ダイナミック ARP インスペクションの設定

この章では、Cisco NX-OS デバイスでダイナミック アドレス解決プロトコル（ARP）インスペクション（DAI）を設定する方法について説明します。

この章は、次の項で構成されています。

DAI について

『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。

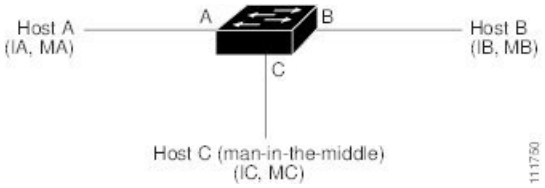
ARP ?????????

ARP ?????? ARP ????????????????????????????ARP ?????????? ARP ?????
??

ARP ???????????????????????????????? ARP ???????????????????????????? 2
??ARP ????????????????????? ARP ?????
??

Figure 1: ARP ????? ??????

?????ARP ????? ??????????????



????A?B?C ?????????????? A?B?C ??
IP ???????? MAC ???????????????? A ????? IP ????? IA?MAC ????? MA ?????? A ???? B ? IP
????????????????????? A ? IP ???? IB ???????? MAC ???????? ARP ????????????????????? B ? ARP
??????????? B ? ARP ?????? IP ???? IA ? MAC ???? MA ??????? ARP ????????????????????IP ????
IA ? MAC ???? MA ????????????? B ?????????? A ?????????? A ? ARP ???????IP ???? IB ? MAC ????
MB ??????? ARP ???????????????????????????? IP ???????????????????????????? ARP ??????????????

??? C ???????????? 2 ???? ARP ?????????????????????? A???? B ? ARP ????????????????????? ARP ???
1 ???IP ???? IA ? MAC ???? MC ???????????? 1 ?? IP ???? IB ? MAC ???? MC ????????????????????????
B ??IA ??????????????? MAC ????????MAC ???? MC ????????????? C ????????????????????????????????
A ??IB ???????????????????? MAC ??????? MC ???????

??? C ? IA ??? IB ?????????? MAC ???????????????? MAC
?? C ????? A ????? B ????????
????????????????????????*man-in-the-middle* ??????????

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。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。

?????????????????? ??????

DAI ??DAI
??DAI ????????????

??

Untrusted

??????????????????

Trusted

??????????????????

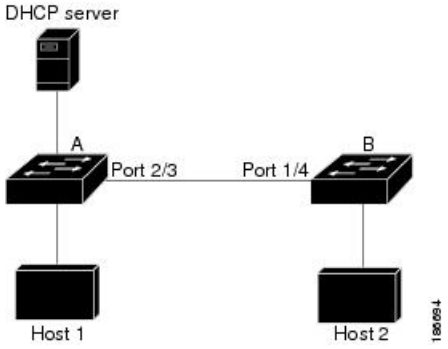
???????????????????????? ARP ????????????????????????????VLAN
??

⚠

Caution ??

Figure 2: DAI ????????? VLAN ?? ARP ??????

?????????? A ??????? B ???????? 1 ?????? 2 ????? VLAN ?? DAI ???????????????? 1 ?????? 2 ??????
A ???????? DHCP ????? IP ?????????????? A ?????? 1 ? IP/MAC ???????????????? A ????? B
???????????????????????? 1 ??? ARP ????????? B ??????????? 1 ?????? 2 ?????????????



?? ?????????????????????? A ? DAI ?????????????
1 ????? B ? ARP ?? 2 ?????????????????? B ? DAI
??????????????????

DAI ??DAI ?? ARP
????????????????????????????DAI
??

VLAN ?????????? DAI ????????????????????????DAI ??

??????

??????? DAI ????????????????????????????

?????

DAI ????????????????????????????

DAI ??DAI ??????????? DAI ???????????????? 3 ???????

Note ??????????????VLAN ?????????? ARP ??????????????????

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ログに記録します。

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。

Note 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。DHCP の設定 を参照してください。
- DAI をイネーブルにする VLAN を設定する必要があります。『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。
- **hardware access-list tcam region arp-ether** コマンドを使用して、DAI 用の ACL TCAM のリージョン サイズを設定する必要があります。arp-ether リージョンが有効でない限り、DAI 設定は受け入れられません。「ACL TCAM リージョン サイズの設定」を参照してください。

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。
- 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、およびポート チャネル 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、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 はサポートされていません。
- Cisco NX-OS リリース 9.3(3) 以降、DAI は Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチでサポートされています。

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。

Table 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。
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。

始める前に

DHCP 機能がイネーブルにされていることを確認します。

DAI をイネーブルにする VLAN が設定されていることを確認します。

DAI（arp-ether）の ACL TCAM リージョン サイズが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：	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。

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	
ステップ 2	[**no**] **ip arp inspection vlan** *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。
ステップ 3	（任意） **show ip arp inspection vlan** *vlan-id* 例： `switch(config)# show ip arp inspection vlan 13`	特定の VLAN の DAI 設定を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `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。

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。

Before you begin

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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。

	Command or Action	Purpose

ステップ 2	**interface** *type port/slot*
	Example:
	`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。

ステップ 3	[**no**] **ip arp inspection trust** **Example:** `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	(Optional) **show ip arp inspection interface** *type port/slot* **Example:** `switch(config-if)# show ip arp inspection interface ethernet 2/1`	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	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# 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。

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 つめの **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 つめ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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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	[] {[] [] []} **noip arp inspection validatesrc-macdst-macip** **Example:** `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。このコマンドの **no** 形式を使用すると、追加の DAI 検証がディセーブルになります。
ステップ 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	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	(Optional) **copy running-config startup-config** **Example:** `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。

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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* **Example:** `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	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	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	(Optional) **copy running-config startup-config** **Example:** `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。

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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** *vlan-list* **logging dhcp-bindings** {**all** | **none** | **permit**} **Example:**	次のようにして、DAI ログ フィルタリングを設定します。このコマンドの **no**

	Command or Action	Purpose
	`switch(config)# ip arp inspection vlan 100 dhcp-bindings permit`	形式を使用すると、DAI ログ フィルタリングは削除されます。 • **all**：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。 • **none**：DHCP バインディングに一致するパケットを記録しません。 • **permit**：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。
ステップ 3	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	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	(Optional) **copy running-config startup-config** **Example:** `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。

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 interfaces [**ethernet** *slot/port* | **port-channel** *number*]	特定のインターフェイスまたはポートチャネルの信頼状態および ARP パケット レートを表示します。
show ip arp inspection log	DAI のログ設定を表示します。
show ip arp inspection vlan *vlan-id*	特定の VLAN の DAI 設定を表示します。
show running-config dhcp [**all**]	DAI の設定を表示します。

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。

コマンド	目的
show ip arp inspection statistics [**vlan** *vlan-id*]	DAI の統計情報を表示します。
clear ip arp inspection statistics vlan *vlan-id*	DAI 統計情報をクリアします。
clear ip arp inspection log	DAI ログを消去します。

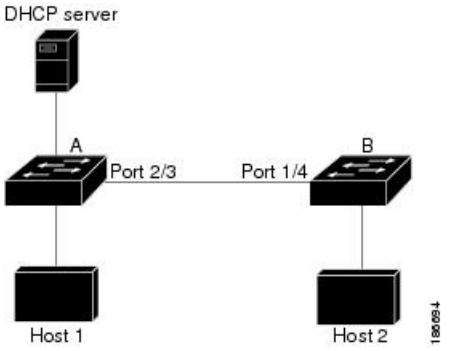
DAI の設定例

DAI ??????? 2 ??????

2 ??????? DAI ?????????? DAI ?????????????

Figure 3: DAI ??????? 2 ??????

???????????????????????????? 1 ????? A ????? 2 ????? B ???????????????????????????????????? VLAN 1 ? DAI ?????????DHCP ???????? A ???????????????????? DHCP ????? IP ?????????????? A ???? 1 ?????? 2 ???????????????? B ???? 2 ????????????????? A ??????? ???????? 2/3 ?????? B ??????? ???????? 1/4 ??????????



DAI ????? ARP ????? ARP ???? IP ????? MAC ??????????????DHCP ?????? ??????? ??????????????????????IP ?????????????? ARP ???????????DHCP ????????????????????

- ??????DHCP ???????? A ???????????????????
- ???????????????????????????????? A ??????? ???????? 2/3???????? B ??????? ???????? 1/4 ????????????????????????

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。

Procedure

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# configure terminal
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 Jan 23 2015])
```

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。

Procedure

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# configure terminal
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 Jan 23 2015])
```

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#
```

DAI に関する追加情報

関連資料

関連項目	マニュアル タイトル
ACL TCAM リージョン	IP ACL の設定
『DHCP and DHCP snooping』	DHCP の設定

標準

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

標準