



ダイナミック ARP インспекションの設定

- [ダイナミック ARP インспекションの制約事項 \(1 ページ\)](#)
- [ダイナミック ARP インспекションに関する情報 \(3 ページ\)](#)
- [ダイナミック ARP インспекションの設定方法 \(8 ページ\)](#)
- [DAI のモニタリング \(17 ページ\)](#)
- [DAI の設定の確認 \(18 ページ\)](#)
- [ダイナミック ARP インспекションの機能履歴 \(18 ページ\)](#)

ダイナミック ARP インспекションの制約事項

ここでは、スイッチにダイナミック Address Resolution Protocol (ARP) インспекションを設定するときの制約事項および注意事項を示します。

- ダイナミック ARP インспекションは入力セキュリティ機能です。出力チェックはまったく行いません。
- ダイナミック ARP インспекションは、ダイナミック ARP インспекションをサポートしていないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されるホストに対しては有効ではありません。中間者攻撃は単一のレイヤ2ブロードキャストドメインに制限されているため、チェックされないドメインと、ダイナミック ARP インспекションによりチェックされるドメインは区別します。このアクションは、ダイナミック ARP インспекションのためにイネーブルにされているドメインでホストの ARP キャッシュを保護します。
- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インспекション 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依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

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または拒否を行います。

- ダイナミック ARP インспекションは、アクセスポート、トランクポート、および EtherChannel ポートでサポートされます。



(注) RSPAN VLAN では、ダイナミック ARP インспекションをイネーブルにしないでください。RSPAN VLAN でダイナミック ARP インспекションをイネーブルにすると、ダイナミック ARP インспекション パケットが RSPAN 宛先ポートに届かない可能性があります。

- 物理ポートを EtherChannel ポート チャンネルに結合するには、この物理ポートとチャンネルポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポートチャンネル内で中断状態のままとなります。ポートチャンネルは、チャンネルと結合され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、チャンネルの信頼状態と一致する必要はありません。

逆に、ポートチャンネルで信頼状態を変更すると、スイッチは、チャンネルを構成するすべての物理ポートで新しい信頼状態を設定します。

- レート制限は、スイッチ スタックの各スイッチで別々に算出されます。クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも高い可能性があることを意味します。たとえば、レート制限が 30 pps に設定された EtherChannel で、スイッチ 1 に 1 つのポート、およびスイッチ 2 に 1 つのポートがある場合、EtherChannel が errdisable にならずに、各ポートは 29 pps でパケットを受信できます。
- ポートチャンネルの動作レートは、チャンネル内のすべての物理ポートによる累積値です。たとえば、ポートチャンネルの ARP レート制限を 400 pps に設定すると、このチャンネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャンネル メンバーからの受信パケットレートの合計となります。EtherChannel ポートのレート制限は、各チャンネル ポート メンバーが受信する ARP パケットのレートを確認してから設定してください。

物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポートチャンネルの設定に照合して検査されます。ポートチャンネルのレート制限設定は、物理ポートの設定には依存しません。

EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャンネル（すべての物理ポートを含む）は errdisable ステートとなります。

- 着信トランクポートでは、ARP パケットを必ずレート制限してください。トランクポートの集約を反映し、複数のダイナミック ARP インспекションがイネーブルにされた VLAN にわたってパケットを処理するために、トランクポートのレートをより高く設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コマンドを使用して、レートを無制限に設定することもできます。1 つの VLAN に高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他の VLAN への DoS 攻撃を招く可能性があります。

- スイッチで、ダイナミック ARP インспекションをイネーブルにすると、ARP トラフィックをポリシングするように設定されたポリサーの有効性は失われます。この結果、すべての ARP トラフィックは CPU に送信されます。

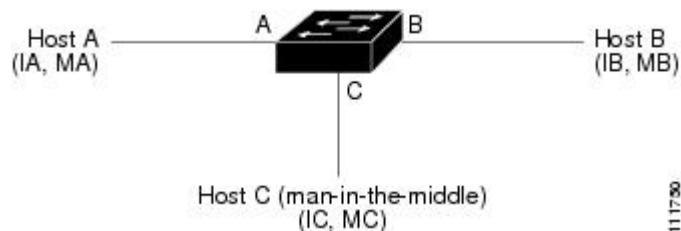
ダイナミック ARP インспекションに関する情報

ダイナミック ARP インспекションの概要

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャストドメイン内の IP 通信を実現します。たとえば、ホスト B はホスト A に情報を送信する必要がありますが、ARP キャッシュにホスト A の MAC アドレスを持っていないとします。ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャストドメインにあるホストすべてに対してブロードキャストメッセージを生成します。このブロードキャストドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。しかし、ARP は、ARP 要求を受信されなかった場合でも、ホストからの余分な応答を許可するため、ARP スプーフィング攻撃や ARP キャッシュのポイズニングが発生することがあります。攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、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。

悪意のあるユーザーは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、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、およびルータを攻撃することができます。図 26-1 に、ARP キャッシュポイズニングの例を示します。

図 1: ARP キャッシュポイズニング



ホスト A、B、および C は、インターフェイス A、B、および C 上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。カッコ内に示されているのは、これらの IP アドレス、および MAC アドレスです。たとえば、ホスト A が使用する IP アドレスは IA、MAC アドレスは MA です。ホスト A が IP レイヤにあるホスト B と通信する必要がある場合、ホスト A は IP アドレス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。スイッチとホスト B は、この ARP 要求を受信すると、IP アドレスが IA で、MAC アドレスが MA のホストに対する ARP バインディングを ARP キャッシュに読み込みます。たとえば、IP アドレス IA は、MAC アドレス MA にバインドされています。ホスト B が応答すると、スイッチ、およびホスト A は、IP アドレスが IB で、MAC アドレスが MB のホストに対するバインディングを ARP に読み込みます。

ホスト C は、IP アドレスが IA (または IB) で、MAC アドレスが MC のホストに対するバインディングを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングすることができます。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 宛でのトラフィックに、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、ホスト C がこのトラフィックを代行受信することになります。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。ホスト C は自身をホスト A からホスト B へのトラフィック ストリームに挿入します。従来の中間者攻撃です。

ダイナミック ARP インспекションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。不正な 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、ログに記録して、廃棄します。この機能により、ネットワークをある種の中間者攻撃から保護することができます。

ダイナミック ARP インспекションにより、有効な ARP 要求と応答だけが確実にリレーされるようになります。スイッチが実行する機能は次のとおりです。

- 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。

ダイナミック ARP インспекションは、信頼できるデータベースである DHCP スヌーピング バインディング データベースに格納されている有効な IP/MAC アドレス バインディングに基づいて、ARP パケットの正当性を判断します。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングが有効になっている場合に、DHCP スヌーピングにより構築されます。信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、この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、スイッチはこのパケットが有効である場合だけ、このパケットを転送します。

非 DHCP 環境では、ダイナミック ARP インспекションは、静的に設定された IP アドレスを持つホストに対するユーザー設定の ARP アクセスコントロールリスト (ACL) と照らし合わせて、ARP パケットの正当性を確認することができます。ARP ACL を定義するには、**arp access-list acl-name** 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。

パケットの IP アドレスが無効である場合、または ARP パケットの本文にある MAC アドレスが、イーサネット ヘッダーで指定されたアドレスと一致しない場合、ARP パケットをドロップするようにダイナミック ARP インспекションを設定することができます。このためには、**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。

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

ダイナミック ARP インспекションは、スイッチ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に到着するパケットは、ダイナミック ARP インспек

ションの確認検査をすべてバイパスし、信頼できないインターフェイスに到着するパケットには、ダイナミック ARP インспекションの検証プロセスを受けます。

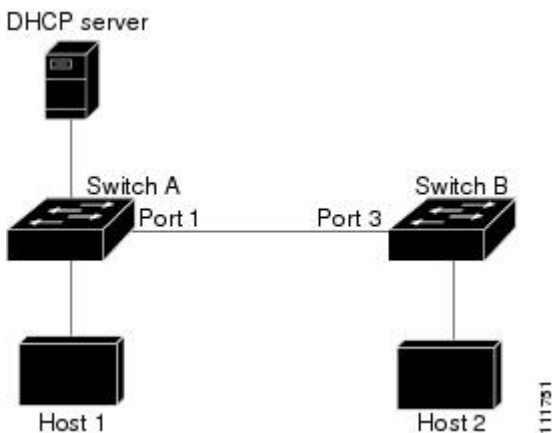
一般的なネットワーク構成では、ホスト ポートに接続されているスイッチ ポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチポートすべてを信頼できるものに設定します。この構成では、指定されたスイッチからネットワークに入ってくる ARP パケットはすべて、セキュリティチェックをバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、`ip arp inspection trust` インターフェイス コンフィギュレーション コマンドを使用します。



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。

次の図では、スイッチ A とスイッチ B の両方が、ホスト 1 とホスト 2 を含む VLAN でダイナミック ARP インспекションを実行しているとします。ホスト 1 とホスト 2 が、スイッチ A に接続している DHCP サーバーから IP アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。したがって、スイッチ A とスイッチ B 間のインターフェイスが信頼できない場合は、ホスト 1 からの ARP パケットはスイッチ B ではドロップされ、ホスト 1 およびホスト 2 の間の接続は切断されます。

図 2: ダイナミック ARP インспекションのために有効にされた VLAN 上の ARP パケット検証



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。スイッチ A でダイナミック ARP インспекションが実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの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）。この状況は、スイッチ B がダイナミック ARP インспекションを実行している場合でも発生します。

ダイナミック ARP インспекションは、ダイナミック ARP インспекションを実行してい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、そのネットワークにあるその他のホストの ARP キャッシュをポイズニングしていないことを保証します。しかし、ダイナミック ARP インспекションにより、ネットワークの他の部分にあるホストが、ダイ

ダイナミック ARP インспекションを実行しているスイッチに接続されているホストのキャッシュをポイズニングできないようにすることはできません。

VLAN のスイッチの一部がダイナミック ARP インспекションを実行し、残りのスイッチは実行していない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定します。ただし、非ダイナミック ARP インспекションスイッチからパケットのバインディングを検証するには、ARP ACL を使用して、ダイナミック ARP インспекションを実行するスイッチを設定します。このようなバインディングが判断できない場合は、レイヤ 3 で、ダイナミック ARP インспекションスイッチを実行していないスイッチから、ダイナミック ARP インспекションを実行しているスイッチを分離します。



- (注) DHCP サーバーとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インспекション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。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 パケット/秒 (pps) です。信頼できるインターフェイスはレート制限されません。この設定を変更するには、**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。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを **errdisable** ステートにします。ユーザーが介入するまで、ポートはこの状態を維持します。**errdisable recovery** 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、**errdisable** ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。



- (注) EtherChannel のレート制限は、スタックにある各スイッチに個別に適用されます。たとえば、EtherChannel で 20 pps の制限が設定されている場合、EtherChannel にあるポートの各スイッチでは、最大 20 pps まで実行できます。スイッチが制限を超過した場合、EtherChannel 全体が **errdisable** ステートになります。

ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インспекションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

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より、ARP ACL の方が優先されます。スイッチが ACL を使用するのには、ACL が **ip arp inspection filter vlan** 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作成されている場合だけです。スイッチは、まず、ARP パケットをユーザー設定の ARP ACL と比較します。DHCP スヌーピングによりデータが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していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

廃棄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 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

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とされる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。

ダイナミック ARP インспекションのデフォルト設定

| 機能 | デフォルト設定 |
|-----------------------|---|
| ダイナミック ARP インспекション | 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。 |
| 着信 ARP パケットのレート制限 | 1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチドネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。 信頼できるすべてのインターフェイスでは、レート制限は行われません。 バースト インターバルは 1 秒です。 |
| 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 | ダイナミック ARP インспекションがイネーブル化されると、拒否またはドロップされた ARP パケットはすべてが記録されます。 ログ内のエントリ数は 32 です。 システムメッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは 1 秒です。 |
| VLAN 単位のロギング | 拒否または廃棄されたすべての ARP パケットが記録されます。 |

ARPA CL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インспекションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

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より、ARP ACL の方が優先されます。スイッチが ACL を使用するのには、ACL が `ip arp inspection filter vlan` 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作成されている場合だけです。スイッチは、まず、ARP パケットをユーザー設定の ARP ACL と比較します。DHCP スヌーピングによりデータが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していても、ARP ACL が ARP パケットを拒否する場合は、スイッチもこのパケットを拒否します。

ダイナミック ARP インспекションの設定方法

非 DHCP 環境での ARP ACL の設定

この手順は、図 2 に示すスイッチ B がダイナミック ARP インспекション、または DHCP スヌーピングをサポートしていないときにダイナミック ARP インспекションを設定する方法を示しています。

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（スイッチ A で ACL 設定を適用することは不可能である）場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを使用してパケットをルートする必要があります。

スイッチ A で ARP ACL を設定するには、次の手順を実行します。この手順は、非 DHCP 環境では必須です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。 |
| ステップ 2 | configure terminal 例： Device# 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。 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 3 | arp access-list <i>acl-name</i> 例 : Device (config) # arp access-list arpacl22 | ARP ACL を定義し、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 4 | permit ip host <i>sender-ip</i> mac host <i>sender-mac</i> 例 : Device (config-arp-nacl) # permit ip host 10.2.2.2 mac host 0018.bad8.3fbd | 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。 <ul style="list-style-type: none"> • <i>sender-ip</i> には、ホスト 2 の IP アドレスを入力します。 • <i>sender-mac</i> には、ホスト 2 の MAC アドレスを入力します。 |
| ステップ 5 | exit 例 : Device (config-arp-nacl) # exit | ARP アクセスリストコンフィギュレーションモードを終了し、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 | ip arp inspection filter <i>arp-acl-name</i> vlan <i>vlan-range</i> [static] 例 : Device (config) # ip arp inspection filter arpacl22 vlan 1-2 | 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。 <ul style="list-style-type: none"> • <i>arp-acl-name</i> には、ステップ 2 で作成した ACL の名前を指定します。 • <i>vlan-range</i> では、スイッチとホストが存在する VLAN を指定します。VLAN ID 番号により識別される単一の 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 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| | | <p>トは廃棄されます。DHCP バインディングは使用されません。</p> <p>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となります。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。</p> <p>IP アドレスと MAC アドレスとのバインディングしか持たない ARP パケットは、ACL に照合されます。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。</p> |
| ステップ 7 | interface <i>interface-type</i> <i>interface-number</i> 例： Device(config)# interface gigabitethernt 0/1/1 | 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 8 | no ip arp inspection trust 例： Device(config-if)# no ip arp inspection trust | <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 untrusted 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は信頼できません。</p> <p>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、代行受信した各パケットが、IP アドレスと MAC アドレスと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。</p> |
| ステップ 9 | end 例： Device(config-if)# end | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---------|--|---|
| ステップ 10 | show arp access-list <i>acl-name</i> 例： Device# show arp access-list arpac122 | 名前付き ACL に関する情報を表示します。 |
| ステップ 11 | show ip arp inspection vlan <i>vlan-range</i> 例： Device# show ip arp inspection vlan 1-2 | 選択した範囲の VLAN の統計情報を表示します。 |
| ステップ 12 | show ip arp inspection interfaces 例： Device# show ip arp inspection interfaces | 指定したインターフェイスに関して ARP パケットの信頼状態とレート制限を表示します。 |

DHCP 環境でのダイナミック ARP インспекションの設定

始める前に

この手順では、2つのスイッチがダイナミック ARP インспек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。ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B にそれぞれ接続されています。スイッチは両方とも、ホストが配置されている VLAN 1 でダイナミック ARP インспекションを実行しています。DHCP サーバーはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバーから IP アドレスを取得します。したがって、スイッチ A はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。



- (注) 着信 ARP 要求、および ARP 応答で IP/MAC アドレスバインディングを検証するために、ダイナミック ARP インспекション 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依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

ダイナミック ARP インспекションを設定するには、次の手順を実行します。この処理は、両方のスイッチで行う必要があります。この手順は必須です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。 |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 2 | show cdp neighbors 例： Device# show cdp neighbors | スイッチ間の接続を確認します。 |
| ステップ 3 | configure terminal 例： Device# 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 4 | ip arp inspection vlan <i>vlan-range</i> 例： Device (config)# ip arp inspection vlan 1 | VLAN 単位で、ダイナミック ARP インспекションをイネーブルにします。デフォルトでは、すべての VLAN 上でダイナミック ARP インспекションはディセーブルになっています。 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 5 | Interface <i>type number</i> 例： Device (config)# interface gigabitethernet 1/0/1 | 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 6 | ip arp inspection trust 例： Device (config-if)# ip arp inspection trust | スイッチ間の接続を trusted に設定します。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。 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。この場合、パケットはそのまま転送されます。 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、代行受信した各パケットが、IP アドレスと MAC アドレスと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 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 |

| | コマンドまたはアクション | 目的 |
|---------|---|--|
| | | 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。 |
| ステップ 7 | end 例： Device(config-if)# end | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 8 | show ip arp inspection interfaces 例： Device# show ip arp inspection interfaces | インターフェイスでダイナミック ARP インспекションの設定を検証します。 |
| ステップ 9 | show ip arp inspection vlan vlan-range 例： Device# show ip arp inspection vlan 1 | VLAN でダイナミック ARP インспекションの設定を検証します。 |
| ステップ 10 | show ip dhcp snooping binding 例： Device# show ip dhcp snooping binding | DHCP バインディングを確認します。 |
| ステップ 11 | show ip arp inspection statistics vlan vlan-range 例： Device# show ip arp inspection statistics vlan 1 | VLAN でダイナミック ARP インспекションの統計情報を確認します。 |

着信 ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インспекション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを errdisable ステートにします。errdisable 回復をイネーブルにして、指定されたタイムアウト時間の後にポートがこのステートから自動的に抜け出すようにするまで、ポートはこのステートのままです。



(注) インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、レート制限をその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。

着信 ARP パケットのレートを制限するには、次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。 |
| ステップ 2 | configure terminal 例： Device# 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 | interface type number 例： Device(config)# interface gigabitethernet 0/1/2 | 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 | ip arp inspection limit {rate pps [burst interval seconds] 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 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。 <ul style="list-style-type: none">• ratepps には、1 秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ~ 2048 pps です。• (任意) burst intervalseconds 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。 |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | | <ul style="list-style-type: none"> • rate none には、処理可能な着信 ARP パケットのレートに上限を指定しません。 |
| ステップ 5 | exit 例： Device(config-if)# exit | インターフェイスコンフィギュレーションモードを終了し、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 | 次のコマンドを使用します。 <ul style="list-style-type: none"> • errdisable detect cause arp-inspection • errdisable recovery cause arp-inspection • errdisable recovery interval interval 例： Device(config)# errdisable recovery cause arp-inspection | (任意) ダイナミック ARP インспекションの errdisable ステートからのエラー回復をイネーブルにし、ダイナミック ARP インспекションの回復メカニズムで使用する変数を設定します。 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、 error-disabled 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 | exit 例： Device(config)# exit | グローバルコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

ダイナミック ARP インспекション検証チェックの実行

ダイナミック ARP インспекションは、不正な 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、ログに記録して、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 パケットで特定のチェックを実行するには、次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。 |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 2 | configure terminal 例 : Device# 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 | ip arp inspection validate {[src-mac] [dst-mac] [ip]} 例 : Device(config)# ip inspection validate 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、検証は実行されません。</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"> • 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 ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。 <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。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</p> |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | | のコマンドが IP 検証だけをイネーブルにすると、2 番目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 4 | exit 例： Device(config)# exit | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 5 | show ip arp inspection vlan <i>vlan-range</i> 例： Device# show ip arp insepction vlan 1-2 | 選択した範囲の VLAN の統計情報を表示します。 |

DAI のモニタリング

DAI をモニターするには、次のコマンドを使用します。

| コマンド | 説明 |
|---|---|
| clear ip arp inspection statistics | ダイナミック ARP インспекション統計情報をクリアします。 |
| show ip arp inspection statistics [vlan <i>vlan-range</i>] | 指定の VLAN において、転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インспекションがイネーブルにされた (アクティブ) VLAN だけの情報を表示します。 |
| clear ip arp inspection log | ダイナミック ARP インспекションログバッファをクリアします。 |
| show ip arp inspection log | ダイナミック ARP インспекションログバッファの設定と内容を表示します。 |

show ip arp inspection statistics コマンドでは、スイッチは信頼されたダイナミック ARP インспекションポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

DAI の設定の確認

DAI の設定を表示して確認するには、次のコマンドを使用します。

| コマンド | 説明 |
|---|--|
| <code>show arp access-list [acl-name]</code> | ARP ACL についての詳細情報を表示します。 |
| <code>show ip arp inspection interfaces [interface-id]</code> | 指定されたインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。 |
| <code>show ip arp inspection vlan vlan-range</code> | 指定された VLAN のダイナミック ARP インспекションの設定および動作ステータスを表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インспекションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。 |

ダイナミック ARP インспекションの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

| リリース | 機能 | 機能情報 |
|------------------------------|----------------------|--|
| Cisco IOS XE Everest 16.5.1a | ダイナミック ARP インспекション | ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ2ブロードキャストドメイン内の IP 通信を実現します。ダイナミック ARP インспекションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。不正な 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、ログに記録して、廃棄します。この機能により、ネットワークをある種の間接攻撃から保護することができます。 |

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

翻訳について

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