CHAPTER 50

ダイナミック ARP インスペクションの設定

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

この章の主な内容は、次のとおりです。

- 「ダイナミック ARP インスペクションについて」（P.50-1）
- 「ダイナミック ARP インスペクションの設定」（P.50-5）

（注） この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で
『Catalyst 4500 Series Switch Cisco IOS Command Reference』と関連資料を参照してください。

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

ダイナミック ARP インスペクションについて

DAI は、ネットワークのアドレス解決プロトコル（ARP）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 MAC/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。

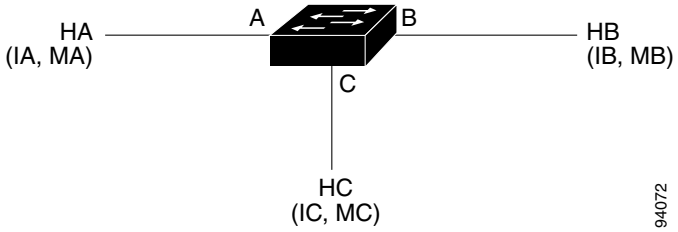
- 「ARP キャッシュ ポイズニング」（P.50-2）
- 「DAI の目的」（P.50-2）
- 「インターフェイスの信頼状態、セキュリティ適用範囲、およびネットワークの構成」（P.50-3）
- 「スタティック バインディング DHCP スヌーピングのエントリの相対的なプライオリティ」（P.50-4）
- 「ドロップされたパケットのロギング」（P.50-4）
- 「ARP パケットのレート制限」（P.50-4）
- 「ポート チャネル機能」（P.50-5）

ARP キャッシュ ポイズニング

ARP キャッシュを「ポイズニング」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。

図 50-1 には、キャッシュ ポイズニングの例を示します。

図 50-1　　ARP キャッシュ ポイズニング



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 ARP 応答を偽造して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。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、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 ストリームにそれ自身を割り込ませたことになります。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。

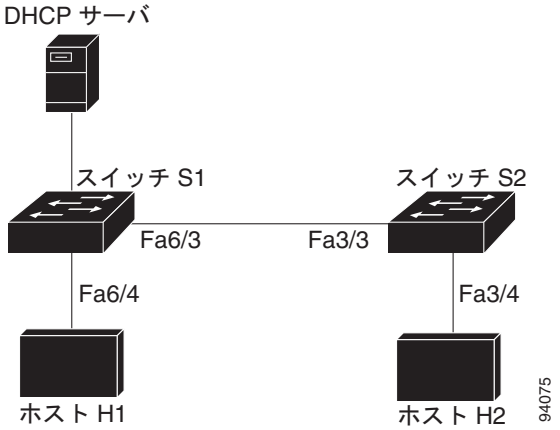
DAI は、ARP パケットの有効性を、信頼性のあるデータベースに格納された有効な MAC/IP アドレスのバインディングに基づいて判別します。このデータベースは、Dynamic Host Configuration Protocol（DHCP）スヌーピングが VLAN および該当するスイッチでイネーブルにされている場合に、DHCP スヌーピングの実行時に作成されます。さらに、DAI は、静的に設定された IP アドレスを使用するホストを処理するために、ユーザが設定した ARP アクセス コントロール リスト（ACL）と ARP パケットを照合できます。

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 50-2　DAI 対応 VLAN における ARP パケットの確認



信頼状態の設定は、慎重に使用してください。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。S1 と S2（図 50-2 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。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、ネットワーク内にセキュリティ ホールが生じます。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記録され、その割合に応じて、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、スイッチにより、ログ バッファからこのエントリが消去されます。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含まれます。

ip arp inspection log-buffer グローバル コンフィギュレーション コマンドを使用して、バッファ内のエントリ数や、システム メッセージ生成までの指定のインターバルに必要なエントリ数を設定します。記録されるパケットの種類を指定するには、**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。設定の詳細については、「ログ バッファの設定」（P.50-14）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 ステートに置かれます。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ト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。設定の詳細については、「着信 ARP パケットのレート制限」（P.50-16）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ときに、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。出力ポート数が CPU の係数ファクタになります。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 の使用率レベルを非常に高くする可能性があります。

ポート チャネル機能

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。したがって、最初の物理ポートの信頼状態は、チャネルの信頼状態と一致する必要はありません。

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 チャネルの設定と照合されます。

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。

ダイナミック ARP インスペクションの設定

ここでは、スイッチで DAI を設定する方法について説明します。

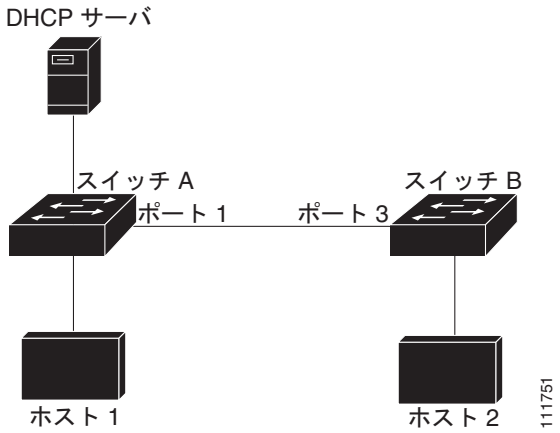
- 「DHCP 環境でのダイナミック ARP インスペクションの設定」（P.50-5）（必須）
- 「DAI の設定例」（P.50-7）
- 「非 DHCP 環境での ARP ACL の設定」（P.50-11）（任意）
- 「ログ バッファの設定」（P.50-14）（任意）
- 「着信 ARP パケットのレート制限」（P.50-16）（任意）
- 「確認検査の実行」（P.50-19）（任意）

DHCP 環境でのダイナミック ARP インスペクションの設定

この手順では、2 つのスイッチがダイナミック ARP インスペクションをサポートしているときに、この機能を設定する方法を示します。図 50-3 に示すとおり、ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B に接続されています。両方のスイッチは、これらのホストが置かれている 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。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 50-3　DAI をイネーブルにした VLAN での ARP パケット検証



（注） DAI では、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を使用して、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスのバインディングを確認します。IP アドレスが動的に割り当てられた ARP パケットを許可するには、DHCP スヌーピングを必ずイネーブルにしてください。設定情報については、第 51 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。

スイッチの 1 つだけがこの機能をサポートしている場合に DAI を設定する方法の詳細については、「非 DHCP 環境での ARP ACL の設定」（P.50-11）を参照してください。

DAI を設定するには、両方のスイッチで次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# show cdp neighbors`	スイッチ間の接続を確認します。
ステップ 2	`Switch# configure terminal`	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)# [no] ip arp inspection vlan` *vlan-range*	VLAN 単位で DAI をイネーブルにします。デフォルトでは、すべての VLAN で DAI はディセーブルです。 DAI をディセーブルにするには、**no ip arp inspection 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。 *vlan-range* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 両方のスイッチに同じ VLAN ID を指定します。
ステップ 4	`Switch(config)# interface` *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。

	コマンド	目的
ステップ 5	`Switch(config-if)# ip arp inspection trust`	スイッチ間の接続を trusted に設定します。 インターフェイスを信頼できない状態に戻すには、**no ip arp inspection trust** 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。 デフォルトでは、すべてのインターフェイスは信頼できません。 スイッチは、信頼できるインターフェイスにあるもう 1 つのスイッチから受信した ARP パケットは確認しません。スイッチは、パケットを転送します。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信されたパケットが有効な IP-to-MAC アドレス バインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットを破棄し、それらを **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、「ログ バッファの設定」（P.50-14）を参照してください。
ステップ 6	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Switch# show ip arp inspection interfaces` `Switch# show ip arp inspection vlan` *vlan-range*	DAI の設定を確認します。
ステップ 8	`Switch# show ip dhcp snooping binding`	DHCP バインディングを確認します。
ステップ 9	`Switch# show ip arp inspection statistics vlan` *vlan-range*	DAI の統計情報を確認します。
ステップ 10	`Switch# copy running-config startup-config`	（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。

DAI の設定例

次の例では、VLAN 100 のスイッチ A で DAI を設定する方法を示します。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
 ---------------  -----------     ----------    --------------
 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          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 環境での ARP ACL の設定

ここでは、図 50-3 のように、スイッチ 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。

スイッチ A のポート 1 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、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 ホールが作り出されます。これを阻止するには、スイッチ A のポート 1 を信頼できないもの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# configure terminal`	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)# arp access-list` *acl-name*	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 リストは定義されません。 （注）　ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。
ステップ 3	`Switch(config-arp-nac)# permit ip host` *sender-ip* `mac host` *sender-mac* [`log`]	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。 • *sender-ip* には、ホスト 2 の IP アドレスを入力します。 • *sender-mac* には、ホスト 2 の MAC アドレスを入力します。 • （任意）パケットが Access Control Entry（ACE; アクセス コントロール エントリ）と一致するときに、ログ バッファにこのパケットをログするには、**log** を指定します。**ip arp inspection vlan logging** グローバル コンフィギュレーション コマンドで **matchlog** キーワードを設定している場合も、一致したパケットがログ記録されます。詳細については、「ログ バッファの設定」（P.50-14）を参照してください。
ステップ 4	`Switch(config-arp-nac)# exit`	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
ステップ 5	`Switch(config)# ip arp inspection filter` *arp-acl-name* **vlan** *vlan-range* [**static**]	VLAN に ARP ACL を適用します。デフォルトでは、定義済みの ARP ACL は、どのような VLAN にも適用されません。 • *arp-acl-name* には、ステップ 2 で作成した ACL の名前を指定します。 • *vlan-range* には、スイッチとホストが存在する 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。 • （任意）**static** を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットは廃棄されます。DHCP バインディングは使用されません。 このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないことになります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。 IP-to-MAC アドレス バインディングしか持たない ARP パケットは、ACL と比較されます。パケットは、アクセス リストで許可された場合だけに許可されます。
ステップ 6	`Switch(config)# interface` *interface-id*	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。
ステップ 7	`Switch(config-if)# no ip arp inspection trust`	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 untrusted として設定します。 デフォルトでは、すべてのインターフェイスは信頼できません。 信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信されたパケットが有効な IP-to-MAC アドレス バインディングを持つことを確認してから、ローカル キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、**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、「ログ バッファの設定」（P.50-14）を参照してください。
ステップ 8	`Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 9	Switch# **show arp access-list** [*acl-name*] Switch# **show ip arp inspection vlan** *vlan-range* Switch# **show ip arp inspection interfaces**	DAI の設定を確認します。
ステップ 10	Switch# **copy running-config startup-config**	（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 に接続された 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記録され、その割合に応じて、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、スイッチにより、ログ バッファからこのエントリが消去されます。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じ ARP パラメータを使用して同じ VLAN 上で多数のパケットを受信した場合、スイッチはこれらのパケットを組み合わせて 1 つのエントリとしてログ バッファに格納し、エントリとして 1 つのシステム 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。このエントリに対しては、その他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# configure terminal`	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)# ip arp inspection log-buffer {entries number | logs number interval seconds}`	DAI のログ バッファを設定します。 デフォルトでは、DAI がイネーブル化されると、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。 キーワードの意味は次のとおりです。 • **entries** *number* は、バッファに記録されるエントリ数を表します。範囲は 0 ～ 1024 です。 • **logs** *number* **interval** *seconds* は、指定されたインターバルでシステム メッセージを生成するエントリの数を表します。 **logs** *number* に指定できる範囲は 0 ～ 1024 です。値 0 は、エントリはログ バッファ内に入力されますが、システム メッセージが生成されないことを意味します。 指定できる **interval** *seconds* の範囲は 0 ～ 86400 秒（1 日）です。0 は、システム メッセージがただちに生成されることを意味します。この場合、ログ バッファは常に空となります。 インターバル値を 0 に設定すると、ログ値 0 は上書きされます。 **logs** および **interval** の設定は、相互に作用します。**logs** *number* X が **interval** *seconds* Y より大きい場合、X 割る Y（X/Y）のシステム メッセージが毎秒送信されます。そうでない場合、1 つのシステム メッセージが Y 割る X（Y/X）秒ごとに送信されます。
ステップ 3	`Switch(config)# [no] ip arp inspection vlan vlan-range logging {acl-match {matchlog | none} | dhcp-bindings {all | none | permit}}`	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は、すべて記録されます。*ログに記録されるという表現は、エントリがログ バッファに格納され、システム メッセージが生成されることを意味しています。* キーワードの意味は次のとおりです。 • *vlan-range* には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ～ 4094 です。 • **acl-match matchlog** は、ACE ロギング設定に基づいてパケットをログに記録します。このコマンドで **matchlog** キーワードを指定し、**permit** または **deny** 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 **log** 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。 • **acl-match none** では、ACL に一致するパケットは記録されません。 • **dhcp-bindings all** では、DHCP バインディングに一致するパケットがすべて記録されます。 • **dhcp-bindings none** では、DHCP バインディングに一致するパケットは記録されません。 • **dhcp-bindings permit** では、DHCP バインディングが許可されたパケットが記録されます。

	コマンド	目的
ステップ 4	`Switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	`Switch# show ip arp inspection log`	設定を確認します。
ステップ 6	`Switch# copy running-config startup-config`	（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 によって DAI 違反チェックが実行されます。したがって、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、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。**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	`Switch# configure terminal`	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)# errdisable detect cause arp-inspection [action shutdown vlan]`	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。 **（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	`Switch(config)# interface interface-id`	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	`Switch(config-if)# [no] ip arp inspection limit {rate pps [burst interval second] | none}`	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。 デフォルト 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。バースト間隔は 1 秒です。 キーワードの意味は次のとおりです。 • **rate** *pps* 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。範囲は 0 ～ 2048 pps です。 • （任意）**burst interval** *seconds* は、レートの高い ARP パケットの有無についてインターフェイスがモニタリングされる間隔（秒）を指定します。指定できる範囲は 1 ～ 15 です。 • **rate none** では、処理できる着信 ARP パケットのレートの上限を設定しません。
ステップ 5	`Switch(config-if)# exit`	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	`Switch(config)# errdisable recovery {cause arp-inspection | interval interval}`	（任意）DAI の errdisable ステートからのエラー回復をイネーブルにします。 デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。 **interval** *interval* には、errdisable 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	`Switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 8	`Switch# show ip arp inspection interfaces`	設定を確認します。
ステップ 9	`Switch# show errdisable recovery`	設定を確認します。
ステップ 10	`Switch# copy running-config startup-config`	（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るには、**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
vmps                 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 は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、記録、および廃棄します。宛先 MAC アドレス、送信側および宛先の IP アドレス、および送信元 MAC アドレスで追加検証を実行するように、スイッチを設定できます。

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# configure terminal`	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)# ip arp inspection validate {[src-mac] [dst-mac] [ip]}`	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。 キーワードの意味は次のとおりです。 • **src-mac** では、イーサネット ヘッダーの送信元 MAC アドレスと ARP 本文の送信元 MAC アドレスが比較されます。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **dst-mac** では、イーサネット ヘッダーの宛先 MAC アドレスと ARP 本文の宛先 MAC アドレスが比較されます。この検査は、ARP 応答に対して実行されます。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。 • **ip** では、ARP 本文から、無効な IP アドレスや予期しない IP アドレスがないかを確認します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。送信元 IP アドレスはすべての ARP 要求および応答内でチェックされ、宛先 IP アドレスは ARP 応答内でのみチェックされます。 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。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが **src** および **dst mac** の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番めのコマンドによって **src** および **dst mac** の検証がディセーブルになります。
ステップ 3	`Switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 4	`Switch# show ip arp inspection vlan` *vlan-range*	設定を確認します。
ステップ 5	`Switch# copy running-config startup-config`	（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。

検証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])
```