CHAPTER 13

Dynamic ARP Inspection の設定

この章では、Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）Inspection（DAI; ダイナミック ARP 検査）の設定方法について説明します。

この章は、次の内容で構成されています。

DAI の概要

ここでは、次の内容について説明します。

ARP について

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。ブロードキャスト ドメイン内の全ホストはこの ARP 要求を受信し、これに対してホスト A は自身の MAC アドレスを返します。

ARP スプーフィング攻撃について

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。図 13-1 に、ARP キャッシュ ポイズニングの例を示します。

図 13-1　ARP キャッシュ ポイズニング

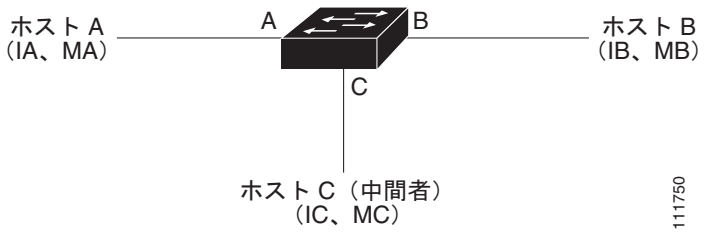


図 13-1 では、ホスト A、B、C はインターフェイス A、B、C を介してデバイスに接続されており、これらのインターフェイスはすべて同じサブネット上にあります。カッコ内は、各ホストの IP アドレスと MAC アドレスを示します。たとえば、ホスト A は IP アドレス IA と MAC アドレス MA を使用します。

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ので、代行受信したトラフィックを転送できます。

DAI と ARP スプーフィングについて

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 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。信頼できるインターフェイスの詳細については、「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」（P.13-3）を参照してください。

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。詳細については、「ARP パケットの検証」（P.13-14）を参照してください。

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（Untrusted）：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（Trusted）：デバイスに接続されているインターフェイス

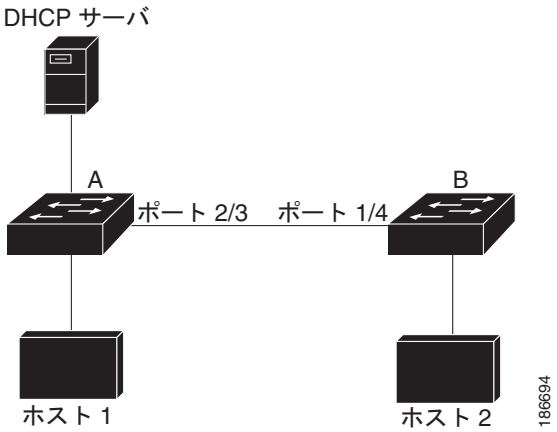
  パケットは、DAI による検証をすべてバイパスします。

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。信頼できるインターフェイスの設定方法については、「信頼できる vEthernet インターフェイスの設定」（P.13-7）を参照してください。

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。

図 13-2 では、デバイス A とデバイス B の両方が VLAN に対して DAI を実行しているとします。この VLAN には、ホスト 1 とホスト 2 が含まれています。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 13-2　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 が稼動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 が稼動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

DAI を設定するための前提条件を次に示します。

- 次の機能を理解している。
  - ARP

    詳細については、IETF 標準 RFC-826『*An Ethernet Address Resolution Protocol*』（http://tools.ietf.org/html/rfc826）を参照してください。
  - DHCP スヌーピング

    詳細については、「DHCP スヌーピングの設定」（P.12-1）を参照してください。
- Cisco Nexus 1000V 上で稼動しているソフトウェアが DAI をサポートしている。
- 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。

  VEM 機能レベルの設定方法については、『*Cisco Nexus 1000V Software Upgrade Guide, Release 4.2(1)SV1(4b)*』を参照してください。

注意事項および制約事項

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。
- 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。詳細については、「DHCP スヌーピングの設定」（P.12-4）を参照してください。
- 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。詳細については、「DHCP スヌーピングの設定」（P.12-4）を参照してください。
- 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。

デフォルト設定

表 13-1 に、DAI のデフォルトを示します。

表 13-1　デフォルトの DAI 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	信頼できない
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 errdisable ステート インターフェイスの検出と回復	errdisable ステート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 の設定

ここでは、次の内容について説明します。

DAI 対象の VLAN の設定

ここでは、1 つまたは複数の VLAN を DAI 対象として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、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、VLAN は DAI の対象としては設定されません。
- DHCP スヌーピングがイネーブルになっている必要があります。詳細については、「DHCP 機能のイネーブル化またはディセーブル化」（P.12-5）を参照してください。
- どの VLAN を DAI の対象として設定するかがわかっており、その VLAN が作成済みであることが必要です。

手順の概要

1. **config t**
2. **[no] ip arp inspection vlan** *list*
3. **show ip arp inspection vlan** *list*
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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 arp inspection vlan** *list* **Example:** `switch(config)# ip arp inspection vlan 13`	指定した 1 つ以上の VLAN を DAI の対象として設定します。

	コマンド	目的
ステップ 3	**show ip arp inspection vlan** *list* **Example:** `switch(config)# show ip arp inspection vlan 13`	（任意）指定した一連の VLAN の DAI ステータスを表示します。
ステップ 4	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

信頼できる vEthernet インターフェイスの設定

ここでは、信頼できる vEthernet インターフェイス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、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*

   port-profile *profilename*
3. [**no**] **ip arp inspection trust**
4. **show ip arp inspection interface** *type slot/number*

   show port-profile *profilename*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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 vethernet** *interface-number*
	Example:
	`switch(config)# interface vethernet 3`
	`switch(config-if)#`
		指定した vEthernet インターフェイスの CLI 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。

	port-profile *profilename*
	Example:
	`switch(config)# port-profile vm-data`
	`switch(config-port-prof)#`
		指定したポート プロファイルの CLI 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	**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。
	ip arp inspection trust **Example:** `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 4	**show ip arp inspection interface vethernet** *interface-number* **Example:** `switch(config-if)# show ip arp inspection interface vethernet 2`	（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。
	show port-profile *profilename* **Example:** `switch(config)# show port-profile vm-data`	（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 5	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

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

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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*
3. **default ip arp inspection trust**
4. **show ip arp inspection interface** *type slot/number*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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 vethernet** *interface-number*
	Example:
	`switch(config)# interface vethernet 3`
	`switch(config-if)#`
		指定した vEthernet インターフェイスの CLI 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	**default ip arp inspection trust** **Example:** `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	**show ip arp inspection interface vethernet** *interface-number* **Example:** `switch(config-if)# show ip arp inspection interface vethernet 3`	（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** **Example:** `switch(config-if)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

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、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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ことが必要です。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*

   port-profile *profilename*
3. **ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**}
4. **show running-config dhcp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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 vethernet** *interface-number*
	Example:
	`switch(config)# interface vethernet 3`
	`switch(config-if)#`
		指定した vEthernet インターフェイスの CLI 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。

	port-profile *profilename*
	Example:
	`switch(config)# port-profile vm-data`
	`switch(config-port-prof)#`
		指定したポート プロファイルの CLI 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。

	コマンド	目的

ステップ 3	**ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**}
	Example:
	`switch(config-if)# ip arp inspection limit rate 30`
	Example:
	`switch(config-port-prof)# ip arp inspection limit rate 30`
		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。
		• **rate**：指定できる値は 1 ～ 2048 パケット/秒（pps）
		– 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 = 1 秒）
		• **none**：パケット/秒の制限なし

ステップ 4	**show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	（任意）DHCP スヌーピング設定を表示します。DAI の設定も表示されます。
ステップ 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DAI レート制限のデフォルト値へのリセット

ARP 要求および応答のレート制限をデフォルトに設定することで、設定されている値を解除するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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ことが必要です。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*
3. **default ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**}
4. **show running-config dhcp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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 vethernet** *interface-number*
	Example:
	`switch(config)# interface vethernet 3`
	`switch(config-if)#`
		指定した vEthernet インターフェイスの CLI 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	目的
ステップ 3	**default ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**} **Example:** `switch(config-if)# default ip arp inspection limit rate`	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。 • **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 4	**show running-config dhcp** **Example:** `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 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

errdisable ステートのインターフェイスの検出と回復

ここでは、errdisable ステートのインターフェイスの検出と回復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、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、インターフェイスは DAI errdisable 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 errdisable ステート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**

手順の概要

1. **config t**
2. **[no] errdisable detect cause arp-inspection**
3. **[no] errdisable recovery cause arp-inspection**
4. **errdisable recovery interval** *timer-interval*
5. **show running-config | include errdisable**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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	**errdisable detect cause arp-inspection** **Example:** `switch(config)# errdisable detect cause arp-inspection`	ARP インスペクションの結果 errdisable ステート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	**errdisable recovery cause arp-inspection** **Example:** `switch(config)# errdisable recovery cause arp-inspection`	ARP インスペクションの結果 errdisable ステート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	**errdisable recovery interval** *timer-interval* **Example:** `switch(config)# errdisable recovery interval 30`	ARP インスペクションの結果 errdisable 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	**show running-config | include errdisable** **Example:** `switch(config)# show running-config | include errdisable`	（任意）errdisable の設定を表示します。
ステップ 6	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

ARP パケットの検証

ここでは、ARP パケットの検証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、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。

- 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。

手順の概要

1. **config t**
2. [**no**] **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]}
3. **show running-config dhcp**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		CLI 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 arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} **Example:** `switch(config)# 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 • 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	**show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	（任意）DHCP スヌーピング設定を表示します。DAI の設定も表示されます。
ステップ 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DAI の設定の確認

DAI の設定を表示して確認するには、次のコマンドを使用します。

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。

コマンド出力の詳しい説明については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

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	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 統計情報を消去します。

コマンド出力の詳しい説明については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

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の 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。

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。コンフィギュレーションについては、第 12 章「DHCP スヌーピングの設定」を参照してください。

この例の DAI を設定するには、次の手順を使用します。

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

```
n1000v# config t
n1000v(config)# ip arp inspection vlan 1
n1000v(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)#
```

ステップ 2　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。

```
n1000v# 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
n1000v#
```

VM 1 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。

```
n1000v# 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
```

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])
```

この場合に表示される統計情報は次のようになります。

```
n1000v# show ip arp inspection statistics vlan 1
n1000v#

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
n1000v#
```

その他の関連資料

DAI の実装に関する詳細情報については、次の項を参照してください。

- 「関連資料」（P.13-18）
- 「標準」（P.13-18）

関連資料

関連項目	参照先
DHCP スヌーピング	「DHCP スヌーピングの設定」（P.12-1）
DAI および DHCP のコマンド：すべてのコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意事項、例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』

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

表 13-2 に、DAI 機能のリリース履歴を示します。

表 13-2　DAI の機能の履歴

機能名	リリース	機能情報
DAI	4.0(4)SV1(2)	この機能が導入されました。