



## DAI の設定

この章では、Catalyst 4500 シリーズ スイッチ上で Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション) を設定する方法について説明します。

この章の主な内容は、次のとおりです。

- 「DAI の概要」 (P.46-1)
- 「DAI の設定」 (P.46-5)



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

<http://www.cisco.com/en/US/products/ps6350/index.html>

## DAI の概要

DAI は、ネットワークの Address Resolution Protocol (ARP; アドレス解決プロトコル) パケットを確認するセキュリティ機能です。DAI によって、ネットワーク管理者は、無効な Media Access Control (MAC; メディア アクセス制御) /IP アドレスのペアを持つ ARP パケットを代行受信、記録、およびドロップすることができます。この機能は、特定の "man-in-the-middle" 攻撃からネットワークを保護します。

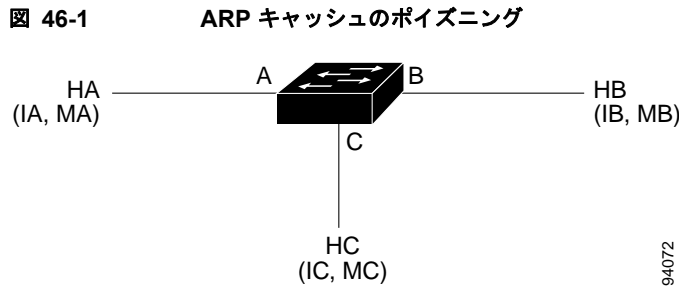
ここでは、次の内容について説明します。

- 「ARP キャッシュのポイズニング」 (P.46-2)
- 「DAI の目的」 (P.46-2)
- 「インターフェイスの信頼状態、セキュリティ適用範囲、およびネットワークの構成」 (P.46-3)
- 「スタティック バインディング DHCP スヌーピングのエントリの相対的なプライオリティ」 (P.46-4)
- 「ドロップされたパケットのロギング」 (P.46-4)
- 「ARP パケットのレート制限」 (P.46-4)
- 「ポート チャネルとその動作」 (P.46-5)

## ARP キャッシュのポイズニング

ARP キャッシュを「ポイズニング (汚染)」することによって、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を攻撃できます。たとえば、悪意のあるユーザが、サブネットに接続されたシステムの ARP キャッシュをポイズニングすることによって、サブネットの他のホストに向けられたトラフィックを代行受信する可能性があります。

次の構成を考えてみます。



ホスト HA、HB、HC は、スイッチのインターフェイス A、B、C に接続されており、すべてが同一のサブネット上にあります。それぞれの IP アドレスと MAC アドレスは、カッコ内に表示されています。たとえば、ホスト HA は、IP アドレス IA と MAC アドレス MA を使用します。HA が IP レイヤの HB と通信する必要がある場合、HA は IB に対応付けられた MAC アドレスの ARP 要求をブロードキャストします。HB が ARP 要求を受信するとすぐに、HB の ARP キャッシュに、IP アドレス IA および MAC アドレス MA を持つホストの ARP バインディングが入力されます。HB が HA に応答すると、HA の ARP キャッシュに IP アドレス IB と MAC アドレス MB を持つホストのバインディングが入力されます。

ホスト HC は、IP アドレス IA (または IB) と MAC アドレス (MC) のホストのバインディングを持つ偽造された ARP 応答をブロードキャストすることによって、HA と HB の ARP キャッシュを「ポイズニング」できます。ポイズニングされた ARP キャッシュを持つホストは、IA または IB に向けられた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。つまり、HC はこのトラフィックを代行受信します。HC は IA と IB に対応付けられた正しい 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れらのホストに代行受信されたトラフィックを転送できます。HC は、HA から HB へのトラフィック ストリームに自分自身を割り込ませたことになりません。これは典型的な "man in the middle" 攻撃です。

## DAI の目的

ARP のポイズニング攻撃を防止するには、スイッチは有効な ARP 要求および応答だけがリレーされることを確認する必要があります。DAI は、すべての ARP 要求と応答を代行受信することによってこれらの攻撃を防ぎます。代行受信された各パケットは、ローカル ARP キャッシュが更新される前、またはパケットが適切な宛先に転送される前に、有効な MAC/IP アドレスのバインディングと照合されます。無効な ARP パケットはドロップされます。

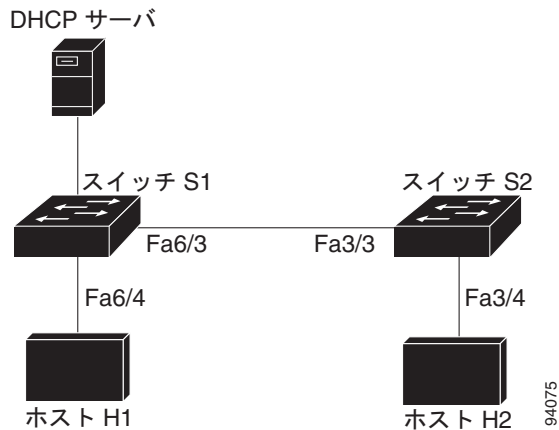
DAI は、ARP パケットの有効性を、信頼性のあるデータベースに格納された有効な MAC/IP アドレスのバインディングに基づいて判別します。このデータベースは、Dynamic Host Configuration Protocol (DHCP) スヌーピングが Virtual LAN (VLAN; 仮想 LAN) および該当するスイッチでイネーブルにされている場合に、DHCP スヌーピングの実行時に作成されます。さらに、DAI は、静的に設定された IP アドレスを使用するホストを処理するために、ユーザが設定した ARP Access Control List (ACL; アクセス コントロール リスト) と ARP パケットを照合できます。

パケットの IP アドレスが無効である場合、または ARP パケットの本体にある 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ように DAI を設定することもできます。

## インターフェイスの信頼状態、セキュリティ適用範囲、およびネットワークの構成

DAI は、システム上の各インターフェイスに信頼状態を対応付けます。信頼できるインターフェイスに着信するパケットは、すべての DAI 確認検査を迂回します。信頼できないインターフェイスに着信するパケットは、DAI 確認処理を受けます。DAI の一般的なネットワーク構成では、ホスト ポートに接続されたすべてのポートは、**untrusted**（信頼できない）に設定されます。スイッチに接続されたすべてのポートは、**trusted**（信頼できる）に設定されています。この設定では、所定のスイッチからネットワークに入ったすべての ARP パケットはセキュリティチェックを通過します。

図 46-2 DAI 対応 VLAN における ARP パケットの確認



信頼状態の設定には、注意が必要です。**trusted** にする必要がある場合に、**untrusted** にインターフェイスを設定すると、接続が失われる可能性があります。S1 と S2（図 46-2 を参照）の両方が、H1 と H2 を保持する VLAN ポート上で DAI を実行していると仮定し、H1 と H2 が S1 に接続された DHCP サーバからの IP アドレスを取得する場合には、S1 だけが IP を H1 の MAC アドレスにバインドします。したがって、S1 と S2 の間のインターフェイスが **untrusted** の場合、H1 からの ARP パケットが S2 でドロップされます。この状態では、H1 と H2 の間の接続が失われます。

実際には **untrusted** の場合に、インターフェイスを **trusted** に設定すると、ネットワークにセキュリティホールが残ります。S1 が DAI を実行していない場合は、H1 は簡単に S2 の ARP（および ISL（スイッチ間リンク））が **trusted** に設定されている場合の H2）をポイズニングできます。この状態は、S2 が DAI を実行していても発生します。

DAI は、DAI を実行するスイッチに接続された（信頼できないインターフェイス上の）ホストが、ネットワークのその他のホストの ARP キャッシュをポイズニングしないようにします。ただし、ネットワークのその他の部分からのホストが、接続されているホストのキャッシュをポイズニングしないとは限りません。

VLAN の一部のスイッチが DAI を実行して、残りのスイッチが DAI を実行しないケースに対処するには、このようなスイッチを接続するインターフェイスを **untrusted** に設定する必要があります。ただし、DAI 非対応スイッチからのパケットのバインディングを確認するには、DAI を実行するスイッチに ARP ACL が設定されている必要があります。このようなバインディングを判別できない場合は、DAI を実行するスイッチを DAI 非対応スイッチからレイヤ 3 で分離する必要があります。



(注)

DHCP サーバおよびネットワークの設定によって、VLAN 内のすべてのスイッチ上で所定の ARP パケットの確認が実行できない場合があります。

## スタティック バインディング DHCP スヌーピングのエントリの相対的なプライオリティ

前述したように、DAI は DHCP スヌーピングを通じて、有効な MAC/IP アドレスのバインディングのデータベースを入力します。また、ARP パケットを静的に設定された ARP ACL と照合します。ここで注意する必要があるのは、ARP ACL が DHCP スヌーピング データベースのエントリより優先されるということです。ARP パケットは最初に、ユーザが設定した ARP ACL と比較されます。ARP ACL が ARP パケットを拒否した場合、DHCP スヌーピングによって入力されたデータベースに有効なバインディングが存在する場合でも、パケットが拒否されます。

## ドロップされたパケットのロギング

スイッチがパケットをドロップすると、ログ バッファにエントリが入力され、次にレート制御単位でシステム メッセージが生成されます。メッセージの生成後、スイッチはログ バッファからエントリをクリアします。各ログ エントリには、フロー情報（受信 VLAN、ポート番号、送信元と宛先 IP アドレス、および送信元と宛先 MAC アドレスなど）が含まれます。

バッファ内のエントリ数およびシステム メッセージを生成するのに指定間隔で必要となるエントリ数を設定するには、**ip arp inspection log-buffer** グローバル コンフィギュレーション コマンドを使用します。記録されるパケット タイプを指定するには、**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドを使用します。詳しい設定手順については、「[ログ バッファの設定](#)」(P.46-14) を参照してください。

## ARP パケットのレート制限

DAI は CPU で確認検査を行うので、DoS 攻撃（サービス拒絶攻撃）を防ぐために着信 ARP パケット数がレート制限されています。デフォルトでは、信頼できないインターフェイスのレートは 15 pps に設定されており、信頼できるインターフェイスにはレート制限がありません。着信 ARP パケットのレートが設定された制限を超える場合は、ポートが **errdisable** ステータスに置かれます。管理者が介入するまで、ポートはそのままの状態です。**errdisable recovery** グローバル コンフィギュレーション コマンドにより、**errdisable** 回復をイネーブルにして、ポートが指定のタイムアウト時間の経過後自動的にこのステータスから回復できるようにします。

インターフェイスに着信する ARP 要求および ARP 応答のレートを制限するには、**ip arp inspection limit** グローバル コンフィギュレーション コマンドを使用します。レート制限がインターフェイス上に明示的に設定されていない限り、インターフェイスの信頼状態を変更すると、その信頼状態のデフォルト値のレート制限に変更されます。つまり、信頼できないインターフェイスは 15 pps で、信頼できるインターフェイスは無制限になります。レート制限が明示的に設定されると、信頼状態が変更されてもインターフェイスはそのレート制限を保持します。**rate limit** コマンドの **no** 形式が適用されると、インターフェイスはいつでもデフォルトのレート制限値に戻ります。詳しい設定手順については、「[着信 ARP パケットのレート制限](#)」(P.46-16) を参照してください。



(注)

DAI がイネーブルの場合、すべての ARP パケットは、CPU によって転送されます（ソフトウェア転送、スローパス）。このメカニズムでは、パケットが複数ポートを介して送信されるたびに、CPU により、出力ポートと同数のパケットのコピーを作成する必要があります。つまり、出力ポート数が CPU の係数ファクタになります。さらに、QoS ポリシングが、CPU によって転送された出力パケット上で適用される場合、QoS は CPU でも適用される必要があります（ハードウェア転送パスは、CPU によって生成されたパケットではオフのため、CPU によって生成されたパケットについて、ハードウェアでは QoS を適用することはできません）。両方のファクタは、CPU の利用率レベルを非常に高くする可能性があります。

## ポート チャネルとその動作

所定の物理ポートは、物理ポートとチャネルの信頼状態が一致した場合にだけチャネルに加入できます。一致しなければ、物理ポートがチャネルで中断されたままの状態になります。チャネルは、チャネルに加入した最初の物理ポートの信頼状態を継承します。そのため、最初の物理ポートの信頼状態は、チャネルの信頼状態に一致する必要がありません。

反対に、信頼状態がチャネル上で変更された場合は、新しい信頼状態がチャネルを構成するすべての物理ポート上に設定されます。

ポート チャネル上のレート制限確認は、他とは異なります。物理ポート上の着信パケットのレートは、物理ポートの設定ではなく、ポート チャネルの設定と比較確認されます。

ポート チャネル上のレート制限設定は、物理ポートの設定に依存しません。

レート制限は、すべての物理ポートで累積されます。つまり、ポート チャネル上の着信パケットのレートは、すべての物理ポートにおけるレートの合計と等しくなります。

トランク上の ARP パケットにレート制限を設定する場合、1 つの VLAN 上の高いレート制限によって、ポートがソフトウェアによって `errdisable` にされたときに、その他の VLAN に "DoS" 攻撃が行われる原因になる可能性がある、VLAN 集約を計上する必要があります。同様に、ポート チャネルが `errdisable` の場合、1 つの物理ポート上の高いレート制限は、チャネル内の他のポートを停止させる原因になります。

## DAI の設定

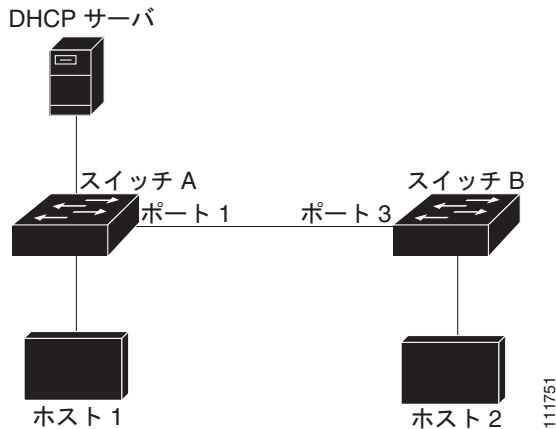
ここでは、スイッチ上で DAI を設定する手順について説明します。

- 「DHCP 環境での DAI の設定」(P.46-6) (必須)
- 「非 DHCP 環境に対する ARP ACL の設定」(P.46-11) (任意)
- 「ログ バッファの設定」(P.46-14) (任意)
- 「着信 ARP パケットのレート制限」(P.46-16) (任意)
- 「確認検査の実行」(P.46-19) (任意)

## DHCP 環境での DAI の設定

次の手順は、2つのスイッチがこの機能をサポートする場合の DAI の設定方法を示しています。ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B に接続されます (図 46-3 を参照)。両方のスイッチは、ホストが存在する VLAN 100 上で DAI を実行しています。DHCP サーバはスイッチ A に接続されます。両方のホストは同じ DHCP サーバから IP アドレスを取得します。つまり、スイッチ A にはホスト 1 のバインディングがあり、スイッチ B にはホスト 2 のバインディングがあります。

図 46-3 DAI がイネーブルな VLAN 上での ARP パケットの確認



(注)

着信 ARP 要求および ARP 応答の IP/MAC アドレス バインディングを確認する場合、DAI は DHCP スヌーピング バインディング データベースのエントリに基づきます。IP アドレスに動的に割り当てられた ARP パケットを許可するために、DHCP スヌーピングがイネーブルであることを確認してください。設定情報については、第 45 章「DHCP スヌーピング、IP ソース ガード、およびスタティック ホストの IPSG の設定」を参照してください。

1 つのスイッチだけが DAI 機能をサポートする場合の DAI の設定方法については、「非 DHCP 環境に対する ARP ACL の設定」(P.46-11) を参照してください。

DAI を設定するには、両方のスイッチ上で次の作業を行います。

|        | コマンド  | 目的   |
|--------|---|--|
| ステップ 1 | Switch# <code>show cdp neighbors</code>                             | スイッチ間の接続を確認します。  |
| ステップ 2 | Switch# <code>configure terminal</code>                             | 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 3 | Switch(config)# <code>[no] ip arp inspection vlan vlan-range</code> | <p>VLAN 単位で DAI をイネーブルにします。デフォルトでは、DAI はすべての VLAN でディセーブルです。</p> <p>DAI をディセーブルにするには、<code>no ip arp inspection vlan vlan-range</code> グローバル コンフィギュレーション コマンドを使用します。</p> <p><code>vlan-range</code> には、VLAN ID 番号で識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定します。指定できる範囲は 1 ~ 4094 です。</p> <p>両方のスイッチに同じ VLAN ID を指定します。</p> |

| コマンド  | 目的  |
|---|---|
| ステップ 4 Switch(config)# <b>interface</b> interface-id  | 他のスイッチに接続されるインターフェイスを指定して、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 5 Switch(config-if)# <b>ip arp inspection trust</b>  | <p>スイッチ間の接続を <b>trusted</b> に設定します。</p> <p>インターフェイスを <b>untrusted</b> ステートに戻すには、<b>no ip arp inspection trust</b> インターフェイス コンフィギュレーション コマンドを使用します。</p> <p>デフォルトでは、すべてのインターフェイスが <b>untrusted</b> です。スイッチは、信頼できるインターフェイス上の他のスイッチから受信した ARP パケットの確認を行いません。単にパケットを転送します。</p> <p>信頼できないインターフェイスの場合、スイッチはすべての ARP 要求と ARP 応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC アドレス バインディングを持つかどうかを検証します。スイッチは、無効なパケットをドロップし、<b>ip arp inspection vlan logging</b> グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログバッファに記録します。詳細については、「<a href="#">ログ バッファの設定</a>」(P.46-14) を参照してください。</p> |
| ステップ 6 Switch(config-if)# <b>end</b>  | 特権 EXEC モードに戻ります。   |
| ステップ 7 Switch# <b>show ip arp inspection interfaces</b><br>Switch# <b>show ip arp inspection vlan</b><br>vlan-range | DAI の設定を確認します。  |
| ステップ 8 Switch# <b>show ip dhcp snooping binding</b>   | DHCP バインディングを確認します。   |
| ステップ 9 Switch# <b>show ip arp inspection statistics</b><br>vlan vlan-range  | DAI の統計情報を確認します。  |
| ステップ 10 Switch# <b>copy running-config startup-config</b>   | (任意) コンフィギュレーション ファイルに設定を保存します。   |

次に、VLAN 100 のスイッチ A 上で DAI を設定する例を示します。スイッチ B でも同様の手順を実行します。

## スイッチ A

```
SwitchA# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID         Local Intrfce   Holdtme    Capability   Platform   Port ID
SwitchB           Gig 3/48        179         R S I        WS-C4506   Gig 3/46

SwitchA# configure terminal
SwitchA(config)# ip arp inspection vlan 100
SwitchA(config)# interface g3/48
SwitchA(config-if)# ip arp inspection trust
SwitchA(config-if)# end
SwitchA# show ip arp inspection interfaces

Interface         Trust State     Rate (pps)     Burst Interval
-----
G11/1             Untrusted      15              1
G11/2             Untrusted      15              1
Gi3/1             Untrusted      15              1
```

```

Gi3/2          Untrusted          15          1
Gi3/3          Untrusted          15          1
Gi3/4          Untrusted          15          1
Gi3/5          Untrusted          15          1
Gi3/6          Untrusted          15          1
Gi3/7          Untrusted          15          1
Gi3/8          Untrusted          15          1
Gi3/9          Untrusted          15          1
Gi3/10         Untrusted          15          1
Gi3/11         Untrusted          15          1
Gi3/12         Untrusted          15          1
Gi3/13         Untrusted          15          1
Gi3/14         Untrusted          15          1
Gi3/15         Untrusted          15          1
Gi3/16         Untrusted          15          1
Gi3/17         Untrusted          15          1
Gi3/18         Untrusted          15          1
Gi3/19         Untrusted          15          1
Gi3/20         Untrusted          15          1
Gi3/21         Untrusted          15          1
Gi3/22         Untrusted          15          1
Gi3/23         Untrusted          15          1
Gi3/24         Untrusted          15          1
Gi3/25         Untrusted          15          1
Gi3/26         Untrusted          15          1
Gi3/27         Untrusted          15          1
Gi3/28         Untrusted          15          1
Gi3/29         Untrusted          15          1
Gi3/30         Untrusted          15          1
Gi3/31         Untrusted          15          1
Gi3/32         Untrusted          15          1
Gi3/33         Untrusted          15          1
Gi3/34         Untrusted          15          1
Gi3/35         Untrusted          15          1
Gi3/36         Untrusted          15          1
Gi3/37         Untrusted          15          1
Gi3/38         Untrusted          15          1
Gi3/39         Untrusted          15          1
Gi3/40         Untrusted          15          1
Gi3/41         Untrusted          15          1
Gi3/42         Untrusted          15          1
Gi3/43         Untrusted          15          1
Gi3/44         Untrusted          15          1
Gi3/45         Untrusted          15          1
Gi3/46         Untrusted          15          1
Gi3/47         Untrusted          15          1
Gi3/48         Trusted           None        N/A

```

```
SwitchA# show ip arp inspection vlan 100
```

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

```

Vlan      Configuration      Operation      ACL Match      Static ACL
----      -
100      Enabled                Active

```

```

Vlan      ACL Logging      DHCP Logging
----      -
100      Deny                Deny

```

```
SwitchA# show ip dhcp snooping binding
```

```

MacAddress      IpAddress      Lease (sec)      Type      VLAN      Interface
-----

```



```
00:01:00:01:00:01 170.1.1.1 3597 dhcp-snooping 100 GigabitEthernet3/27
Total number of bindings: 1
```

```
SwitchA# show ip arp inspection statistics vlan 100
```

| Vlan | Forwarded | Dropped | DHCP Drops | ACL Drops |
|------|-----------|---------|------------|-----------|
| 100  | 15        | 0       | 0          | 0         |

| Vlan | DHCP Permits | ACL Permits | Source MAC Failures |
|------|--------------|-------------|---------------------|
| 100  | 0            | 0           | 0                   |

| Vlan | Dest MAC Failures | IP Validation Failures | Invalid Protocol Data |
|------|-------------------|------------------------|-----------------------|
| 100  | 0                 | 0                      | 0                     |

```
SwitchA#
```

## スイッチ B

```
SwitchB# show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
```

| Device ID | Local Intrfce | Holdtme | Capability | Platform  | Port ID  |
|-----------|---------------|---------|------------|-----------|----------|
| SwitchA   | Gig 3/46      | 163     | R S I      | WS-C4507R | Gig 3/48 |

```
SwitchB#
```

```
SwitchB# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SwitchB(config)# ip arp inspection vlan 100
```

```
SwitchB(config)# interface g3/46
```

```
SwitchB(config-if)# ip arp inspection trust
```

```
SwitchB(config-if)# end
```

```
SwitchB#
```

```
SwitchB# show ip arp inspection interfaces
```

| Interface | Trust State | Rate (pps) | Burst Interval |
|-----------|-------------|------------|----------------|
| Gi1/1     | Untrusted   | 15         | 1              |
| Gi1/2     | Untrusted   | 15         | 1              |
| Gi3/1     | Untrusted   | 15         | 1              |
| Gi3/2     | Untrusted   | 15         | 1              |
| Gi3/3     | Untrusted   | 15         | 1              |
| Gi3/4     | Untrusted   | 15         | 1              |
| Gi3/5     | Untrusted   | 15         | 1              |
| Gi3/6     | Untrusted   | 15         | 1              |
| Gi3/7     | Untrusted   | 15         | 1              |
| Gi3/8     | Untrusted   | 15         | 1              |
| Gi3/9     | Untrusted   | 15         | 1              |
| Gi3/10    | Untrusted   | 15         | 1              |
| Gi3/11    | Untrusted   | 15         | 1              |
| Gi3/12    | Untrusted   | 15         | 1              |
| Gi3/13    | Untrusted   | 15         | 1              |
| Gi3/14    | Untrusted   | 15         | 1              |
| Gi3/15    | Untrusted   | 15         | 1              |
| Gi3/16    | Untrusted   | 15         | 1              |
| Gi3/17    | Untrusted   | 15         | 1              |
| Gi3/18    | Untrusted   | 15         | 1              |
| Gi3/19    | Untrusted   | 15         | 1              |
| Gi3/20    | Untrusted   | 15         | 1              |
| Gi3/21    | Untrusted   | 15         | 1              |
| Gi3/22    | Untrusted   | 15         | 1              |

```

Gi3/23      Untrusted      15      1
Gi3/24      Untrusted      15      1
Gi3/25      Untrusted      15      1
Gi3/26      Untrusted      15      1
Gi3/27      Untrusted      15      1
Gi3/28      Untrusted      15      1
Gi3/29      Untrusted      15      1
Gi3/30      Untrusted      15      1
Gi3/31      Untrusted      15      1
Gi3/32      Untrusted      15      1
Gi3/33      Untrusted      15      1
Gi3/34      Untrusted      15      1
Gi3/35      Untrusted      15      1
Gi3/36      Untrusted      15      1
Gi3/37      Untrusted      15      1
Gi3/38      Untrusted      15      1
Gi3/39      Untrusted      15      1
Gi3/40      Untrusted      15      1
Gi3/41      Untrusted      15      1
Gi3/42      Untrusted      15      1
Gi3/43      Untrusted      15      1
Gi3/44      Untrusted      15      1
Gi3/45      Untrusted      15      1
Gi3/46      Trusted        None     N/A
Gi3/47      Untrusted      15      1
Gi3/48      Untrusted      15      1

```

SwitchB# **show ip arp inspection vlan 100**

```

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

```

| Vlan | Configuration | Operation | ACL Match | Static ACL |
|------|---------------|-----------|-----------|------------|
| 100  | Enabled       | Active    |           |            |

| Vlan | ACL Logging | DHCP Logging |
|------|-------------|--------------|
| 100  | Deny        | Deny#        |

SwitchB# **show ip dhcp snooping binding**

| MacAddress        | IpAddress | Lease(sec) | Type          | VLAN | Interface           |
|-------------------|-----------|------------|---------------|------|---------------------|
| 00:02:00:02:00:02 | 170.1.1.2 | 3492       | dhcp-snooping | 100  | GigabitEthernet3/31 |

Total number of bindings: 1

SwitchB# **show ip arp insp statistics vlan 100**

| Vlan | Forwarded | Dropped | DHCP Drops | ACL Drops |
|------|-----------|---------|------------|-----------|
| 100  | 2398      | 0       | 0          | 0         |

| Vlan | DHCP Permits | ACL Permits | Source MAC Failures |
|------|--------------|-------------|---------------------|
| 100  | 2398         | 0           | 0                   |

| Vlan | Dest MAC Failures | IP Validation Failures | Invalid Protocol Data |
|------|-------------------|------------------------|-----------------------|
| 100  | 0                 | 0                      | 0                     |

SwitchB#

## 非 DHCP 環境に対する ARP ACL の設定

次の手順は、スイッチ B (図 46-3 (P.46-6) を参照) が DAI または DHCP スヌーピングをサポートしない場合の DAI の設定方法を示しています。

スイッチ A のポート 1 を **trusted** に設定した場合、スイッチ A およびホスト 1 はスイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが発生します。この可能性を防止するには、スイッチ A のポート 1 を **untrusted** に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 を設定し、VLAN 100 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なく、スイッチ A の ACL 設定を適用できない場合は、レイヤ 3 でスイッチ A とスイッチ B を分離し、これらのスイッチ間のパケット ルーティングにはルータを使用する必要があります。

(非 DHCP 環境のスイッチ A 上で) ARP ACL を設定するには、次の作業を実行します。

|        | コマンド  | 目的  |
|--------|---|---|
| ステップ 1 | Switch# <b>configure terminal</b>   | グローバル コンフィギュレーション モードを開始します。  |
| ステップ 2 | Switch(config)# <b>arp access-list acl-name</b>                                   | ARP ACL を定義して、ARP アクセスリスト コンフィギュレーション モードを開始します。デフォルトでは、ARP アクセス リストは定義されていません。<br><b>(注)</b> ARP アクセス リストの末尾には、暗黙の <b>deny ip any mac any</b> コマンドがあります。   |
| ステップ 3 | Switch(config-arp-nac)# <b>permit ip host sender-ip mac host sender-mac [log]</b> | 指定されたホスト (ホスト 2) からの ARP パケットを許可します。<br><ul style="list-style-type: none"> <li>• <i>sender-ip</i> には、ホスト 2 の IP アドレスを入力します。</li> <li>• <i>sender-mac</i> には、ホスト 2 の MAC アドレスを入力します。</li> <li>• (任意) <b>log</b> を指定して、Access Control Entry (ACE; アクセス コントロール エントリ) に一致するパケットをログ バッファに記録します。<b>ip arp inspection vlan logging</b> グローバル コンフィギュレーション コマンドで <b>matchlog</b> キーワードを設定した場合も、一致するパケットが記録されます。詳細については、「<a href="#">ログ バッファの設定</a>」(P.46-14) を参照してください。</li> </ul> |
| ステップ 4 | Switch(config-arp-nac)# <b>exit</b>   | グローバル コンフィギュレーション モードに戻ります。   |

| コマンド  | 目的   |
|---|--|
| <b>ステップ 5</b> Switch(config)# <b>ip arp inspection filter arp-acl-name</b><br><b>vlan vlan-range [static]</b> | <p>VLAN に ARP ACL を適用します。デフォルトでは、いずれの VLAN にも ARP ACL は定義されていません。</p> <ul style="list-style-type: none"> <li>• <i>arp-acl-name</i> には、ステップ 2 で作成された ACL 名を指定します。</li> <li>• <i>vlan-range</i> には、スイッチおよびホストが存在する VLAN を指定します。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。</li> <li>• (任意) ARP ACL 内の暗黙の拒否を明示的な拒否として取り扱い、ACL 内の前の句に一致しないパケットをドロップするために、<b>static</b> を指定します。DHCP バインディングは使用されません。</li> </ul> <p>このキーワードを指定しない場合は、パケットを拒否する明示的な拒否が ACL 内がないことを意味し、パケットが ACL 内の句に一致しないと DHCP バインディングがパケットの許可または拒否を決定します。</p> <p>IP/MAC アドレス バインディングのみを含む ARP パケットは、ACL と比較されます。アクセス リストが許可したパケットだけが許可されます。</p> |
| <b>ステップ 6</b> Switch(config)# <b>interface interface-id</b>   | <p>スイッチ B に接続されたスイッチ A のインターフェイスを指定し、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。</p>   |
| <b>ステップ 7</b> Switch(config-if)# <b>no ip arp inspection trust</b>  | <p>スイッチ B に接続されたスイッチ A のインターフェイスを <b>untrusted</b> として設定します。</p> <p>デフォルトでは、すべてのインターフェイスが <b>untrusted</b> です。</p> <p>信頼できないインターフェイスの場合、スイッチはすべての ARP 要求と ARP 応答を代行受信します。ローカル キャッシュを更新し、該当する宛先にパケットを転送する前に、代行受信したパケットが有効な IP/MAC アドレス バインディングを持つかどうかを検証します。スイッチは、無効なパケットをドロップし、<b>ip arp inspection vlan logging</b> グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。詳細については、「<a href="#">ログ バッファの設定</a>」(P.46-14) を参照してください。</p>  |
| <b>ステップ 8</b> Switch(config-if)# <b>end</b>   | <p>特権 EXEC モードに戻ります。</p>   |

|         | コマンド  | 目的                             |
|---------|---|--------------------------------|
| ステップ 9  | Switch# <b>show arp access-list</b> [acl-name]<br>Switch# <b>show ip arp inspection vlan</b> vlan-range<br>Switch# <b>show ip arp inspection interfaces</b> | DAI の設定を確認します。                 |
| ステップ 10 | Switch# <b>copy running-config startup-config</b>   | (任意) コンフィギュレーションファイルに設定を保存します。 |

ARP ACL を削除するには、**no arp access-list** グローバル コンフィギュレーション コマンドを使用します。VLAN に対応付けられた ARP ACL を削除するには、**no ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* グローバル コンフィギュレーション コマンドを使用します。

次に、スイッチ A 上の *hostB* という名前の ARP ACL を設定し、ホスト B からの ARP パケット (IP アドレス 170.1.1.2、MAC アドレス 2.2.2) を許可し、VLAN 100 に ACL を適用し、スイッチ A 上のポート 1 を **untrusted** に設定する例を示します。

```
SwitchA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)# arp access-list hostB
SwitchA(config-arp-nacl)# permit ip host 170.1.1.2 mac host 2.2.2 log
SwitchA(config-arp-nacl)# exit
SwitchA(config)# ip arp inspection filter hostB vlan 100 static
SwitchA(config)# interface g3/48
SwitchA(config-if)# no ip arp inspection trust
SwitchA(config-if)# end
SwitchA# show arp access-list hostB
ARP access list hostB
    permit ip host 170.1.1.2 mac host 0002.0002.0002 log
```

```
SwitchA# show ip arp inspection interfaces
```

| Interface | Trust State | Rate (pps) | Burst Interval |
|-----------|-------------|------------|----------------|
| Gi1/1     | Untrusted   | 15         | 1              |
| Gi1/2     | Untrusted   | 15         | 1              |
| Gi3/1     | Untrusted   | 15         | 1              |
| Gi3/2     | Untrusted   | 15         | 1              |
| Gi3/3     | Untrusted   | 15         | 1              |
| Gi3/4     | Untrusted   | 15         | 1              |
| Gi3/5     | Untrusted   | 15         | 1              |
| Gi3/6     | Untrusted   | 15         | 1              |
| Gi3/7     | Untrusted   | 15         | 1              |
| Gi3/8     | Untrusted   | 15         | 1              |
| Gi3/9     | Untrusted   | 15         | 1              |
| Gi3/10    | Untrusted   | 15         | 1              |
| Gi3/11    | Untrusted   | 15         | 1              |
| Gi3/12    | Untrusted   | 15         | 1              |
| Gi3/13    | Untrusted   | 15         | 1              |
| Gi3/14    | Untrusted   | 15         | 1              |
| Gi3/15    | Untrusted   | 15         | 1              |
| Gi3/16    | Untrusted   | 15         | 1              |
| Gi3/17    | Untrusted   | 15         | 1              |
| Gi3/18    | Untrusted   | 15         | 1              |
| Gi3/19    | Untrusted   | 15         | 1              |
| Gi3/20    | Untrusted   | 15         | 1              |
| Gi3/21    | Untrusted   | 15         | 1              |
| Gi3/22    | Untrusted   | 15         | 1              |
| Gi3/23    | Untrusted   | 15         | 1              |
| Gi3/24    | Untrusted   | 15         | 1              |
| Gi3/25    | Untrusted   | 15         | 1              |
| Gi3/26    | Untrusted   | 15         | 1              |
| Gi3/27    | Untrusted   | 15         | 1              |

```

Gi3/28      Untrusted      15          1
Gi3/29      Untrusted      15          1
Gi3/30      Untrusted      15          1
Gi3/31      Untrusted      15          1
Gi3/32      Untrusted      15          1
Gi3/33      Untrusted      15          1
Gi3/34      Untrusted      15          1
Gi3/35      Untrusted      15          1
Gi3/36      Untrusted      15          1
Gi3/37      Untrusted      15          1
Gi3/38      Untrusted      15          1
Gi3/39      Untrusted      15          1
Gi3/40      Untrusted      15          1
Gi3/41      Untrusted      15          1
Gi3/42      Untrusted      15          1
Gi3/43      Untrusted      15          1
Gi3/44      Untrusted      15          1
Gi3/45      Untrusted      15          1
Gi3/46      Untrusted      15          1
Gi3/47      Untrusted      15          1
Gi3/48      Untrusted      15          1

```

```
SwitchA# show ip arp inspection statistics vlan 100
```

```

Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
----      -
100       15             169          160             9

Vlan      DHCP Permits      ACL Permits      Source MAC Failures
----      -
100       0                 0                0

Vlan      Dest MAC Failures      IP Validation Failures      Invalid Protocol Data
----      -
100       0                       0                             0

```

```
SwitchA#
```

## ログバッファの設定

スイッチがパケットをドロップすると、ログバッファにエントリが入力され、次にレート制御単位でシステムメッセージが生成されます。メッセージの生成後、スイッチはログバッファからエントリをクリアします。各ログエントリには、フロー情報（受信 VLAN、ポート番号、送信元と宛先 IP アドレス、および送信元と宛先 MAC アドレスなど）が含まれます。

ログバッファエントリは、複数のパケットを表すことができます。たとえば、インターフェイスが同一 VLAN 上で同じ ARP パラメータを持つ多数のパケットを受信した場合、スイッチはログバッファでこれらのパケットを 1 つのエントリとして結合し、エントリに単一のシステムメッセージを生成します。

ログバッファがオーバーフローする場合は、ログイベントがログバッファに収まらないことを意味しており、**show ip arp inspection log** 特権 EXEC コマンドの出力が影響を受けます。このエントリに関してそれ以外の統計情報は表示されません。

ログバッファを設定するには、次の作業を行います。

| コマンド   | 目的   |
|--|--|
| ステップ 1 Switch# <code>configure terminal</code>   | グローバル コンフィギュレーション モードを開始します。   |
| ステップ 2 Switch(config)# <code>ip arp inspection log-buffer {entries number   logs number interval seconds}</code>                                     | <p>ダイナミック ARP インスペクション ログ バッファを設定します。</p> <p>デフォルトでは、DAI がイネーブルの場合、拒否またはドロップされた ARP パケットが記録されます。ログ エントリ数は、32 です。システム メッセージの数は 1 秒あたり 5 つに制限されています。ロギングレート間隔は 1 秒です。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>entries number</b> には、バッファに記録されるエントリ数を指定します。指定できる範囲は 0 ~ 1024 です。</li> <li>• <b>logs number interval seconds</b> には、指定の間隔でシステム メッセージを生成するエントリ数を指定します。</li> </ul> <p><b>logs number</b> に指定できる範囲は 0 ~ 1024 です。値を 0 に設定すると、エントリはログ バッファに配置されますが、システム メッセージが生成されません。</p> <p>指定できる <b>interval seconds</b> の範囲は 0 ~ 86400 秒 (1 日) です。値を 0 に設定すると、システム メッセージがただちに生成されます (ログ バッファは常に空になります)。</p> <p>0 の間隔設定は、0 のログ設定を上書きします。</p> <p><b>logs</b> および <b>interval</b> の設定は、相互に作用します。<b>logs number X</b> が <b>interval seconds Y</b> より大きい場合は、X を Y で割って (X/Y) 求められたシステム メッセージ数が 1 秒間に送信されます。それ以外の場合は、Y を X で割って (Y/X) 求められた間隔 (秒) で 1 つのシステム メッセージが送信されます。</p> |
| ステップ 3 Switch(config)# <code>[no] ip arp inspection vlan vlan-range logging {acl-match matchlog   none}   dhcp-bindings {all   none   permit}</code> | <p>VLAN 単位で記録するパケットのタイプを制御します。デフォルトでは、拒否またはドロップされたパケットがすべて記録されます。<b>logged</b> という用語は、エントリがログ バッファ内に存在し、システム メッセージが生成されることを意味します。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>vlan-range</b> には、VLAN ID 番号で識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定します。指定できる範囲は 1 ~ 4094 です。</li> <li>• <b>acl-match matchlog</b> では、ACE ロギング設定に基づいてパケットを記録します。このコマンドで <b>matchlog</b> キーワードを指定し、<b>permit</b> または <b>deny</b> の ARP アクセスリスト コンフィギュレーション コマンドで <b>log</b> キーワードを指定した場合、ログ キーワードを持つ ACE で許可または拒否された ARP パケットが記録されます。</li> <li>• <b>acl-match none</b> では、ACL に一致するパケットを記録しません。</li> <li>• <b>dhcp-bindings all</b> では、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。</li> <li>• <b>dhcp-bindings none</b> では、DHCP バインディングに一致するパケットを記録しません。</li> <li>• <b>dhcp-bindings permit</b> では、DHCP バインディングが許可したパケットを記録します。</li> </ul>  |

|        | コマンド  | 目的                              |
|--------|---|---------------------------------|
| ステップ 4 | Switch(config)# <b>exit</b>                       | 特権 EXEC モードに戻ります。               |
| ステップ 5 | Switch# <b>show ip arp inspection log</b>         | 設定を確認します。                       |
| ステップ 6 | Switch# <b>copy running-config startup-config</b> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

デフォルトのログ バッファ設定に戻すには、**no ip arp inspection log-buffer** グローバル コンフィギュレーション コマンドを使用します。デフォルトの VLAN ログ設定に戻すには、**no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings}** グローバル コンフィギュレーション コマンドを使用します。ログ バッファをクリアするには、**clear ip arp inspection log** 特権 EXEC コマンドを使用します。

次の例では、ログ バッファのエントリ数を 1024 に設定する方法を示します。また、10 秒ごとに 100 の比率でバッファからログを生成する必要があるようにするために、Catalyst 4500 シリーズ スイッチを設定する方法も示します。

```
SwitchB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchB(config)# ip arp inspection log-buffer entries 1024
SwitchB(config)# ip arp inspection log-buffer logs 100 interval 10
SwitchB(config)# end
SwitchB# show ip arp inspection log
Total Log Buffer Size : 1024
Syslog rate : 100 entries per 10 seconds.
```

```
Interface   Vlan   Sender MAC           Sender IP             Num Pkts   Reason              Time
-----
Gi3/31     100    0002.0002.0003      170.1.1.2            5          DHCP Deny           02:05:45 UTC
Fri Feb 4 2005
SwitchB#
```

## 着信 ARP パケットのレート制限

スイッチの CPU が DAI の確認検査を行うので、DoS 攻撃を防ぐために着信 ARP パケット数がレート制限されています。



(注)

インターフェイス上のレート制限を明示的に設定しない限り、インターフェイスの信頼状態を変更することは、レート制限を信頼状態のデフォルト値に変更することになります。レート制限を設定すると、インターフェイスはその信頼状態が変更された場合でも設定されたレート制限を維持します。**no ip arp-inspection limit** インターフェイス コンフィギュレーション コマンドを入力すると、インターフェイスはデフォルトのレート制限に戻ります。

デフォルトでは、着信 ARP パケットのレートが設定された制限を超える場合は、ポートが **error-disabled** ステートに置かれます。ポートのシャットダウンを防ぐには、**errdisable detect cause arp-inspection action shutdown vlan** グローバル コンフィギュレーション コマンドを使用すると、違反の発生時にポートで問題になっている VLAN のみをシャットダウンできます。

**errdisable recovery cause arp-inspection** グローバル コンフィギュレーション コマンドを設定すると、セキュアポートが **errdisable** ステートの場合に実行してこのステートを自動的に解除できます。また、**shutdown** および **no shutdown** のインターフェイス コンフィギュレーション コマンドを入力する



と、手動で再びイネーブルにできます。ポートが VLAN 単位で `errdisable` モードの場合、`clear errdisable interface name vlan range` コマンドを使用すると、ポート上の VLAN を再度イネーブルにすることもできます。

着信 ARP パケットのレートを制限するには、次の作業を行います。

| コマンド   | 目的  |
|--|---|
| ステップ 1 <code>Switch# configure terminal</code>   | 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 <code>Switch(config)# errdisable detect cause arp-inspection [action shutdown vlan]</code>              | VLAN 単位でエラー ディセーブル検出をイネーブルにします。<br>(注) このコマンドは、デフォルトでイネーブルに設定されており、違反が発生するとインターフェイスがシャットダウンされます。  |
| ステップ 3 <code>Switch(config)# interface interface-id</code>   | レート制限されるインターフェイスを指定して、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 4 <code>Switch(config-if)# [no] ip arp inspection limit {rate pps [burst interval seconds]   none}</code> | インターフェイス上の着信 ARP 要求および ARP 応答のレートを制限します。<br><br>デフォルトのレートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。バースト インターバルは 1 秒に設定されています。<br><br>キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>rate pps</b> には、1 秒間に処理される着信パケット数の上限を指定します。指定できる範囲は 0 ~ 2048 pps です。</li> <li>• (任意) <b>burst interval seconds</b> には、高いレートの ARP パケットに関してインターフェイスをモニタリングする連続した間隔を秒数で指定します。指定できる範囲は 1 ~ 15 です。</li> <li>• <b>rate none</b> では、処理できる着信 ARP パケットのレートに上限を指定しません。</li> </ul> |
| ステップ 5 <code>Switch(config-if)# exit</code>  | グローバル コンフィギュレーション モードに戻ります。   |
| ステップ 6 <code>Switch(config)# errdisable recovery {cause arp-inspection   interval interval}</code>             | (任意) DAI の <code>errdisable</code> ステートからのエラー回復をイネーブルにします。<br><br>デフォルトでは、回復はディセーブルで、回復間隔は 300 秒です。<br><br><b>interval interval</b> には、 <code>errdisable</code> ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ~ 86400 です。  |
| ステップ 7 <code>Switch(config)# exit</code>   | 特権 EXEC モードに戻ります。   |
| ステップ 8 <code>Switch# show ip arp inspection interfaces</code>  | 設定を確認します。   |
| ステップ 9 <code>Switch# show errdisable recovery</code>   | 設定を確認します。   |
| ステップ 10 <code>Switch# copy running-config startup-config</code>  | (任意) コンフィギュレーション ファイルに設定を保存します。   |

デフォルトのレート制限設定に戻すには、`no ip arp inspection limit` インターフェイス コンフィギュレーション コマンドを使用します。DAI のエラー回復をディセーブルにするには、`no errdisable recovery cause arp-inspection` グローバル コンフィギュレーション コマンドを使用します。

次に、着信パケット数の上限 (100 pps) を設定し、バースト間隔 (1 秒) を指定する例を示します。

```
SwitchB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchB(config)# interface g3/31
```

```
SwitchB(config-if)# ip arp inspection limit rate 100 burst interval 1
SwitchB(config-if)# exit
SwitchB(config)# errdisable recovery cause arp-inspection
SwitchB(config)# exit
SwitchB# show ip arp inspection interfaces
```

| Interface | Trust State | Rate (pps) | Burst Interval |
|-----------|-------------|------------|----------------|
| Gi1/1     | Untrusted   | 15         | 1              |
| Gi1/2     | Untrusted   | 15         | 1              |
| Gi3/1     | Untrusted   | 15         | 1              |
| Gi3/2     | Untrusted   | 15         | 1              |
| Gi3/3     | Untrusted   | 15         | 1              |
| Gi3/4     | Untrusted   | 15         | 1              |
| Gi3/5     | Untrusted   | 15         | 1              |
| Gi3/6     | Untrusted   | 15         | 1              |
| Gi3/7     | Untrusted   | 15         | 1              |
| Gi3/8     | Untrusted   | 15         | 1              |
| Gi3/9     | Untrusted   | 15         | 1              |
| Gi3/10    | Untrusted   | 15         | 1              |
| Gi3/11    | Untrusted   | 15         | 1              |
| Gi3/12    | Untrusted   | 15         | 1              |
| Gi3/13    | Untrusted   | 15         | 1              |
| Gi3/14    | Untrusted   | 15         | 1              |
| Gi3/15    | Untrusted   | 15         | 1              |
| Gi3/16    | Untrusted   | 15         | 1              |
| Gi3/17    | Untrusted   | 15         | 1              |
| Gi3/18    | Untrusted   | 15         | 1              |
| Gi3/19    | Untrusted   | 15         | 1              |
| Gi3/20    | Untrusted   | 15         | 1              |
| Gi3/21    | Untrusted   | 15         | 1              |
| Gi3/22    | Untrusted   | 15         | 1              |
| Gi3/23    | Untrusted   | 15         | 1              |
| Gi3/24    | Untrusted   | 15         | 1              |
| Gi3/25    | Untrusted   | 15         | 1              |
| Gi3/26    | Untrusted   | 15         | 1              |
| Gi3/27    | Untrusted   | 15         | 1              |
| Gi3/28    | Untrusted   | 15         | 1              |
| Gi3/29    | Untrusted   | 15         | 1              |
| Gi3/30    | Untrusted   | 15         | 1              |
| Gi3/31    | Untrusted   | 100        | 1              |
| Gi3/32    | Untrusted   | 15         | 1              |
| Gi3/33    | Untrusted   | 15         | 1              |
| Gi3/34    | Untrusted   | 15         | 1              |
| Gi3/35    | Untrusted   | 15         | 1              |
| Gi3/36    | Untrusted   | 15         | 1              |
| Gi3/37    | Untrusted   | 15         | 1              |
| Gi3/38    | Untrusted   | 15         | 1              |
| Gi3/39    | Untrusted   | 15         | 1              |
| Gi3/40    | Untrusted   | 15         | 1              |
| Gi3/41    | Untrusted   | 15         | 1              |
| Gi3/42    | Untrusted   | 15         | 1              |
| Gi3/43    | Untrusted   | 15         | 1              |
| Gi3/44    | Untrusted   | 15         | 1              |
| Gi3/45    | Untrusted   | 15         | 1              |
| Gi3/46    | Trusted     | None       | N/A            |
| Gi3/47    | Untrusted   | 15         | 1              |
| Gi3/48    | Untrusted   | 15         | 1              |

```
SwitchB# show errdisable recovery
ErrDisable Reason    Timer Status
-----
udld                  Disabled
bpduguard             Disabled
```

```

security-violatio Disabled
channel-misconfig Disabled
vmmps Disabled
pagp-flap Disabled
dtp-flap Disabled
link-flap Disabled
l2ptguard Disabled
psecure-violation Disabled
gbic-invalid Disabled
dhcp-rate-limit Disabled
unicast-flood Disabled
storm-control Disabled
arp-inspection Enabled

```

```
Timer interval: 300 seconds
```

```
Interfaces that will be enabled at the next timeout:
```

```

SwitchB#
1w2d: %SW_DAI-4-PACKET_RATE_EXCEEDED: 101 packets received in 739 milliseconds on Gi3/31.
1w2d: %PM-4-ERR_DISABLE: arp-inspection error detected on Gi3/31, putting Gi3/31 in
err-disable state
SwitchB# show clock
*02:21:43.556 UTC Fri Feb 4 2005
SwitchB#
SwitchB# show interface g3/31 status

Port      Name              Status      Vlan      Duplex  Speed Type
Gi3/31                    err-disabled 100        auto     auto 10/100/1000-TX
SwitchB#
SwitchB#
1w2d: %PM-4-ERR_RECOVER: Attempting to recover from arp-inspection err-disable state on
Gi3/31
SwitchB# show interface g3/31 status

Port      Name              Status      Vlan      Duplex  Speed Type
Gi3/31                    connected   100        a-full   a-100 10/100/1000-TX
SwitchB# show clock
*02:27:40.336 UTC Fri Feb 4 2005
SwitchB#

```

## 確認検査の実行

DAI では、無効な IP/MAC アドレスバインディングを持つ ARP パケットを代行受信し、記録して、ドロップします。スイッチが宛先 MAC アドレス、送信側とターゲット IP アドレス、および送信元 MAC アドレスで追加の検査を実行するよう設定できます。

着信 ARP パケットで特定の検査を実行するには、次の作業を行います。

|        | コマンド   | 目的  |
|--------|--|---|
| ステップ 1 | Switch# <b>configure terminal</b>  | グローバル コンフィギュレーション モードを開始します。  |
| ステップ 2 | Switch(config)# <b>ip arp inspection validate</b> {[src-mac] [dst-mac] [ip]} | <p>着信 ARP パケットで特定の検査を実行します。デフォルトでは、追加の検査は実行されません。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>src-mac</b> では、ARP の本体内の送信側 MAC アドレスに対してイーサネット ヘッダー内の送信元 MAC アドレスを検査します。この検証は、ARP 要求と ARP 応答に両方に対して実行されます。このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、ドロップされます。</li> <li>• <b>dst-mac</b> では、ARP の本体内のターゲット MAC アドレスに対してイーサネット ヘッダー内の宛先 MAC アドレスを検査します。この検証は、ARP 応答に対して実行されます。このチェックがイネーブルの場合、異なる MAC アドレスを持つパケットは無効として分類され、ドロップされます。</li> <li>• <b>ip</b> では、無効で予期しない IP アドレスに関して ARP の本体を検査します。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これに該当します。送信側 IP アドレスはすべての ARP 要求および ARP 応答で検査され、ターゲット IP アドレスは、ARP 応答でのみ検査されます。</li> </ul> <p>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。各コマンドは、以前のコマンドの設定を上書きします。つまり、コマンドが <b>src</b> および <b>dst mac</b> 確認をイネーブルにし、2 番目のコマンドが IP 確認のみをイネーブルにした場合、<b>src</b> および <b>dst mac</b> 確認は 2 番目のコマンドによりディセーブルになります。</p> |
| ステップ 3 | Switch(config)# <b>exit</b>  | 特権 EXEC モードに戻ります。   |
| ステップ 4 | Switch# <b>show ip arp inspection vlan</b> vlan-range                        | 設定を確認します。   |
| ステップ 5 | Switch# <b>copy running-config startup-config</b>                            | (任意) コンフィギュレーション ファイルに設定を保存します。   |

検査をディセーブルにするには、**no ip arp inspection validate [src-mac] [dst-mac] [ip]** グローバル コンフィギュレーション コマンドを使用します。転送、ドロップ、MAC 確認の失敗、および IP 確認の失敗パケットの統計情報を表示するには、**show ip arp inspection statistics** 特権 EXEC コマンドを使用します。

次に、送信元 MAC 確認を設定する例を示します。イーサネット ヘッダー内の送信元アドレスが ARP ボディ内の送信側ハードウェア アドレスに一致しない場合、パケットはドロップされ、エラー メッセージが生成される可能性があります。

```
SwitchB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchB(config)# ip arp inspection validate src-mac
SwitchB(config)# exit
SwitchB# show ip arp inspection vlan 100

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

Vlan      Configuration      Operation      ACL Match      Static ACL
```

```
-----  
100      Enabled      Active  
  
Vlan     ACL Logging      DHCP Logging  
-----  
100      Deny          Deny  
SwitchB#  
1w2d: %SW_DAI-4-INVALID_ARP: 9 Invalid ARPs (Req) on Gi3/31, vlan  
100.([0002.0002.0002/170.1.1.2/0001.0001.0001/170.1.1.1/02:30:24 UTC Fri Feb 4 2005])
```

