュレーション内の ACL を表示します。