初期ホップ セキュリティの構成

この章は、次の内容で構成されています。

VXLAN BGP EVPN 中の DHCP スヌーピングの概要

初期ホップセキュリティ（FHS）は、アクセス（ホストがネットワーク内の最初のスイッチに接続する場所）でネットワークにセキュリティを提供するアクセス セキュリティ機能です。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。これらのセキュリティ機能が連携してホストを許可および認証し、正当なホストだけがネットワークを使用できるようにすることで、ネットワークを保護します。

現在、ダイナミック ARP 検査（DAI）および IP ソース ガード（IPSG）などの DHCP スヌーピングおよび関連する機能は、シングルスイッチに制限されています。Cisco NX-OS リリース 10.4(1)F 以降、これらの 3 機能のサポートは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2 プラットフォーム スイッチや、9700-EX/FX/GX ライン カードを搭載した Cisco Nexus 9500 スイッチで VXLAN ファブリック全体に拡張されます。

VXLAN トポロジでの DHCP スヌーピング

VXLAN ファブリックでは、ホストを 1 つの VTEP のインターフェイスに接続し、DHCP サーバーを別の VTEP のインターフェイスに接続できます。

図に示すように、ホスト H1 は VTEP1 に接続され、DHCP サーバは VTEP3 に接続されます。

初期ホップ セキュリティの構成

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、一般に 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、「Offer」および「Ack」メッセージ（DORA シーケンスの一部）と、それらが DHCP サーバーから来ていること、そして VTEP3 の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「DHCP スヌーピング DB」エントリを作成します。この DB には、ホストの MAC アドレス、DHCP サーバー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」などのその他の詳細が含まれています。この機能の主な仕組みは、「ローカル スヌーピング DB エントリ」としてホスト（H1）の VTEP1 で作成されたスヌーピング DB エントリが、BGP-EVPN を使用してリモート VTEP にも伝播され、ホスト（H1）からの「リモート スヌーピング DB エントリ」と見なされることです。したがって、この DHCP スヌーピング DB は VTEP 全体で「分散 DB」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。

ホストへの IP アドレス割り当てが事前に定義されているユース ケースでは、**ip source binding** *ip address* **vlan** *vlan-id* **interface** *interface* コマンドを使用してスヌーピング DB エントリを構成できます。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、これらもすべての VTEP に分散されます。

分散 DHCP スヌーピング DB は次のように使用されます。

- DAI を使用してホストから送信された ARP/GARP を検証します。これにより、異なるホスト クレデンシャルを使用した ARP/GARP のスプーフィング、そしてその後のネットワーク内での悪意のある ARP ストームが防止されます。

  VXLAN 環境では、host-move を考慮する必要があります。DHCP スヌーピング DB はファブリック全体に複製されるため、DAI は host-move の後もファブリック全体で動作できるようになりました。したがって、コントロールプレーンは VXLAN 環境で保護されます。

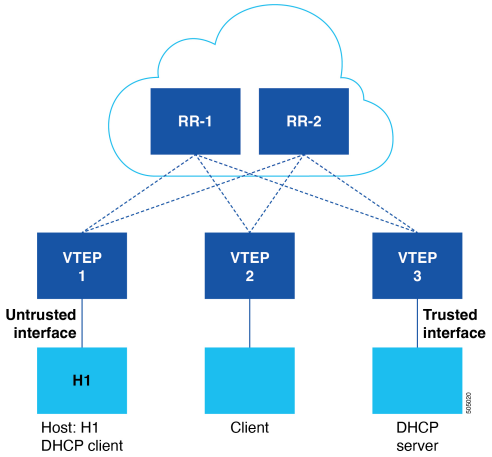
（注） DB に一致するエントリがない場合、ARP/GARP はドロップされます。

- 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。これにより、データ トラフィックが検証され、悪意のあるホストがネットワークにデータ トラフィックを送信するのを防ぐことができます。

  DHCP スヌーピング エントリは、ファブリック全体に複製されます。その VTEP のローカル DHCP クライアントのみが IPSG で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。

図 *1 : VXLAN* での *DHCP* スヌーピング



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、次の構成の注意事項および制約事項があります。

- 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-EX/FX/FX2/FX3/GX/GX2 プラットフォーム スイッチおよび 9700-EX/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。
- 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。

- 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。

- 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。したがって、基本的に 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。
- vPC VTEP の場合、物理 MCT のみがサポートされます。
- 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。
- 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。
- 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。

DHCP スヌーピングの前提条件

DHCP の前提条件は、次のとおりです。

- DHCP スヌーピングまたは DHCP リレー エージェントを設定するためには、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 でディセーブルになります。

初期ホップ セキュリティの構成

始める前に

- DHCP 機能がイネーブルにされていることを確認します。
- **nv overlay evpn** コマンドが構成されていることを確認します。
- DHCP スヌーピング、DAI、および IPSG 機能が有効になっていることを確認します。詳細については、DHCP スヌーピングの前提条件 （4 ページ） セクションを参照してください。
- DHCP スヌーピングと DAI がすべての VXLAN ノードで有効になっていることを確認します。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 サーバー 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が有効になっていることを確認します。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 ガードが有効になっていることを確認します。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。

手順の概要

1. **configure terminal**
2. [**no**] **ip dhcp snooping vlan** *vlan-list* **evpn**
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	[**no**] **ip dhcp snooping vlan** *vlan-list* **evpn** 例： `switch(config)# ip dhcp snooping vlan 100,200,250-252 evpn`	*vlan-list* で指定する VLAN の DHCP スヌーピングをイネーブルにします。 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。

	コマンドまたはアクション	目的
		（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** キーワードを指定した vlan-list-1 と、evpn キーワードを指定しない vlan-list-2 を使用できます。 このコマンドの **no** 形式を使用すると、指定した VLAN の DHCP スヌーピングがディセーブルになります。
ステップ 3	（任意） **show running-config dhcp** 例： `switch(config)# show running-config dhcp`	DHCP 設定を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

永続的な凍結後の重複ホストのクリア

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 バインディングの確認

DHCP スヌーピング バインディング情報を表示するには、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。