初期ホップ セキュリティの構成

この章で説明する内容は、次のとおりです。

VXLAN BGP EVPN 中の DHCP スヌーピングの

VXLAN BGP EVPN 中の DHCP スヌーピングは、以下のようなプロセスです：

- ホストから送信された ARP/GARP パケットを検証し、ARP スプーフィングと悪意のある ARP ストームを防止します。
- IPSG を使用してホストからのデータプレーン トラフィックを検証し、悪意のあるホストがデータ トラフィックを送信するのを防ぎます。
- VXLAN ファブリック全体に DHCP スヌーピング エントリを複製し、ホストが移動した後でも DAI と IPSG がファブリック全体で機能できるようにします。

ファーストホップ セキュリティ

ファースト ホップ セキュリティ（FHS）は、次のようなアクセス セキュリティ 機能です：

- ホストが最初のスイッチに接続するアクセス ポイントでネットワークにセキュリティを提供します。
- ホストを承認および認証します。
- 許可されたホストのみがネットワーク アクセスを許可されるようにすることにより、ネットワークを保護します。

Dot1x、ポート セキュリティ、DHCP スヌーピングは、アクセス セキュリティ機能の例です。

DHCP スヌーピング データベース

DHCPスヌーピングデータベース（DB）は、次のようなデータベースです：

- ホストの MAC アドレス、DHCP サーバによってホストに割り当てられた IP アドレス、VLAN、およびリース時間などその他の詳細が含まれています。
- ローカルまたはリモートのスヌーピング DB エントリを含めることができます。
- **ip source binding** *ip address* **vlan** *vlan-id* **interface** *interface* インターフェイス コマンドを使用して設定できます。

（注） このコマンドを使用して追加されたスヌーピング エントリは、スタティック エントリと呼ばれ、すべての VTEP に分散されます。

分散 DHCP スヌーピング データベース

分散 DHCP スヌーピング DB は、次のようなデータベースです：

- DAI を使用してホストから送信された ARP/GARP を検証します。

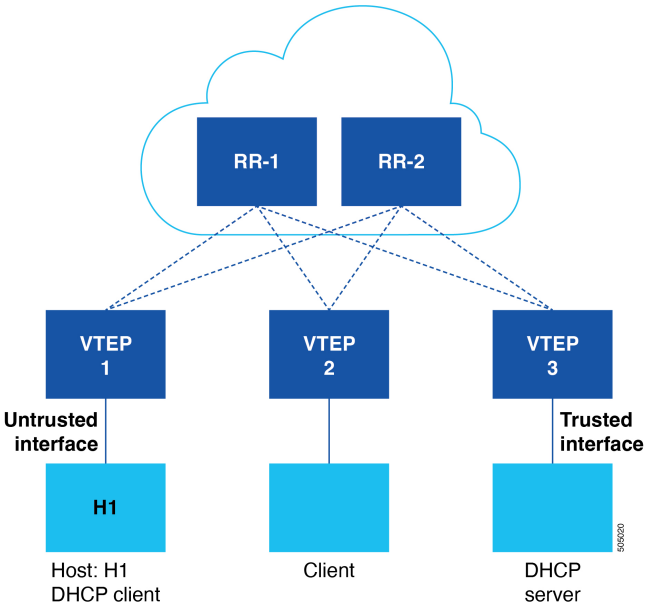
（注） DB に一致するエントリがない場合、ARP/GARP をドロップします。

- IPSG を使用してホストからのデータプレーン トラフィックを検証します。
- ファブリック全体に複製されます。

VXLAN での DHCP スヌーピングの仕組み

VXLAN プロセスでの DHCP スヌーピングには、VXLAN ファブリック全体のホストと DHCP サーバー間の交換が含まれます。ARP /GARP パケットとデータプレーン トラフィックを検証する DHCP スヌーピング データベースを作成および配布します。

図 *1 : VXLAN* での *DHCP* スヌーピング



このプロセスに関与する主要なコンポーネントは次のとおりです。

- **ホスト**は IP アドレスを要求します。ホスト H1 は VTEP1 に接続されています
- **VTEP**：ホストを VXLAN ファブリックに接続し、セキュリティ ポリシーを適用します。
- **DHCP サーバ**：IP アドレスと構成パラメータをホストに割り当てます。DHCP サーバは VTEP3 に接続されています。
- **VXLAN ファブリック**：VTEP を接続し、ホストとサーバ間の通信を可能にするネットワーク インフラストラクチャ。
- **DHCP スヌーピング データベース**：IP から MAC アドレスへのバインディング、およびその他のホスト情報を保存します。

このプロセスには、次の段階が含まれます。

- ホストは、 DHCP サーバを検索するために、 DHCP 検出メッセージを送信します。
- DHCP サーバは、ホストに IP アドレスを提案する DHCP 提供メッセージを送信します。
- ホストは、 DHCP 要求メッセージを送信して、提供された IP アドレスを受け入れます。
- DHCP サーバは DHCP Ack メッセージを送信して、IP アドレス割り当てを確認します。

（注）

- ホストと DHCP サーバーは、このホスト IP 割り当て手順の一部として一連のメッセージを交換します。これらは、Discover-Offer-Request-Ack（DORA）交換メッセージとして知られています。
- 特定のホスト（H1）の DORA 交換は、リモート DHCP サーバー（VTEP3）に到達するために VXLAN ファブリックを介して送信する必要があります。
- VTEP3 は、DHCP サーバから来た「Offer」および「Ack」メッセージ（DORA シーケンスの一部）が、信頼できるインターフェイスで受信されたことを確認します。

- DORA 交換が完了すると、VTEP1 はホストのために DHCP スヌーピング データベース エントリを作成します。
- ローカル DHCP スヌーピング データベース エントリが BGP-EVPN を使用してリモート VTEP に伝播されます。
- リモート VTEP は、スヌーピング データベース エントリをリモート エントリとして保存します。
- DAI は、スプーフィングを防ぐために、DHCP スヌーピングデータベースに対して ARP /GARP パケットを検証します。
- IPSG は、悪意のあるトラフィックを防ぐために、DHCP スヌーピング データベースに対してデータプレーン トラフィックを検証します。

  IPSG では、VTEP のローカル DHCP クライアントのみがプログラムされます。ローカル DHCP クライアントは、DHCP スヌーピング テーブルでアンカー フラグが true に設定されて識別されます。ホストが別の VTEP に移動して安定した場合、IPSG は新しい VTEP の背後にあるクライアントを再プログラムして、データトラフィックを検証する必要があります。古い VTEP では、IPSG はこの DHCP クライアントを削除する必要があります。アンカーフラグはそれに応じて変更されます。ホストの移動は、ホストが移動した新しい VTEP で受信されたホストからの ARP 要求の受信によってトリガーされます。
- DHCP スヌーピング データベースは、ホストが別の VTEP に移動すると、新しい場所を反映するように更新されます。

  この DHCP スヌーピング データベースは VTEP 全体での「分散データベース」と見なされ、スヌーピング エントリはすべての VTEP と同期されます。

VXLAN プロセスでの DHCP スヌーピングは、IP から MAC アドレスへのバインディングの分散データベースに対してトラフィックを検証することにより、セキュアな IP アドレス割り当てを確保し、悪意のある活動を防止します。

VXLAN 上の DHCP スヌーピングの注意事項および制約事項

VXLAN 機能での DHCP スヌーピングには、次の注意事項および制約事項があります。

構成の注意事項および制約事項

- DHCP スヌーピング、DAI、および IPSG がすべての VTEP で同時に有効になっていることを確認します。

（注） DAI と IPSG は DHCP スヌーピングに依存します。DHCP スヌーピングはスヌーピング DB を作成し、この DB は DAI と IPSG によって使用されます。

- ホスト移動は、ARP/GARP/RARP 受信によって示されます。RARP（MAC 情報のみを含む）の場合、VTEP は MAC に対して学習した IP の ARP 更新を開始します。実質的に ARP-GARP はホスト移動のトリガであり、他のデータ パケットではありません。
- 入力 SUP リージョンでは、 **hardware access-list tcam region ing-sup** コマンドを使用して入力 ACL を設定するには、TCAM をデフォルトの 512 エントリではなく 768 エントリにカービングする必要があります。TCAM カービングの変更を反映するには、スイッチのリロードが必要です。
- I/O モジュールに Atomic アップデートに必要なリソースがない場合は、**no hardware access-list update atomic** コマンドを使用して Atomic アップデートをディセーブルにすることができますが、デバイスで既存の ACL を削除して、アップデートされた ACL を適用するには、多少の時間がかかります。ACL が適用されるトラフィックは、デフォルトでドロップされます。
- ACL が適用されるすべてのトラフィックを許可し、同時に非 Atomic アップデートを受信するようにするには、**hardware access-list update default-result permit** コマンドを使用してください。
- マルチサイトで vPC BGW を使用する場合、vPC BGW で DHCP スヌーピングが有効になっている場合は、DHCP クライアントと DHCP サーバが同じサイトにあることを確認します。

（注）
- DHCP スヌーピングは、DHCP サービスを使用する必要がある DHCP ホストに属する VLAN に対して（VTEP で）有効にする必要があります。
- ファブリック内の DHCP サーバがサービスを提供するすべての VLAN は、ファブリックのすべての VTEP で DHCP スヌーピングを有効にする必要があります。

サポートされる機能とプラットフォーム

- Cisco NX-OS リリース 10.4(1)F 以降では、DHCP スヌーピングと、ダイナミック ARP 検査（DAI）や IP ソース ガード（IPSG）のサポートなどの関連機能が、Cisco Nexus 9300-/FX/FX2/FX3/GX/GX2 プラットフォーム スイッチおよび X97160YC-EX および 9700-FX/GX ライン カードを使用する Cisco Nexus 9500 スイッチの VXLAN ファブリックに拡張されています。

  Cisco NX-OS リリース 10.4(2)F 以降、初期ホップ セキュリティ機能は Cisco Nexus 9332D-H2R、および 93400LD-H1 スイッチでサポートされます。

  Cisco NX-OS リリース 10.4(2)F 以降、初期ホップ セキュリティ機能は Cisco Nexus 9364C-H1 スイッチでサポートされます。

- Cisco NX-OS リリース 10.5(2)F 以降、ファースト ホップ セキュリティの機能は N9K-X9736C-FX3 ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチでサポートされています。

- IPv4 マルチキャスト アンダーレイのみがサポートされています。ただし、IPv4 入力レプリケーション アンダーレイ、IPv6 入力レプリケーション アンダーレイ、および IPv6 マルチキャスト アンダーレイはサポートされていません。

- IPv4 DHCP ホストのみがサポートされます。

- vPC VTEP の場合、物理 MCT のみがサポートされます。

- vPC ノードでは、静的 DHCP スヌーピングは vPC ポートチャネル ポートでのみサポートされ、孤立ポートではサポートされません。

サポートされない機能とプラットフォーム

- ファースト ホップ セキュリティ機能は EoR ではサポートされていません。

- DHCP サーバーを EoR の背後に展開することはできません。

- この機能は、FabricPath から VXLAN への移行機能およびカウンタ ACL（CNT ACL）機能と共存できません。

DHCP スヌーピングの前提条件

DHCPスヌーピングには、次の前提条件があります。

- DHCP スヌーピングまたはDHCP リレー エージェントを構成するためには、DHCP についての知識が必要です。
- DHCP スヌーピング、DAI、および IPSG 機能がリーフ VTEP で同時に有効になっていることを確認します。

VXLAN での DHCP スヌーピングの有効化

シングルボックス機能でDHCPスヌーピングを有効または無効にすることも、ファブリック全体のVLANに対してこの機能を有効にすることもできます。デフォルトでは、DHCPスヌーピングはすべての VLAN で無効になっています。

VXLAN 上で DHCP スヌーピングを有効ににするには、次の手順に従います。

始める前に

- DHCP 機能を有効にしたことを確認します。
- **nv overlay evpn** コマンドを構成したことを確認します。
- DHCP スヌーピング、DAI、および IPSG 機能を有効にしたことを確認します。詳細は、DHCP スヌーピングの前提条件 （7 ページ） のセクションを参照してください。
- DHCP スヌーピングと DAI をすべての VXLAN ノードで有効にしたことを確認します。構成の詳細については『Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド』の「**DHCP スヌーピングの構成**」 を参照してください。
- DHCP サーバ ノードに接続されているインターフェイスで、DHCP スヌーピングの信頼と ARP インスペクションの信頼を有効にしたことを確認します。構成の詳細については『Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド』の「**DHCP スヌーピングの構成**」 を参照してください。
- DHCP クライアント ノードに接続されているインターフェイスで IP ソース ガード機能を有効にしたことを確認します。構成の詳細については『Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド』の「**DHCP スヌーピングの構成**」 を参照してください。

手順

ステップ 1 **configure terminal** コマンドを実行して、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。

例：

```
switch# configure terminal
switch(config)#
```

ステップ 2 [**no**] **ip dhcp snooping vlan** *vlan-list* **evpn** コマンドを実行して、 *vlan-list* で指定した VLAN の DHCP スヌーピングを有効にします。

例：

```
switch(config)# ip dhcp snooping vlan 100,200,250-252 evpn
```

Cisco NX-OS リリース 10.4(1)F 以降では、同じ VTEP または他の VTEP 上の他のインターフェイスへのホストの移動をサポートするための **evpn** オプションが提供されています。

（注）
- **evpn** オプションを使用してこの機能を有効にすると、 **nve** は信頼できるインターフェイスとして暗黙的に追加されます。
- **evpn** キーワードを含むVLANリストと **no evpn** キーワードを含む別のVLANリストを含めることができます。

このコマンドの **no** 形式を使用すると、指定した VLAN の DHCP スヌーピングが無効になります。

ステップ 3 （任意） **show running-config dhcp** を実行します コマンドを実行して、DHCP 構成を検証します。

例：

```
switch(config)# show running-config dhcp
```

ステップ 4 （任意） **copy running-config startup-config** コマンドを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例：

```
switch(config)# copy running-config startup-config
```

永続的な凍結後の重複ホストのクリア

MACまたはMAC-IPアドレスが永続的に凍結された場合、モビリティの再起動や重複のチェックのために自動的に回復することはできません。

FHS 対応 VTEP の DHCP クライアントのモビリティおよび重複検出ロジックは、BGP EVPN モビリティおよび重複検出ロジックと同じです。ただし、非 FHS 展開のいずれかの VTEP で重複検出が発生する可能性があります。FHS 展開では、DHCP バインディング エントリがリモートである VTEP でホストの重複が常に検出されます。

モビリティと重複検出の詳細については、「IP アドレスと MAC アドレスの重複データ検出」セクションを参照してください。

MAC または MAC-IP が永続的に凍結された場合に、モビリティまたは重複チェックシーケンスを再開する自動回復メカニズムはありません。MAC および MAC-IP の永続的な凍結状態をクリアするには、次のコマンドを使用します。

- MAC の場合：

```
clear l2route evpn mac [mac-address] [topo] permanently-frozen-list
```

- MAC-IP の場合：

```
clear fabric forwarding dup-host [{ ip|ipv6 address }] [vrf {vrf-name | vrf-known-name
 | all}]
```

DHCP スヌーピング構成の確認

DHCPスヌーピングの構成を検証するには、次のコマンドを入力します。

コマンド	目的
show ip dhcp snooping binding evpn	DHCP スヌーピング バインディング データベースからすべてのエントリを表示します。
show l2route fhs [**topology** *topology id* | **all**]	L2RIB データベースのすべてのエントリを表示します。

次の例は、**show ip dhcp snooping binding evpn** コマンドのサンプル出力を示しています。

```
switch(config)# show ip dhcp snooping binding evpn
MacAddress          IpAddress        Lease(Sec)  Type      BD    Interface       anchor
     Freeze
----------------- -------------- ----------- ---------- ---- ----------------- ----------
 ---------
00:10:00:10:00:10  10.10.10.10      infinite  static      2001  Ethernet1/48         YES
       NONE
00:15:06:00:00:01  100.1.150.156    86282     dhcp-snoop  2001  Ethernet1/31         YES
       NONE
00:17:06:00:00:01  100.1.150.155    86265     dhcp-snoop  2001  nve1(peer-id: 1)     NO
        NONE
```

次の例は、**show l2route fhs** コマンドのサンプル出力を示しています。

```
switch(config)# show l2route fhs all
Flags - (Stt):Static (Dyn):Dynamic (R):Remote
Topo ID  Mac Address     Host IP             Prod          Flags      Seq No     Next-Hops
---- -- ---- ----------- ------------------ ---------- ----------- ------------
-------------
2001     0015.0600.0001  100.1.150.156      DHCP_DYNAMIC  Dyn,       0          Eth1/31
2001     0017.0600.0001  100.1.150.155      BGP           Dyn,R,     0          1.13.13.13
 (Label: 0)
switch(config)#
```

次の例は、DHCP クライアントを使用した VTEP の DHCP 構成を示しています。

```
feature dhcp
service dhcp
ip dhcp snooping
ip dhcp snooping vlan 2001-2002 evpn
ip arp inspection vlan 2001-2002

interface Ethernet1/31
ip verify source dhcp-snooping-vlan
```

次の例は、DHCP サーバーを使用した VTEP の DHCP 構成を示しています。

```
feature dhcp
service dhcp
ip dhcp snooping
ip dhcp snooping vlan 2001-2002 evpn
ip arp inspection vlan 2001-2002

interface Ethernet1/47
ip dhcp snooping trust
ip arp inspection trust
```

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。