



DHCP グリーニング

このセクションでは、DHCP グリーニングについて説明します。

- [DHCP グリーニングの前提条件](#) (1 ページ)
- [DHCP グリーニングに関する情報](#) (1 ページ)
- [DHCP グリーニングの設定方法](#) (2 ページ)
- [DHCP グリーニングの設定例](#) (4 ページ)
- [DHCP グリーニングに関する追加情報](#) (4 ページ)
- [DHCP グリーニングの機能情報](#) (5 ページ)

DHCP グリーニングの前提条件

- インターフェイスがレイヤ2インターフェイスとして設定されていることを確認します。
- グローバルスヌーピングが有効になっていることを確認します。

DHCP グリーニングに関する情報

DHCP グリーニングの概要

グリーニングは、Dynamic Host Configuration Protocol (DHCP) リレーエージェントによってメッセージが転送される際に、DHCPメッセージからロケーション情報を抽出するのに役立ちます。このプロセスは完全にパッシブなスヌーピング機能であり、DHCPパケットのブロックも変更も行われません。またグリーニングは、エンドユーザに接続されている信頼できないデバイスポートと、DHCPサーバに接続されている信頼できるポートを区別するのに役立ちます。

DHCP グリーニングは、コンポーネントが DHCP バージョン 4 パケットのみを登録およびグリーニングできるようにする読み取り専用 DHCP スヌーピング機能です。DHCP グリーニングを有効にすると、DHCP スヌーピングが無効になっているすべてのアクティブインターフェイスで読み取り専用スヌーピングが実行されます。プライベート VLAN にセカンダリ VLAN を

追加できます。セカンダリ VLAN をプライベート VLAN に追加する場合は、プライマリ VLAN でスヌーピングが無効になっている場合でも、セカンダリ VLAN でグリーニングが有効になっていることを確認します。デフォルトでは、グリーニング機能は無効になっています。ただし、デバイスセンサーを有効にすると、DHCP グリーニングが自動的に有効になります。

DHCP スヌーピング

Dynamic Host Configuration Protocol (DHCP) スヌーピングは、信頼できないホストと信頼された DHCP サーバとの間のファイアウォールのように機能するセキュリティ機能です。DHCP スヌーピング機能では、次のアクティビティが実行されます。

- 信頼できないソースからの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外する。
- 信頼できるソースおよび信頼できないソースからの DHCP トラフィックのレートを制限する。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

動的な Address Resolution Protocol (ARP) などの他のセキュリティ機能でも、DHCP スヌーピング バインディング データベースに保存されている情報が使用されます。

DHCP スヌーピングは、VLAN ベースごとにイネーブルに設定されます。デフォルトでは、すべての VLAN でこの機能は非アクティブです。この機能は、1つの VLAN または特定の VLAN 範囲で有効にできます。

DHCP グリーニングの設定方法

DHCP グリーニングの信頼された送信元または信頼できない送信元としてのインターフェイスの設定

デバイスでの DHCP グリーニングを有効化または無効化できます。DHCP メッセージの信頼された送信元または信頼できない送信元としてインターフェイスを設定できます。信頼できないインターフェイスまたはデバイスポートで DHCP グリーニングが有効になっている場合、DHCP パケットがドロップされないことを確認します。



(注) デフォルトでは、DHCP グリーニングは無効になっています。

DHCP の信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 ポート チャネル インターフェイス



(注) 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。

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。 • パスワードを入力します（要求された場合）。
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 dhcp snooping glean 例： Device(config)# ip dhcp snooping glean	インターフェイスで DHCP グリーニングを有効にします。
ステップ 4	interface type number 例： Device(config)# interface gigabitEthernet 1/0/1	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。 <i>type number</i> は、DHCP スヌーピングのために信頼状態を設定するレイヤ 2 イーサネット インターフェイスです。
ステップ 5	[no] ip dhcp snooping trust 例： Device(config-if)# ip dhcp snooping trust	DHCP スヌーピングに関して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します。 no オプションを使用すると、ポートは信頼できないインターフェイスとして設定されます。
ステップ 6	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 7	show ip dhcp snooping statistics 例： Device# show ip dhcp snooping statistics	信頼できないインターフェイスとして設定されたデバイスポートでドロップされたパケットを表示します。

	コマンドまたはアクション	目的
ステップ 8	show ip dhcp snooping 例： Device# show ip dhcp snooping	DHCP グリーニングに関する情報など、DHCP スヌーピングの設定情報を表示します。

DHCP グリーニングの設定例

例：DHCP グリーニングの信頼された送信元または信頼できない送信元としてのインターフェイスの設定

Dynamic Host Configuration Protocol (DHCP) グリーニングを有効にし、インターフェイスを信頼されたインターフェイスとして設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping glean
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# ip dhcp snooping trust
Device(config-if)# end
```

DHCP グリーニングに関する追加情報

標準および RFC

標準/RFC	タイトル
RFC-2131	『 <i>Dynamic Host Configuration Protocol</i> 』
RFC-4388	<i>DHCP</i> リースクエリ

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	http://www.cisco.com/support

DHCP グリーニングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1: DHCP グリーニングの機能情報

機能名	リリース	機能情報
DHCP グリーニング	Cisco IOS XE Fuji 16.8.1a	DHCP グリーニングは、コンポーネントが DHCP バージョン 4 パケットのみを登録およびグリーニングできるようにする読み取り専用 DHCP スヌーピング機能です。

