



ダイナミック ARP インспекションの設定

この章の内容は、次のとおりです。

- [ダイナミック ARP インспекション \(DAI\) に関する情報, 1 ページ](#)
- [DAI の前提条件, 5 ページ](#)
- [DAI の注意事項と制約事項, 5 ページ](#)
- [DAI のデフォルト設定, 5 ページ](#)
- [DAI 機能の設定, 6 ページ](#)
- [DAI の設定の確認, 16 ページ](#)
- [DAI のモニタリング, 16 ページ](#)
- [DAI の設定例, 16 ページ](#)
- [標準, 19 ページ](#)
- [DAI の機能の履歴, 19 ページ](#)

ダイナミック ARP インспекション (DAI) に関する情報

DAI 機能の詳細については、次の項を参照してください。

ARP

ダイナミック ARP インспекション (DAI) とは、有効な ARP 要求と応答だけが中継されるようにするための機能です。信頼できないポート上でのすべての ARP 要求と応答は、この機能によって代行受信されます。代行受信されたパケットが有効な IP-to-MAC アドレス バインディングを持つことが検証されると、ローカル ARP キャッシュが更新されるか、適切な宛先にパケットが転送されます。この機能がイネーブルのときは、無効な ARP パケットはドロップされます。

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 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 アドレスに関連付けられた MAC アドレスを取得するため、このブロードキャストドメイン内の全ホストに対してブロードキャストメッセージを送信します。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。

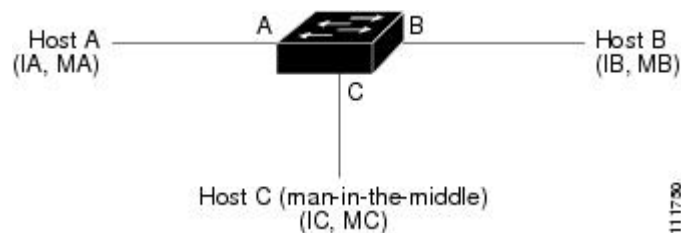
Release 4.2(1)SV2(1.1)からは、IP アドレスと MAC アドレスのペアに基づくトラフィックのフィルタリングではなく、送信元 IP アドレスにのみ基づいてトラフィックをフィルタリングできます。詳細については、[送信元 IP によるフィルタリングのイネーブル化](#)を参照してください。

ARP スプーフィング攻撃

ARP スプーフィング攻撃とは、要求されていない ARP 応答を送りつけてホストのキャッシュを更新するというものです。それ以降は、攻撃者が検出されて ARP キャッシュ内の情報が修正されない限り、トラフィックは攻撃者を介して転送されます。

ARP スプーフィング攻撃を受けると、レイヤ 2 ネットワークに接続されたホスト、スイッチ、およびルータの ARP キャッシュに偽りの情報が送信されるので、これらの機器に影響が及ぶ可能性があります。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



この図では、ホスト A、B、C はインターフェイス A、B、C を介してデバイスに接続されており、これらのインターフェイスはすべて同じサブネット上にあります。カッコ内は、各ホストの IP アドレスと 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 と 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。デバイスおよびホスト B がこの ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持つホストを表すバインディングが、デバイスおよびホスト B の ARP キャッシュに追加されます。

ホスト B が応答すると、IP アドレス IB および MAC アドレス MB を持つホストを表すバインディングが、デバイスとホスト A の ARP キャッシュに追加されます。

ホスト C は、次の 2 つの ARP 応答を偽造してブロードキャストすれば、ホスト A とホスト B を欺く（スプーフィング）ことができます。

- IP アドレス IA と MAC アドレス MC を持つホストの応答
- IP アドレス IB と MAC アドレス MC を持つホストの応答

このような応答を受け取ると、ホスト B は、IA に送られるはずであったトラフィックの宛先 MAC アドレスとして MC を使用します。つまり、そのトラフィックはホスト C によって代行受信されます。同様に、ホスト A とデバイスは、IB に送られるはずのトラフィックの宛先 MAC アドレスとして MC を使用します。

ホスト C は IA および IB の本当の MAC アドレスを知っているため、代行受信したトラフィックを転送できます。

DAI および ARP スプーフィング

DAI は、ARP の要求と応答を検証するための機能です。具体的には、次のような処理を実行します。

- 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。
- ARP キャッシュの更新やパケットの転送を行う前に、そのパケットに対応する有効な IP アドレスと MAC アドレスのバインディングが存在することを確認します。
- 無効な ARP パケットはドロップします。

DAI によって ARP パケットの有効性を判断するときの基準となる有効な IP-to-MAC バインディングは、Dynamic Host Configuration Protocol (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ます。このデータベースは、VLAN とデバイスに対して DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピング機能によって構築されます。このデータベースには、管理者が作成したスタティック エントリが格納されていることもあります。

信頼できるインターフェイス上で受信された ARP パケットは、一切の検査なしで転送されます。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。

管理者は、ARP パケットの宛先 MAC アドレス、送信元 MAC アドレス、および IP アドレスの検証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。

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 によって、インターフェイスは「信頼できる」と「信頼できない」に分類されます。

一般的なネットワークでは、インターフェイスは次のように設定されます。

- 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。
パケットは DAI によって検証されます。
- 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。
パケットは、DAI による検証をすべてバイパスします。

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。

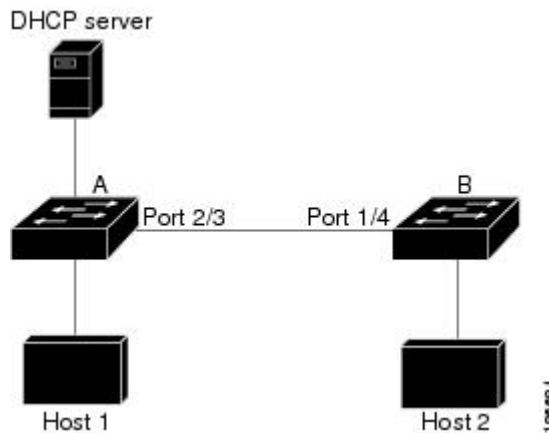


注意

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 アドレスと 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発生する場合があります。

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。



(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。

DAI の前提条件

- 次のものを理解している必要があります。
 - ARP
 - DHCP スヌーピング
- Cisco Nexus 1000V 上で動作するソフトウェアが DAI をサポートしている必要があります。
- VEM 機能レベルが、DAI をサポートするリリースに更新されている必要があります。

DAI の注意事項と制約事項

- 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。
- ホストが接続されているデバイスが DAI をサポートしていない場合や、そのデバイスで DAI がイネーブルになっていない場合は、DAI の効果はありません。1つのレイヤ2ブロードキャストドメインだけを標的とする攻撃を防ぐには、DAI が有効なドメインと、そうではないドメインとを分離させてください。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 によって、着信 ARP 要求および ARP 応答内の IP-to-MAC アドレス バインディングが検証されます。スタティック エントリが設定されていない場合は、DAI が設定されている VLAN に対して DHCP スヌーピングもイネーブルにする必要があります。
- DAI がサポートされるのは、vEthernet インターフェイスとプライベート VLAN ポートです。
- DAI が ARP パケットの有効性を判断するためにダイナミック 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、DHCP スヌーピングが設定されていることを確認します。
- 仮想サービス ドメイン (VSD) サービス VM ポートは、デフォルトで信頼できるポートとなっています。管理者が VSD ポートを「信頼できない」と設定しても、DAI では信頼できるポートとして扱われます。

DAI のデフォルト設定

パラメータ	デフォルト
VLAN	VLAN は DAI の対象としては設定されません。
VSD 内ではない vEthernet インターフェイスの信頼状態	信頼しない

パラメータ	デフォルト
VSD 内の vEthernet インターフェイスの信頼状態	信頼できる
イーサネット ポート チャンネルの信頼状態	信頼できる
信頼できないインターフェイスに対する着信 ARP パケット レート制限	15 パケット/秒 (pps)
信頼できるインターフェイスに対する着信 ARP パケット レート制限	無制限
レート制限バースト間隔	1 秒
DAI error-disabled 状態インターフェイスの検出と回復	error-disabled 状態の検出と回復は設定されません。
有効性検査	検査は実行されません。
VLAN 統計情報	ARP 要求および応答の統計情報

DAI 機能の設定

DAI 対象の VLAN の設定

デフォルトでは、VLAN は DAI の対象としては設定されません。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- DHCP スヌーピングをイネーブルにしていること。
- DAI の対象として設定する VLAN が作成されていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# 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	switch(config)# ip arp inspection vlan list	指定した 1 つ以上の VLAN を DAI の対象として設定します。
ステップ 3	switch(config)# show ip arp inspection vlan list	(任意) 指定した VLAN のリストの DAI ステータスを表示します。
ステップ 4	switch(config)# copy running-config startup-config	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。

```
switch# configure terminal
switch(config)# ip arp inspection vlan 13
switch(config)# show ip arp inspection vlan 13
switch(config)# copy running-config startup-config
```

信頼できる vEthernet インターフェイスの設定

はじめる前に

この手順を開始する前に、次の情報を知っている必要があります。

- デフォルトでは、vEthernet インターフェイスの状態は「信頼できない」です（VSD に属している場合を除く）。
- インターフェイスが信頼できない状態である場合は、すべての ARP 要求および応答の検証が行われ、IP-MAC アドレス バインディング が有効な場合にのみ、ローカル キャッシュ が更新されてパケットが転送されます。パケットの IP-MAC アドレス バインディング が無効な場合は、パケットがドロップされます。
- 信頼できるインターフェイスで受信された ARP パケットは、転送されますが、検証は行われません。
- 信頼できるインターフェイスの設定は、次のどちらでも行うことができます。
 - インターフェイス自体
 - インターフェイスが割り当てられている既存のポート プロファイル
 信頼できるインターフェイスの設定をポート プロファイルで行う場合は、ポート プロファイルが作成済みで名前がわかっていることが必要です。

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# 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	switch(config)# interface vethernet <i>interface-number</i> • switch(config)# port-profile <i>profilename</i> 指定したポート プロファイルの ポートプロファイルコンフィギュ レーションモードを開始します。	指定した vEthernet インターフェイスの インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# [no] ip arp inspection trust	DHCP スヌーピングに関してインターフェ イスを信頼できるインターフェイスとして 設定します。 no オプションを使用すると、 ポートは信頼できないインターフェイスと して設定されます。
ステップ 4	switch(config-if)# ip arp inspection trust • switch(config-port-prof)# ip arp inspection trust このポートプロファイルに割り当 てられる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。	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。
ステップ 5	switch(config-if)# show ip arp inspection interface vethernet <i>interface-number</i>	(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 6	switch(config-if)# show port-profile <i>profilename</i>	(任意) ポート プロファイル設定を表示します。 ARP 信頼状態も表示されます。
ステップ 7	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。

```
switch# configure terminal
switch(config)# interface vethernet 3
```



```

switch(config-if)# ip arp inspection trust
switch(config-if)# show ip arp inspection interface vethernet 3
switch(config-if)# copy running-config startup-config

switch(config)# port-profile vm-data
switch(config-port-profile)# ip arp inspection trust
switch(config-port-profile)# show port-profile vm-data
switch(config-port-profile)# copy running-config startup-config

```

vEthernet インターフェイスの信頼できないインターフェイスへのリセット

デフォルトでは、vEthernet インターフェイスの状態は「信頼できない」です（VSDに属している場合を除く）。vEthernet インターフェイスから信頼できるという指定を削除し、デフォルトの信頼できないという指定に戻すには、次の手順を実行します。

インターフェイスが信頼できない状態である場合は、すべての ARP 要求および応答の検証が行われ、IP-MAC アドレス バインディングが有効な場合にのみ、ローカル キャッシュが更新されてパケットが転送されます。パケットの IP-MAC アドレス バインディングが無効な場合は、パケットがドロップされます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# 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	switch(config)# interface vethernet <i>interface-number</i>	指定した vEthernet インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# default ip arp inspection trust	インターフェイスから信頼できるという指定を削除し、デフォルトの信頼できない状態に戻します。
ステップ 4	switch(config-if)# show ip arp inspection interface vethernet <i>interface-number</i>	(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	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。

```
switch# config t
switch(config)# interface vethernet 3
switch(config-if)# default ip arp inspection trust
switch(config-if)# show ip arp inspection interface vethernet 3
switch(config-if)# copy running-config startup-config
```

DAI レート制限の設定

ここでは、ARP 要求と応答のレート制限を設定する手順を説明します。

はじめる前に

この手順を開始する前に、次のことを知っておく必要があります。

- トランク ポートでは集約が行われるので、トランク ポートのレート上限は高く設定してください。
- 着信パケットのレートが設定レートを超えると、インターフェイスは自動的に errdisable 状態になります。
- デフォルトの DAI レート制限は次のとおりです。
 - 信頼できないインターフェイス = 15 パケット/秒
 - 信頼できるインターフェイス = 無制限
 - バースト間隔 = 1 秒
- インターフェイスのレート制限は、次のどちらでも行うことができます。
 - インターフェイス自体
 - インターフェイスが割り当てられている既存のポートプロファイル
ポートプロファイルを設定する場合は、ポートプロファイルが作成済みで名前がわかっている必要があります。

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# 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	switch(config)# interface vethernet <i>interface-number</i> • switch(config)# port-profile <i>profilename</i>	指定した vEthernet インターフェイスのインターフェイス 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
	指定したポートプロファイルのポートプロファイ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	<code>switch(config-if)# ip arp inspection limit {rate pps [burst interval l bint] none}</code>	<p>インターフェイスまたはポートプロファイルでの ARP インспекションの制限値を、次のとおりに設定します。</p> <p>次のキーワードと引数があります。</p> <ul style="list-style-type: none"> • rate : 指定できる値は 1 ~ 2048 パケット/秒 (pps) で、この範囲の値を指定します。 <ul style="list-style-type: none"> ◦ 信頼できないインターフェイスのデフォルト = 15 パケット/秒。 ◦ 信頼できるインターフェイスのデフォルト = 無制限。 • burst interval : 指定できる値は 1 ~ 15 秒 (デフォルトは 1 秒) で、この範囲の値を指定します。 • none : パケット/秒が無制限であることを指定します。
ステップ 4	<code>switch(config-if)# show running-config dhcp</code>	(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 5	<code>switch(config-if)# copy running-config startup-config</code>	(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。

```

switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# ip arp inspection limit rate 30
switch(config-if)# show running-config dhcp
switch(config-if)# copy running-config startup-config

switch# configure terminal
switch(config)# port-profile vm-data
switch(config-port-prof)# ip arp inspection limit rate 30
switch(config-port-prof)# show running-config dhcp
switch(config-port-prof)# copy running-config startup-config

```

DAI レート制限のデフォルト値へのリセット

ここでは、ARP 要求と応答のレート制限を設定する手順を説明します。

この手順を開始する前に、次のことを知っておく必要があります。

- トランク ポートでは集約が行われるので、トランク ポートのレート上限は高く設定してください。
- 着信パケットのレートが設定レートを超過すると、インターフェイスは自動的に `errdisable` 状態になります。
- デフォルトの DAI レート制限は次のとおりです。
 - 信頼できないインターフェイス = 15 パケット/秒
 - 信頼できるインターフェイス = 無制限
 - バースト間隔 = 1 秒
- インターフェイスのレート制限は、次のどちらでも行うことができます。
 - インターフェイス自体
 - インターフェイスが割り当てられている既存のポート プロファイル
ポートプロファイルを設定する場合は、ポートプロファイルが作成済みで名前がわかっている必要があります。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch# 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>switch(config)# feature dhcp</code>	DAI 機能をイネーブルにします。 DAI はライセンスを必要とする高度な機能として使用できます。
ステップ 3	<code>switch(config)# interface vethernet interface-number</code>	指定した vEthernet インターフェイスのインターフェイス コンフィギュレーションモードを開始します。
ステップ 4	<code>switch(config-if)# default ip arp inspection limit {rate pps [burst intervall bint] none}</code>	設定されている DAI レート制限をインターフェイスから削除し、デフォルト値に戻します。 次のキーワードと引数があります。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • rate : 信頼できないインターフェイスのデフォルト = 15 パケット/秒。 <ul style="list-style-type: none"> ◦ 信頼できないインターフェイスのデフォルト = 15 パケット/秒。 ◦ 信頼できるインターフェイスのデフォルト = 無制限。 • burst interval : デフォルト = 1 秒。 • none : パケット/秒の制限なし
ステップ 5	switch(config)# show running-config dhcp	(任意) DAI レート制限を含む DHCP スヌーピング設定を表示します。
ステップ 6	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。

```
switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# default ip arp inspection limit rate
switch(config)# show running-config dhcp
switch(config)# copy running-config startup-config
```

Error-Disabled 状態のインターフェイスの検出と回復

デフォルトでは、インターフェイスは DAI error-disabled 回復を行うようには設定されません。インターフェイスを error-disabled 状態から手動で回復するには、次の順でコマンドを実行します。

- 1 shutdown
- 2 no shutdown

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# 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	switch(config)# [no] errdisable detect cause arp-inspection	ARP インспекションの結果 error-disabled 状態となったインターフェイスを検出するように設定します。 no オプションを使用すると、検出がディセーブルになります。
ステップ 3	switch(config)# [no] errdisable recovery cause arp-inspection	ARP インспекションの結果 error-disabled 状態となったインターフェイスを回復するように設定します。
ステップ 4	switch(config)# errdisable recovery interval timer-interval	ARP インспекションの結果 error-disabled となったインターフェイスの回復間隔を設定します。 <i>timer-interval</i> : 指定できる値は 30 ~ 65535 秒です。
ステップ 5	switch(config)# show running-config include errdisable	(任意) errdisable の設定を表示します。
ステップ 6	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。

```
switch# configure terminal
switch(config)# errdisable detect cause arp-inspection
switch(config)# errdisable recovery cause arp-inspection
switch(config)# errdisable recovery interval 30
switch(config)# show running-config | include errdisable
switch(config-if)# copy running-config startup-config
```

ARP パケットの検証

検証の対象は次のアドレスです。デフォルトでは、これらの検証はディセーブルになっています。

- 宛先 MAC アドレス

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、MAC アドレスが無効であるパケットをドロップします。

- IP アドレス

ARP 本体を検査し、無効な、および予期しない IP アドレス (0.0.0.0、255.255.255.255、IP マルチキャストアドレスなど) を検出します。送信元 IP アドレスの検証は、ARP 要求と応答の両方で行われます。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。

• 送信元 MAC アドレス

ARP 要求および応答について、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、MAC アドレスが無効である場合はパケットをドロップします。



(注) 管理者が検証の設定を行うと、それまでの検証設定は上書きされます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# 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	switch(config)# [no] ip arp inspection validate {[src-mac] [dst-mac] [ip]}	指定した検証をイネーブルにします。以前保存された既存の検証設定がある場合は上書きします。 <ul style="list-style-type: none"> • 送信元 MAC • 宛先 MAC • IP この 3 つすべての検証を指定することもできますが、少なくとも 1 つを指定する必要があります。 検証をディセーブルにするには、 no オプションを使用します。
ステップ 3	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	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。

```
switch# configure terminal
switch(config)# ip arp inspection validate src-mac dst-mac ip
```

```
switch(config)# show running-config dhcp
switch(config)# copy running-config startup-config
```

DAI の設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show running-config dhcp	DAI の設定を表示します。
show ip arp inspection	DAI のステータスを表示します。
show ip arp inspection interface vethernet interface-number	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。
show ip arp inspection vlan vlan-ID	特定の VLAN の DAI 設定を表示します。

DAI のモニタリング

DAI をモニタするには、次のいずれかのコマンドを使用します。

コマンド	目的
show ip arp inspection statistics	DAI の統計情報を表示します。
show ip arp inspection statistics vlan vlan-ID	指定されている VLAN の DAI 統計情報を表示します。
clear ip arp inspection statistics	DAI 統計情報をクリアします。

DAI の設定例

この例では、次の 2 つの VEM が存在するネットワークで DAI を設定する方法を示します。

- 一方の VEM は、真正な Web サーバと DHCP サーバをホスティングしています。
- 他方の VEM は、クライアント仮想マシン (VM1) と、不正な Web サーバが存在する仮想マシン (VM2) をホスティングしています。VM1 は、vEthernet インターフェイス 3 に接続されています。このインターフェイスはデフォルトで信頼できない状態となっており、VLAN 1 に属しています。VM2 は、vEthernet 10 と VLAN 1 に接続されています。

DAI がイネーブルでないときは、VM2 が VM1 の ARP キャッシュに偽の情報を送る（スプーフィング）こともできてしまいます。その方法は、ARP 要求が生成されていないけれどもパケットを送信するというものです。このパケットを受け取った VM1 は、自身のトラフィックを、真正な Web サーバではなく VM2 の Web サーバに送信します。

DAI がイネーブルならば、VM2 が VM1 の ARP キャッシュをスプーフィングしようとして、要求されていないにもかかわらず送信した ARP パケットは、ドロップされます。その IP-to-MAC バインディングが不正であることが、DAI によって検出されるからです。ARP キャッシュをスプーフィングする試みは失敗に終わり、VM1 は真正な Web サーバに接続されます。



- (注) DAI によって着信 ARP 要求および ARP 応答の IP-to-MAC アドレス バインディングを検証するには、DHCP スヌーピング データベースが必要です。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。

VLAN 1 での DAI のイネーブル化と設定の確認

```
switch# configure terminal
switch(config)# ip arp inspection vlan 1
switch(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
n1000v(config)#
```

DAI がパケットを処理する前後の統計情報の確認

```
switch# 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
switch#
```

2つの ARP 要求の許可

VM1 が 2 つの ARP 要求を送信し、この要求で指定された IP アドレスは 10.0.0.1、MAC アドレスは 0002.0002.0002 であるとします。要求が両方とも許可されたことは、次のコマンド出力で確認できます。

```
switch# 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
```

ARP 要求パケットのドロップとエラーメッセージのロギング

VM2 が IP アドレス 10.0.0.3 を指定して ARP 要求を送信しようとする、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 vEthernet3, vlan
1. ([0002.0002.0002/10.0.0.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Fri Jul 13 2008])
```

DAI の統計情報の表示例

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

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
switch#
```

標準

標準	タイトル
RFC-826	『An Ethernet Address Resolution Protocol』 http://tools.ietf.org/html/rfc826

DAI の機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
ライセンスの変更	4.2(1)SV2(1.1)	DAIを高度な機能として使用できるようになりました。機能をイネーブルにするには、 feature dhcp コマンドを使用します。
送信元 IP によるフィルタリングのイネーブル化	4.2(1)SV2(1.1)	Cisco Nexus 1000V スイッチで、送信元 IP に基づくフィルタリングをイネーブルにできるようになりました。
DAI	4.0(4)SV1(2)	この機能が導入されました。

