



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, on page 1](#)
- [DAIの前提条件, on page 6](#)
- [DAIの注意事項と制約事項 \(6 ページ\)](#)
- [DAIのDHCP リレーの注意事項と制約事項 \(7 ページ\)](#)
- [DAIのデフォルト設定, on page 7](#)
- [DAIの設定, on page 8](#)
- [DAIの設定の確認, on page 14](#)
- [DAIの統計情報のモニタリングとクリア, on page 14](#)
- [DAIの設定例, on page 14](#)
- [DHCP リレーの DAI の例, on page 19](#)
- [DAIに関する追加情報, on page 20](#)

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。

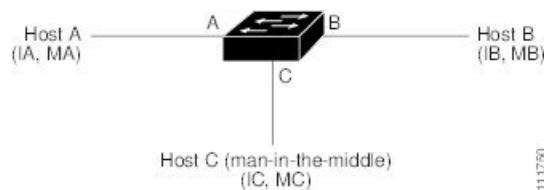
ARP スプーフィング攻撃

ARP では、たとえ ARP 要求を受信していないくとも、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イフィックは、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イフィックの代行受信も可能です。

Figure 1: ARP キャッシュ ポイズニング

次の図に、ARP キャッシュ ポイズニングの例を示します。



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。ホスト B が ARP 要求を受信すると、ホスト B の ARP キャッシュに IP アドレス IA と MAC アドレス MA を持つホストの ARP バインディングが設定されます。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 が応答し、応答がホスト A に到達すると、ホスト A の ARP キャッシュに、IP アドレス IB と MAC アドレス MB を持つホストの ARP バインディングが設定されます。要求と応答の両方がローカル IP アドレスを宛先としているため、その間のデバイスは ARP キャッシュに入力されません。

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、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 は、IA を宛先とするトライフィックの宛先 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 がこのトライ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 は、IB に送られるはずのトライフィックの宛先 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、代行受信したトライ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。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。

Untrusted

ホストに接続されているインターフェイス

Trusted

デバイスに接続されているインターフェイス

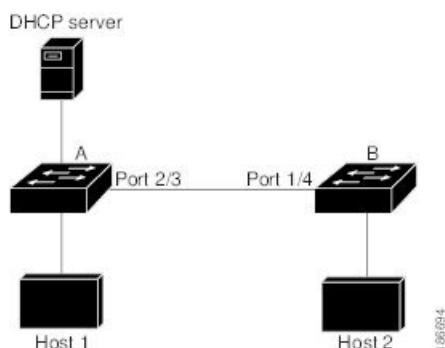
この設定では、デバイスからネットワークに送信される ARP パケットはすべて、セキュリティ検査をバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。

**Caution**

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。

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

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 アドレスをバインディングします。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。



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 を実行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。

**Note**

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 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。

ダイナミック ARP インスペクションを使用した DHCP リレー

DAI は、DHCP スヌーピング クライアント バインディング データベースを使用して ARP パケットを検証します。Cisco NX-OS リリース 10.1(1)よりも前のリリースでは、このデータベースはスイッチで実行される DHCP スヌーピング プロセスによって構築されていました。スイッチが DHCP リレーとして動作する場合、バインディング データベースは構築されません。スヌーピング、DHCP リレー、および DAI を同時にイネーブルにすると、着信 DHCP パケットを処理するために、リレープロセスがスヌーピングよりも優先されます。したがって、スヌーピングはバインディング データベースを構築しません。DAI はバインディング データベースに依存しているため、DHCP リレーでは動作できません。ただし、Cisco NX-OS リリース 10.1(1) 以降では、DHCP リレー DAI を使用してバインディング データベースを構築できます。

スイッチが DHCP 要求を受信すると、クライアントの MAC アドレス、VLAN、および着信インターフェイスで構成される一時バインディング エントリが作成されます。サーバから DHCPACK を受信すると、バインディング エントリが修飾されます。提供された IP アドレスが限定一時エントリに追加され、バインディング エントリ タイプが `dhcp-relay` として更新されます。

Cisco NX-OS リリース 10.1(1) 以降のリリースにアップグレードし、この機能を有効にすると、ISSU はエラーなしで処理されます。Cisco NX-OS リリース 10.1(1) から以前のリリースにダウングレードする前に、この機能を無効にしてください。

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。『[DHCP の設定](#)』を参照してください。
- DAI を有効にする VLAN を設定する必要があります。『*Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド*』を参照してください。
- **hardware access-list tcam region ipsg** コマンドを使用して、DAI の ACL TCAM 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、またはこの機能が無効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 機能を無効にすると、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 機能が無効になった設定から、DHCP 機能が無効になった設定に変更するために使用する方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 機能を無効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 スヌーピングが無効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 DHCP リレーの注意事項と制約事項

- 次の Cisco Nexus プラットフォーム スイッチは、この機能をサポートしています。
 - Cisco Nexus 9300-FX プラットフォーム スイッチ
 - バインディング データベース エントリはハードウェアに保存されません。
 - バインディング データベースは、すべての VRF に共通です。複数の VRF がある場合は、各 VRF を一意の VLAN にマッピングします。
 - IP ソース ガード (IPSG) はこの機能をサポートしていません。
 - IPv4 エントリだけがバインディング データベースに保存されます。IPv6 はサポートされていません。
 - この機能は vPC をサポートしていません。

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。

DAI の設定

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 の有効化と無効化

VLAN に対して DAI を有効または無効にすることができます。デフォルトでは、DAI はすべての VLAN で無効です。

始める前に

DHCP 機能が有効にされていることを確認します。

DAI を有効にする VLAN が設定されている。

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： 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 <i>vlan-list</i> 例： switch(config)# ip arp inspection vlan 13	VLAN の特定のリストに対して DAI を有効にします。 no オプションを使用すると、指定した VLAN の DAI が無効になります。
ステップ 3	(任意) show ip arp inspection vlan <i>vlan-id</i> 例： switch(config)# show ip arp inspection vlan 13	特定の VLAN の DAI 設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	(任意) copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	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 を有効にする場合は、DHCP 機能が有効であることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal</pre> <pre>switch(config)#</pre>	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 type port/slot Example: <pre>switch(config)# interface ethernet 2/1</pre> <pre>switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	[no] ip arp inspection trust Example: <pre>switch(config-if)# ip arp inspection trust</pre>	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。

追加検証の有効化または無効化

	Command or Action	Purpose
ステップ 4	(Optional) show ip arp inspection interface <i>type port/slot</i> Example: <pre>switch(config-if)# show ip arp inspection interface ethernet 2/1</pre>	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: <pre>switch(config-if)# copy running-config startup-config</pre>	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。

追加検証の有効化または無効化

ARP パケットの追加検証を有効または無効にできます。デフォルトでは、ARP パケットの追加検証は有効になりません。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、ARP 送信元 MAC アドレスと ARP 送信者 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、追加検証を有効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。有効にすると、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。有効にすると、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。

追加検証を有効にする場合は、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 検証を有効にし、2つめの **ip arp inspection validate** コマンドで IP 検証を有効にした場合は、2つめのコマンドを入力した時点で src-mac と dst-mac の検証が無効になります。

Procedure

	Command or Action	Purpose
ステップ1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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]} Example: <pre>switch(config)# ip arp inspection validate src-mac dst-mac ip</pre>	追加の DAI 検証を有効にします。このコマンドの no 形式を使用すると、DAI の厳密な検証が無効になります。
ステップ3	(Optional) show running-config dhcp Example: <pre>switch(config)# show running-config dhcp</pre>	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: <pre>switch(config)# copy running-config startup-config</pre>	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: <pre>switch# configure terminal switch(config)#</pre>	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

DAI のログ フィルタリングの設定

	Command or Action	Purpose
ステップ 2	[no] ip arp inspection log-buffer entries <i>number</i> 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 <i>vlan-list</i> logging dhcp-bindings {all none permit} Example: switch(config)# ip arp inspection vlan 100 dhcp-bindings permit	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 形式を使用すると、DAI ログ フィルタリングが削除されます。 <ul style="list-style-type: none"> • all : DHCP バインディングと一致するすべてのパケットをロギングします。 • 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。

	Command or Action	Purpose
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 を使用した DHCP リレーの有効化

DHCP リレーと DAI が有効になっている場合は、バインディングデータベースを作成できます。この機能は、デフォルトで無効にされています。

Before you begin

DAI および DHCP リレーを有効にします。DHCP スヌーピングをグローバルおよび VLAN で有効にします。詳細については、「*DHCP の設定*」の章を参照してください。

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	ip dhcp relay dai Example: switch(config)# ip dhcp relay dai	リレーでのバインディングデータベースの作成を有効にします。
ステップ 3	(Optional) show ip dhcp snooping binding relay Example: switch(config)# show ip dhcp snooping binding relay	dhcp-relay タイプのバインディングエントリを表示します。
ステップ 4	(Optional) show system internal dhcp database global config Example: switch(config)# show system internal dhcp database global config	リレー DAI 機能が有効かどうかを表示します。

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 ログをクリアします。

DAI の設定例

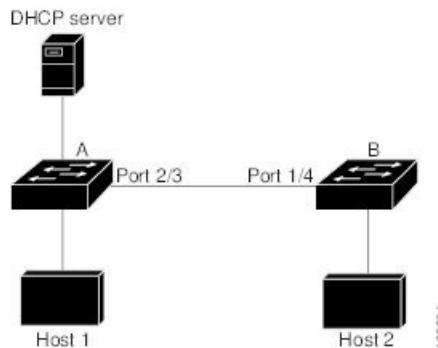
DAI をサポートする 2 つのデバイス

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。

Figure 3: DAI をサポートする 2 つのデバイス

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。



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。

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

```

■ デバイス A の設定

```

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.([0002.0002.0002/10.0.0.3/0000.0000/0.0.0.0/02:42:35 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
```

■ デバイス B の設定

```
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#
```

```
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#
```

DHCP リレーの DAI の例

次の例では、DHCP リレー DAI 機能がイネーブルかどうかを示します。この機能が有効でない場合、データベースの **DHCP Relay DAI enabled** エントリの値は **No** になっています。

```
switch(config)# show system internal dhcp database global config

Snooping enabled: Yes
Snoop option-82 enabled: No
Relay enabled: Yes
.
.
DHCP Relay DAI enabled : No
Validate source mac: No
Validate destination mac: No
```

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 の構成
『DHCP and DHCP snooping』	DHCP の設定

標準

標準	タイトル
RFC-826	イーサネットアドレス解決プロトコル (https://datatracker.ietf.org/doc/html/rfc826)

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。