Cisco Catalyst レイヤ 3 固定構成スイッチでのレイヤ 2 セキュリティ機能の設定例

目次

概要
前提条件
要件
使用するコンポーネント
関連製品
表記法
背景説明
設定
ネットワーク図
ポート セキュリティ
DHCP スヌーピング
ダイナミック ARP インスペクション
IP ソース ガード
確認
トラブルシューティング
関連情報

概要

このドキュメントでは、Cisco Catalyst レイヤ 3 固定構成スイッチに実装できる、ポート セキュリティ、DHCP スヌーピング、ダイナミック Address Resolution Protocol（ARP）インスペクション、IP ソース ガードなど、一部のレイヤ 2 セキュリティ機能の設定例を説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、バージョン 12.2(25)SEC2 を搭載した Cisco Catalyst 3750 シリーズ スイッチに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始して

います。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、次のハードウェアにも使用できます。

- Cisco Catalyst 3550 シリーズ スイッチ
- Cisco Catalyst 3560 シリーズ スイッチ
- Cisco Catalyst 3560-E シリーズ スイッチ
- Cisco Catalyst 3750-E シリーズ スイッチ

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

ルータと同様に、レイヤ 2 とレイヤ 3 のスイッチには両方とも、一連の独自のネットワーク セキュリティの要件があります。 スイッチは、ルータと同じレイヤ 3 の攻撃の多くを受ける可能性があります。 ところが、一般的にスイッチと OSI 参照モデルのレイヤ 2 とでは、ネットワーク攻撃の対象となる方法が異なります。 これには次のものがあります。

- **Content Addressable Memory (CAM) テーブル オーバーフロー**Content Addressable Memory (CAM) テーブルはサイズが制限されています。 他のエントリが期限切れになる前に十分な数のエントリが CAM テーブルに入ると、CAM テーブルがいっぱいになって新しいエントリを受け入れることができなくなります。 通常、ネットワーク侵入者は、CAM テーブルがいっぱいになるまで、大量の無効な発信元 MAC アドレスでスイッチをフラッドさせます。 このような状態が発生すると、スイッチでは CAM テーブル内の特定の MAC アドレスのポート番号を検出できないため、すべてのポートで着信トラフィックによるフラッドが発生します。 スイッチは、実質的にハブと同じ動作をします。 侵入者が無効な発信元 MAC アドレスのフラッドを維持し続けない場合、スイッチでは最終的に CAM テーブルで古い MAC アドレス エントリがタイムアウトして、再びスイッチとして動作するようになります。 CAM テーブル オーバーフローではローカル VLAN 内部のトラフィックのみがフラッドされるため、侵入者が認識できるのは自身が接続しているローカル VLAN 内部のトラフィックだけです。CAM テーブル オーバーフロー攻撃は、スイッチ上でポート セキュリティを設定することで緩和できます。 このオプションにより、特定のスイッチ ポート上で MAC アドレスを指定できるか、スイッチ ポートで学習可能な MAC アドレスの数を指定できるようになります。 ポート上で無効な MAC アドレスが検出されると、スイッチは問題のある MAC アドレスをブロックするか、ポートをシャット ダウンすることができます。 スイッチ ポート上で MAC アドレスを指定することは、実稼働環境でのソリューションとしてはほとんど管理不可能です。 スイッチ ポート上での MAC アドレス数の制限は、管理可能です。 管理上、さらにスケーラブルなソリューションとして、スイッチでのダイナミック ポート セキュリティの実装があります。 ダイナミック ポート セキュリティを実装するには、学習される MAC アドレスの最大数を指定します。
- **Media Access Control (MAC) アドレス スプーフィング**Media Access Control (MAC) スプーフィング攻撃には、ターゲットのスイッチに、リモート ホストが宛先であるフレームをネットワーク攻撃者に転送させるよう、別のホストの既知の MAC アドレスを使用する方法が

含まれます。 他方のホストの発信元イーサネット アドレスを使用して 1 つのフレームが送信された時点で、ネットワーク攻撃者は CAM テーブル エントリを上書きして、スイッチに、そのホストが宛先になっているパケットをネットワーク攻撃者に転送させるようにします。 そのホストがトラフィックを送信するまでは、トラフィックが受信されることはありません。 ホストがトラフィックを送出すると、再び CAM テーブル エントリが上書きされて、元のポートに戻るようにされます。MAC スプーフィング攻撃を緩和するには、ポート セキュリティ機能を使用します。 ポート セキュリティでは、特定のポートに接続されたシステムの MAC アドレスを指定する機能が提供されます。 またポート セキュリティでは、ポート セキュリティ違反が発生した場合に行うアクションを指定する機能も提供されます。

- **Address Resolution Protocol (ARP) スプーフィング**ARP は、同じサブネットのホストが存在する local area network (LAN; ローカル エリア ネットワーク) セグメント内で IP アドレッシングを MAC アドレスにマップするために使用されます。 通常、ホストが特定の IP アドレスを持つ別のホストの MAC アドレスを検出するためにブロードキャスト ARP 要求を送出すると、要求に一致するアドレスを持つホストから ARP 応答が送られてきます。 続いて要求側のホストは、この ARP 応答をキャッシュします。 ARP プロトコル内部では、ホストが非要請 ARP 応答を実行するために別のプロビジョンが行われます。 非要請 ARP 応答は Gratuitous ARP (GARP) と呼ばれます。 GARP は、LAN セグメント上の IP アドレスの識別情報をスプーフィングするために攻撃者により悪用される可能性があります。 これは一般的に、「man-in-the-middle」(中間者) 攻撃で 2 つのホスト間の識別情報、またはデフォルト ゲートウェイを通過するすべてのトラフィックをスプーフィングするために使用されます。ARP 応答に細工を施すと、ネットワーク攻撃者は自身のシステムを、送信側により捜索されている宛先ホストであるかのように装うことができます。 この ARP 応答により、送信側は ARP キャッシュにネットワーク攻撃者のシステムの MAC アドレスを保存します。 この MAC アドレスは、スイッチにより CAM テーブル内にも保存されます。 このようにしてネットワーク攻撃者は、送信側のスイッチの CAM テーブルと ARP キャッシュの両方に、自身のシステムの MAC アドレスを挿入してしまいます。 これにより、ネットワーク攻撃者はスプーフィングしているホストが宛先になっているフレームを捕捉できるようになります。インターフェイスの設定メニューでホールドダウン タイマーを使用すると、エントリが ARP キャッシュ内に留まる時間の長さを設定することにより、ARP スプーフィング攻撃を緩和できます。 ただし、ホールドダウン タイマーだけでは不十分です。 スタティック ARP エントリだけでなく、すべてのエンド システム上で ARP キャッシュの有効時間を変更することが必要になります。 ARP を基にしたさまざまなネットワークの悪用の緩和に使用できるもう 1 つのソリューションとしては、ダイナミック ARP インスペクションとともに DHCP スヌーピングを使用する方法があります。 これらの Catalyst の機能は、ネットワーク内の ARP パケットを検証し、IP アドレス バインディングに対して無効な MAC アドレスを持つ ARP パケットの捕捉、ロギング、および廃棄を許可します。DHCP スヌーピングは、セキュリティを実現するため、信頼できる DHCP メッセージのフィルタリングを行います。 続いて、これらのメッセージは、DHCP スヌーピング バインディング テーブルを構築および維持するために使用されます。 DHCP スヌーピングでは、DHCP サーバ ポートではないユーザ側のポートが発信元である DHCP メッセージが、信頼できないとみなされます。 DHCP スヌーピングの観点から見ると、これらの信頼できないユーザ側のポートでは、DHCPOFFER、DHCPACK、DHCPNAK などの DHCP サーバ タイプの応答を送信できません。 DHCP スヌーピング バインディング テーブルには、MAC アドレス、IP アドレス、リース時間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカル インターフェイスに対応するインターフェイス情報が含まれます。 DHCP スヌーピング バインディング テーブルには、信頼できるインターフェイスで相互接続されているホストに関する情報は含まれていません。 信頼できないインターフェイスとは、ネットワークまたはファイアウォールの外部からのメッセージを受信するように設定されているインターフェイスです。 信頼できるイ

ンターフェイスとは、ネットワーク内部からのメッセージだけを受信するように設定されているインターフェイスです。 DHCP スヌーピング バインディング テーブルは、IP アドレス バインディングに対する、ダイナミックとスタティック両方の MAC アドレスを含むことができます。ダイナミック ARP インスペクションでは、DHCP スヌーピング データベースに格納されている IP アドレス バインディングに対して有効な MAC アドレスに基づいて、ARP パケットの有効性を判別します。 また、ダイナミック ARP インスペクションでは、ユーザ設定可能な Access Control List (ACL; アクセス コントロール リスト) に基づいて、ARP パケットを検証できます。 これにより、スタティックに設定された IP アドレスを使用するホストの ARP パケットを検査できるようになります。 ダイナミック ARP インスペクションにより、ポート単位および VLAN Access Control List (VACL; VLAN アクセス コントロール リスト) を使用して、特定の MAC アドレスに対する特定の IP アドレスの ARP パケットを制限することができます。

- **ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) 枯渇**DHCP 枯渇攻撃は、スプーフィングされた MAC アドレスを持つ DHCP 要求のブロードキャストにより作動します。 十分な要求を送信すると、ネットワーク攻撃者は、一定期間 DHCP サーバが使用できるアドレス空間を使い尽くすことができます。 次に、ネットワーク攻撃者は自身のシステム上に不正な DHCP サーバを設定して、ネットワーク上のクライアントからの新しい DHCP 要求に応答することができます。 ネットワーク上に不正な DHCP サーバが配置されていると、ネットワーク攻撃者がクライアントにアドレスなどのネットワーク情報を提供できます。通常、DHCP 応答にはデフォルト ゲートウェイと DNS サーバ情報が含まれているため、ネットワーク攻撃者は自身のシステムをデフォルト ゲートウェイおよび DNS サーバとして提供することができます。 これは、中間者攻撃になります。 ただし、不正な DHCP サーバを導入するには、DHCP アドレスのすべてを使い尽くす必要はありません。DHCP スヌーピングなどの Catalyst ファミリ スイッチの追加機能を使用すると、DHCP 枯渇攻撃に対する防止策として活用できます。 DHCP スヌーピングとは、信頼できない DHCP メッセージをフィルタリングし、DHCP スヌーピング バインディング テーブルの構築と維持を行うセキュリティ機能です。 バインディング テーブルに納められる情報には、MAC アドレス、IP アドレス、リース時間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカル インターフェイスに対応するインターフェイス情報があります。 信頼できないメッセージとは、ネットワークやファイアウォールの外部から受信されたメッセージです。 信頼できないスイッチ インターフェイスとは、ネットワークやファイアウォールの外部からこのようなメッセージを受信するよう設定されているスイッチ インターフェイスです。IP ソース ガードなどのその他の Catalyst スイッチの機能は、DHCP 枯渇や IP スプーフィングなどの攻撃に対する追加の防御策を提供できます。 DHCP スヌーピングと同様に、IP ソース ガードは、信頼できないレイヤ 2 ポートに対して有効になります。 DHCP スヌーピング プロセスにより捕捉された DHCP パケットを除き、すべての IP トラフィックは最初の時点でブロックされます。 クライアントが DHCP サーバから有効な IP アドレスを受信すると、そのポートには PACL が適用されます。 これにより、クライアント IP トラフィックは、バインディングで設定されている発信元 IP アドレスに制限されます。 バインディング内のアドレス以外の発信元アドレスを持つその他の IP トラフィックはすべてフィルタリングされます。

設定

このセクションでは、ポート セキュリティ、DHCP スヌーピング、ダイナミック ARP インスペクション、および IP ソース ガードのセキュリティ機能を設定するための情報を説明します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool (登録ユーザ専用) を使用してください。

Catalyst 3750 スイッチの設定には次の要素が含まれます。

- ポート セキュリティ
- DHCP スヌーピング
- ダイナミック ARP インスペクション
- IP ソース ガード

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

- PC 1 および PC 3 はスイッチに接続されているクライアントです。
- PC 2 はスイッチに接続されている DHCP サーバです。
- スイッチのすべてのポートは同じ VLAN (VLAN 1) 内にあります。
- DHCP サーバは、クライアントの MAC アドレスに基づいてクライアントに IP アドレスを割り当てるように設定されています。

ポート セキュリティ

ポート セキュリティ機能を使用すると、ポートにアクセスできるステーションの MAC アドレスを制限および識別することができます。 これにより、インターフェイスへの入力が制限されます。 セキュア ポートにセキュア MAC アドレスを割り当てた場合、ポートでは、定義済みアドレスのグループ外の発信元アドレスを持つパケットは転送されません。 セキュア MAC アドレスの数を 1 に制限し、1 つのセキュア MAC アドレスを割り当てた場合、そのポートに接続されたワークステーションには、ポートの完全な帯域幅が保証されます。 ポートがセキュア ポートとして設定され、セキュア MAC アドレスの最大数に到達した場合、そのポートにアクセスしようとするステーションの MAC アドレスが、特定されたセキュア MAC アドレスと異なると、セキュリティ違反が発生します。 また、1 つのセキュア ポート上で設定または学習されたセキュア MAC アドレスを持つステーションが、別のセキュア ポートへのアクセスを試みた場合、違反のフラグが発生します。 デフォルトでは、セキュア MAC アドレスの最大数を超えた場合、ポートはシャットダウンします。

注: Catalyst 3750 スイッチがスタックに加入する際、その新しいスイッチは設定済みのセキュア アドレスを受信します。 新しいスタック メンバにより、その他のスタック メンバから、すべてのダイナミックなセキュア アドレスがダウンロードされます。

ポート セキュリティの設定方法のガイドラインについては、『設定のガイドライン』を参照してください。

ここでは、ファーストイーサネット 1/0/2 インターフェイス上にはポート セキュリティ機能が設定済と表示されています。 デフォルトでは、インターフェイスのセキュア MAC アドレスの最大数は 1 です。 show port-security interface コマンドを発行すると、インターフェイスのポート セキュリティの状態を確認できます。

ポート セキュリティ

```
Cat3750#show port-security interface fastEthernet 1/0/2
Port Security : Disabled Port Status : Secure-down
Violation Mode : Shutdown Aging Time : 0 mins Aging Type
: Absolute SecureStatic Address Aging : Disabled Maximum
MAC Addresses : 1 Total MAC Addresses : 0 Configured MAC
Addresses : 0 Sticky MAC Addresses : 0 Last Source
Address:Vlan : 0000.0000.0000:0 Security Violation Count
```

```
: 0 !--- Default port security configuration on the
switch. Cat3750#conf t Enter configuration commands, one
per line. End with CNTL/Z. Cat3750(config)#interface
fastEthernet 1/0/2 Cat3750(config-if)#switchport port-
security Command rejected: FastEthernet1/0/2 is a
dynamic port. !--- Port security can only be configured
on static access ports or trunk ports. Cat3750(config-
if)#switchport mode access !--- Sets the interface
switchport mode as access. Cat3750(config-if)#switchport
port-security !--- Enables port security on the
interface. Cat3750(config-if)#switchport port-security
mac-address 0011.858D.9AF9 !--- Sets the secure MAC
address for the interface. Cat3750(config-if)#switchport
port-security violation shutdown !--- Sets the violation
mode to shutdown. This is the default mode. Cat3750# !--
- Connected a different PC (PC 4) to the FastEthernet
1/0/2 port !--- to verify the port security feature.
00:22:51: %PM-4-ERR_DISABLE: psecure-violation error
detected on Fa1/0/2, putting Fa1/0/2 in err-disable
state 00:22:51: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
0011.8565.4B75 on port FastEthernet1/0/2. 00:22:52:
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0/2, changed state to down 00:22:53:
%LINK-3-UPDOWN: Interface FastEthernet1/0/2, changed
state to down !--- Interface shuts down when a security
violation is detected. Cat3750#show interfaces
fastEthernet 1/0/2 FastEthernet1/0/2 is down, line
protocol is down (err-disabled) !--- Output Suppressed.
!--- The port is shown error-disabled. This verifies the
configuration. !--- Note: When a secure port is in the
error-disabled state, !--- you can bring it out of this
state by entering !--- the errdisable recovery cause
psecure-violation global configuration command, !--- or
you can manually re-enable it by entering the !---
shutdown and no shutdown interface configuration
commands. Cat3750#show port-security interface
fastEthernet 1/0/2 Port Security : Enabled Port Status :
Secure-shutdown Violation Mode : Shutdown Aging Time : 0
mins Aging Type : Absolute SecureStatic Address Aging :
Disabled Maximum MAC Addresses : 1 Total MAC Addresses :
1 Configured MAC Addresses : 1 Sticky MAC Addresses : 0
Last Source Address:Vlan : 0011.8565.4B75:1 Security
Violation Count : 1
```

注: 同じ MAC アドレスはスイッチの異なるポートのセキュアおよび静的なMACアドレスで設定するべきではありません。

IP Phone が voice VLAN のために設定されるスイッチポートを通してスイッチに接続されるとき電話はタグが付いていない CDPパケットおよびタグ付けされた音声 CDPパケットを送信します。 従って IP Phone の MAC アドレスは PVID および VVID 両方で学習されます。 セキュリティ保護アドレスの適切な桁数が設定されない場合、エラーメッセージをこのメッセージに類似したに得ることができます:

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 001b.77ee.eeee on port GigabitEthernet1/0/18.
PSECURE: Assert failure: psecure_sb->info.num_addrs <= psecure_sb->max_addrs:
```

この問題を解決することがアクセス VLAN でできるセキュリティ保護アドレスの最大数と 2 へのポートのセキュリティ保護アドレスを (IP Phone のために) 与えられる最大を設定 して下さい。

詳細については、『ポート セキュリティの設定』を参照してください。

DHCP スヌーピング

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間のファイアウォールのように動作します。 DHCP スヌーピングを使用すると、エンドユーザに接続された信頼できないインターフェイスと、DHCP サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。 スイッチが信頼できないインターフェイス上でパケットを受信し、そのインターフェイスが DHCP スヌーピングが有効になっている VLAN に属する場合、スイッチは発信元 MAC アドレスと DHCP クライアント ハードウェアのアドレスを比較します。 アドレスが一致する場合（デフォルト）、スイッチはパケットを転送します。 アドレスが一致しない場合、スイッチはパケットを廃棄します。 スイッチが DHCP パケットを廃棄するのは、次のいずれかの状況が発生した場合です。

- DHCPOFFER、DHCPACK、DHCPNAK、または DHCPLEASEQUERY パケットなどの DHCP サーバからのパケットが、ネットワークまたはファイアウォールの外部から受信された。
- 信頼できないインターフェイス上でパケットが受信され、発信元 MAC アドレスと DHCP クライアント ハードウェアのアドレスが一致しない。
- DHCP スヌーピング バインディング データベース内にある MAC アドレスを持つ DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージがスイッチで受信されたが、バインディング データベース内のインターフェイス情報が、メッセージが受信されたインターフェイスと一致しない。
- DHCP リレー エージェントが DHCP パケットを転送し、このパケットに 0.0.0.0 ではないリレー エージェント IP アドレスが含まれている、またはリレー エージェントが option-82 情報を含むパケットを信頼できないポートに転送している。

DHCP スヌーピングの設定方法のガイドラインについては、『DHCP スヌーピング設定のガイドライン』を参照してください。

注: DHCP スヌーピングが正しく動作するためには、すべての DHCP サーバが、信頼できるインターフェイスを通じてスイッチに接続されている必要があります。

注: Catalyst 3750 スイッチによるスイッチ スタック内では、DHCP スヌーピングはスタック マスター上で管理されます。 新しいスイッチがスタックに加入する場合、そのスイッチはスタック マスターから DHCP スヌーピング設定を受信します。 メンバがスタックから離脱する場合、そのスイッチと関連付けられているすべての DHCP スヌーピング バインディングはエージング アウトします。

注: データベースのリース時間を正確にするため、Cisco では NTP を有効にして設定することを推奨いたします。 NTP が設定されていれば、スイッチのシステム クロックが NTP と同期している場合にのみ、スイッチはバインディングの変更をバインディング ファイルに書き込みます。

不正な DHCP サーバの問題は、DHCP スヌーピング機能により緩和できます。 スイッチ上でグローバルに DHCP を有効にするには、ip dhcp snooping コマンドを発行します。 DHCP スヌーピングを使用して設定された場合、VLAN 内のすべてのポートは DHCP 応答に関して信頼されません。 次の例では、DHCP サーバに接続されたファーストイーサネット インターフェイス 1/0/3 のみが信頼できるものとして設定されています。

DHCP スヌーピング
Cat3750#**conf t** Enter configuration commands, one per line. End with CNTL/Z. Cat3750(config)#**ip dhcp snooping**

```
!--- Enables DHCP snooping on the switch.
Cat3750(config)#ip dhcp snooping vlan 1 !--- DHCP
snooping is not active until DHCP snooping is enabled on
a VLAN. Cat3750(config)#no ip dhcp snooping information
option !--- Disable the insertion and removal of the
option-82 field, if the !--- DHCP clients and the DHCP
server reside on the same IP network or subnet.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip dhcp snooping trust !---
Configures the interface connected to the DHCP server as
trusted. Cat3750#show ip dhcp snooping Switch DHCP
snooping is enabled DHCP snooping is configured on
following VLANs: 1 Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed Verification
of hwaddr field is enabled Interface Trusted Rate limit
(pps) ------------------------ ------- ----------------
FastEthernet1/0/3 yes unlimited !--- Displays the DHCP
snooping configuration for the switch. Cat3750#show ip
dhcp snooping binding MacAddress IpAddress Lease(sec)
Type VLAN Interface ------------------ --------------- -
--------- ------------ ---- --------------------
00:11:85:A5:7B:F5 10.0.0.2 86391 dhcp-snooping 1
FastEtheret1/0/1 00:11:85:8D:9A:F9 10.0.0.3 86313 dhcp-
snooping 1 FastEtheret1/0/2 Total number of bindings: 2
!--- Displays the DHCP snooping binding entries for the
switch. Cat3750# !--- DHCP server(s) connected to the
untrusted port will not be able !--- to assign IP
addresses to the clients.
```

詳細については、『DHCP 機能の設定』を参照してください。

ダイナミック ARP インスペクション

ダイナミック ARP インスペクションは、ネットワーク内の ARP パケットを検証するセキュリティ機能です。 無効な IP から MAC へのアドレス バインディングを持つ ARP パケットを捕捉、ログ記録、および廃棄します。 この機能は、ある種の中間者攻撃からネットワークを保護します。

ダイナミック ARP インスペクションにより、有効な ARP 要求および応答のみがリレーされるようになります。 スイッチは次の動作を実行します。

- 信頼できないポート上のすべての ARP 要求および応答を捕捉する
- ローカル ARP キャッシュを更新する前、またはパケットを適切な宛先に転送する前に、捕捉されたこれらの各パケットが、有効な IP から MAC へのアドレス バインディングを持っていることを確認する
- 無効な ARP パケットを廃棄する

ダイナミック ARP インスペクションは、信頼できるデータベースつまり 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 から MAC へのアドレス バインディングに基づいて、ARP パケットの有効性を判別します。 DHCP スヌーピングが VLAN およびスイッチ上で有効になっている場合、このデータベースは 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上で ARP パケットが受信された場合、スイッチはチェックを行うことなくそ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上では、スイッチはパケットが有効である場合にのみパケットを転送します。

非 DHCP 環境では、ダイナミック ARP インスペクションは、スタティックに設定された IP アドレスを持つホストのユーザ設定 ARP ACL に照らし合わせて ARP パケットを検証することができます。 arp access-list グローバル設定コマンドを発行すると、ARP ACL を定義できます。 ARP

ACL 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よりも優先されます。スイッチが ACL を使用するのは、ユーザが ip arp inspection filter vlan グローバル設定コマンドを発行して ACL を設定する場合のみです。 スイッチはまず、ARP パケットをユーザ設定 ARP ACL と照合します。 ARP ACL で ARP パケットが拒否されると、DHCP スヌーピングにより入力されるデータベース内に有効なバインディングが存在する場合であっても、スイッチはそのパケットを拒否します。

ダイナミック ARP インスペクションの設定方法のガイドラインについては、『ダイナミック ARP インスペクション設定のガイドライン』を参照してください。

VLAN 単位でダイナミック ARP インスペクションを有効にするには、ip arp inspection vlan グローバル設定コマンドを発行します。 次の例では、ip arp inspection trust コマンドを使用して、DHCP サーバに接続されたファーストイーサネット インターフェイス 1/0/3 のみが信頼できるものとして設定されています。 ダイナミックに割り当てられる IP アドレスを持つ ARP パケットを許可するには、DHCP スヌーピングを有効にする必要があります。 DHCP スヌーピングの設定に関しては、このドキュメントの「DHCP スヌーピング」のセクションを参照してください。

ダイナミック ARP インスペクション

```
Cat3750#conf t Enter configuration commands, one per
line. End with CNTL/Z. Cat3750(config)#ip arp inspection
vlan 1 !--- Enables dynamic ARP inspection on the VLAN.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip arp inspection trust !---
Configures the interface connected to the DHCP server as
trusted. Cat3750#show ip arp inspection vlan 1 Source
Mac Validation : Disabled Destination Mac Validation :
Disabled IP Address Validation : Disabled Vlan
Configuration Operation ACL Match Static ACL ---- ------
------- --------- --------- ---------- 1 Enabled Active
Vlan ACL Logging DHCP Logging ---- ----------- ---------
--- 1 Deny Deny !--- Verifies the dynamic ARP inspection
configuration. Cat3750#
```

詳細については、『ダイナミック ARP インスペクションの設定』を参照してください。

IP ソース ガード

IP ソース ガードは、非ルーテッド レイヤ 2 インターフェイス上の IP トラフィックを制限するため、DHCP スヌーピング バインディング データベースと、手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングするセキュリティ機能です。 IP ソース ガードを使用すると、ホストがネイバーの IP アドレスを使用しようとしたときに発生するトラフィック攻撃を防止できます。 IP ソース ガードは IP/MAC スプーフィングを防止します。

信頼できないインターフェイス上で DHCP スヌーピングが有効になっている場合、IP ソース ガードを有効にすることができます。 あるインターフェイス上で IP ソース ガードが有効にされた後は、DHCP スヌーピングにより許可される DHCP パケットを除き、そのインターフェイス上で受信されるすべての IP トラフィックはスイッチによりブロックされます。 そのインターフェイスにはポート ACL が適用されます。 ポート ACL は、IP ソース バインディング テーブル内にある送信元 IP アドレスを持つ IP トラフィックだけを許可し、その他すべてのトラフィックを拒否します。

IP ソース バインディング テーブルには、DHCP スヌーピングにより学習されたバインディング、または手動で設定されたバインディング（スタティック IP ソース バインディング）があります。 このテーブルのエントリには、IP アドレス、それに関連付けられた MAC アドレス、および

それに関連付けられた VLAN 番号が含まれます。 スイッチが IP ソース バインディング テーブルを使用するのは、IP ソース ガードが有効である場合のみです。

IP ソース ガードの設定では、発信元 IP アドレス フィルタリング、または発信元 IP および MAC アドレス フィルタリングを使用できます。 このオプションを使用して IP ソース ガードが有効になっていると、IP トラフィックは発信元 IP アドレスに基づいてフィルタリングされます。 スイッチが IP トラフィックを転送するのは、発信元 IP アドレスが、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、または IP ソース バインディング テーブル内のバインディングに一致する場合です。 このオプションを使用して IP ソース ガードが有効になっていると、IP トラフィックは発信元の IP アドレスと MAC アドレスに基づいてフィルタリングされます。 スイッチがトラフィックを転送するのは、発信元の IP アドレスと MAC アドレスが、IP ソース バインディング テーブル内のエントリに一致する場合のみです。

注: IP ソース ガードはレイヤ 2 ポート上でのみサポートされます。これにはアクセスポートとトランク ポートが含まれます。

IP ソース ガードの設定方法のガイドラインについては、『IP ソース ガード設定のガイドライン』を参照してください。

次の例では、発信元 IP フィルタリングを使用した IP ソース ガードが、ip verify source コマンドを使用して、ファーストイーサネット 1/0/1 インターフェイス上で設定されています。 発信元 IP フィルタリングを使用する IP ソース ガードが VLAN 上で有効である場合、インターフェイスが属するアクセス VLAN 上で DHCP スヌーピングを有効にする必要があります。 スイッチ上の IP ソース ガードの設定を確認するには、show ip verify source コマンドを発行します。

IP ソース ガード

```
Cat3750#conf t Enter configuration commands, one per
line. End with CNTL/Z. Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 1 !--- See the
DHCP Snooping section of this document for !--- DHCP
snooping configuration information.
Cat3750(config)#interface fastEthernet 1/0/1
Cat3750(config-if)#ip verify source !--- Enables IP
source guard with source IP filtering. Cat3750#show ip
verify source Interface Filter-type Filter-mode IP-
address Mac-address Vlan --------- ----------- ---------
-- --------------- ---------------- ----- Fa1/0/1 ip
active 10.0.0.2 1 !--- For VLAN 1, IP source guard with
IP address filtering is configured !--- on the interface
and a binding exists on the interface. Cat3750#
```

詳細は、『IP ソース ガードについて』を参照してください。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- プライベート VLAN および VLAN アクセス コントロール リストによるネットワーク セキュリティの確保
- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems