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。

ダイナミック ARP インスペクションに関する情報

ARP

ダイナミック ARP インスペクション（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。

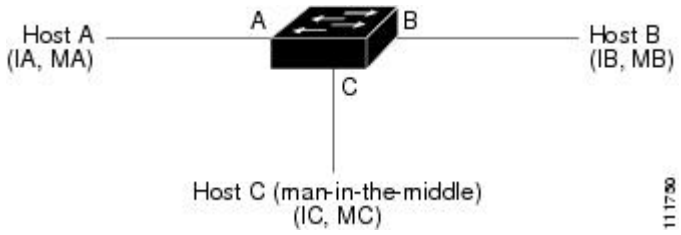
ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャスト ドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロードキャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。

ARP スプーフィング攻撃

ARP 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。

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。

- 送信元 IP アドレス IA と送信元 MAC アドレス MC を持つホスト B の ARP 応答
- 送信元 IP アドレス IB と送信元 MAC アドレス MC を持つホスト A の ARP 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、中間者攻撃の典型的な例です。

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-to-MAC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。

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。

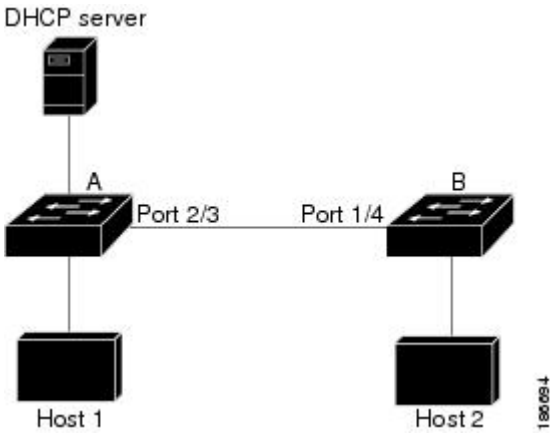
  パケットは、DAIによる検証をすべてバイパスします。

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。

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 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ためにスタティック 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は、DHCP スヌーピングのみを設定する必要があります。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。
- 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。
- 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。
vEthernet インターフェイスの信頼状態	信頼しない
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）

パラメータ	デフォルト
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。
検証チェック（送信元 MAC/宛先 MAC/IP）	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

- CLI に EXEC モードでログインします。
- DHCP スヌーピングをイネーブルにします。
- DAI の対象として設定する VLAN を作成します。

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)# **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。

	コマンドまたはアクション	目的
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。

次に、DAI の対象として VLAN を設定する例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection vlan 13
switch(config)# show ip arp inspection vlan 13
Source Mac Validation      : Disabled
Destination Mac Validation      : Disabled
IP Address Validation      : Disabled

Filter Mode (For Static bindings): IP-MAC

Vlan : 13
-----------
Configuration        : Enabled
Operation State      : Active
DHCP logging options : Deny
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。
- 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***interface-number*	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)# # **port-profile***profilename*	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 4	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 5	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。
ステップ 6	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。
ステップ 7	switch(config-if)# **show ip arp inspection interface vethernet***interface-number*	（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 8	switch(config-if)# **show port-profile***profilename*	（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 9	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。

次に、信頼できる vEthernet インターフェイスを設定する例を示します。

```
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
 Interface        Trust State        Pkt Limit      Burst Interval
 -------------    -----------        ---------      ----------------
 Vethernet3          Trusted             15               5
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 name vm-data
port-profile vm-data
 type: Vethernet
 description:
 status: enabled
 max-ports: 32
 min-ports: 1
 inherit:
 config attributes:
  switchport mode access
  switchport access vlan 13
  ip arp inspection trust
  no shutdown
 evaluated config attributes:
  switchport mode access
  switchport access vlan 13
  ip arp inspection trust
  no shutdown
 assigned interfaces:
 port-group: vm-data
 system vlans: none
 capability l3control: no
 capability iscsi-multipath: no
 capability vxlan: no
 capability l3-vservice: no
 port-profile role: none
 port-binding: static
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。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

CLI に EXEC モードでログインします。

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** *interface-number*	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
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** *interface-number*	（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。

次に、vEthernet インターフェイスを信頼できない状態にリセットする例を示します。

```
switch(config-if)# default ip arp inspection trust
switch(config-if)# show ip arp inspection interface vethernet 3
Interface     Trust State Pkt Limit Burst Interval
------------- ----------- --------- ----------------
Vethernet3     Untrusted   15          5
switch(config-if)# copy running-config startup-config
```

DAI レート制限の設定

ARP 要求および応答のレート制限を設定できます。

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：15 パケット/秒
- バースト間隔：5 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ことが必要です。

はじめる前に

CLI に EXEC モードでログインします。

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***interface-number*	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)# **port-profile***profilename*	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 4	switch(config-if)# **ip arp inspection limit** {**rate***pps* [**burst interval** l *bint*] | **none**}	インターフェイスまたはポート プロファイルでの ARP インスペクションの制限値を、次のとおりに設定します。 次のキーワードと引数があります。 • 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。 ◦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 = 15 パケット/秒。 • 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 5	switch(config-if)# **show ip arp inspection interface vethernet interface-number**	（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)# **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。

次に、DAI レート制限を作成する例を示します。

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

```
switch(config-if)#ip arp inspection limit rate 30
switch# show ip arp inspection interfaces vethernet 3

Interface Trust State Pkt Limit Burst Interval
------------ ----------- --------- -----------------
Vethernet9 Untrusted    30          5
switch#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 = 15 パケット/秒
  - バースト間隔 = 5 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（作成済みで名前がわかっているポート プロファイルを設定する場合）。

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)# **feature dhcp**	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	switch(config)# **interface vethernet***interface-number*	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
ステップ 4	switch(config-if)# **default ip arp inspection limit** {**rate***pps* [**burst interval**l *bint*] | **none**}	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。 • 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。 ◦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 = 5 秒。 • none：パケット/秒の制限なし
ステップ 5	switch(config)# **show ip arp inspection interface vethernet interface-number**	（任意） 指定したインターフェイスのデフォルトの ARP パケット レートを表示します。
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。

次に、DAI レート制限をデフォルト値にリセットする例を示します。

```
switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# default ip arp inspection limit rate

switch# show ip arp inspection interface vethernet 3
<------no output expected for this, since interface moved to default---->

switch# 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 インスペクションの結果 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 インスペクションの結果 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 インスペクションの結果 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。 *timer-interval*：指定できる値は 30 ～ 65535 秒です。
ステップ 5	switch(config)# **show errdisable detect**	（任意） errdisable の設定を表示します。
ステップ 6	switch(config)# **show errdisable recovery**	（任意） errdisable の設定を表示します。
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。

次に、error-disabled 状態のインターフェイスを検出および回復する例を示します。

```
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 errdisable detect
ErrDisable Reason            Timer Status
-----------------            ------------
link-flap                    enabled
dhcp-rate-limit              enabled
arp-inspection               enabled
ip-addr-conflict             enabled
11:22 AM
```

```
switch(config)# sh errdisable recovery
ErrDisable Reason              Timer Status
-----------------              ------------
link-flap                      disabled
dhcp-rate-limit                disabled
arp-inspection                 enabled
security-violation             disabled
psecure-violation              disabled
failed-port-state              enabled
ip-addr-conflict               disabled

        Timer interval: 30
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。 • 送信元 MAC

	コマンドまたはアクション	目的
		• 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 ip arp inspection**	（任意） DAI の設定を表示します。
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。

次に、ARP パケットを検証する例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection
switch(config)# show ip arp inspection
Source Mac Validation      : Enabled
Destination Mac Validation      : Enabled
IP Address Validation      : Enabled

Filter Mode (for static bindings) : IP-MAC
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。

次に、IP ARP 統計情報を表示する例を示します。

```
switch# show ip arp inspection statistics

Vlan : 13
-----------
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

Vlan : 1054
-----------
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

Vlan : 1058
-----------
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# show ip arp inspection statistics vlan 13
```

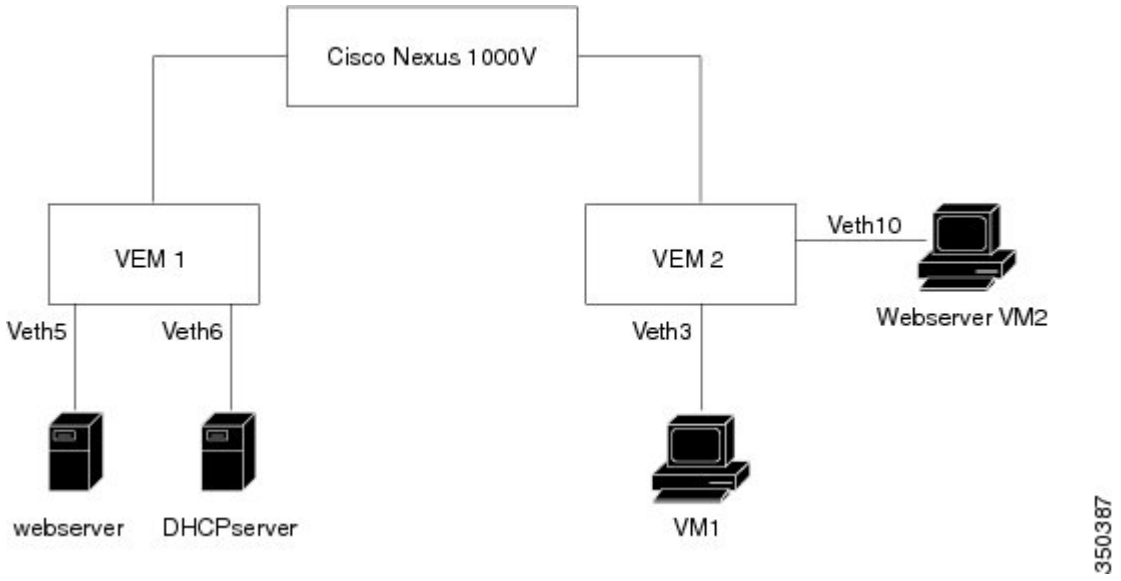
```
Vlan : 13
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switch#
```

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（VM 1）と、不正な Web サーバが存在する仮想マシン（VM 2）をホスティングしています。VM 1 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。VM 2 は、vEthernet 10 と VLAN 1 に接続されています。

図 *3*：ネットワークでの *DAI* の設定



DAI がイネーブルでないときは、VM 2 が VM 1 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 VM 1 は、自身のトラフィックを、真正な Web サーバではなく VM 2 の Web サーバに送信します。

DAI がイネーブルならば、VM 2 が VM 1 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、VM 1 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

次に、VLAN 1 で DAI をイネーブルにして、インターフェイス veth5 で Web サーバに対するスタティック バインディングを追加する例を示します。

```
switch# configure terminal
switch(config)# feature dhcp

switch(config)# ip arp inspection vlan 1

switch# show ip arp inspection vlan 1

Source Mac Validation      : Enabled
Destination Mac Validation      : Enabled
IP Address Validation      : Enabled

Filter Mode (for static bindings): IP-MAC

Vlan : 1
-----------
Configuration        : Enabled
Operation State      : Active
DHCP logging options : Deny

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

Note: Validate helps in inspecting the dst-mac,src-mac and ip of ARP packet and Ethernet
Header, while sending the ARP packet.

switch(config)# ip source binding 192.168.2.22 00:50:56:1e:2c:1c vlan 1 interface vethernet
 5
switch# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type         VLAN  Interface
------------------  ---------------  --------  -----------  ----  --------------
00:50:56:1e:2c:1c  22.22.22.23      infinite   static       1     Vethernet5

switch(config)# int vethernet 6
switch(config-if)# ip arp inspection trust

switch# show ip arp inspection interfaces vethernet 6

 Interface        Trust State        Pkt Limit      Burst Interval
 -------------    -----------        ---------      ----------------
 Vethernet6          Trusted             15               5


switch(config)# interface vethernet 3
switch(config-if)# ip arp inspection limit rate 20
switch# show ip arp inspection interfaces vethernet 3

 Interface        Trust State        Pkt Limit      Burst Interval
```

```
 -------------    -----------        ---------      ----------------
 Vethernet3          Untrusted           20               5

switch(config)# errdisable detect cause arp-inspection

switch# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type         VLAN  Interface
------------------  ---------------  --------  -----------  ----  -------------
00:50:56:1e:2c:1c  192.168.2.22     infinite   static       1     Vethernet5
00:50:56:82:56:43  192.168.2.2      infinite   static       1     Vethernet6
00:50:56:82:56:3e  192.168.2.11     9000       dhcp-snoop   1     Vethernet1
00:50:56:82:56:3f  192.168.2.12     9000       dhcp-snoop   1     Vethernet3
00:50:56:82:56:40  192.168.2.13     9000       dhcp-snoop   1     Vethernet10


If the Rouge-server sends an ARP packet with an IP of 192.168.2.22 (IP of the webserver)
and a MAC address of 00:50:56:82:56:40, ARP packet will be
dropped. An error message will be logged as shown below:

2013 Mar  6 03:54:04 switch %DHCP_SNOOP-SLOT130-3-DHCPDENIEDARP: ARP frame denied due to
DHCP snooping binding on interface Veth10 vlan 1 sender
mac 00:50:56:82:56:40 sender ip 192.168.2.22 target mac 00:50:56:82:56:3f target ip
192.168.2.12.

If Veth3 send ARP packets greater than the configured limit, Veth3 will be placed into error
 disabled state with the following message.
2013 Mar  6 05:26:22 switch %DHCP_SNOOP-4-ERROR_DISABLED: Interface Vethernet3 has moved
to error disabled state due to excessive rate 20 of
ingress ARP packets
```

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

VM 2 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 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
DAI	5.2(1)SM1(5.1)	この機能が導入されました。