アカウンティングおよびセキュリティ対応の DHCP サービスの設定

Cisco IOS ソフトウェアは、Public Wireless LAN（PWLAN; パブリック ワイヤレス LAN）で DHCP のセキュリティ、信頼性、およびアカウンティングを拡張する複数の機能をサポートしています。この機能は、他のネットワーク実装でも使用できます。このモジュールでは、アカウンティングおよびセキュリティ対応の DHCP サービスを設定するために必要な概念および作業について説明します。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリースノートを参照してください。このモジュールに記載されている機能に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「アカウンティングおよびセキュリティ対応の DHCP サービスの機能情報」（P.21）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、およびシスコのソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

アカウンティングおよびセキュリティ対応の DHCP サービスを設定するための前提条件

アカウンティングおよびセキュリティ対応の DHCP サービスを設定する前に、「DHCP の概要」モジュールで説明されている概念を理解する必要があります。

アカウンティングおよびセキュリティ対応の DHCP サービスに関する情報

パブリック ワイヤレス LAN での DHCP の動作

PWLAN での DHCP の設定により、ワイヤレス クライアントの設定が簡単になり、ネットワークをメンテナンスするために必要なオーバーヘッドが削減されます。DHCP クライアントは、DHCP サーバから IP アドレスをリースし、その後、Service Selection Gateway（SSG）により認証され、ネットワーク サービスへのアクセスが許可されます。DHCP サーバとクライアントは、IP アドレスの割り当てに関する DHCP メッセージを交換します。DHCP サーバがクライアントに IP アドレスを割り当てると、DHCP バインディングが作成されます。クライアントが明示的に IP アドレスをリリースし、ネットワークから切断するまで、IP アドレスはクライアントにリースされます。クライアントがアドレスをリリースせずに切断すると、サーバは、リース期間が終了した後、リースを終了します。どちらの場合も、DHCP サーバはバインディングを削除し、IP アドレスはプールに戻されます。

パブリック ワイヤレス LAN のセキュリティの脆弱性

PWLAN を使用し始める人が増えているため、セキュリティが重要な懸案事項になっています。ユーザは、ホット スポット（コーヒー店、空港ターミナル、ホテルなど）にいる間、IP アドレスを DHCP サーバから取得し、セッション中、その IP アドレスを使用します。このため、PWLAN の実装の大部分は DHCP に依存します。

IP スプーフィングは、ハッカーが IP アドレスをスプーフするために使用する一般的な方法です。たとえば、お客様 A が DHCP から IP アドレスを取得し、PWLAN を使用するための認証を受けた後、ハッカーがお客様 A の IP アドレスをスプーフし、その IP アドレスを使用してトラフィックを送受信するということがあります。お客様 A は、サービスを使用していないのに、サービスの料金を請求されます。

Address Resolution Protocol（ARP; アドレス解決プロトコル）テーブル エントリは、設計によりダイナミックです。ネットワーク内のすべてのネットワーク デバイスで、要求 ARP パケットおよび応答 ARP パケットが送受信されます。DHCP ネットワークでは、DHCP サーバは、クライアントの MAC アドレスまたはクライアント ID に対してリースした IP アドレスを、DHCP バインディングに保存します。ただし、ARP エントリはダイナミックに学習されるため、DHCP サーバが付与した IP アドレスを、不正なクライアントがスプーフして使用し始めることができます。ARP テーブル内の許可クライアントの MAC アドレスが、この不正クライアントの MAC アドレスに置き換えられ、それにより、不正クライアントが、スプーフした IP アドレスを自由に使用できるようになります。

セキュリティおよびアカウンティング対応の DHCP サービスの概要

DHCP セキュリティおよびアカウンティング機能は、PWLAN のセキュリティ問題を解決するために設計および実装されていますが、他のネットワーク実装でも使用できます。

DHCP アカウンティングは、DHCP 対応の Authentication, Authorization and Accounting（AAA; 認証、許可、アカウンティング）のサポート、および RADIUS のサポートを提供します。AAA および RADIUS のサポートにより、セキュアな START および STOP アカウンティング メッセージを送信することで、セキュリティが強化されます。DHCP アカウンティングの設定により、セキュリティのレイヤが追加されます。このセキュリティのレイヤにより、適切な RADIUS START および STOP アカウンティング レコードに対して、DHCP リースの割り当てと終了がトリガーできるようになり、それにより、SSG などのアップストリーム デバイスが、セッション状態を正しく保持します。この追加セキュリティの支援により、ハッカーや不正クライアントは、許可済みの DHCP リースをスプーフしてネットワークに不正にアクセスすることができなくなります。

PWLAN のセキュリティ問題を解決するために、他に 3 つの機能が設計および実装されています。1 つめの機能では、DHCP データベース内の DHCP リースに対する ARP テーブル エントリを保護します。このセキュアな ARP 機能により、DHCP サーバのデータベースを ARP テーブルと同期させてアドレスのハイジャックを回避することで、IP スプーフィングを防止します。アドレスが割り当てられると、セキュア ARP により、クライアントの ARP テーブルにエントリが追加されます。バインディングが期限切れになった場合に限り、DHCP サーバはこれを削除できます。

2 つめの機能は DHCP 許可 ARP です。この機能では、DHCP が明示的にユーザ ログアウト時を認識する必要性に対応することで完全性の高いソリューションを提供します。DHCP 許可 ARP が登場する前、ユーザがシステムから連絡なしで去ったかどうかを DHCP サーバに通知するメカニズムはありませんでした。このため、お客様がログアウトした一方で、システムがそれを検出できず、その顧客に必要以上の請求が行われる可能性がありました。この問題に対処するために、DHCP 許可 ARP は、1 分ごとに定期 ARP メッセージを送信して、ユーザが現在ログインしているかどうかを確認します。許可ユーザのみが ARP 要求に応答できます。無許可ユーザからの ARP 応答は、DHCP サーバでブロックされるため、1 つ上のレベルのセキュリティが提供されます。

さらに、DHCP 許可 ARP では、インターフェイスにおけるダイナミック ARP 学習がディセーブルになります。アドレス マッピングを組み込むことができるのは、**arp authorized** インターフェイス コンフィギュレーション コマンドで指定した許可コンポーネントのみです。DHCP は、ARP エントリの組み込みを許可された唯一の許可コンポーネントです。

3 番めの機能は ARP 自動ログオフで、これにより、許可ユーザがいつログアウトしたかプローブする機能を詳細に制御できます。**arp probe interval** コマンドで、プローブをいつ開始するか（timeout）、どれくらいの頻度でピアをプローブするか（interval）、および再試行の最大回数（count）を指定します。

DHCP リース制限

DHCP リース制限を設定することで、リース先の数を、グローバルにまたはインターフェイスごとに制御できます。この機能により、ISP は、クライアントが使用できるリースの数を、世帯ごとまたは接続ごとに制限できます。

アカウンティングおよびセキュリティ対応の DHCP サービスを設定する方法

ここでは、次の作業について説明します。

- 「DHCP アカウンティング対応の AAA および RADIUS の設定」（P.4）

DHCP アカウンティング対応の AAA および RADIUS の設定

DHCP アカウンティング対応の AAA および RADIUS を設定するには、この作業を実行します。

RADIUS は、セキュア START および STOP メッセージを転送するためのアカウンティング機能を提供します。AAA および RADIUS は、DHCP アカウンティングを設定する前にイネーブルにしますが、非セキュア DHCP ネットワークを保護するためにイネーブルにすることもできます。新規または既存のネットワークで DHCP アカウンティングを設定する場合、このセクションの設定手順が必要になります。

RADIUS アカウンティング アトリビュート

DHCP アカウンティングでは、表 1 に示されているアトリビュートが導入されています。DHCP アカウンティングがイネーブルになると、これらのアトリビュートは RADIUS サーバにより直接処理されます。これらのアトリビュートは、**debug radius** コマンドの出力で監視できます。この出力では、DHCP リースの状態、およびクライアントに関する特定の設定詳細が示されます。**debug radius** コマンドで **accounting** キーワードを使用することで、出力をフィルタリングし、DHCP アカウンティング メッセージのみ表示できます。

表 1　　RADIUS アカウンティング アトリビュート

アトリビュート	説明
Calling-Station-ID	このアトリビュートの出力では、クライアントの MAC アドレスが表示されます。
Framed-IP-Address	このアトリビュートの出力では、クライアントにリースされている IP アドレスが表示されます。
Acct-Terminate-Cause	このアトリビュートの出力では、クライアントが明示的に切断しなかった場合に、「session-timeout」メッセージが表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name*
5. **server** *ip-address* **auth-port** *port-number* **acct-port** *port-number*
6. **exit**
7. **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

8. **aaa session-id** {**common** | **unique**}
9. **ip radius source-interface** *type number* [**vrf** *vrf-name*]
10. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]
11. **radius-server retransmit** *number-of-retries*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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	**aaa new-model** **例：** `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。 • DHCP アカウンティングは、アクセス コントロール モデルでのみ機能します。 **（注）** TACACS コマンドおよび拡張 TACACS コマンドは、このコマンドを設定した後使用できなくなり、DHCP アカウントでサポートされなくなります。
ステップ 4	**aaa group server radius** *group-name* **例：** `Router(config)# aaa group server radius RGROUP-1`	AAA または TACACS+ サービスのサーバ グループを作成し、サーバ グループ RADIUS コンフィギュレーション モードを開始します。 • この手順でサーバ グループが作成されるため、アカウンティング サービスを適用できます。
ステップ 5	**server** *ip-address* **auth-port** *port-number* **acct-port** *port-number* **例：** `Router(config-sg-radius)# server 10.0.0.1 auth-port 1645 acct-port 1646`	ステップ 4 で作成したサーバ グループのメンバとなるサーバを指定します。 • 認証およびアカウンティング用のポート番号を開放する必要があります。1645 が認証用のデフォルト ポート番号で、1646 がアカウンティング用のデフォルト ポート番号です。指定できるポート番号の範囲は 0 ～ 65535 です。 • **auth-port** *port-number* および **acct-port** *port-number* キーワードおよび引数に対して入力する値は、ステップ 10 で設定するポート番号と同じにする必要があります。
ステップ 6	**exit** **例：** `Router(config-sg-radius)# exit`	サーバ グループ RADIUS コンフィギュレーション モードを終了し、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。

	コマンドまたはアクション	目的
ステップ 7	**aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name* **例：** `Router(config)# aaa accounting network RADIUS-GROUP1 start-stop group RGROUP-1`	指定したサーバ グループに対し RADIUS アカウンティングを設定します。 • 最初の *list-name* 引数（RADIUS-GROUP1）で RADIUS アカウンティング サーバを指定し、2 番めの *group-name* 引数（RGROUP-1）でターゲット サーバ グループを指定します。 • このコマンドにより、DHCP アカウンティングのアカウンティングの開始および停止がイネーブルになります。**start-stop** キーワードにより、START と STOP の両方のアカウンティング メッセージの転送がイネーブルになります。**stop-only** キーワードにより、STOP アカウンティング メッセージの生成および検証のみイネーブルになります。
ステップ 8	**aaa session-id** {**common** | **unique**} **例：** `Router(config)# aaa session-id common`	コール内の各 AAA アカウンティング サービス タイプに、同じセッション ID を使用するかどうか、または、各アカウンティング サービス タイプに対して異なるセッション ID を割り当てるかどうかを指定します。
ステップ 9	**ip radius source-interface** *type number* [**vrf** *vrf-name*] **例：** `Router(config)# ip radius source-interface Ethernet 0`	すべての発信 RADIUS パケットに対し、指定したインターフェイスの IP アドレスを使用するよう強制します。
ステップ 10	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] **例：** `Router(config)# radius-server host 10.1.1.1 auth-port 1645 acct-port 1646`	RADIUS サーバ ホストを指定します。 • **auth-port** *port-number* および **acct-port** *port-number* キーワードおよび引数に対して入力する値は、ステップ 5 で設定したポート番号と同じにする必要があります。
ステップ 11	**radius-server retransmit** *number-of-retries* **例：** `Router(config)# radius-server retransmit 3`	Cisco IOS ソフトウェアが RADIUS サーバ ホストを検出する回数を指定します。

トラブルシューティングのヒント

RADIUS アカウンティングの設定を監視およびトラブルシューティングするには、次のコマンドを使用します。

debug radius accounting

DHCP アカウンティングの設定

DHCP アカウンティングを設定するには、この作業を実行します。

DHCP アカウンティング

DHCP アカウンティングは、**accounting** DHCP プール コンフィギュレーション コマンドを使用してイネーブルにします。このコマンドにより、AAA および RADIUS で DHCP が動作するように設定され、セキュア START および STOP アカウンティング メッセージがイネーブルになります。この設定により、セキュリティのレイヤが追加されます。このセキュリティのレイヤにより、適切な RADIUS START および STOP アカウンティング レコードに対して、DHCP リースの割り当てと終了がトリガーできるようになり、それにより、SSG などのアップストリーム デバイスが、セッション状態を正しく保持します。

DHCP アカウンティングは、クライアント単位またはリース単位で設定します。個別の DHCP アカウンティング処理をプール単位に設定できます。

前提条件

クライアント認証用の SSG を設定する必要があります。DHCP アカウンティングを動作させる前に、AAA および RADIUS をイネーブルにする必要があります。

制約事項

DHCP アカウンティングには、次の制約事項が適用されます。

- DHCP アカウンティングは、DHCP ネットワーク プールに対してのみ設定できます。DHCP ネットワーク プールでは、バインディングが自動的に作成され、リースが終了した時点で、またはクライアントが DHCPRELEASE メッセージを送信した時点で破棄されます。
- DHCP バインディングは、**clear ip dhcp binding** コマンドまたは **no service dhcp** コマンドを入力すると破棄されます。また、これにより、アカウンティング STOP メッセージがトリガーされます。DHCP アカウンティングでプールが設定されている場合にこれらのコマンドを入力すると、警告を受け取ります。これは、これらのコマンドがアクティブなリースをクリアするためです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **accounting** *method-list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 pool** *pool-name* **例：** `Router(config)# ip dhcp pool WIRELESS-POOL`	DHCP アドレス プールを設定し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 4	**accounting** *method-list-name* **例：** `Router(config-dhcp)# accounting RADIUS-GROUP1`	指定したサーバ グループを設定して RADIUS アカウンティングを実行する場合に、DHCP アカウンティングをイネーブルにします。 • この例では、RADIUS-GROUP1 が start-stop グループとして設定された場合に、DHCP アカウンティングの START および STOP メッセージを送信するように設定しています。STOP メッセージは、RADIUS-GROUP1 が stop-only グループとして設定された場合に限り送信されます。詳細については、「DHCP アカウンティング対応の AAA および RADIUS の設定」セクションのステップ 7 を参照してください。

DHCP アカウンティングの確認

DHCP アカウンティング設定を確認するには、この作業を実行します。

debug radius、**debug radius accounting**、**debug ip dhcp server events**、**debug aaa accounting**、および **debug aaa id** コマンドを一緒にまたは同じセッションで発行する必要はありません。これは、提供される情報に違いがあるためです。ただし、これらのコマンドを使用して、DHCP アカウンティングの開始および停止イベント、AAA アカウンティング メッセージ、および AAA と DHCP のホストとクライアントに関する情報を表示できます。DHCP アカウンティングで導入された AAA アトリビュートのリストについては、このモジュールの 「RADIUS アカウンティング アトリビュート」セクションを参照してください。**show running-config | begin dhcp** コマンドを使用すると、DHCP アカウンティングの設定など、ローカル DHCP 設定を表示できます。

手順の概要

1. **enable**
2. **debug radius accounting**
3. **debug ip dhcp server events**
4. **debug aaa accounting**
5. **debug aaa id**

6. **show running-config | begin dhcp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug radius accounting** **例：** `Router# debug radius accounting`	ルータのコンソールに RADIUS イベントを表示します。 • これらのイベントは、RADIUS プロセスに関する情報を提供します。**accounting** キーワードを使用して、DHCP アカウンティング情報をフィルタリングできます。START および STOP アカウンティング メッセージが出力に表示されます。
ステップ 3	**debug ip dhcp server events** **例：** `Router# debug ip dhcp server events`	DHCP IP アドレスの割り当て、DHCP リースの期限、および DHCP データベースの変更を表示します。
ステップ 4	**debug aaa accounting** **例：** `Router# debug aaa accounting`	AAA アカウンティング イベントを表示します。 • START および STOP アカウンティング メッセージが出力に表示されます。
ステップ 5	**debug aaa id** **例：** `Router# debug aaa id`	AAA イベントが固有の AAA セッション ID に関連している場合にそれらの AAA イベントを表示します。
ステップ 6	**show running-config | begin dhcp** **例：** `Router# show running-config | begin dhcp`	ルータのローカル設定を表示します。 • この出力例は、**begin** キーワードを使用してフィルタリングされており、実行コンフィギュレーションの DHCP セクションからの出力が表示されています。

DHCP リースに対する ARP テーブル エントリの保護

DHCP データベース内にある、DHCP リースに対する ARP テーブル エントリを保護するには、この作業を実行します。

update arp コマンドを使用すると、すべての新規リースおよび DHCP バインディングについて、ARP テーブル エントリおよび対応する DHCP リースが自動的に保護されます。ただし、既存のアクティブ リースは保護されません。これらのリースは更新されるまで非セキュアです。リースが更新されると、そのリースは新規リースとして扱われ、自動的に保護されます。DHCP サーバでこのコマンドがディセーブルの場合、既存のすべてのセキュア ARP テーブル エントリがダイナミック ARP エントリに自動的に変更されます。

手順の概要

1. **enable**
2. **configure terminal**

3. **ip dhcp pool** *pool-name*
4. **update arp**
5. **renew deny unknown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 pool** *pool-name* **例：** `Router(config)# ip dhcp pool WIRELESS-POOL`	DHCP アドレス プールを設定し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 4	**update arp** **例：** `Router(config-dhcp)# update arp`	対応する DHCP リースに対する非セキュア ARP テーブル エントリを保護します。 • 既存のアクティブ DHCP リースは更新されるまで保護されません。**no update arp** コマンドを使用すると、セキュア ARP テーブル エントリがダイナミック ARP テーブル エントリに再び変更されます。
ステップ 5	**renew deny unknown** **例：** `Router(config-dhcp)# renew deny unknown`	（任意）不明クライアントの更新ポリシーを設定します。 • このコマンドをいつ使用するかについては、「トラブルシューティングのヒント」セクションを参照してください。

トラブルシューティングのヒント

ワイヤレス ホット スポットなど、DHCP とセキュア ARP の両方を設定する一部の使用シナリオでは、接続されるクライアント デバイスが一定期間スリープ状態またはサスペンド状態になる場合があります。サスペンド時間がセキュア ARP タイムアウト（デフォルトは 91 秒）を上回り、DHCP リース時間にはまだ達していない場合、クライアントは有効なリースを使用して起動できますが、クライアントは非アクティブであるため、セキュア ARP タイムアウトによりリース バインディングは削除されます。クライアントが起動したとき、クライアント側ではリースを所有していますが、トラフィックの送信はブロックされます。クライアントは IP アドレスを更新しようとしますが、DHCP サーバは、クライアントのリースを所有していないため、この要求を無視します。クライアントは、リースが期限切れになるのを待つ必要があり、その後で復旧してトラフィックを再び送信できます。

この状況に対処するには、DHCP プール コンフィギュレーション モードで **renew deny unknown** コマンドを使用します。このコマンドにより、更新要求されたアドレスが DHCP サーバに存在するけれどもリースされていない場合、サーバはクライアントからの更新要求を拒否します。DHCP サーバは DHCPNAK 拒否メッセージをクライアントに送信し、これにより、クライアントは初期状態に戻ります。この後、クライアントは、古いリースが期限切れになるのを待つことなく、ただちに新しいリースについてネゴシエーションできます。

DHCP 許可 ARP の設定

DHCP 許可 ARP を設定して、インターフェイスでのダイナミック ARP 学習をディセーブルにするには、この作業を実行します。

ARP プローブの動作

DHCP 許可 ARP には、正確な 1 分間の課金のサポートに関して制限があります。DHCP 許可 ARP は、30 秒に 1 回または 2 回、許可ユーザをプローブします。ビジー状態のネットワークでは、応答パケットが失われる可能性が高くなり、それにより、予定よりも早くログオフが実行される場合があります。許可ユーザのプローブをより正確および詳細に制御する必要がある場合、**arp probe interval** コマンドを設定します。このコマンドでは、プローブを開始する時期、不成功プローブの間隔、および自動ログオフをトリガーするまでの最大試行回数を指定します。

制約事項

スタティック ARP と許可 ARP の両方で同じ ARP エントリを組み込むと、スタティック設定が許可 ARP より優先されます。**arp** グローバル コンフィギュレーション コマンドを使用することで、スタティック ARP エントリを組み込むことができます。非ダイナミック ARP エントリを組み込んだのと同じ方法で、非ダイナミック ARP エントリのみ削除できます。

ARP タイムアウト時間は 30 秒未満に設定しないでください。**arp timeout** コマンドで指定した ARP タイムアウト時間になる前の最初の 90 秒間に、ARP メッセージを 30 秒間隔で送信するように、この機能は設計されています。この動作により、クライアントが断念する前に、少なくとも 3 回はクライアントのプローブが可能になります。ARP タイムアウトを 60 秒に設定した場合は、ARP メッセージは 2 回送信され、30 秒に設定した場合、ARP メッセージは 1 回送信されます。ARP タイムアウト時間を 30 秒未満に設定した場合、予期しない結果が発生する場合があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **arp authorized**
6. **arp timeout** *seconds*
7. **arp probe interval** *seconds* **count** *number*
8. **end**
9. **show arp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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	**interface** *type number* **例：** `Router(config)# interface ethernet 1`	インターフェイス タイプを設定し、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。
ステップ 4	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 209.165.200.224 209.165.200.224`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 5	**arp authorized** **例：** `Router(config-if)# arp authorized`	インターフェイスのダイナミック ARP 学習をディセーブルにします。 • IP アドレスと MAC アドレスのマッピングを組み込むことができるのは、許可されているサブシステムのみです。
ステップ 6	**arp timeout** *seconds* **例：** `Router(config-if)# arp timeout 60`	エントリを ARP キャッシュに残す時間を設定します。 • 「制約事項」（P.11）で説明されているように、このタイムアウト時間を 30 秒未満に設定しないでください。
ステップ 7	**arp probe interval** *seconds* **count** *number* **例：** `Router(config-if)# arp probe interval 5 count 30`	（任意）プローブ再試行の間隔（秒単位）と回数を指定します。 • *seconds*：間隔（秒単位）。この秒数が経過した後、次のプローブが送信され、ピアが存在するかどうか確認されます。範囲は 1 ～ 10 です。 • *count-number*：プローブ再試行の回数。この回数に達した後、応答がない場合、ピアはログオフしていることになります。範囲は 1 ～ 60 です。 **（注）** プローブ プロセスを停止するには、このコマンドの **no** 形式を使用する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**end** **例：** `Router(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 9	**show arp** **例：** `Router# show arp`	（任意）ARP テーブル内のエントリを表示します。

リース先の数をグローバルに制御するための DHCP リース制限の設定

ATM Routed Bridged Encapsulation（RBE）アンナンバード インターフェイスまたはシリアル アンナンバード インターフェイスの背後で、クライアントに許可する DHCP リースの数をグローバルに制御するには、この作業を実行します。

この機能により、ISP は、クライアントが使用できるリースの数を、世帯ごとまたは接続ごとにグローバルに制限できます。

アンナンバード インターフェイスを介してクライアントに接続する Cisco IOS DHCP リレー エージェントにおいてこの機能をイネーブルにすると、リレー エージェントは、サブインターフェイスごとにクライアントに提供される DHCP リースについての情報を保持します。DHCPACK メッセージがクライアントに転送されると、リレー エージェントは、そのサブインターフェイスにおいてクライアントに提供されているリースの数をインクリメントします。新しい DHCP クライアントが IP アドレスを取得しようとし、一方で、リースの数が設定済みのリース制限にすでに達している場合、クライアントからの DHCP メッセージはドロップされ、DHCP サーバに転送されません。

アンナンバード インターフェイスを介してクライアントに直接接続する Cisco IOS DHCP サーバでこの機能をイネーブルにすると、サーバは、アドレスを割り当て、サブインターフェイスごとにリースの数をインクリメントします。新しいクライアントが IP アドレスを取得しようとし、一方で、サブインターフェイスでのリースの数が設定済みのリース制限にすでに達している場合、サーバは IP アドレスを提供しません。

DHCP リース制限に関する制約事項

この機能は、ナンバード インターフェイスではサポートされません。リース制限は、RBE アンナンバード インターフェイスまたはシリアル アンナンバード インターフェイスでの ATM に対してのみ適用できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp limit lease log**
4. **ip dhcp limit lease per interface** *lease-limit*
5. **end**
6. **show ip dhcp limit lease** [***type number***]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 limit lease log** **例：** `Router(config)# ip dhcp limit lease log`	（任意）DHCP リース制限しきい値を超えた場合、DHCP リース違反ロギングをイネーブルにします。 • このコマンドを設定すると、**show ip dhcp limit lease** コマンドの出力に、リース制限違反が表示されます。
ステップ 4	**ip dhcp limit lease per interface** *lease-limit* **例：** `Router(config)# ip dhcp limit lease per interface 2`	ATM RBE アンナンバード インターフェイスまたはシリアル ナンバード インターフェイスの背後で、DHCP クライアントに提供されるリースの数を制限します。
ステップ 5	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**show ip dhcp limit lease** [*type number*] **例：** `Router# show ip dhcp limit lease`	（任意）リース制限しきい値の違反が発生した回数を表示します。 • **clear ip dhcp limit lease** 特権 EXEC コマンドを使用して、保存されているリース違反エントリを手動でクリアできます。

トラブルシューティングのヒント

debug ip dhcp server packet コマンドおよび **debug ip server events** コマンドを使用して、DHCP リース制限をトラブルシューティングできます。

インターフェイスにおいてリース先の数を制御するための DHCP リース制限の設定

インターフェイスで許可する DHCP リースの数を制限するには、この作業を実行します。

この機能により、ISP は、クライアントが使用できるリースの数を、インターフェイスにおいて世帯ごとまたは接続ごとに制限できます。

アンナンバード インターフェイスを介してクライアントに直接接続する Cisco IOS DHCP サーバでこの機能をイネーブルにすると、サーバは、アドレスを割り当て、サブインターフェイスごとにリースの数をインクリメントします。新しいクライアントが IP アドレスを取得しようとし、一方で、サブインターフェイスでのリースの数が設定済みのリース制限にすでに達している場合、サーバは IP アドレスを提供しません。

制約事項

この機能は、ナンバード インターフェイスではサポートされません。リース制限は、RBE アンナンバード インターフェイスまたはシリアル アンナンバード インターフェイスでの ATM に対してのみ適用できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp limit lease log**
4. **interface** *type number*
5. **ip dhcp limit lease** *lease-limit*
6. **end**
7. **show ip dhcp limit lease** [***type number***]
8. **show ip dhcp server statistics** [*type number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 limit lease log** **例：** `Router(config)# ip dhcp limit lease log`	（任意）DHCP リース制限しきい値を超えた場合、DHCP リース違反ロギングをイネーブルにします。 • このコマンドを設定すると、**show ip dhcp limit lease** コマンドの出力に、リース制限違反が表示されます。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface Seria l0/0`	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。
ステップ 5	**ip dhcp limit lease** *lease-limit* **例：** `Router(config-if)# ip dhcp limit lease 6`	インターフェイスごとに DHCP クライアントに提供されるリースの数を制限します。 • インターフェイス コンフィギュレーションは、**ip dhcp limit lease per interface** グローバル コンフィギュレーション コマンドで指定したグローバル設定よりも優先されます。
ステップ 6	**end** **例：** `Router(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。

	コマンドまたはアクション	目的
ステップ 7	**show ip dhcp limit lease** [*type number*] **例：** `Router# show ip dhcp limit lease Serial 0/0`	（任意）リース制限しきい値の違反が発生した回数を表示します。 • **clear ip dhcp limit lease** 特権 EXEC コマンドを使用して、保存されているリース違反エントリを手動でクリアできます。
ステップ 8	**show ip dhcp server statistics** [*type number*] **例：** `Router# show ip dhcp server statistics Serial0/0`	（任意）DHCP サーバ統計情報を表示します。 • インターフェイス レベルの DHCP 統計情報を表示するために、このコマンドは Cisco IOS Release 12.2(33)SRC で変更されました。

トラブルシューティングのヒント

debug ip dhcp server packet コマンドおよび **debug ip server events** コマンドを使用して、DHCP リース制限をトラブルシューティングできます。

アカウンティングおよびセキュリティ対応の DHCP サービスの設定例

ここでは、次の設定例について説明します。

例：DHCP アカウンティング対応の AAA および RADIUS の設定

次の例は、DHCP アカウンティング対応の AAA および RADIUS の設定方法を示しています。

```
aaa new-model
aaa group server radius RGROUP-1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 exit
aaa accounting network RADIUS-GROUP1 start-stop group RGROUP-1
aaa session-id common
ip radius source-interface Ethernet 0
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
exit
```

例：DHCP アカウンティングの設定

DHCP アカウンティングは、クライアント単位またはリース単位で設定します。個別の DHCP アカウンティング処理をプール単位に設定できます。次の例は、RADIUS-GROUP1 が start-stop グループとして設定された場合に、DHCP アカウンティング START および STOP メッセージが送信されるように設定する方法を示しています。

```
ip dhcp pool WIRELESS-POOL
 accounting RADIUS-GROUP1
 exit
```

例：DHCP アカウンティングの確認

DHCP 対応の RADIUS と AAA の両方を設定した後、DHCP アカウンティングをイネーブルにします。DHCP START および STOP アカウンティング生成情報は、**debug radius accounting** コマンドおよび **debug ip dhcp server events** コマンドを使用して監視できます。DHCP アカウンティングで導入された AAA アトリビュートのリストについては、「RADIUS アカウンティング アトリビュート」（P.4）を参照してください。

以下は、**debug radius accounting** コマンドの出力例です。この出力では、DHCP リース セッション ID、MAC アドレス、およびクライアント インターフェイスの IP アドレスが示されています。

```
00:00:53: RADIUS: Pick NAS IP for uid=2 tableid=0 cfg_addr=10.0.18.3 best_addr=0.0.0.0
00:00:53: RADIUS(00000002): sending
00:00:53: RADIUS(00000002): Send to unknown id 21645/1 10.1.1.1 :1646, Accounting-Request,
len 76
00:00:53: RADIUS: authenticator C6 FE EA B2 1F 9A 85 A2 - 9A 5B 09 B5 36 B5 B9 27
00:00:53: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:00:53: RADIUS: Framed-IP-Address [8] 6 10.0.0.10
00:00:53: RADIUS: Calling-Station-Id [31] 16 "00000c59df76"
00:00:53: RADIUS: Acct-Status-Type [40] 6 Start [1]
00:00:53: RADIUS: Service-Type [6] 6 Framed [2]
00:00:53: RADIUS: NAS-IP-Address [4] 6 10.0.18.3
00:00:53: RADIUS: Acct-Delay-Time [41] 6 0
```

以下は、**debug ip dhcp server events** コマンドの出力例です。この出力は、DHCP サーバで生成されたもので、DHCP リースをネゴシエーションするクライアントとサーバの間の DHCP メッセージの交換が示されています。DHCP サーバに送信される、クライアントが割り当てられた IP アドレスを受け入れたことを示す確認応答により、アカウンティング START メッセージがトリガーされます。これは、次の出力では最後の行に示されています。

```
00:45:50:DHCPD:DHCPDISCOVER received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31 on
interface Ethernet0.

00:45:52:DHCPD:assigned IP address 10.10.10.16 to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31.

00:45:52:DHCPD:Sending DHCPOFFER to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31(10.10.10.16)

00:45:52:DHCPD:broadcasting BOOTREPLY to client 0001.42c9.ec75.

00:45:52:DHCPD:DHCPREQUEST received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31.

00:45:52:DHCPD:Sending DHCPACK to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31
(10.10.10.16).
```

```
00:45:52:DHCPD:broadcasting BOOTREPLY to client 0001.42c9.ec75.

00:45:52:DHCPD:triggered Acct Start for 0001.42c9.ec75 (10.10.10.16).
```

以下は、**debug ip dhcp server events** コマンドの出力例です。この出力は、DHCP サーバで生成されたもので、DHCP クライアントからの明示的なリリース メッセージの受信を示しています。DHCP サーバは、アカウンティング STOP メッセージをトリガーし、次に IP アドレスを DHCP プールに戻します。次の出力の 3 行目に、アカウンティング STOP メッセージに関する情報が示されています。

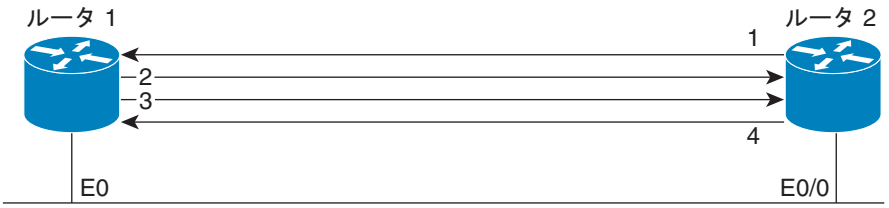
```
00:46:26:DHCPD:DHCPRELEASE message received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31 (10.10.10.16)

00:46:26:DHCPD:triggered Acct Stop for (10.10.10.16).

00:46:26:DHCPD:returned 10.10.10.16 to address pool WIRELESS-POOL.
```

例：DHCP 許可 ARP の設定

ルータ 1 は、IP アドレスをシークするルータに IP アドレスを割り当てる DHCP サーバで、ルータ 2 は、DHCP サーバを通じて IP アドレスを取得するように設定されている DHCP クライアントです。ルータ 1 では、**update arp** DHCP プール コンフィギュレーション コマンドが設定されているため、ルータはセキュア ARP エントリを ARP テーブルに組み込みます。**arp authorized** コマンドにより、そのインターフェイスでダイナミック ARP が停止します。ルータ 1 は定期 ARP をルータ 2 に送信して、クライアントが現在アクティブであることを確認します。ルータ 2 は、ARP 応答を使用して応答します。不正クライアントは、これらの定期 ARP に応答できません。不正 ARP 応答は、DHCP サーバでブロックされます。ルータ 1 は、許可クライアントから応答を受け取ると、エントリのタイマーを更新します。

トポロジの例については、図 1 を参照してください。

図 1　　DHCP 許可 ARP のトポロジ例



1. IP アドレスの要求を送信します。
2. IP アドレスを割り当て、それに対するセキュアな ARP エントリをルータ 1 にインストールします。
3. ルータ 2 がアクティブの状態を維持していることを確認するため、定期的な ARP を送信します。
4. 定期的な ARP に対して応答します。

103063

ルータ 1（DHCP サーバ）

```
ip dhcp pool name1
 network 10.0.0.0 255.255.255.0
 lease 0 0 20
 update arp
!
interface Ethernet 0
 ip address 10.0.0.1 255.255.255.0
 half-duplex
```

```
 arp authorized
 arp timeout 60
! optional command to adjust the periodic ARP probes sent to the peer
 arp probe interval 5 count 15
```

ルータ 2（DHCP クライアント）

```
interface Ethernet 0/0
 ip address dhcp
 half-duplex
```

例：DHCP 許可 ARP の確認

以下は、ルータ 1 での **show arp** コマンドの出力例です（図 1 を参照）。

```
Router1# show arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.3               0   0004.dd0c.ffcb  ARPA   Ethernet01
Internet  10.0.0.1               -   0004.dd0c.ff86  ARPA   Ethernet0
```

以下は、ルータ 2 での **show arp** コマンドの出力例です（図 1 を参照）。

```
Router2# show arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.3               -   0004.dd0c.ffcb  ARPA   Ethernet0/02
Internet  10.0.0.1               0   0004.dd0c.ff86  ARPA   Ethernet0/0
```

例：DHCP リース制限の設定

次の例では、4 つ以上のクライアントが ATM インターフェイス 4/0.1 から IP アドレスを取得しようとした場合、DHCPDISCOVER パケットは DHCP サーバに転送されません。DHCP サーバが同じルータに存在する場合、DHCP は 4 つ以上のクライアントに対して応答しません。

```
ip dhcp limit lease per interface 3
!
interface loopback 0
 ip address 10.1.1.129 255.255.255.192
!
interface ATM 4/0.1
 no ip address
!
interface ATM 4/0.1 point-to-point
 ip helper-address 172.16.1.2
 ip unnumbered loopback 0
 atm route-bridged ip
  pvc 88/800
  encapsulation aal5snap
```

次の例では、5 つの DHCP クライアントが IP アドレスを受け取ることを許可されます。6 つめのクライアントが IP アドレスを取得しようとした場合、DHCPDISCOVER メッセージは DHCP サーバに転送されず、トラップが SNMP マネージャに送信されます。

```
ip dhcp limit lease log
!
ip dhcp pool pool1
 network 10.1.1.0 255.255.255.0
```

```
!
interface loopback 0
 ip address 10.1.1.1 255.255.255.0
!
interface serial 0/0.2 point-to-point
 ip dhcp limit lease 5
 ip unnumbered loopback 0
 exit
snmp-server enable traps dhcp interface
```

参考資料

関連資料

関連項目	参照先
ARP コマンド：コマンド構文の詳細、コマンド モード、デフォルト、使用上の注意事項、および例	『*Cisco IOS IP Addressing Services Command Reference*』
DHCP コマンド：コマンド構文の詳細、コマンド モード、デフォルト、使用上の注意事項、および例	『*Cisco IOS IP Addressing Services Command Reference*』
DHCP の概念情報	『*Cisco IOS IP Addressing Configuration Guide*』の「DHCP Overview」モジュール
DHCP サーバ設定	『*Cisco IOS IP Addressing Configuration Guide*』の「Configuring the Cisco IOS DHCP Server」モジュール
DHCP ODAP の設定	『*Cisco IOS IP Addressing Configuration Guide*』の「Configuring the DHCP Server On-Demand Address Pool Manager」モジュール
DHCP クライアント設定	『*Cisco IOS IP Addressing Configuration Guide*』の「Configuring the Cisco IOS DHCP *Client*」モジュール
DHCP リレー エージェント設定	『*Cisco IOS IP Addressing Configuration Guide*』の「Configuring the Cisco IOS DHCP Relay Agent」モジュール
Edge-Session 管理用の DHCP 拡張機能	『*Cisco IOS IP Addressing Configuration Guide*』の「Configuring DHCP Enhancements for Edge-Session Management」モジュール
AAA および RADIUS の設定作業	『*Cisco IOS Security Configuration Guide*』
AAA および RADIUS コマンド：コマンド構文の詳細、コマンド モード、デフォルト、使用上の注意事項、および例	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	選択したプラットフォーム、シスコのソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能による新規または変更された RFC のサポートはありません。また、この機能による既存の RFC サポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポートおよびドキュメンテーション Web サイトでは、オンライン リソースを提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。これらのリソースは、ソフトウェアのインストールと設定や、シスコ製品とテクノロジーに関する技術上の問題のトラブルシューティングおよび解決に使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

アカウンティングおよびセキュリティ対応の DHCP サービスの機能情報

表 2 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア 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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 2 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。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。

表 2　アカウンティングおよびセキュリティ対応の DHCP サービスの機能情報

機能名	リリース	機能情報
インターフェイスごとの DHCP リース制限および統計情報	12.2(33)SRC	この機能は、インターフェイス上の DHCP クライアントに提供する DHCP リース数を制限します。DHCP サーバ統計情報レポートは、インターフェイスレベルの統計情報を表示するために拡張されました。 次のセクションで、この機能に関する情報を参照できます。 • 「インターフェイスにおいてリース先の数を制御するための DHCP リース制限の設定」 • 「例：DHCP リース制限の設定」 この機能により、次のコマンドが導入または変更されました。**clear ip dhcp limit lease**、**ip dhcp limit lease**、**ip dhcp limit lease log**、**show ip dhcp limit lease**、**show ip dhcp server statistics**。
ATM RBE アンナンバード インターフェイスごとの DHCP リース制限	12.2(28)SB 12.3(2)T 15.1(1)S	この機能は、DHCP サーバまたは DHCP リレー エージェントの ATM RBE アンナンバード インターフェイスまたはシリアル アンナンバード インターフェイスから接続される DHCP クライアントに対して提供される DHCP リースの数をサブインターフェイスごとに制限します。 次のセクションで、この機能に関する情報を参照できます。 • 「リース先の数をグローバルに制御するための DHCP リース制限の設定」 この機能により、次のコマンドが導入されました。 **ip dhcp limit lease per interface**。
ARP 自動ログオフ	12.3(14)T	ARP 自動ログオフ機能は、許可クライアントの詳細な制御およびプローブを提供することで DHCP 許可 ARP を拡張し、ログオフを検出します。 次のセクションで、この機能に関する情報を参照できます。 • 「セキュリティおよびアカウンティング対応の DHCP サービスの概要」 • 「DHCP 許可 ARP の設定」 • 「例：DHCP 許可 ARP の設定」 この機能により、次のコマンドが導入されました。 **arp probe interval**。

表 2　アカウンティングおよびセキュリティ対応の DHCP サービスの機能情報 （続き）

機能名	リリース	機能情報
DHCP 許可 ARP	12.2(33)SRC 12.3(4)T	DHCP 許可 ARP は、Cisco IOS ソフトウェアの DHCP および ARP コンポーネントを拡張し、モバイル ユーザまたは許可ユーザへの IP アドレスのリースを制限します。この機能は、DHCP サーバで無許可ユーザからの ARP 応答をブロックすることで、PWLAN のセキュリティを強化します。 次のセクションで、この機能に関する情報を参照できます。 • 「セキュリティおよびアカウンティング対応の DHCP サービスの概要」 • 「DHCP 許可 ARP の設定」 • 「例：DHCP 許可 ARP の設定」 この機能により、次のコマンドが導入されました。**arp authorized**。
DHCP アカウンティング	12.2(15)T 12.2(28)SB 12.2(33)SRB	DHCP アカウンティングにより、DHCP 設定対応の AAA および RADIUS サポートが導入されます。 次のセクションで、この機能に関する情報を参照できます。 • 「セキュリティおよびアカウンティング対応の DHCP サービスの概要」 • 「DHCP アカウンティングの設定」 この機能により、次のコマンドが導入されました。**accounting**。
DHCP セキュア IP アドレス割り当て	12.2(15)T 12.2(28)SB 12.2(33)SRC	DHCP セキュア IP アドレス割り当ては、DHCP データベース内で DHCP リースに対する ARP テーブル エントリを保護する機能を提供します。この機能は、クライアントの MAC アドレスを保護し、MAC アドレスと DHCP バインディングを同期することで、ハッカーまたは不正クライアントが、DHCP サーバをスプーフィングして、許可クライアントの DHCP リースを奪い取ることができないようにします。 次のセクションで、この機能に関する情報を参照できます。 • 「セキュリティおよびアカウンティング対応の DHCP サービスの概要」 • 「DHCP リースに対する ARP テーブル エントリの保護」 この機能により、次のコマンドが導入または変更されました。**show ip dhcp server statistics**、**update arp**。