CHAPTER 12

DHCP スヌーピングの設定

この章では、Dynamic Host Configuration Protocol（DHCP）スヌーピングを設定する方法について説明します。次の項で構成されています。

- 「DHCP スヌーピングの概要」（P.12-1）
- 「DHCP スヌーピングの前提条件」（P.12-3）
- 「注意事項および制約事項」（P.12-4）
- 「デフォルト設定」（P.12-4）
- 「DHCP スヌーピングの設定」（P.12-4）
- 「DHCP スヌーピング設定の確認」（P.12-16）
- 「DHCP スヌーピングのモニタリング」（P.12-17）
- 「DHCP スヌーピングの設定例」（P.12-17）
- 「その他の関連資料」（P.12-17）
- 「DHCP スヌーピングの機能の履歴」（P.12-18）

DHCP スヌーピングの概要

ここでは、次の内容について説明します。

- 「概要」（P.12-1）
- 「信頼できるソースおよび信頼できないソース」（P.12-2）
- 「DHCP スヌーピング バインディング データベース」（P.12-2）

概要

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバとの間でファイアウォールのような役割を果たします。具体的には、次の処理を実行します。

- 信頼できない発信元からの DHCP メッセージを検証するとともに、DHCP サーバからの無効な応答メッセージを除外します。
- 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。

Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）および IP ソース ガードも、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た情報を使用します。この 3 つの機能の詳細については、第 13 章「Dynamic ARP Inspection の設定」と第 14 章「IP ソース ガードの設定」を参照してください。

DHCP スヌーピングは、VLAN ごとにグローバルにイネーブルになっています。デフォルトでは、すべての VLAN で DHCP スヌーピング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 範囲でイネーブルにできます。

信頼できるソースおよび信頼できないソース

DHCP スヌーピングでは、ポートを「信頼できる」または「信頼できない」として識別します。DHCP スヌーピングをイネーブルにすると、デフォルトでは、vEthernet ポートはすべて「信頼できない」となり、イーサネット ポート（アップリンク）、ポート チャネル、特殊な vEthernet ポート（VSD などの機能の動作に使用される）はすべて「信頼できる」となります。トラフィックの送信元を DHCP の処理において信頼できるものと見なすかどうかを設定できます。

企業ネットワークでは、信頼できる送信元はその企業の管理制御下にあるデバイスです。ファイアウォールを越えるデバイスやネットワーク外のデバイスは信頼できない送信元です。一般的に、ホスト ポートは信頼できない送信元として扱われます。

サービス プロバイダーの環境では、サービス プロバイダー ネットワークにないデバイスは、信頼できない送信元です（カスタマー スイッチなど）。ホスト ポートは、信頼できない送信元です。

Cisco Nexus 1000V では、接続インターフェイスの信頼状態を設定することにより送信元が信頼されることを示します。アップリンク ポート（アップリンク機能を持つことがポート プロファイルで定義されている）は、信頼できるポートです。したがって、信頼できないポートであると設定することはできません。このような制約があるので、レート制限への非適合や DHCP 応答が理由でアップリンクがシャットダウンされることはなくなります。

管理者は、他のインターフェイスも「信頼できる」と設定することができますが、それには、そのインターフェイスがネットワーク内部のデバイス（スイッチやルータなど）に接続されているか、管理者が DHCP サーバを VM 内で実行していることが条件となります。ホスト ポート インターフェイスは、通常、信頼できるインターフェイスとしては設定しません。

（注）　DHCP スヌーピングを適切に機能させるためには、すべての DHCP サーバが信頼できるインターフェイスを介してデバイスと接続される必要があります。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングが代行受信した DHCP メッセージから抽出された情報を使用して、各 VEM 上のデータベースが動的に構築され、維持されます。DHCP スヌーピングがイネーブルにされた VLAN に、ホストが関連付けられている場合、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各ホストのエントリが保存されています。データベースには、信頼できるインターフェイスを介して接続するホストに関するエントリは保存されません。

（注）　DHCP スヌーピング バインディング データベースは、「DHCP スヌーピング バインディング テーブル」と呼ばれることもあります。

デバイスが特定の DHCP メッセージを受信すると、DHCP スヌーピングはデータベースをアップデートします。たとえば、デバイスが DHCPACK メッセージをサーバから受信すると、この機能によってデータベースにエントリが追加されます。このデータベースからエントリが削除されるのは、IP アドレスのリース期限が過ぎたとき、またはデバイスが DHCP クライアントから DHCPRELEASE または DHCP DECLINE を受信したとき、またはデバイスが DHCP サーバから DHCPNACK を受信したときです。

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各エントリには、ホストの MAC アドレス、リース IP アドレス、リース期間、バインディング タイプ、VLAN 番号、およびホストに関連するインターフェイス情報が保存されます。

動的に追加されたエントリをバインディング データベースから削除するには、**clear ip dhcp snooping binding** コマンドを使用します。詳細については、「DHCP スヌーピング バインディング データベースのクリア」（P.12-13）を参照してください。

リレー エージェント情報オプション

DHCP パケットに VSM MAC アドレスおよび vEthernet ポートを追加するように DHCP を設定できます。これは、DHCP リレー エージェント情報オプションまたはオプション 82 と呼ばれ、DHCP パケットの転送時に DHCP リレー エージェントによって挿入されます。サーバ管理者は、この情報を使用して、IP アドレスの割り当てポリシーを実装できます。

リレー エージェントでは、次が識別されます。

情報オプション	説明
回線 ID	vEthernet ポート名
リモート ID	VSM MAC アドレス

リレー エージェント情報オプションの詳細については、「*RFC-3046, DHCP Relay Agent Information Option*」を参照してください。

リレー エージェントを設定するには、「DHCP のスイッチおよび回線情報のリレー」（P.12-15）の手順を参照してください。

ハイ アベイラビリティ

VEM 上に作成された DHCP スヌーピング バインディング テーブルとすべてのデータベース エントリは、VSM にエクスポートされ、VSM のリブート後も維持されます。

DHCP スヌーピングの前提条件

DHCP スヌーピングの前提条件は次のとおりです。

- DHCP スヌーピングを設定するには、DHCP に関する知識が必要です。

注意事項および制約事項

DHCP スヌーピングに関する注意事項と制約事項は次のとおりです。

- DHCP スヌーピング データベースは各 VEM 上に作成され、1 つのデータベースに最大 1024 個のバインディングを格納できます。
- DHCP スヌーピングをシームレスにするために、仮想サービス ドメイン（VSD）サービス VM ポートは、デフォルトで信頼できるポートとなっています。これらのポートを「信頼できない」と設定しても、その設定は無視されます。
- VSM の接続に VEM が使用される場合、つまり VSM の VSM AIPC、管理、およびインバンドのポートが特定の VEM 上にある場合は、これらの仮想イーサネット インターフェイスが信頼できるインターフェイスとして設定されている必要があります。
- Cisco Nexus 1000V からのデバイス アップストリームの接続インターフェイスは、このデバイスで DHCP スヌーピングがイネーブルになっている場合、「信頼できる」として設定する必要があります。
- 128 を超える ACL（MAC と IP ACL の組み合わせ）を設定する場合は、VSM RAM が 3GB（3072 Mb）に設定されていることを確認します。RAM を 3GB に変更する手順は、「Setting the VSM RAM size to 3072 Mb」（ハイパーリンク）で説明されています。

デフォルト設定

表 12-1 に、DHCP スヌーピングのデフォルトを示します。

表 12-1　DHCP スヌーピング パラメータのデフォルト値

パラメータ	デフォルト
DHCP 機能	ディセーブル
DHCP スヌーピング グローバル	ディセーブル
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピングの MAC アドレス検証	イネーブル
DHCP スヌーピング信頼状態	信頼できる：イーサネット インターフェイス、vEthernet インターフェイス、およびポート チャネル（VSD 機能に参加しているもの）信頼できない：VSD 機能に参加していない vEthernet インターフェイス

DHCP スヌーピングの設定

ここでは、次の内容について説明します。

- 「DHCP スヌーピングの最小設定」（P.12-5）
- 「DHCP 機能のイネーブル化またはディセーブル化」（P.12-5）
- 「DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化」（P.12-6）
- 「VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化」（P.12-7）
- 「DHCP スヌーピングの MAC アドレス検証のイネーブル化またはディセーブル化」（P.12-8）

- 「インターフェイスの信頼状態の設定」（P.12-9）
- 「DHCP パケットのレート制限の設定」（P.12-10）
- 「DHCP レート制限違反がディセーブルなポートの検出」（P.12-11）
- 「DHCP レート制限違反がディセーブルなポートの回復」（P.12-12）
- 「DHCP スヌーピング バインディング データベースのクリア」（P.12-13）
- 「DHCP のスイッチおよび回線情報のリレー」（P.12-15）

DHCP スヌーピングの最小設定

DHCP スヌーピングの最小設定は次のとおりです。

ステップ 1　DHCP 機能をイネーブルにします。詳細については、「DHCP 機能のイネーブル化またはディセーブル化」（P.12-5）を参照してください。

ステップ 2　DHCP スヌーピングをグローバルにイネーブル化します。詳細については、「DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化」（P.12-6）を参照してください。

ステップ 3　少なくとも 1 つの VLAN で、DHCP スヌーピングをイネーブルにします。詳細については、「VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化」（P.12-7）を参照してください。

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。

ステップ 4　DHCP サーバとデバイスが、信頼できるインターフェイスを使用して接続されていることを確認します。詳細については、「インターフェイスの信頼状態の設定」（P.12-9）を参照してください。

DHCP 機能のイネーブル化またはディセーブル化

DHCP 機能をグローバルにイネーブルまたはディセーブルにするには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、DHCP はディセーブルです。

手順の概要

1. **config t**
2. **feature dhcp**
3. **show feature**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(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	**feature dhcp** **Example:** n1000v(config)# feature dhcp **Example:** n1000v(config)# no feature dhcp	DHCP スヌーピングをグローバルにイネーブル化します。**no** オプションを使用すると、DHCP スヌーピングがディセーブルになりますが、既存の DHCP スヌーピング設定は維持されます。
ステップ 3	**show feature** **Example:** n1000v(config)# show feature Feature Name　　Instance　State --------------------　--------　-------- dhcp-snooping　　1　　enabled http-server　　1　　enabled lacp　　1　　enabled netflow　　1　　disabled port-profile-roles　　1　　enabled private-vlan　　1　　disabled sshServer　　1　　enabled tacacs　　1　　enabled telnetServer　　1　　enabled n1000v(config)#	使用可能な各機能の状態（イネーブルまたはディセーブル）を示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化

ここでは、DHCP スヌーピングをグローバルにイネーブルまたはディセーブルにする手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- デフォルトでは、DHCP スヌーピングはグローバルにディセーブルです。
- DHCP スヌーピングがグローバルにディセーブルになると、DHCP スヌーピングはすべて停止し、DHCP メッセージは中継されなくなります。
- DHCP スヌーピングを設定した後でグローバルにディセーブルにした場合も、残りの設定は維持されます。

手順の概要

1. **config t**
2. **[no] ip dhcp snooping**
3. **show running-config dhcp**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(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** **Example:** n1000v(config)# ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブル化します。**no** オプションを使用すると、DHCP スヌーピングがディセーブルになりますが、既存の DHCP スヌーピング設定は維持されます。
ステップ 3	**show running-config dhcp** **Example:** n1000v(config)# show running-config dhcp	DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化

ここでは、1 つまたは複数の VLAN に対して DHCP スヌーピングをイネーブルまたはディセーブルにする手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。

手順の概要

1. **config t**
2. **[no] ip dhcp snooping vlan** *vlan-list*
3. **show running-config dhcp**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(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* **Example:** n1000v(config)# ip dhcp snooping vlan 100,200,250-252	*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。**no** オプションを使用すると、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	**show running-config dhcp** **Example:** n1000v(config)# show running-config dhcp	DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP スヌーピングの MAC アドレス検証のイネーブル化またはディセーブル化

ここでは、DHCP スヌーピングの MAC アドレス検証をイネーブルまたはディセーブルにする手順を説明します。信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合、アドレス検証によってデバイスはパケットをドロップします。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- MAC アドレス検証はデフォルトでイネーブルになります。

手順の概要

1. **config t**
2. **[no] ip dhcp snooping verify mac-address**
3. **show running-config dhcp**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(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 verify mac-address** **Example:** n1000v(config)# ip dhcp snooping verify mac-address	DHCP スヌーピングの MAC アドレス検証をイネーブルにします。**no** オプションを使用すると MAC アドレス検証がディセーブルになります。
ステップ 3	**show running-config dhcp** **Example:** n1000v(config)# show running-config dhcp	DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

インターフェイスの信頼状態の設定

ここでは、特定の仮想インターフェイスが DHCP メッセージの送信元として信頼できるものかどうかを設定する手順を説明します。次のものの DHCP 信頼状態を設定できます。

- レイヤ 2 vEthernet インターフェイス
- レイヤ 2 vEthernet インターフェイスのポート プロファイル

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、vEthernet インターフェイスは「信頼できない」となっています。ただし、信頼できる他の機能（VSD など）によって使用される特殊な vEthernet ポートは例外です。
- vEthernet 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てください。
- DHCP スヌーピング、DAI、および IP ソース ガードをシームレスにするために、仮想サービス ドメイン（VSD）サービス VM ポートはデフォルトで信頼できるポートとなっています。これらのポートを「信頼できない」と設定しても、その設定は無視されます。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*

   port-profile *profilename*
3. [**no**] **ip dhcp snooping trust**

4. **show running-config dhcp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(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	**interface vethernet** *interface-number* **Example:** n1000v(config)# interface vethernet 3 n1000v(config-if)#	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。*interface-number* は、DHCP スヌーピングにおいて信頼できるものとして扱うかどうかを設定する vEthernet インターフェイスです。
	port-profile *profilename* **Example:** n1000v(config)# port-profile vm-data n1000v(config-port-prof)#	指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。*profilename* は最大 80 文字の一意の名前です。
ステップ 3	[**no**] **ip dhcp snooping trust** **Example:** n1000v(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 4	**show running-config dhcp** **Example:** n1000v(config-if)# show running-config dhcp	DHCP スヌーピングの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v(config-if)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP パケットのレート制限の設定

各ポートで受信する DHCP パケット / 秒のレートの制限を設定するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- ポートは、この手順で設定した DHCP パケット / 秒のレートの制限を超えると、errdisabled 状態になります。
- インターフェイスまたはポート プロファイルにレート制限を設定できます。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*
   port-profile *profilename*
3. **[no] ip dhcp snooping limit rate** *rate*
4. **show running-config dhcp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(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	**interface vethernet** *interface-number* **Example:** n1000v(config)# interface vethernet 3 n1000v(config-if)#	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。*interface-number* は、DHCP パケット/秒の制限を設定する vEthernet インターフェイスです。
	port-profile *profilename* **Example:** n1000v(config)# port-profile vm-data n1000v(config-port-prof)#	指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。*profilename* は最大 80 文字の一意の名前です。
ステップ 3	[**no**] **ip dhcp snooping limit rate** *rate* **Example:** n1000v(config-port-prof)# ip dhcp snooping limit rate 30	DHCP パケット/秒（1 ～ 2048）のレートに制限を設定します。**no** オプションはレート制限を削除します。
ステップ 4	**show running-config dhcp** **Example:** n1000v(config-if)# show running-config dhcp	DHCP スヌーピングの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v(config-if)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP レート制限違反がディセーブルなポートの検出

DHCP レート制限の超過がディセーブルになっているポートの検出をグローバルに設定するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 設定されたレートに違反すると、ポートは自動的に errdisable 状態になります。
- **shutdown** コマンドを入力し、**no shutdown** コマンドを入力して errdisable ステートから手動でインターフェイスを回復する必要があります。

手順の概要

1. **config t**
2. **[no] errdisable detect cause dhcp-rate-limit**
3. **show running-config dhcp**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(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] errdisable detect cause dhcp-rate-limit** **Example:** n1000v(config)# errdisable detect cause dhcp-rate-limit	DHCP errdisable 検出をイネーブルにします。**no** オプションを使用すると、DHCP errdisable 検出がディセーブルになります。
ステップ 3	**show running-config dhcp** **Example:** n1000v(config)# show running-config dhcp	DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP レート制限違反がディセーブルなポートの回復

DHCP レート制限の違反がディセーブルになっているポートの自動リカバリをグローバルに設定するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- レートによって errdisable ステートになるポート。
- **shutdown** コマンドを入力し、**no shutdown** コマンドを入力して errdisable ステートから手動でインターフェイスを回復する必要があります。

手順の概要

1. **config t**
2. **[no] errdisable recovery cause dhcp-rate-limit**
3. **errdisable recovery interval** *timer-interval*
4. **show running-config dhcp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(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] errdisable recovery cause dhcp-rate-limit** **Example:** n1000v(config)# errdisable detect cause dhcp-rate-limit	DHCP errdisable 回復をイネーブルにします。**no** オプションを使用すると、DHCP errdisable 回復がディセーブルになります。
ステップ 3	**errdisable recovery interval** *timer-interval* **Example:** n1000v(config)# errdisable recovery interval 30	DHCP errdisable 回復間隔を設定します。*timer-interval* は秒数（30 ～ 65535）です。
ステップ 4	**show running-config dhcp** **Example:** n1000v(config)# show running-config dhcp	DHCP スヌーピングの設定を表示します。
ステップ 5	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP スヌーピング バインディング データベースのクリア

ここでは、次の手順について説明します。

- 「すべてのバインディング エントリの消去」（P.12-13）
- 「インターフェイスのバインディング エントリの消去」（P.12-14）

すべてのバインディング エントリの消去

ここでは、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削除する手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **clear ip dhcp snooping binding**
2. **show ip dhcp snooping binding**

手順の詳細

	コマンド	目的
ステップ 1	**clear ip dhcp snooping binding** **Example:** `n1000v# clear ip dhcp snooping binding`	DHCP スヌーピング バインディング データベースに動的に追加されたエントリを消去します。
ステップ 2	**show ip dhcp snooping binding** **Example:** `n1000v# show ip dhcp snooping binding`	DHCP スヌーピング バインディング データベースを表示します。

インターフェイスのバインディング エントリの消去

DHCP スヌーピング データベースからインターフェイスのバインディング エントリを削除するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- インターフェイスに関する次の情報があること。
  - VLAN ID
  - IP アドレス
  - MAC アドレス

手順の概要

1. **clear ip dhcp snooping binding** [{**vlan** *vlan-id* **mac** *mac-addr* **ip** *ip-addr* **interface** *interface-id*} | **vlan** *vlan-id1* | **interface** *interface-id1*]
2. **show ip dhcp snooping binding**

手順の詳細

	コマンド	目的
ステップ 1	**clear ip dhcp snooping binding** [{**vlan** *vlan-id* **mac** *mac-addr* **ip** *ip-addr* **interface** *interface-id*} | **vlan** *vlan-id1* | **interface** *interface-id1*] **Example:** n1000v# clear ip dhcp snooping binding vlan 10 mac EEEE.EEEE.EEEE ip 10.10.10.1 interface vethernet 1	DHCP スヌーピング バインディング データベースから、動的に追加されたインターフェイスのエントリを消去します。
ステップ 2	**show ip dhcp snooping binding** **Example:** n1000v# show ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを表示します。

DHCP のスイッチおよび回線情報のリレー

DHCP パケットの VSM MAC アドレスおよび vEthernet ポート情報のリレーをグローバルに設定するには、次の手順を実行します。これは、オプション 82 およびリレー エージェント情報オプションとも呼ばれます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 詳細については、次の説明を参照してください。
  - 「リレー エージェント情報オプション」（P.12-3）
  - *RFC-3046『DHCP Relay Agent Information Option』*

手順の概要

1. **config t**
2. **[no] ip dhcp snooping information option**
3. **show runing-config dhcp**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** n1000v# config t n1000v(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。

	コマンド	目的
ステップ 2	**[no] ip dhcp snooping information option** **Example:** n1000v(config)# ip dhcp snooping information option n1000v(config)#	DHCP パケットの VSM MAC アドレスおよび vEthernet ポート情報をリレーするよう DHCP を設定します。 この設定を削除するには、**no** オプションを使用します。
ステップ 3	**show running-config dhcp** **Example:** n1000v(config)# show running-config dhcp !Command: show running-config dhcp !Time: Fri Dec 17 11:30:22 2010 version 4.2(1)SV1(4) ip dhcp snooping information option service dhcp ip dhcp relay ip dhcp relay information option n1000v(config)#	（任意）確認のために DHCP スヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

DHCP スヌーピング設定の確認

DHCP スヌーピング設定を確認するには、次のコマンドを使用します。

コマンド	目的
show running-config dhcp	DHCP スヌーピングの設定を表示します。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング テーブルの内容を表示します。
show feature	DHCP などの使用可能な機能と、それらがイネーブルかどうかを表示します。

これらのコマンドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

DHCP スヌーピングのモニタリング

DHCP スヌーピングの統計情報をモニタするには、**show ip dhcp snooping statistics** コマンドを使用します。このコマンドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』を参照してください。

DHCP スヌーピングの設定例

次に、2 つの VLAN 上で DHCP スヌーピングをイネーブルにする例を示します。vEthernet インターフェイス 5 が「信頼できる（trusted）」となっているのは、DHCP サーバがこのインターフェイスに接続されているからです。

```
feature dhcp

interface vethernet 5
ip dhcp snooping trust
ip dhcp snooping vlan 1, 50
```

その他の関連資料

DHCP スヌーピングの実装に関する詳細情報については、次の項を参照してください。

- 「関連資料」（P.12-17）
- 「標準」（P.12-17）

関連資料

関連項目	参照先
IPSG	『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4a)*』、第 14 章「IP ソース ガードの設定」
Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）	『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4a)*』、第 13 章「Dynamic ARP Inspection の設定」
DHCP スヌーピングのコマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*』

標準

標準	タイトル
RFC-2131	『*Dynamic Host Configuration Protocol*』（http://tools.ietf.org/html/rfc2131）
RFC-3046	『*DHCP Relay Agent Information Option*』（http://tools.ietf.org/html/rfc3046）

DHCP スヌーピングの機能の履歴

表 12-2 は、この機能のリリースの履歴です。

表 12-2　DHCP スヌーピングの機能の履歴

機能名	リリース	機能情報
リレー エージェント（オプション 82）	4.2(1)SV1(4)	DHCP パケットの VSM MAC およびポート情報のリレーを設定できます。
feature dhcp コマンド	4.2(1)SV1(4)	DHCP 機能をグローバルにイネーブルにするコマンドが追加されました。
DHCP スヌーピング	4.0(4)SV1(2)	この機能が導入されました。