CHAPTER 15

DAI 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。

この章の内容は次のとおりです。

DAI の概要

ここでは、次の内容について説明します。

ARP の概要

ARP では、IP アドレスを MAC（メディア アクセス制御）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。

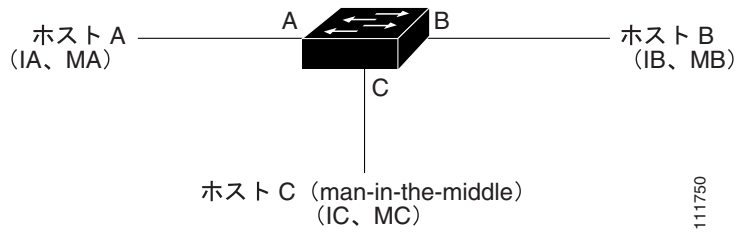
ホスト B は、ホスト A の IP アドレスに関連付けられた MAC アドレスを取得するため、このブロードキャスト ドメイン内の全ホストに対してブロードキャスト メッセージを送信します。ブロードキャスト ドメイン内の全ホストはこの ARP 要求を受信し、これに対してホスト A は自身の MAC アドレスを返します。

ARP スプーフィング攻撃の概要

ARP では、たとえ ARP 要求を受信していなくても、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、攻撃を受けた機器からのすべてのトラフィックは、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フィックの代行受信も可能です。図 15-1 に ARP キャッシュ ポイズニングの例を示します。

図 15-1　ARP キャッシュ ポイズニング



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。すべてのホストが同一サブネットに属します。カッコ内は、各ホストの IP および 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、および 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。デバイスとホスト B はこの ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持つホストの ARP バインディングを、それぞれの ARP キャッシュ内に書き込みます。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 が応答すると、デバイスとホスト A は、IP アドレス IB および MAC アドレス MB を持つホストのバインディングを、それぞれの ARP キャッシュ内に書き込みます。

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、デバイス、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 とデバイスは、IA を宛先とするトラフィックの宛先 MAC アドレスとして、MAC アドレス MC を使用します。同様に、ホスト A とデバイスは、IB を宛先とするトラフィックの宛先 MAC アドレスとして MAC アドレス MC を使用します。

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、*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の概要

DAI を使用することで、有効な ARP 要求および応答だけが中継されることを保証できます。DAI をイネーブルにして適切に設定すると、NX-OS デバイスが次の動作を実行します。

- 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。このデータベースは、VLAN およびデバイス上で DHCP スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。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。信頼できるインターフェイス上で ARP パケットを受信した場合、デバイスはそ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では、デバイスは有効性を確認できたパケットのみを転送します。

DAI では、スタティックに設定した IP アドレスを持つホストに対し、ユーザ定義の ARP Access Control List（ACL; アクセス コントロール リスト）と照合することで ARP パケットを検証できます（「DAI フィルタリングを目的とした ARP ACL の VLAN への適用」[p.15-10] を参照）。デバイスは、ドロップされたパケットを記録します（「DAI パケットのロギング」[p.15-5] を参照）。

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（「追加検証のイネーブル化またはディセーブル化」[p.15-11] を参照）。

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信頼状態を設定します。

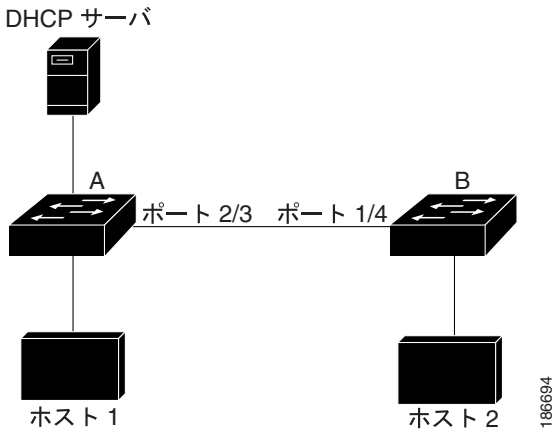
- Untrusted（信頼できない）— ホストに接続されているインターフェイス
- Trusted（信頼できる）— デバイスに接続されているインターフェイス

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。インターフェイスの信頼状態の設定については、「レイヤ 2 インターフェイスの DAI 信頼状態の設定」（p.15-9）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 15-2 では、デバイス A とデバイス B は両方とも、ホスト 1 およびホスト 2 を含む VLAN で DAI を実行しています。ホスト 1 とホスト 2 が、デバイス A に接続されている DHCP サーバからそれぞれの IP アドレスを取得する場合、デバイス A がバインドするのはホスト 1 の IP アドレスと MAC アドレスだけです。デバイス A とデバイス B の間のインターフェイスが信頼できない場合、ホスト 1 からの ARP パケットはデバイス B によってドロップされ、ホスト 1 とホスト 2 の間の接続は切断されます。

図 15-2　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。

- Untrusted（信頼できない）— ホスト、または DAI が*稼働していない*デバイスに接続されているインターフェイス
- Trusted（信頼できる）— DAI が*稼働している*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を検証するには、DAI が稼働しているデバイスに ARP ACL を設定します。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。設定の詳細については、「例 2：1 つのデバイスが DAI をサポートする場合」（p.15-20）を参照してください。

（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。

ARP ACL および DHCP スヌーピング エントリのプライオリティ

デフォルトでは、DAI は DAI パケットを、DHCP スヌーピング データベース内の IP-MAC アドレス バインディングと照合することにより、DAI トラフィックをフィルタリングします。

ARP ACL をトラフィックに適用すると、その ARP ACL はデフォルトのフィルタリング動作よりも優先されます。デバイスはまず、ARP パケットを、ユーザが設定した ARP ACL と照合します。ARP ACL が ARP パケットを拒否した場合、DHCP スヌーピング データベースに有効な IP-MAC バインディングがあるかどうかに関係なく、デバイスはそのパケットを拒否します。

（注）　VLAN ACL（VACL）は、ARP ACL と DHCP スヌーピング エントリのどちらよりも優先されます。たとえば、VACL と ARP ACL を VLAN に適用し、VACL が ARP トラフィックに作用するように設定した場合、デバイスは、ARP ACL や DHCP スヌーピングのエントリではなく、VACL に基づいて ARP トラフィックの許可または拒否を判断します。

ARP ACL の設定については、「ARP ACL の設定」（p.15-23）を参照してください。ARP ACL の適用については、「DAI フィルタリングを目的とした ARP ACL の VLAN への適用」（p.15-10）を参照してください。

DAI パケットのロギング

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、送信元および宛先 IP アドレス、送信元および宛先 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、NX-OS 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。設定の詳細については、「DAI のログ フィルタリングの設定」（p.15-13）を参照してください。

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。詳細については、「DAI のログ バッファ サイズの設定」（p.15-13）を参照してください。

（注）　NX-OS は、ログに記録される DAI パケットに関して、システム メッセージを生成します。

バーチャライゼーション サポート

Virtual Device Context（VDC; バーチャル デバイス コンテキスト）で使用される DAI には、次の事項が適用されます。

- IP-MAC アドレス バインディングは各 VDC に固有です。
- ARP ACL は各 VDC に固有です。ある VDC に作成した ACL を別の VDC に使用することはできません。
- ACL が複数の VDC に共有されることはないので、ACL 名は他の VDC に再利用できます。
- システムは、ARP ACL や ルールを VDC 単位では制限しません。

DAI のライセンス要件

この機能のライセンス要件は次の表のとおりです。

製品	ライセンス要件
NX-OS	DAI にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能は、Cisco NX-OS システム イメージにバンドルされており、追加料金なしで利用できます。NX-OS のライセンス スキームに関する詳細は、『*Cisco NX-OS Licensing Guide*』を参照してください。

DAI の前提条件

DAI を設定する前に、次の事項について十分に理解しておく必要があります。

- ARP（アドレス解決プロトコル）
- DHCP スヌーピング

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。
- 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。
- DAI では、受信する ARP 要求および ARP 応答内の IP および MAC アドレス 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のにスタティック 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、DHCP スヌーピングの設定はイネーブルにするだけで済みます。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。設定の詳細については、「DHCP スヌーピングの設定」（p.14-7）を参照してください。
- DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可および拒否を行う必要があります。
- 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、およびプライベート VLAN 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す。
- 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。
- 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 スヌーピング機能がイネーブルになっていること、およびスタティック IP-MAC アドレス バインディングが設定されていることを確認します。設定の詳細については、「DHCP スヌーピングの設定」（p.14-7）を参照してください。
- 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（「DHCP スヌーピングの設定」[p.14-7] を参照）。

DAI の設定

ここでは、次の内容について説明します。

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。

作業を開始する前に

デフォルトでは、DAI はすべての VLAN でディセーブルです。

DAI をイネーブルにする場合は、次の点を確認してください。

- DHCP スヌーピングがイネーブルになっている。詳細については、「DHCP スヌーピング機能のイネーブル化またはディセーブル化」（p.14-8）を参照してください。
- DAI をイネーブルにする VLAN が設定されている。

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**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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** *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	**show ip arp inspection vlan** *list* **例：** `switch(config)# show ip arp inspection vlan 13`	（任意）VLAN の特定リストの DAI ステータスを表示します。

	コマンド	目的
ステップ 4	**copy running-config startup-config** **例：** `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。

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。詳細については、「DAI のログ フィルタリングの設定」（p.15-13）を参照してください。

作業を開始する前に

デフォルトでは、すべてのインターフェイスは信頼できない（untrusted）状態です。

DAI をイネーブルにする場合は、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。詳細については、「DHCP スヌーピング機能のイネーブル化またはディセーブル化」（p.14-8）を参照してください。

手順の概要

1. **config t**
2. **interface** *type slot/number*
3. **[no] ip arp inspection trust**
4. **show ip arp inspection interface** *type slot/number*
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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	**interface** *type slot/number*
	例：
	`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** **例：** `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。

	コマンド	目的
ステップ 4	**show ip arp inspection interface** *type slot/number* **例：** `switch(config-if)# show ip arp inspection interface ethernet 2/1`	（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** **例：** `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。

DAI フィルタリングを目的とした ARP ACL の VLAN への適用

1 つまたは複数の VLAN に ARP ACL を適用できます。デバイスがパケットを許可するのは、ACL がそのパケットを許可する場合だけです。

作業を開始する前に

デフォルトでは、どの VLAN にも ARP ACL は適用されません。

適用したい ARP ACL が正しく設定されていることを確認します。ARP ACL の設定については、「ARP ACL の設定」（p.15-23）を参照してください。

手順の概要

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

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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 filter** *acl-name* **vlan** *list* **例：** `switch(config)# ip arp inspection filter arp-acl-01 vlan 100`	ARP ACL を VLAN のリストに適用します。あるいは、**no** オプションを使用して ARP ACL を VLAN のリストから削除します。
ステップ 3	**show ip arp inspection vlan** *list* **例：** `switch(config)# show ip arp inspection vlan 100`	（任意）特定の VLAN リストの DAI ステータスを表示します（ARP ACL が適用されているかどうかも含む）。
ステップ 4	**copy running-config startup-config** **例：** `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。

DAI Error-Disabled 回復のイネーブル化またはディセーブル化

デバイスの DAI error-disabled 回復をイネーブルまたはディセーブルに設定できます。

作業を開始する前に

デフォルトでは、DAI error-disabled 回復はディセーブルです。

手順の概要

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

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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*] **errdisable recovery cause arp-inspection** **例**： `switch(config)# errdisable recovery cause arp-inspection`	DAI の error-disabled 回復をイネーブルにします。**no** オプションを使用すると、DAI error-disabled 回復がディセーブルになります。
ステップ 3	**show running-config | include errdisable** **例**： `switch(config)# show running-config | include errdisable`	（任意）errdisable の設定を表示します。
ステップ 4	**copy running-config startup-config** **例**： `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。

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。

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、ログ記録、およびドロップします。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。

作業を開始する前に

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。

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**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例**： switch# config t 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 validate** {[***src-mac***] [***dst-mac***] [***ip***]} **例**： 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。あるいは、**no** オプションを使用して、追加の DAI 検証をディセーブルにします。
ステップ 3	**show running-config dhcp** **例**： 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	**copy running-config startup-config** **例**： 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。

追加検証では、以下を実行します。

- **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、ドロップされます。
- **ip —** ARP 本体を検査し、無効かつ予期されない IP アドレスの有無を確認します。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。送信者 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、ターゲット IP アドレスは ARP 応答内のみで検査されます。
- **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、ドロップされます。

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** コマンドは、それまでに指定したコマンドの設定を上書きします。**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 検証のみ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。

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。

作業を開始する前に

デフォルトのバッファ サイズは 32 メッセージです。

手順の概要

1. **config t**
2. [*no*] **ip arp inspection log-buffer entries** *number*
3. **show running-config dhcp**
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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* **例**： `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、0 ～ 2048 メッセージです。
ステップ 3	**show running-config dhcp** **例**： `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	**copy running-config startup-config** **例**： `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。

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。

作業を開始する前に

デフォルトでは、デバイスはドロップされる DAI パケットを記録します。

手順の概要

1. **config t**
2. [*no*] **ip arp inspection vlan** *vlan-list* ***logging dhcp-bindings*** {***all*** | ***none*** | ***permit***}
3. **show running-config dhcp**
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例**： switch# config t 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***} **例**： switch(config)# ip arp inspection vlan 100 dhcp-bindings permit	DAI ログ フィルタリングを設定します。**no** オプションを使用すると、DAI ログ フィルタリングが削除されます。
ステップ 3	**show running-config dhcp** **例**： 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	**copy running-config startup-config** **例**： 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。

DAI のログ フィルタリングを設定する場合は、次の点に注意してください。

- デフォルトでは、拒否されたすべてのパケットがログ記録されます。
- **dhcp-bindings all —** DHCP バインディングと一致したすべてのパケットがログ記録されます。
- **dhcp-bindings none —** DHCP バインディングと一致したパケットはログ記録されません。
- **dhcp-bindings permit —** DHCP バインディングによって許可されたパケットがログ記録されます。

DAI の設定の確認

DAI の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config arp	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 ethernet *slot*/***port***	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。
show arp access-lists	ARP ACL を表示します。
show ip arp inspection log	DAI のログ設定を表示します。

これらのコマンドの出力フィールドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

DAI の統計情報の表示とクリア

DAI の統計情報の表示およびクリアには、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 arp ethernet *slot*/*port* **statistics**	インターフェイス固有の DAI の統計情報を表示します。
clear ip arp inspection statistics	DAI の統計情報をクリアします。

これらのコマンドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

DAI の設定例

ここでは、次の例を取り上げます。

例 1：2 つのデバイスが DAI をサポートする場合

2 つのデバイスがこの機能をサポートする場合の DAI の設定手順を示します。図 15-2（p.15-4）に示すように、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。両方のデバイスは、これらのホストが置かれている VLAN 1 上で 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。

（注）

- DAI では、受信する ARP 要求および ARP 応答内の IP および MAC アドレス 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。詳細については、第 14 章「DHCP スヌーピングの設定」を参照してください。
- 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。

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# config t
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 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。

```
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。

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# config t
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。

```
witchB# 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 Jun 13 2008])
switchB#
```

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#
```

例 2：1 つのデバイスが DAI をサポートする場合

ここでは、図 15-2（p.15-4）のように、デバイス B が、DAI も DHCP スヌーピングもサポートしていない場合の DAI の設定方法を示します。

デバイス B が DAI も DHCP スヌーピングもサポートしていない場合は、デバイス A のイーサネット 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と、セキュリティ ホールが生じます。これは、デバイス A およびホスト 1 が、デバイス B またはホスト 2 によって攻撃される可能性があるためです。

この可能性を排除するには、デバイス A のイーサネット インターフェイス 2/3 を信頼できないインターフェイスとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない場合は、デバイス A に ACL を適切に設定できなくなるため、レイヤ 3 でデバイス B からデバイス A を切り離す必要があります。これらのスイッチ間では、ルータを使用してパケットをルーティングします。

デバイス A に対して ARP ACL をセットアップするには、次の作業を行います。

ステップ 1　IP アドレス 10.0.0.1 および MAC アドレス 0001.0001.0001 を許可するアクセス リストを設定して、設定内容を確認します。

```
switchA# config t
switchA(config)# arp access-list H2
switchA(config-arp-acl)# permit ip host 10.0.0.1 mac host 0001.0001.0001
switchA(config-arp-acl)# exit
switchA(config)# show arp access-lists H2

ARP access list H2
10 permit ip host 1.1.1.1 mac host 0001.0001.0001
switchA(config)#
```

ステップ 2　VLAN 1 に ACL を適用して、設定を確認します。

```
switchA(config)# ip arp inspection filter H2 vlan 1
switchA(config)# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan : 200
-----------
Configuration    : Enabled
Operation State  : Active
ACL Match/Static : H2 / No
```

ステップ 3　イーサネット インターフェイス 2/3 を信頼できないインターフェイスとして設定し、設定内容を確認します。

（注）　デフォルトでは、ポートは信頼できない状態（untrusted）になります。

```
switchA(config)# interface ethernet 2/3
switchA(config-if)# no ip arp inspection trust
switchA(config-if)# exit
switchA# show ip arp inspection interface ethernet 2/3
switchA#
```

このインターフェイスはデフォルトの設定であり、信頼できない状態になっているので、**show ip arp inspection interface** コマンドでは出力は表示されません。

ホスト 2 がデバイス A のイーサネット インターフェイス 2/3 から 5 つの ARP 要求を送信し、1 つの get 要求がデバイス A によって許可された場合、統計情報は次のようにアップデートされます。

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

Vlan : 1
-----------
ARP Req Forwarded  = 5
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#
```

ARP ACL の設定

ここでは、次の内容について説明します。

Session Manager のサポート

Session Manager は ARP ACL の設定をサポートしています。この機能を使用すると、設定セッションを作成し、ARP ACL の設定変更を実行コンフィギュレーションにコミットする前に確認できます。Session Manager についての詳細は、『*Cisco NX-OS System Management Guide*』を参照してください。

ARP ACL の作成

デバイスに ARP ACL を作成し、これにルールを追加できます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **config t**
2. **arp access-list** *name*
3. [*sequence-number*] {**permit** | **deny**} **ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

   [*sequence-number*] {**permit** | **deny**} **request ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

   [*sequence-number*] {**permit** | **deny**} **response ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} {**any** | **host** *target-IP* | *target-IP target-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**any** | **host** *target-MAC* | *target-MAC target-MAC-mask*] [**log**]
4. **show arp access-lists** *acl-name*
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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	**arp access-list** *name* **例：** switch(config)# arp access-list arp-acl-01 switch(config-arp-acl)#	ARP ACL を作成し、ARP ACL 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	[*sequence-number*] {**permit** | **deny**} **ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**] **例：** switch(config-arp-acl)# permit ip 192.168.2.0 0.0.0.255 mac 00C0.4F00.0000 ffff.ff00.0000	メッセージ送信者の IP アドレスおよび MAC アドレスに基づいて、ARP メッセージを許可または拒否するルールを作成します。シーケンス番号を使用すると、ACL 内のルールの位置を指定できます。シーケンス番号を使用しないと、ルールの最後に追加されます。
	[*sequence-number*] {**permit** | **deny**} **request ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**] **例：** switch(config-arp-acl)# permit request ip 192.168.102.0 0.0.0.255 mac any	メッセージ送信者の IP アドレスおよび MAC アドレスに基づいて、ARP 要求メッセージを許可または拒否するルールを作成します。シーケンス番号を使用すると、ACL 内のルールの位置を指定できます。シーケンス番号を使用しないと、ルールの最後に追加されます。
	[*sequence-number*] {**permit** | **deny**} **response ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} [**any** | **host** *target-IP* | *target-IP target-IP-mask*]] **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**any** | **host** *target-MAC* | *target-MAC target-MAC-mask*] [**log**] **例：** switch(config-arp-acl)# permit response ip host 192.168.202.32 any mac host 00C0.4FA9.BCF3 any	メッセージの送信者およびターゲットの IP アドレスおよび MAC アドレスに基づいて、ARP 応答メッセージを許可または拒否するルールを作成します。シーケンス番号を使用すると、ACL 内のルールの位置を指定できます。シーケンス番号を使用しないと、ルールの最後に追加されます。
ステップ 4	**show arp access-lists** *acl-name* **例：** switch(config-arp-acl)# show arp access-lists arp-acl-01	（任意）ARP ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** switch(config-arp-acl)# 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。

ARP ACL の変更

既存の ARP ACL のルールの追加および削除を実行できます。既存のルールを変更することはできません。ルールを変更したい場合は、そのルールを削除し、目的の変更を加えたルールを再作成します。

既存のルールの間に、現在のシーケンス番号では許容できない数のルールを追加する必要がある場合は、**resequence** コマンドを使用することにより、シーケンス番号を再割り当てできます。詳細については、「ARP ACL のシーケンス番号の変更」（p.15-26）を参照してください。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **config t**
2. **arp access-list** *name*
3. [*sequence-number*] {**permit | deny**} [**request** | **response**] **ip** *IP-data* **mac** *MAC-data*
4. **no** {*sequence-number* | {**permit | deny**} [**request** | **response**] **ip** *IP-data* **mac** *MAC-data*}
5. **show arp access-lists**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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	**arp access-list** *name*
	
	例：
	`switch(config)# arp access-list arp-acl-01`
	`switch(config-acl)#`
		名前を指定する ACL の ARP ACL 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	[*sequence-number*] {**permit** | **deny**} [**request** | **response**] **ip** *IP-data* **mac** *MAC-data* **例：** `switch(config-arp-acl)# 100 permit request ip 192.168.132.0 0.0.0.255 mac any`	（任意）ルールを作成します。**permit** コマンドおよび **deny** コマンドについての詳細は、「ARP ACL の作成」（p.15-23）を参照してください。 シーケンス番号を使用すると、ACL 内のルールの位置を指定できます。シーケンス番号を使用しないと、ルールの最後に追加されます。
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**} [**request** | **response**] **ip** *IP-data* **mac** *MAC-data* **例：** `switch(config-arp-acl)# no 80`	（任意）指定したルールを ARP ACL から削除します。**permit** コマンドおよび **deny** コマンドについての詳細は、「ARP ACL の作成」（p.15-23）を参照してください。
ステップ 5	**show arp access-lists** **例：** `switch(config-arp-acl)# show arp access-lists`	ARP ACL の設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config-arp-acl)# 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。

ARP ACL の削除

ARP ACL をデバイスから削除できます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

その ACL が VLAN に適用されているかどうかを確認します。削除できるのは、現在 適用されている ACL です。ACL を削除しても、その ACL が適用されている VLAN の設定には影響しません。デバイスは削除された ACL を空であるとみなします。

手順の概要

1. **config t**
2. **no arp access-list** *name*
3. **show arp access-lists**
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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 arp access-list** *name* **例：** `switch(config)# no arp access-list arp-acl-01`	名前を指定した ARP ACL を実行コンフィギュレーションから削除します。
ステップ 3	**show arp access-lists** **例：** `switch(config)# show arp access-lists`	ARP ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** **例：** `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。

ARP ACL のシーケンス番号の変更

ARP ACL 内のルールに割り当てられているすべてのシーケンス番号を変更できます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **config t**
2. **resequence arp access-list** *name starting-sequence-number increment*
3. **show arp access-lists** *name*
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例**： switch# config t 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	**resequence arp access-list** *name starting-sequence-number increment* **例**： switch(config)# resequence arp access-list arp-acl-01 100 10 switch(config)#	ACL 内のルールにシーケンス番号を割り当てます。指定した開始シーケンス番号は最初のルールに割り当てられます。その後ろの各ルールには、前のルールよりも 一定数だけ大きい番号が割り当てられます。番号の差異は、指定した増分によって決まります。
ステップ 3	**show arp access-lists** *name* **例**： switch(config)# show arp access-lists arp-acl-01	*name* に名前を指定した ACL の ARP ACL 設定を表示します。
ステップ 4	**copy running-config startup-config** **例**： 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。

ARP ACL の設定の確認

ARP ACL 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 arp access-lists	ARP ACL の設定を表示します。
show running-config aclmgr	実行コンフィギュレーション内の ACL を表示します。

これらのコマンドの出力フィールドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

デフォルト設定

表 15-1 に DAI パラメータのデフォルトの設定値を示します。

表 15-1　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
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
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、拒否またはドロップされたすべての ARP パケットがログ記録されます。 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	拒否またはドロップされたすべての ARP パケットが記録されます。

その他の参考資料

DAI の実装に関する詳細情報については、次を参照してください。

- 関連資料（p.15-28）
- 規格（p.15-28）

関連資料

関連事項	タイトル
DHCP スヌーピング	DHCP スヌーピングの概要（p.14-2）
DAI コマンド：完全なコマンド構文、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、例	『*Cisco NX-OS Security Command Reference*』
DHCP スヌーピングのコマンド：完全なコマンド構文、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、例	『*Cisco NX-OS Security Command Reference*』

規格

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