DHCP サーバ RADIUS プロキシ

DHCP サーバ RADIUS プロキシ機能は、RADIUS-based アドレス割り当てメカニズムです。この機能では、Dynamic Host Configuration Protocol（DHCP）サーバがリモート クライアントを許可し、RADIUS サーバからの応答に基づいてアドレスを割り当てます。

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、「DHCP サーバ RADIUS プロキシの機能情報」（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

DHCP サーバ RADIUS プロキシの前提条件

DHCP サーバ RADIUS プロキシ機能の設定前に、DHCPv4 以降のバージョンを実行している必要があります。リリースおよびプラットフォーム サポートの詳細については、「DHCP サーバ RADIUS プロキシの機能情報」（P.21）を参照してください。

DHCP サーバ RADIUS プロキシの制約事項

DHCP サーバ RADIUS プロキシは、ルータ上の 1 つのアドレス許可プールのみをサポートします。

DHCP サーバ RADIUS プロキシについて

DHCP サーバ RADIUS プロキシの概要

DHCP サーバ RADIUS プロキシ 機能は、DHCP リースの RADIUS-based 許可のアドレス割り当てメカニズムです。この機能は、DHCP Option 60 および 121 をサポートします。

RADIUS サーバを使用したクライアント許可のプロセスは次のとおりです。

1. DHCP サーバは、クライアント情報を RADIUS サーバに渡します。
2. RADIUS サーバは、すべての必要な情報を RADIUS アトリビュートとして DHCP サーバに返します。
3. DHCP サーバは、RADIUS アトリビュートを DHCP オプションに変換してこの情報を DHCP OFFER メッセージで RADIUS に返します。
4. DHCP バインディングは RADIUS サーバがクライアント セッションを許可した後で同期されます。

ローカル プールおよび許可プールがルータ上に設定されている場合、DHCP サーバは両方のプールから別々のクライアント インターフェイスにアドレスを割り当てられます。

DHCP サーバ RADIUS プロキシ拡張機能

DHCP サーバ RADIUS プロキシ拡張機能は、Cisco IOS Release 15.0(1)S で導入された DHCP サーバ RADIUS プロキシ機能の拡張です。この機能は、DHCP Option 60 および 121 をサポートします。

RADIUS サーバを使用したクライアント許可のプロセスは次のとおりです。

1. DHCP サーバは、クライアント情報を RADIUS サーバに渡します。

2. RADIUS サーバは、Classname 情報および他のオプション情報（Session-Timeout および Session-Duration）を RADIUS アトリビュートとして DHCP サーバに返します。
3. DHCP サーバは、指定されたクラスがあればそこから IP アドレスを割り当て、RADIUS サーバから受信した他のオプションのアトリビュートがあれば DHCP オプションに変換します。情報は DHCP クライアントに DHCP OFFER メッセージとして送信されます。
4. DHCP バインディングは RADIUS サーバがクライアント セッションを許可した後で同期されます。

DHCP サーバ RADIUS プロキシ アーキテクチャ

DHCP および RADIUS プロキシ アーキテクチャのアドレス割り当ては、次のようなシーケンスで行われます。

1. クライアントは、レジデンシャル ゲートウェイからネットワークにアクセスして DHCP DISCOVER ブロードキャスト メッセージをリレー エージェントに送信します。DHCP DISCOVER メッセージには、クライアント IP アドレス、ホスト名、ベンダー クラス ID、およびクライアント ID が含まれます。
2. リレー エージェントは、次の情報を含む DHCP DISCOVER ユニキャスト メッセージをルータに送信します。
   - 内側および外側 VLAN ID を含むリモート ID サブオプションを伴うリレー エージェント情報（Option 82）。
   - DHCP DISCOVER パケット内のクライアント情報。

   ルータは、DHCP パケットを受信するインターフェイスの IP ヘルパー アドレスから DHCP サーバのアドレスを決定します。
3. RADIUS は、DHCP オプションを RADIUS アトリビュートに変換するための Access-Request メッセージを受信します。
4. RADIUS は、Access-Accept メッセージで応答し、次のアトリビュートを DHCP サーバに配信します。
   - Framed-IP-Address
   - Framed-IP-Netmask
   - Session-Timeout
   - Session-Duration
5. DHCP サーバは、RADIUS サーバ Access-Accept メッセージからの次の変換を含む OFFER ユニキャスト メッセージをクライアントに送信します。
   - DHCP ヘッダーに挿入された Framed-IP-Address。
   - DHCP Option 1（サブネット マスク）に挿入された Framed-IP-Netmask。
   - DHCP Option 51（IP アドレス リース時間）に挿入された Session-Timeout。
   - 標準の Cisco Framed-Route 形式から DHCP Option 121 または DHCP デフォルト ゲートウェイ オプション（ネットワークおよびネットマスクがデフォルト ルートに対して適切な場合）に変換された Framed-Route。
   - リレー エージェント情報（Option 82）のコピー。DHCP クライアントがパケットを受信する前に、リレーは Option 82 を削除します。
   - Session-Timeout に設定された T1 時間および Session-Duration に設定された T2 時間。
6. クライアントは、DHCPREQUEST ブロードキャスト メッセージで、提示された IP アドレスの正式な要求を DHCP サーバに戻します。

7. DHCP は、リース情報および DHCP オプションを含む DHCP ACK ユニキャスト メッセージをクライアントに返すことにより、IP アドレスがクライアントに割り当てられたことを確認します。
8. RADIUS サーバ アカウンティング要求が開始され、その後に Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サブシステムが使用する RADIUS サーバ アカウンティング応答が続きます。

RADIUS サーバ アトリビュートが Access-Accept メッセージ内にない場合、対応する DHCP オプションは DHCP クライアントに送信されません。特定の RADIUS サーバ アトリビュートを生成することに必要な情報を DHCP サーバが入手できない場合、DHCP サーバは RADIUS パケットに情報を含めません。含めないということは、アトリビュートを送信しない（情報がまったくない場合）、またはアトリビュートから情報を省略する（CLI-based 形式の文字列の場合）という形をとれます。

DHCP オプションが DHCP サーバに提供されているが無効な場合は、DHCP サーバは Access-Request 内の対応する RADIUS アトリビュートを送信しない、または無効な RADIUS サーバ アトリビュートを送信する可能性があります。

DHCP サーバ RADIUS プロキシ拡張機能アーキテクチャ

DHCP および RADIUS プロキシ拡張機能アーキテクチャのアドレス割り当ては、次のようなシーケンスで行われます。

1. クライアントは、レジデンシャル ゲートウェイからネットワークにアクセスして DHCP DISCOVER ブロードキャスト メッセージをリレー エージェントに送信します。DHCP DISCOVER メッセージには、クライアント IP アドレス、ホスト名、ベンダー クラス ID、およびクライアント ID が含まれます。
2. リレー エージェントは、次の情報を含む DHCP DISCOVER ユニキャスト メッセージをルータに送信します。
   - 内側および外側 VLAN ID を含むリモート ID サブオプションを伴うリレー エージェント情報（Option 82）。
   - DHCP DISCOVER パケット内のクライアント情報。

   ルータは、DHCP パケットを受信するインターフェイスの IP ヘルパー アドレスから DHCP サーバのアドレスを決定します。
3. RADIUS サーバは、DHCP オプションを RADIUS アトリビュートに変換するための Access-Request メッセージを受信します。
4. RADIUS サーバは、Access-Accept メッセージで応答し、次のアトリビュートを DHCP サーバに配信します。
   - Classname
   - Session-Timeout（任意）
   - Session-Duration（任意）
5. DHCP サーバは、指定された Classname の下に設定されたアドレスを識別してクライアントにアドレスを割り当てます。
6. DHCP サーバは、RADIUS サーバ Access-Accept メッセージからの次の変換を含む OFFER ユニキャスト メッセージをクライアントに送信します。
   - DHCP Option 51（IP アドレス リース時間）に挿入された Session-Timeout。
   - 標準の Cisco Framed-Route 形式から DHCP Option 121 または DHCP デフォルト ゲートウェイ オプションに変換された Framed-Route。

  - リレー エージェント情報（Option 82）のコピー。DHCP クライアントがパケットを受信する前に、リレーは Option 82 を削除します。
  - Session-Timeout に設定された T1 時間および Session-Duration に設定された T2 時間。

7. クライアントは、DHCP REQUEST ブロードキャスト メッセージで、提示された IP アドレスの正式な要求を DHCP サーバに戻します。
8. DHCP サーバは、リース情報および DHCP オプションを含む DHCP ACK ユニキャスト メッセージをクライアントに返すことにより、IP アドレスが割り当てられたことを確認します。
9. RADIUS サーバ アカウンティング要求が開始され、その後に AAA サブシステムが使用する RADIUS サーバ アカウンティング応答が続きます。

（注）

- Classname アトリビュートが受信した Access-Accept メッセージ内にない場合、DHCP サーバはデフォルト Classname と仮定してデフォルト クラスから IP アドレスの割り当てを試みます。デフォルト クラスの IP アドレスが使用可能な場合のみ、IP アドレスはクライアントに割り当てられます。
- Framed-IP-Address、Framed-IP-Netmask、Session-Timeout、および Session-Duration アトリビュートが Access-Accept メッセージ内にある場合、Classname アトリビュートは無視されて DHCP サーバは Framed-IP-Address アトリビュート内の受信した IP アドレスをクライアントに割り当てます。

DHCP サーバと RADIUS 変換

表 1 に、DHCP DISCOVER メッセージ内の DHCP オプションから RADIUS サーバ Access-Request メッセージ内のアトリビュートへの変換を一覧で示します。

表 1　DCHP DISCOVER から RADIUS Access-Request への変換

DHCP DISCOVER	RADIUS Access-Request
Client ID	DHCP Option 61 の 16 進形式のエンコードされた値と等しい Cisco Attribute-Value（AV; アトリビュート値）ペア dhcp-client-id
D-router 上の VLAN パラメータを含められる DHCP リレー情報オプション	DHCP Option 82 の 16 進形式のエンコードされた値と等しい Cisco AV ペア dhcp-relay-info
リレー エージェントのゲートウェイ アドレス（DHCP パケットの giaddr フィールド）	NAS-identifier
Hostname	DHCP Option 12 の値と等しい Cisco AV ペア client-hostname
該当なし	DHCP サーバに設定された User-Password
ベンダー クラス	DHCP Option 60 の 16 進形式のエンコードされた値と等しい Cisco AV ペア dhcp-vendor-class
レジデンシャル ゲートウェイの仮想 MAC アドレス	User-Name

表 2 に、RADIUS サーバ Access-Accept メッセージ内のアトリビュートから DHCP OFFER メッセージ内の DHCP オプションへの変換を一覧で示します。

表 2　RADIUS Access-Accept から DHCP OFFER への変換

RADIUS Access-Accept	DHCP OFFER
秒単位の Cisco AV ペア session-duration で、この秒は Session-Timeout アトリビュートの秒数以上です	DHCP サーバのセッション コントロールを提供します。このアトリビュートは、DHCP クライアントに送信されません。
Classname	DHCP サーバのアドレス割り当てに使用するクラスを指定する文字列を含みます。
Framed-IP-Address	レジデンシャル ゲートウェイの IP アドレス。
Framed-IP-Netmask	サブネット マスク（Option 1）。
Framed-Route（RADIUS アトリビュート 22）。各 DHCP オプションに 1 つのルート、1 つの RADIUS パケットに最大 16 の Framed-Route オプションが可能です	1 つのオプション（Option 121）に最大 16 のクラスレス ルートを含みます。
Session-Timeout	IP アドレス リース時間（Option 51）。

DHCP サーバ RADIUS プロキシに対する RADIUS プロファイル

DHCP サーバ RADIUS プロキシに対して RADIUS サーバ ユーザ プロファイルを設定する場合は、次の注意事項に従います。

- Session-Timeout アトリビュートには、秒単位の値が含まれる必要があります。このアトリビュートがない場合、DHCP OFFER はクライアントに送信されません。
- RADIUS ユーザ プロファイルには、次のアトリビュートが含まれる必要があります。
  - Framed-IP-Address
  - Framed-IP-Netmask
  - Framed-Route
  - Session-Timeout
  - Session-Duration : Session-Duration は、Cisco AV ペア session-duration = seconds です。*seconds* は、すべての更新を含むリース期間の最長時間です。Session-Duration の値は Session-Timeout アトリビュート値以上である必要があり、またゼロになれません。
- 追加の RADIUS サーバ アトリビュートも可能ですが必須ではありません。DHCP サーバは、追加のアトリビュートで理解できないものは無視します。RADIUS サーバ ユーザ プロファイルに空の必須のアトリビュートが含まれている場合、DHCP サーバは DHCP オプションを生成しません。

DHCP サーバ RADIUS プロキシ拡張機能に対する RADIUS プロファイル

Classname に対して DHCP サーバ RADIUS プロキシ拡張機能の RADIUS サーバ ユーザ プロファイルを設定する場合は、次の注意事項に従います。

- Session-Timeout アトリビュートがある場合は、秒単位の値が含まれる必要があります。
- RADIUS ユーザ プロファイルには、次のアトリビュートが含められます。
  - Classname（このアトリビュートがない場合、デフォルト Classname が考慮されます）。
  - Framed-Route
  - Session-Timeout

  - Session-Duration：Session-Duration は、Cisco AV ペア session-duration = seconds です。「seconds」は、すべての更新を含むリース期間の最長時間です。Session-Duration の値は Session-Timeout アトリビュート値以上である必要があり、またゼロになれません。
- 追加の RADIUS サーバ アトリビュートも可能ですが必須ではありません。DHCP サーバは、追加のアトリビュートで理解できないものは無視します。

DHCP サーバ RADIUS プロキシの設定方法

ここでは、次の作業について説明します。

- 「DHCP サーバ RADIUS プロキシに対する AAA-Related コマンド設定」（P.7）（必須）
- 「RADIUS プロキシに対する DHCP サーバ許可の設定」（P.11）（任意）
- 「DHCP サーバ プロキシ拡張機能の設定」（P.14）（任意）
- 「DHCP サーバのモニタリングおよびメンテナンス」（P.16）（任意）

DHCP サーバ RADIUS プロキシに対する AAA-Related コマンド設定

DHCP サーバ RADIUS プロキシ機能および DHCP サーバ RADIUS プロキシ拡張機能の設定に必要な AAA-related コマンドの設定には次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **service dhcp**
4. **aaa new-model**
5. **aaa group server radius** *group-name*
6. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
7. **exit**
8. **aaa authorization network** *method-list-name* **group** *group-name*
9. **aaa accounting network** *method-list-name* **start-stop group** *group-name*
10. **interface type** *slot*/*subslot*/*port*[**.***subinterface*]
11. **encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id* [**,***vlan-id* [**-***vlan-id*]]}
12. **ip address** *address mask*
13. **no shutdown**
14. **exit**
15. **radius-server host** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
16. **radius-server key** {**0** *string* | **7** *string* | *string*}
17. **exit**

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	**service dhcp** **例：** `Router(config)# service dhcp`	ルータ上の DHCP サーバ機能およびリレー エージェント機能をイネーブルにします。 • デフォルトでルータ上のこれらの機能はイネーブルです。
ステップ 4	**aaa new-model** **例：** `Router(config)# aaa new-model`	AAA アクセス コントロール システムをイネーブルにします。
ステップ 5	**aaa group server radius** *group-name* **例：** `Router(config)# aaa group server radius group1`	RADIUS サーバ ホストをグループ化するためにサーバ ホスト リストの名前を指定して、server-group コンフィギュレーション モードを開始します。 • *group-name*：サーバ グループの名前を表す文字列。次の語はグループ名として使用できません。 – auth-guest – enable – guest – if-authenticated – if-needed – krb5 – krb-instance – krb-telnet – line – local – none – radius – rcmd – tacacs – tacacsplus

	コマンドまたはアクション	目的
ステップ 6	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **例：** `Router(config-sg-radius)# server 10.1.1.1 auth-port 1700 acct-port 1701`	定義済みのサーバ グループの RADIUS サーバ ホストの IP アドレスを指定します。 • サーバ グループに関連付ける各 RADIUS サーバ ホストに対してこのコマンドを繰り返します。 – *ip-address* : RADIUS サーバ ホストの IP アドレス。 – **auth-port** *port-number* :（任意）認証要求のための UDP 宛先ポートを指定します。デフォルト値は 1645 です。 – **acct-port** *port-number* :（任意）アカウンティング要求のための UDP 宛先ポートを指定します。デフォルト値は 1646 です。
ステップ 7	**exit** **例：** `Router(config-sg-radius)# exit`	server-group コンフィギュレーション モードを終了します。
ステップ 8	**aaa authorization network** *method-list-name* **group** *group-name* **例：** `Router(config)# aaa authorization network auth1 group group1`	DHCP 許可のための方式リストおよびサーバ グループを指定します。 • *method-list-name* : 許可方式リストの名前を表す文字列。 • **group** : サーバ グループを指定します。 • *group-name* : DHCP 許可を適用するサーバ グループの名前。
ステップ 9	**aaa accounting network** *method-list-name* **start-stop group** *group-name* **例：** `Router(config)# aaa accounting network acct1 start-stop group group1`	AAA アカウンティングをすべてのネットワーク サービス要求に実行することを指定します。 • *method-list-name* : アカウンティング方式リストの名前を表す文字列。 • **start-stop** : プロセスの最初にアカウンティング開始通知を送信し、プロセスの最後にアカウンティング停止通知を送信します。アカウンティング開始レコードは、バックグラウンドで送信されます。アカウンティング開始通知がアカウンティング サーバで受信されたかどうかにかかわらず、要求されたユーザ プロセスが開始されます。 • **group** : サーバ グループを指定します。 • *group-name* : DHCP アカウンティングを適用するサーバ グループの名前。
ステップ 10	**interface** *type slot*/*subslot*/*port*[.*subinterface*] **例：** `Router(config)# interface ethernet 1/10/0.0`	DHCP クライアントが DHCP サーバから IP アドレスを取得することを許可するインターフェイスまたはサブインターフェイスを設定して、サブインターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id* [,*vlan-id* [-*vlan-id*]]} **例：** `Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`	（任意）VLAN のサブインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化をイネーブルにします。 • *vlan-id*：VLAN ID で、1 ～ 4094 の範囲の整数。VLAN ID の範囲を定義することに使用する VLAN ID の開始値と終了値を区切るには、ハイフンを入力します。（任意）各 VLAN ID の範囲を次の範囲と区切るには、カンマを入力します。 • **second-dot1q**：IEEE 802.1Q-in-Q VLAN Tag Termination 機能をサポートして内側 VLAN ID を設定します。 • **any**：1 ～ 4094 の範囲の任意の秒タグ。
ステップ 12	**ip address** *address mask* **例：** `Router(config-subif)# ip address 192.168.1.1 255.255.255.0`	インターフェイスまたはサブインターフェイスの IP アドレスを指定します。 • *address* は、インターフェイスまたはサブインターフェイスの IP アドレスです。 • *mask* は、IP アドレスのサブネット アドレスです。
ステップ 13	**no shutdown** **例：** `Router(config-subif)# no shutdown`	インターフェイスまたはサブインターフェイスをイネーブルにします。
ステップ 14	**exit** **例：** `Router(config-subif)# exit`	サブインターフェイス 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。
ステップ 15	**radius-server host** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **例：** `Router(config)# radius-server host 10.1.1.1`	RADIUS サーバ ホストを指定します。 • *ip-address* は、RADIUS サーバ ホストの IP アドレスです。 • **auth-port** *port-number*：（任意）認証要求のための UDP 宛先ポートを指定します。デフォルト値は 1645 です。 • **acct-port** *port-number*：（任意）アカウンティング要求のための UDP 宛先ポートを指定します。デフォルト値は 1646 です。

	コマンドまたはアクション	目的
ステップ 16	**radius-server key** {**0** *string* | **7** *string* | *string*} **例：** `Router(config)# radius-server key string1`	ルータと RADIUS デーモンとの間におけるすべての RADIUS 通信用の認証および暗号化キーを指定します。 • **0** *string*：暗号化されていない（平文）共有キーを指定します。 • **7** *string*：秘密の共有キーを指定します。 **（注）** 入力するキーはすべて RADIUS デーモン上のキーと一致する必要があります。先頭のスペースはすべて無視されますが、キーの中間および末尾のスペースは使用できます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
ステップ 17	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

RADIUS プロキシに対する DHCP サーバ許可の設定

RADIUS プロキシに対する DHCP サーバ機能を設定するには、次の作業を実行します。

前提条件

RADIUS プロキシに対する DHCP サーバ機能を設定する前に AAA 設定を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp use class** [**aaa**]
4. **ip dhcp pool** *name*
5. **accounting** *method-list-name*
6. **authorization method** *method-list-name*
7. **authorization shared-password** *password*
8. **authorization username** *string*
9. **exit**

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 use class** [**aaa**] **例：** `Router(config)# ip dhcp use class aaa`	AAA サーバを使用してクラス名を取得するように DHCP サーバを設定します。
ステップ 4	**ip dhcp pool** *name* **例：** `Router(config)# ip dhcp pool pool1`	DHCP サーバ アドレス プールの名前を指定し、DHCP プール コンフィギュレーション モードを開始します。 • *name*：プールの名前。
ステップ 5	**accounting** *method-list-name* **例：** `Router(dhcp-config)# accounting acct1`	DHCP アカウンティングをイネーブルにします。 • *method-list-name*：アカウンティング方式リストの名前。
ステップ 6	**authorization method** *method-list-name* **例：** `Router(dhcp-config)# authorization method auth1`	DHCP 許可をイネーブルにします。 • *method-list-name*：許可方式リストの名前。
ステップ 7	**authorization shared-password** *password* **例：** `Router(dhcp-config)# authorization shared-password password1`	RADIUS ユーザ プロファイルに設定したパスワードを指定します。

	コマンドまたはアクション	目的
ステップ 8	**authorization username** *string* **例：** `Router(dhcp-config)# authorization username %c-user1`	DHCP クライアントに設定情報をダウンロードするときに、RADIUS が DHCP サーバに送信するパラメータを指定します。 • *string* 引数には、DHCP クライアント情報を挿入するための次の形式の文字が含まれます。 – **%%** : RADIUS サーバに送信した文字列内のパーセント記号（%）文字を送信します。 – **%c** : ASCII 形式の DHCP クライアント（chaddr フィールド）のイーサネット アドレス。 – **%C** : 16 進形式の DHCP クライアントのイーサネット アドレス。 – **%g** : DHCP リレー エージェント（giaddr フィールド）のゲートウェイ アドレス。 – **%i** : ASCII 形式の DHCP リレー情報（Option 82）からの内側 VLAN ID。 – **%I** : 16 進形式の DHCP リレー情報からの内側 VLAN ID。 – **%o** : ASCII 形式の DHCP リレー情報（Option 82）からの外側 VLAN ID。 – **%O** : 16 進形式の DHCP リレー情報（Option 82）からの外側 VLAN ID。 – **%p** : ASCII 形式の DHCP リレー情報（Option 82）からのポート番号。 – **%P** : 16 進形式の DHCP リレー情報（Option 82）からのポート番号。 – **%u** : ASCII 形式の DHCP リレー情報からの回線 ID。 – **%U** : 16 進形式の DHCP リレー情報からの回線 ID。 – **%r** : ASCII 形式の DHCP リレー情報からのリモート ID。 – **%R** : 16 進形式の DHCP リレー情報からのリモート ID。 **（注）** パーセント（%）記号は、特定の文字に関連付けられた DHCP クライアント情報を挿入するためのマーカーです。% は、%% 文字を指定しない限り RADIUS サーバに送信されません。
ステップ 9	**exit** **例：** `Router(dhcp-config)# exit`	DHCP プール コンフィギュレーション モードを終了します。

DHCP サーバ プロキシ拡張機能の設定

DHCP サーバ プロキシ拡張機能を設定するには、次の作業を実行します。

前提条件

RADIUS プロキシに対する DHCP サーバ機能を設定する前に AAA 設定を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp use class aaa**
4. **ip dhcp pool** *name*
5. **accounting** *server-group-name*
6. **authorization method** *method-list-name*
7. **authorization shared-password** *password*
8. **authorization username** *username*
9. **exit**
10. **ip dhcp pool** *name*
11. **network** *network-number* [*mask* [**secondary**] | */prefix-length* [**secondary**]]
12. **class** *class-name*
13. **address range** *start-ip end-ip*

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 use class aaa** **例：** `Router(config)# ip dhcp use class aaa`	クラス名の取得に AAA サーバを使用することを指定します。
ステップ 4	**ip dhcp pool** *name* **例：** `Router(config)# ip dhcp pool pool1`	DHCP サーバに対し 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。

	コマンドまたはアクション	目的
ステップ 5	**accounting** *server-group-name* **例：** `Router(dhcp-config)# accounting list1`	サーバ グループの DHCP アカウンティングをイネーブルにします。
ステップ 6	**authorization method** *method-list-name* **例：** `Router(dhcp-config)# authorization method list1`	DHCP に対して RADIUS を使用する、アドレス割り当てに使用する方式リストを指定します。
ステップ 7	**authorization shared-password** *password* **例：** `Router(dhcp-config)# authorization shared-password password1`	DHCP クライアントに設定情報をダウンロードするときに、RADIUS が DHCP または RADIUS サーバに送信するパスワードを指定します。
ステップ 8	**authorization username** *username* **例：** `Router(dhcp-config)# authorization username user1`	DHCP クライアントに設定情報をダウンロードするときに、RADIUS が DHCP サーバに送信するパラメータを指定します。
ステップ 9	**exit** **例：** `Router(dhcp-config)# exit`	DHCP プール 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 モードに戻ります。
ステップ 10	**ip dhcp pool** *name* **例：** `Router(config)# ip dhcp pool name2`	DHCP サーバに対し 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 11	**network** *network-number* [*mask* [**secondary**] | **/***prefix-length* [**secondary**]] **例：** `Router(config)# network 10.0.0.1 255.255.255.0`	Cisco IOS DHCP サーバの DHCP アドレス プール プライマリまたはセカンダリ サブネットに、ネットワーク番号およびマスクを設定します。
ステップ 12	**class** *class-name* **例：** `Router(config)# class name1`	クラスを DHCP アドレス プールに関連付け、DHCP プール クラス コンフィギュレーション モードを開始します。
ステップ 13	**address range** *start-ip end-ip* **例：** `Router(config-dhcp-pool-class)# address range 10.0.0.1 10.0.0.5`	DHCP サーバ アドレス プールの DHCP クラスにアドレス範囲を設定します。

DHCP サーバのモニタリングおよびメンテナンス

DHCP サーバ情報の確認およびモニタをするには、次の作業を実行します。ルータが特権 EXEC モードになったら、コマンドを任意の順序で入力できます。

手順の概要

1. **enable**
2. **debug ip dhcp server packet**
3. **debug ip dhcp server events**
4. **show ip dhcp binding** [*address*]
5. **show ip dhcp server statistics**
6. **show ip dhcp pool** [*name*]
7. **show ip route dhcp** [*address*]

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 ip dhcp server packet** **例：** `Router# debug ip dhcp server packet`	（任意）DHCP サーバ デバッグをイネーブルにします。
ステップ 3	**debug ip dhcp server events** **例：** `Router# debug ip dhcp server events`	（任意）アドレス割り当てやデータベース更新などの DHCP サーバ イベントを報告します。
ステップ 4	**show ip dhcp binding** [*address*] **例：** `Router# show ip dhcp binding`	（任意）特定の DHCP サーバに作成されているすべてのバインディングのリストを表示します。 • **show ip dhcp binding** コマンドを使用すると、すでに割り当てられている IP アドレスが表示されます。アドレス プールに空きがあることを確認します。必要に応じて、プールを再作成してより大きいアドレス プールを作成します。 • **show ip dhcp binding** コマンドを使用して、ホストの IP アドレスのリース有効期限の日時を表示します。
ステップ 5	**show ip dhcp server statistics** **例：** `Router# show ip dhcp server statistics`	（任意）サーバの統計情報に関するカウント情報および送受信したメッセージを表示します。

	コマンドまたはアクション	目的
ステップ 6	**show ip dhcp pool** [*name*] **例：** `Router# show ip dhcp pool`	（任意）DHCP サーバおよびリレー エージェントによってルーティング テーブルに追加されたルートを表示します。
ステップ 7	**show ip route dhcp** [*address*] **例：** `Router# show ip route dhcp [address]`	（任意）DHCP アドレス プールに関する情報を表示します。

DHCP サーバ RADIUS プロキシの設定例

ここでは、次の設定例について説明します。

- 「例：RADIUS プロキシに対する DHCP サーバ設定」（P.17）
- 「例：RADIUS プロキシに対する RADIUS プロファイルの設定」（P.18）
- 「例：RADIUS プロキシ拡張機能に対する DHCP サーバ設定」（P.18）
- 「例：RADIUS プロキシ拡張機能に対する RADIUS プロファイルの設定」（P.19）

例：RADIUS プロキシに対する DHCP サーバ設定

次に、DHCP リースの RADIUS-based 許可のために DHCP サーバを設定する方法の例を示します。この例では、DHCP クライアントはイーサネット インターフェイス 4/0/1 およびイーサネット サブインターフェイス 4/0/3.10 に接続できます。username 文字列（%c-user1）は、RADIUS サーバが user1 という名前の DHCP クライアントのイーサネット アドレスを DHCP サーバに送信することを指定します。

```
Router> enable
Router# configure terminal
Router(config)# service dhcp
Router(config)# aaa new-model
Router(config)# aaa group server radius rad1
Router(config-sg)# server 10.1.1.1
Router(config-sg)# server 10.1.5.10
Router(config-sg)# exit
Router(config)# aaa authorization network auth1 group group1
Router(config)# aaa accounting network acct1 start-stop group group1
Router(config)# aaa session-id common
Router(config)# ip dhcp database tftp://172.16.1.1/router-dhcp write-delay 100 timeout 5
!
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# accounting acct1
Router(config-dhcp)# authorization method auth1
Router(config-dhcp)# authorization shared-password cisco
Router(config-dhcp)# authorization username %c-user1
Router(config-dhcp)# exit
!
Router(config)# interface ethernet 4/0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# exit
Router(config-if)# interface ethernet 4/0/3.10
Router(config-if)# encapsulation dot1q 100 second-dot1q 200
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# exit
```

```
Router(config)# radius-server host 10.1.3.2
Router(config)# radius-server key cisco
Router(config)# exit
```

例：RADIUS プロキシに対する RADIUS プロファイルの設定

次に、DHCP サーバに送信する Access-Accept メッセージ内のアトリビュートに一般的な RADIUS ユーザ プロファイルを設定する方法の例を示します。

```
DHCP-00059A3C7800 Password = “password”
Service-Type = Framed,
Framed-Ip-Address = 10.3.4.5,
Framed-Netmask = 255.255.255.0,
Framed-Route = "0.0.0.0 0.0.0.0 10.3.4.1",
Session-Timeout = 3600,
Cisco:Cisco-Avpair = "session-duration=7200”
```

例：RADIUS プロキシ拡張機能に対する DHCP サーバ設定

次に、classname の RADIUS-based 許可のために DHCP サーバを設定する方法の例を示します。この例では、DHCP クライアントはイーサネット インターフェイス 4/0/1 およびイーサネット サブインターフェイス 4/0/3.10 に接続できます。username 文字列（%c-user1）は、RADIUS サーバが user1 という名前の DHCP クライアントのイーサネット アドレスを DHCP サーバに送信することを指定します。

```
Router> enable
Router# configure terminal
Router(config)# service dhcp
Router(config)# aaa new-model
Router(config)# aaa group server radius rad1
Router(config-sg)# server 10.1.1.1
Router(config-sg)# server 10.1.5.10
Router(config-sg)# exit
Router(config)# aaa authorization network auth1 group group1
Router(config)# aaa accounting network acct1 start-stop group group1
Router(config)# aaa session-id common
Router(config)# ip dhcp database tftp://172.0.2.1/router-dhcp write-delay 100 timeout 5
!
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# accounting acct1
Router(config-dhcp)# authorization method auth1
Router(config-dhcp)# authorization shared-password password1
Router(config-dhcp)# authorization username %c-user1
Router(config-dhcp)# exit
!
Router(config)# ip dhcp pool pool_subnet
Router(config-dhcp)# network 10.3.4.0 255.255.255.0
Router(config-dhcp)# class class-1
Router(config-dhcp)# address range 10.3.4.1 10.3.4.10
Router(config-dhcp)# exit
!
Router(config)# interface ethernet 4/0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# exit
Router(config-if)# interface ethernet 4/0/3.10
Router(config-if)# encapsulation dot1q 100 second-dot1q 200
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# exit
Router(config)# radius-server host 10.1.3.2
Router(config)# radius-server key cisco
Router(config)# exit
```

例：RADIUS プロキシ拡張機能に対する RADIUS プロファイルの設定

次に、DHCP サーバに送信する Access-Accept メッセージ内のアトリビュートに一般的な RADIUS ユーザ プロファイルを設定する方法の例を示します。

```
DHCP-00059A3C7800 Password = “password”
Service-Type = Framed,
Classname = "class-1"
Framed-Route = "0.0.0.0 0.0.0.0 10.3.4.1",
Session-Timeout = 3600,
Cisco:Cisco-Avpair = "session-duration=7200”
```

参考資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
DHCP リレー設定	『*Cisco IOS DHCP リレー エージェント設定*』
DHCP コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト、使用上の注意事項、および例	『*Cisco IOS IP Addressing Services Command Reference*』

規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	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
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対する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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

DHCP サーバ RADIUS プロキシの機能情報

表 3 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 3 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 3　Cisco IOS DHCP サーバ RADIUS プロキシの機能情報

機能名	リリース	機能情報
DHCP サーバ RADIUS プロキシ	12.2(31)ZV1 12.2(34)SB 12.2(33)XNE 15.0(1)S	DHCP サーバ RADIUS プロキシ機能により、サーバはリモート クライアント許可およびサーバからの応答に基づくアドレス割り当てが可能になります。 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。 • 「DHCP サーバ RADIUS プロキシの概要」（P.2） • 「DHCP サーバ RADIUS プロキシ アーキテクチャ」（P.3） • 「RADIUS プロキシに対する DHCP サーバ許可の設定」（P.11） この機能により次のコマンドが変更されました。**authorization method**（DHCP）、**authorization shared-password**、**authorization username**（DHCP）。
DHCP RADIUS プロキシ拡張機能	15.0(1)S	DHCP RADIUS プロキシ拡張機能では、クライアントに割り当てるためのクラス名または IP アドレスのいずれかを受け入れるように DHCP サーバを設定するオプションを提供します。 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。 • 「DHCP サーバ RADIUS プロキシ拡張機能」（P.2） • 「DHCP サーバ RADIUS プロキシ拡張機能アーキテクチャ」（P.4） • 「DHCP サーバ プロキシ拡張機能の設定」（P.14） 次のコマンドが導入または変更されました。**accounting**（DHCP）、**address range**、**authorization method**（DHCP）、**authorization shared-password**、**authorization username**（DHCP）、**class**（DHCP）、**network**（DHCP）。

用語集

DHCP：Dynamic Host Configuration Protocol。

giaddr：ゲートウェイ IP アドレス。DHCP メッセージの giaddr フィールドは、クライアントが属する IP アドレス サブネットの情報を DHCP サーバに提供します。また、応答メッセージの送信先の IP アドレスも DHCP サーバに提供します。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。

VPN：Virtual Private Network（バーチャル プライベート ネットワーク）。トンネリングを使用してパブリック TCP/IP ネットワーク経由で IP トラフィックをセキュアに転送できるようにします。

VRF：VPN Routing and Forwarding（VPN ルーティングおよび転送）インスタンス。VRF は、IP ルーティング テーブル、取得された転送テーブル、その転送テーブルを使用する一連のインターフェイス、転送テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。一般に、VRF には、PE ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。PE ルータでインスタンス化された各 VPN は独自の VRF を持ちます。

クライアント：DHCP プロトコルまたは BOOTP プロトコルを使用して、インターフェイスの設定（IP アドレスの取得）を試行しているホスト。

サーバ：DHCP サーバまたは BOOTP サーバ。

リレー エージェント：異なるサブネット上のサーバとクライアント間で DHCP メッセージおよび BOOTP メッセージを転送するルータ。