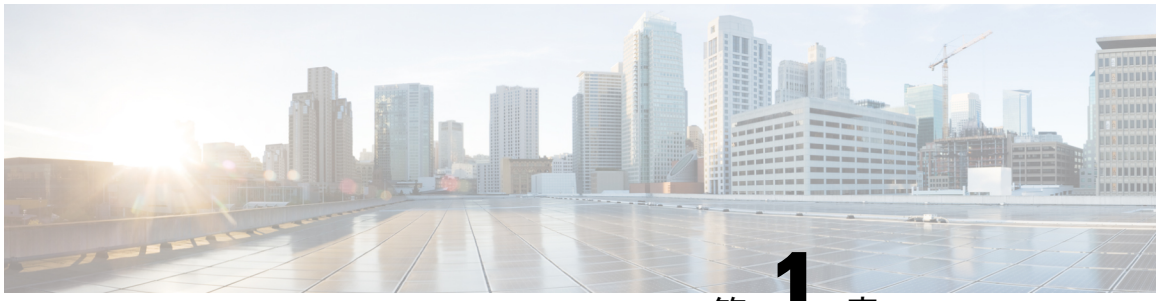
Cisco IOS XE Gibraltar 16.10.x RADIUS コンフィギュレーションガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE Release 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE Release 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、単一バージョンのコンバージドリリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

機能情報

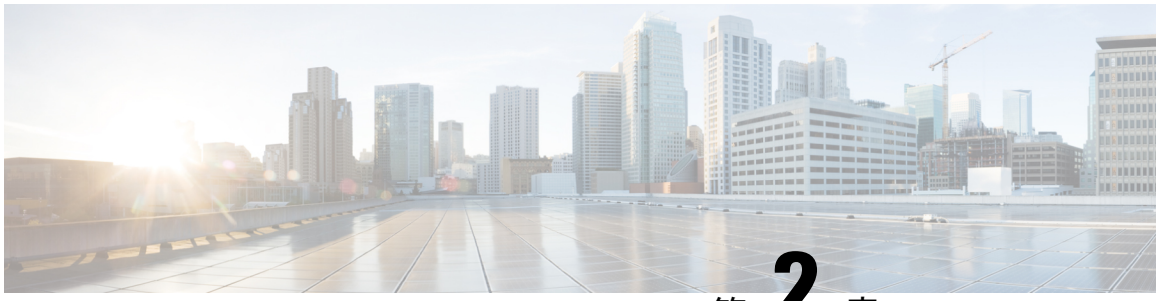
機能のサポート、プラットフォームのサポート、およびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- 『Cisco IOS Command References, All Releases』

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 2 章

RADIUS の設定

RADIUS セキュリティ システムは、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。シスコの実装では、RADIUS クライアントはシスコ デバイス上で実行され、すべてのユーザ認証およびネットワーク サービス アクセス情報を持つ中央の RADIUS サーバに認証要求を送信します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RADIUS の前提条件

シスコ デバイスまたはアクセス サーバで RADIUS を設定するには、次のタスクを実行する必要があります。

- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、認証、認可、およびアカウンティング（AAA）をイネーブルにします。RADIUS を使用する予定がある場合、AAA を設定する必要があります。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。

RadSec の制限（RADIUS セキュリティ）

RadSec は、シスコ エンタープライズ ルーティング プラットフォームではサポートされていません。

RADIUS の概要

RADIUS ネットワーク環境

シスコは、認証、認可、およびアカウンティング（AAA）セキュリティ パラダイムに基づいて RADIUS をサポートします。RADIUS は、TACACS+、Kerberos、ローカル ユーザ名の検索など、他の AAA セキュリティ プロトコルと併用できます。RADIUS はすべての Cisco プラットフォームでサポートされますが、RADIUS でサポートされる一部の機能は、指定されたプラットフォームだけで実行されます。

RADIUS は、リモート ユーザのネットワーク アクセスを維持すると同時に高度なレベルのセキュリティを必要とするさまざまなネットワーク環境に実装されています。

RADIUS は、アクセスのセキュリティが必要な次のネットワーク環境で使用できます。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カード アクセス コントロール システムを使用するアクセス環境。その例として、ユーザの検証とネットワーク リソースへのアクセス許可に、RADIUS が Enigma のセキュリティ カードとともに使用されています。
- すでに RADIUS を使用中のネットワーク。RADIUS 機能を持つ Cisco デバイスをネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。

- ユーザが単一のサービスにだけアクセスする必要があるネットワーク。RADIUS を使用すると、単一ホスト、単一ユーティリティ（Telnet など）、または単一プロトコル（PPP など）に対するユーザ アクセスを制御できます。たとえば、ユーザがログインすると、RADIUS は、IP アドレス 10.2.3.4 を使用してそのユーザが PPP を実行する権限を持っていることを識別し、定義済みのアクセス リストが開始されます。
- リソースアカウンティングが必要なネットワーク。RADIUSアカウンティングは、RADIUS認証またはRADIUS認可とは個別に使用できます。RADIUSアカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。ISP は、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。
- 事前認証をサポートしているネットワーク。ネットワークに RADIUS サーバを導入すると、AAA 事前認証を設定し、事前認証のプロファイルを設定できます。サービス プロバイダーが事前認証を使用すると、既存のRADIUS ソリューションを使用するポートの管理性が向上し、共有リソースを効率的に管理して、各種のサービスレベル契約を提供できるようになります。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は次のプロトコルをサポートしていません。
  - AppleTalk Remote Access（ARA）
  - NetBIOS Frame Control Protocol（NBFCP）
  - NetWare Asynchronous Services Interface（NASI）
  - X.25 Packet Assemblers/Disassemblers（PAD）接続
- デバイスからデバイスへの状況。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスがRADIUS認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

RADIUS の動作

ユーザがログインを試行し、RADIUSを使用してアクセス サーバから認証を受ける場合、次の手順が発生します。

1. ユーザ名とパスワードの入力を求めるプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由でRADIUSサーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   1. ACCEPT：ユーザが認証されたことを表します。

2. CHALLENGE：RADIUS サーバによってチャレンジが発行されます。チャレンジは、ユーザから追加データを収集します。
3. CHANGE PASSWORD：RADIUS サーバからユーザに対して新しいパスワードの選択を求める要求が発行されます。
4. REJECT：ユーザは認証されず、ユーザ名とパスワードの再入力を求められるか、アクセスを拒否されます。

ACCEPT 応答または REJECT 応答には、EXEC 許可またはネットワーク許可に使用される追加データが含まれています。RADIUS 認可を使用するには、まず RADIUS 認証を完了する必要があります。ACCEPT または REJECT パケットに含まれる追加データの内容は次のとおりです。

- ユーザがアクセスできるサービス。Telnet、rlogin、またはローカル エリア トランスポート（LAT）などの接続や、PPP、Serial Line Internet Protocol（SLIP）、または EXEC サービスなどのサービスを含む。
- ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ。

RADIUS 属性

ネットワーク アクセス サーバは、各ユーザ プロファイルで RADIUS 属性で定義されている RADIUS 認可機能およびアカウンティング機能をモニタします。

ベンダー独自の RADIUS 属性

RADIUS の Internet Engineering Task Force（IETF）標準規格には、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー独自の情報を伝達する際の方式が規定されています。さらに、一部のベンダーが固有の方法で RADIUS 属性を拡張しています。Cisco ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

RADIUS トンネル属性

RADIUS は、元は Livingston, Inc. が開発したセキュリティ サーバの AAA プロトコルです。RADIUS は属性値（AV）ペアを使用して、セキュリティ サーバとネットワーク アクセス サーバの間で通信します。

RFC 2138 と RFC 2139 では、RADIUS の基本機能と、AAA 情報の送信に使用される IETF 標準規格の AV ペアの初期セットについて説明しています。「RADIUS Attributes for Tunnel Protocol Support」および「RADIUS Accounting Modifications for Tunnel Protocol Support」という 2 つの IETF 標準規格は、VPN 固有の属性を含むように IETF が定義した AV ペア セットを拡張します。これらの属性は、RADIUS サーバとトンネルイニシエータの間でトンネリング情報を伝送するために使用されます。

RFC 2865 と RFC 2868 は IETF が定義した AV ペア セットを拡張して、VPN の強制トンネリングに固有の属性を追加しています。この属性を使用して、ユーザはネットワーク アクセス サーバおよび RADIUS サーバの認証名を指定できます。

シスコ デバイスとアクセス サーバでは、新しい RADIUS IETF 標準規格の仮想プライベート ダイヤルアップ ネットワーク（VPDN）トンネル属性がサポートされています。

RADIUS サーバ上の事前認証

RADIUS 属性は、事前認証の動作を指定するために RADIUS 事前認証プロファイルで設定されています。シスコ デバイスで事前認証を設定するだけでなく、RADIUS サーバでも事前認証プロファイルを設定する必要があります。

DNIS または CLID 事前認証のための RADIUS プロファイル

RADIUS 事前認証プロファイルを設定するには、着信番号識別サービス（DNIS）または発信側回線 ID（CLID）の番号をユーザ名として使用し、**dnis** または **clid** コマンドで定義されたパスワードをパスワードとして使用します。

（注） 事前認証プロファイルのサービス タイプは常に「outbound」になります。これは、パスワードがネットワーク アクセス サーバ（NAS）で事前定義されているためです。この方法で事前認証プロファイルを設定することで、DNIS 番号、CLID 番号、またはコール タイプのユーザ名と、わかりやすいパスワードを使用してユーザが NAS にログインする操作を回避できます。「outbound」サービス タイプは、RADIUS サーバに送信される Access-Request パケットにも含まれます。

コール タイプの事前認証のための RADIUS プロファイル

RADIUS 事前認証プロファイルを設定するには、コール タイプ文字列をユーザ名として使用し、**ctype** コマンドで定義したパスワードをパスワードとして使用します。以下の表に、事前認証プロファイルで使用できるコール タイプ文字列の一覧を示します。

表 *1*：事前認証で使用されるコール タイプ文字列

コールタイプストリング	ISDN ベアラ機能
digital	無制限のデジタル、制限付きのデジタル。
speech	音声、3.1 kHz オーディオ、7 kHz オーディオ。 （注） これは個別線信号方式（CAS）で使用できる唯一のコール タイプです。
v.110	V.110 ユーザ情報レイヤがある任意のコール。
v.120	V.120 ユーザ情報レイヤがある任意のコール。

（注） 事前認証プロファイルのサービス タイプは必ず「outbound」になります。これは、パスワードがNASで事前定義されているためです。この方法で事前認証プロファイルを設定することで、DNIS 番号、CLID 番号、またはコール タイプのユーザ名と、わかりやすいパスワードを使用してユーザが NAS にログインする操作を回避できます。「outbound」サービス タイプは、RADIUS サーバに送信された Access-Request パケットにも含まれます。また、RADIUS サーバがチェックインアイテムをサポートする場合、チェックインアイテムにする必要があります。

コールバック用の事前認証の機能拡張のための RADIUS プロファイル

在宅勤務者などのリモート ネットワーク ユーザは、コールバックを使用すると課金を受けずに NAS にダイヤルインできます。コールバックが必要な場合、NAS は現在の通話を終了し、呼び出し元にダイヤルします。NASがコールバックを実行する場合は、発信接続の情報だけが適用されます。事前認証 access-accept メッセージからの残りの属性は廃棄されます。

（注） RADIUS サーバからのコールバックに宛先の IP アドレスは必要ありません。

次に、コールバック番号が 555-0101 でサービス タイプが outbound に設定された RADIUS プロファイル設定の例を示します。cisco-avpair = “preauth:send-name=<string>” では文字列 “user1” を使用し、cisco-avpair = “preauth:send-secret=<string>” ではパスワード “cisco” を使用します。

```
5550101 password = “cisco”, Service-Type = Outbound
Service-Type = Callback-Framed
Framed-Protocol = PPP,
Dialback-No = “5550119”
Class = “ISP12”
cisco-avpair = “preauth:send-name=user1”
cisco-avpair = “preauth:send-secret=cisco”
```

大規模なダイヤルアウトに使用するリモート ホスト名の RADIUS プロファイル

次の例では、正しい電話番号をコールして誤ったデバイスにアクセスするアクシデントを防ぐために、大規模なダイヤルアウトで使用するリモート デバイスの名前を指定しています。

```
5550101 password = "PASSWORD1", Service-Type = Outbound
       Service-Type = Callback-Framed
       Framed-Protocol = PPP,
       Dialback-No = "5550190"
       Class = "ISP12"
       cisco-avpair = "preauth:send-name=user1"
       cisco-avpair = "preauth:send-secret=PASSWORD1"
       cisco-avpair = "preauth:remote-name=Device2"
```

モデム管理用の RADIUS プロファイル

DNIS、CLID、またはコール タイプの事前認証を使用する場合、NAS の RADIUS サーバからの肯定応答には、ベンダー固有属性（VSA）26 を介して、モデム管理用のモデム文字列を含めることができます。モデム管理 VSA の構文は次のとおりです。

```
cisco-avpair = "preauth:modem-service=modem min-speed <
x
> max-speed <
y
>
modulation <
z
> error-correction <
a
> compression <
b
>"
```

以下の表に、VSA 内のモデム管理文字列要素の一覧を示します。

表 *2:* モデム管理文字列

コマンド	引数
min-speed	300 ～ 56000、any
max-speed	300 ～ 56000、any
modulation	K56Flex、v22bis、v32bis、v34、v90、any
error-correction	lapm、mnp4
compression	mnp5、v42bis

VSA の形式で RADIUS サーバからモデム管理文字列を受信すると、その情報は Cisco ソフトウェアに渡され、コールごとに適用されます。Modem ISDN Channel Aggregation（MICA）モデムには、コール設定時にメッセージを送信できるコントロール チャネルがあります。そのため、このモデム管理機能をサポートするのは、MICA モデムだけです。この機能は Microcom モデムではサポートされません。

後続の認証のための RADIUS プロファイル

事前認証に成功すると、事前認証プロファイルのベンダー独自の RADIUS 属性 201（Require-Auth）を使用して、後続の認証を実行するかどうかを決定できます。access-accept メッセージで返される属性 201 の値が 0 の場合、後続の認証は実行されません。属性 201 の値が 1 の場合、後続の認証は通常どおり実行されます。

属性 201 の構文は次のとおりです。

```
cisco-avpair = "preauth:auth-required=<
n
>"
```

ここで、<*n*> は、属性 201と同じ値の範囲です（つまり、0 または 1）。

事前認証プロファイルに属性 201 が含まれない場合、値 1 と仮定され、後続の認証が実行されます。

（注） 後続の認証を実行する前に、事前認証プロファイルに加えて、通常のユーザプロファイルを設定する必要があります。

後続の認証タイプのための RADIUS プロファイル

事前認証プロファイルに後続の認証を指定した場合、後続の認証に使用する認証タイプも指定する必要があります。後続の認証で使用できる認証タイプを指定するには、次の VSA を使用します。

```
cisco-avpair = "preauth:auth-type=<
string
>"
```

以下の表に、<*string*> 要素で使用できる値の一覧を示します。

表 *3* : *<string>* 要素の値

文字列	説明
chap	PPP 認証の Challenge Handshake Authentication Protocol（CHAP）のユーザ名とパスワードが必要です。
ms-chap	PPP 認証の MS-CHAP のユーザ名とパスワードが必要です。
pap	PPP 認証の Password Authentication Protocol（PAP）のユーザ名とパスワードが必要です。

複数の認証タイプを許可するように指定するには、事前認証プロファイルでこの VSA の複数インスタンスを設定できます。事前認証プロファイルに指定する認証タイプ VSA の順序は、PPP ネゴシエーションに使用する認証タイプの順序にもなるため、重要です。

この VSA はユーザ別の属性であり、**ppp authentication** インターフェイス コンフィギュレーション コマンドで指定された認証タイプ リストを置き換えます。

（注） これは後続の認証用の認証タイプを指定する VSA なので、後続の認証が必要な場合にだけ使用してください。

ユーザ名を含めるための RADIUS プロファイル

コールの認証に事前認証のみを使用する場合、発信するときに NAS がユーザ名を見つけられない可能性があります。RADIUS は、NAS が RADIUS 属性 1（User-Name）または Access-Accept

パケットで返されるVSAを介して使用するユーザ名を提供できます。ユーザ名を指定するVSAの構文は次のとおりです。

```
cisco-avpair = “preauth:username=<
string
>”
```

ユーザ名を指定しない場合、DNIS 番号、CLID 番号、またはコール タイプが使用されます。これは、設定した最後の事前認証コマンドによって変わります（たとえば、**clid** が最後に設定された事前認証コマンドの場合、CLID 番号がユーザ名として使用されます）。

後続の認証を使用してコールを認証する場合、2 つのユーザ名が存在する可能性があります。RADIUSから提供されたユーザ名と、ユーザが指定したユーザ名です。この場合、ユーザが指定したユーザ名は、RADIUS事前認証プロファイルに含まれているユーザ名を上書きします。ユーザが指定したユーザ名は、認証およびアカウンティングの両方に使用されます。

双方向認証のための RADIUS プロファイル

双方向認証の場合、発信側のネットワーク デバイスは NAS を認証する必要があります。PAP のユーザ名とパスワードや CHAP のユーザ名とパスワードを NAS 上でローカルに設定する必要はありません。代わりに、事前認証の Access-Accept メッセージにユーザ名とパスワードを含めることができます。

（注） **radius** コマンドを使用する場合、**ppp authentication** コマンドは設定しないでください。

PAP をセットアップする場合、インターフェイスで **ppp pap sent-name password** コマンドは設定しないでください。VSA「preauth:send-name」および「preauth:send-secret」は、アウトバウンド認証の PAP ユーザ名と PAP パスワードとして使用されます。

CHAP の場合、「preauth:send-name」はアウトバウンド認証だけでなく、インバウンド認証にも使用されます。CHAP インバウンドの場合、NAS は、発信側のネットワーク デバイスに対するチャレンジ パケットで「preauth:send-name」に定義されている名前を使用します。CHAP アウトバウンドの場合、「preauth:send-name」と「preauth:send-secret」の両方が応答パケットで使用されます。

次に、双方向認証を指定する設定の例を示します。

```
5550101 password = "PASSWORD2", Service-Type = Outbound
Service-Type = Framed-User
cisco-avpair = "preauth:auth-required=1"
cisco-avpair = "preauth:auth-type=pap"
cisco-avpair = "preauth:send-name=user1"
cisco-avpair = "preauth:send-secret=PASSWORD2"
class = "<some class>"
```

（注） リソース プーリングをイネーブルにする場合、双方向認証は機能しません。

認可をサポートするための RADIUS プロファイル

事前認証のみが設定されている場合、後続の認証はバイパスされます。ユーザ名とパスワードを使用できないため、認可もバイパスされます。ただし、事前認証プロファイルにauthorization属性を含めてユーザ別の属性を適用することで、認可のために後でRADIUSに処理を戻す必要がなくなります。認可プロセスを開始するには、NAS で **aaa authorization network** コマンドも設定する必要があります。

事前認証プロファイルに authorization 属性を設定できますが、service-type 属性（属性 6）という 1 つの例外があります。service-type 属性は、事前認証プロファイルで VSA に変換する必要があります。この VSA の構文は次のとおりです。

```
cisco-avpair = "preauth:service-type=<
n
>"
```

ここで、<*n*> は、属性 6 に関する標準の RFC 2865 値の 1 つです。

（注） 後続の認証が必要な場合、事前認証プロファイルの authorization 属性は適用されません。

RADIUS 認証

RADIUS サーバを指定し、RADIUS 認証キーを定義した後は、RADIUS 認証の方式リストを定義する必要があります。AAA によって RADIUS 認証が容易になるため、**aaa authentication** コマンドを入力し、認証方式として RADIUS を指定する必要があります。

RADIUS 許可

AAA 認可を使用すると、ユーザのアクセスをそのネットワークに制限するパラメータを設定できます。RADIUS を使用する認可は、1 回限りの認可や各サービスに対する認可、各ユーザに対するアカウント リストおよびプロファイル、ユーザ グループのサポート、IP、IPX、AppleTalk Remote Access（ARA）、および Telnet のサポートなど、リモート アクセスをコントロールするための方法を提供します。AAA によって RADIUS 認可は容易になるため、認可方式として RADIUS を指定して、**aaa authorization** コマンドを入力する必要があります。

RADIUS アカウンティング

AAA アカウンティング機能を使用すると、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。AAA によって RADIUS アカウンティングは容易になるため、アカウンティング方式として RADIUS を指定して、**aaa accounting** コマンドを入力する必要があります。

RADIUS Login-IP-Host

ネットワーク アクセス サーバ（NAS）が、ダイヤルイン ユーザに対する接続を試行するときに複数のログイン ホストを試行できるようにするため、RADIUS サーバのユーザ プロファイルに 3 つの Login-IP-Host エントリを入力できます。次に、ユーザ *user1* 用に 3 つの Login-IP-Host インスタンスを設定し、接続に TCP-Clear を使用する例を示します。

```
user1 Password = xyz
        Service-Type = Login,
        Login-Service = TCP-Clear,
        Login-IP-Host = 10.0.0.0,
        Login-IP-Host = 10.2.2.2,
        Login-IP-Host = 10.255.255.255,
        Login-TCP-Port = 23
```

ホストの入力順は、試行される順序になります。**ip tcp synwait-time** コマンドを使用して、NAS がリストの次のホストに対して接続を試行するまでに待機する秒数を設定します。デフォルトは 30 秒です。

使用している RADIUS サーバが 4 つ以上の Login-IP-Host エントリを許可していても、NAS が Access-Accept パケットでサポートするのは 3 つのホストだけです。

RADIUS Prompt

Access-Challenge パケットに対するユーザの応答を画面にエコーするかどうかを制御するには、RADIUS サーバのユーザ プロファイルで Prompt 属性を設定します。この属性は、Access-Challenge パケットにだけ含まれます。次に、No-Echo に設定された Prompt 属性の例を示します。この設定で、ユーザの応答はエコーされません。

```
user1 Password = xyz
Service-Type = Login,
Login-Service = Telnet,
Prompt = No-Echo,
Login-IP-Host = 172.31.255.255
```

ユーザの応答をエコーするには、この属性を Echo に設定します。Prompt 属性をユーザ プロファイルに含めない場合、デフォルトで応答はエコーされま。

この属性は、アクセス サーバに設定されている **radius-server challenge-noecho** コマンドの動作よりも優先されます。たとえば、アクセス サーバがエコーを表示しないように設定され、個人のユーザ プロファイルではエコーを許可している場合、ユーザ応答はエコーされます。

（注） Prompt 属性を使用する場合、Access-Challenge パケットをサポートするように RADIUS サーバを設定する必要があります。

ベンダー固有の RADIUS 属性

IETF 標準規格では、ネットワーク アクセス サーバと RADIUS サーバの間で、ベンダー固有属性（属性 26）を使用してベンダー固有の情報を伝達する方法を指定しています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 で、サポートされるオプションはベンダー タイプ 1、名前は「cisco-avpair」です。この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

「protocol」は、特定の認可タイプに対するシスコの「protocol」属性の値です。使用可能なプロトコルには、IP、Internetwork Packet Exchange（IPX）、VPDN、VoIP、セキュア シェル（SSH）、Resource Reservation Protocol（RSVP）、シリアル インターフェイス プロセッサ（SIP）、AirNet、およびアウトバウンドなどがあります。「attribute」と「value」は、Cisco TACACS+ 仕様で定義されている適切な AV ペアで、「sep」は、必須属性では「=」、省略可能な属性では「*」です。この設定により、TACACS+ 認可で使用できる機能一式を RADIUS でも使用できるようになります。

たとえば、次の AV ペアにより、シスコの「複数の名前付き IP アドレス プール」機能が、IP 認可中（PPP のインターネット プロトコル制御プロトコル（IPCP）アドレスの割り当て中）に有効化されます。

```
cisco-avpair= ”ip:addr-pool=first“
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」は省略可能になります。任意の AV ペアを省略可能にすることができます。

```
cisco-avpair= ”ip:addr-pool*first“
```

次に、ネットワーク アクセス サーバからユーザがログインしたときに、すぐに EXEC コマンドを実行する方法の例を示します。

```
cisco-avpair= ”shell:priv-lvl=15“
```

他のベンダーには、そのベンダー固有の ID、オプション、関連 VSA があります。

RADIUS サーバのスタティック ルートと IP アドレス

RADIUS のベンダー固有実装の一部では、ネットワーク内にある個々のネットワーク アクセス サーバの代わりに、ユーザが RADIUS サーバのスタティック ルートおよび IP プールを定義できます。各ネットワーク アクセス サーバは、スタティック ルートと IP プール情報について RADIUS サーバに照会します。

シスコ デバイスが起動したときに、そのデバイスまたはアクセス サーバがスタティック ルートと IP プール定義を RADIUS サーバに照会するには、**radius-server configure-nas** コマンドを使用します。

radius-server configure-nas コマンドは、シスコ デバイスの起動時に実行されるため、**copy system:running-config nvram:startup-config** コマンドを入力するまで有効になりません。

RADIUS の設定方法

ベンダー独自の RADIUS サーバとの通信に関するデバイス設定

IETF の RADIUS 標準規格では、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー独自の情報を受け渡す方法を指定していますが、一部のベンダーはRADIUS属性セットを独自の方法で拡張しています。Cisco ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

RADIUS を設定するには（ベンダー独自または IETF 準拠のいずれの場合も）、**radius-server** コマンドを使用して、RADIUS サーバデーモンを実行しているホストと、そのホストがシスコデバイスと共有する秘密テキスト文字列を指定する必要があります。RADIUS サーバがRADIUS のベンダー独自実装を使用していることを示すには、 **radius-server host non-standard** コマンドを使用します。**radius-server host non-standard** コマンドを使用しないと、ベンダー独自の属性はサポートされません。

（注） **radius-server host** コマンドは、Cisco IOS リリース 15.4(2)S 以降では廃止されています。IPv4 または IPv6 RADIUS サーバを設定するには、**radius server** *name* コマンドを使用します。 **radius server** コマンドの詳細については、『*Cisco IOS Security Command Reference: Commands M to R*』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **radius server** *server-name*
5. **address ipv4** *ip-address*
6. **non-standard**
7. **key** {**0** *string* | **7** *string* | *string*}
8. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**radius-server vsa send** [**accounting** | **authentication**] 例： `Device(config)# radius-server vsa send`	RADIUS IETF 属性 26 の定義に従って、ネットワーク アクセス サーバが VSA を認識および使用できるようにします。
ステップ 4	**radius server** *server-name* 例： `Device(config)# radius server rad1`	RADIUS サーバの名前を指定します。 （注） **radius-server host** コマンドは、Cisco IOS リリース 15.4(2)S 以降では廃止されています。IPv4 または IPv6 RADIUS サーバを設定するには、**radius server** *name* コマンドを使用します。 **radius server** コマンドの詳細については、『*Cisco IOS Security Command Reference: Commands M to R*』を参照してください。
ステップ 5	**address ipv4** *ip-address* 例： `Device(config-radius-server)# address ipv4 10.45.1.2`	RADIUS サーバに IP アドレスを割り当てます。
ステップ 6	**non-standard** 例： `Device(config-radius-server)# non-standard`	セキュリティ サーバが RADIUS のベンダー独自の実装を使用していることを示します。
ステップ 7	**key** {**0** *string* | **7** *string* | *string*} 例： `Device(config-radius-server)# key myRaDIUSpassword`	デバイスとベンダー独自仕様の RADIUS サーバとの間で使用される共有秘密テキスト文字列を指定します。 • デバイスと RADIUS サーバはこのテキスト文字列を使用してパスワードを暗号化し、応答を交換します。
ステップ 8	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

ネットワーク アクセス サーバのポート情報を拡張するためのデバイス設定

コール自体が着信したインターフェイスとは別のインターフェイスでPPP認証またはログイン認証が発生する場合があります。たとえば、V.120 ISDN コールでは、ログイン認証またはPPP認証は仮想非同期インターフェイス「ttt」で発生しますが、コール自体は ISDN インターフェイスのチャネルの 1 つで発生します。

radius-server attribute nas-port extended コマンドは、RADIUS を設定して NAS-Port 属性（RADIUS IETF 属性 5）フィールドのサイズを 32 ビットに拡張します。NAS-Port 属性の上位16ビットは、制御インターフェイスの種類と番号を示します。下位16ビットは、インターフェイスで実行中の認証を示します。

（注） **radius-server attribute nas-port format** コマンドは、**radius-server extended-portnames** コマンドおよび **radius-server attribute nas-port extended** コマンドの代わりに使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server configure-nas**
4. **radius-server attribute nas-port format**
5. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**radius-server configure-nas** 例： `Device(config)# radius-server configure-nas`	（任意）シスコデバイスまたはアクセスサーバが、そのドメイン内で使用するスタティックルートとIPプール定義についてRADIUSサーバに照会するように指定します。

	コマンドまたはアクション	目的
		（注） **radius-server configure-nas** コマンドは、シスコデバイスの起動時に使用されるため、**copy system:running-config nvram:startup-config** コマンドを発行するまで有効になりません。
ステップ 4	**radius-server attribute nas-port format** 例： `Device(config)# radius-server attribute nas-port format`	NAS-Port 属性のサイズを 16 ビットから 32 ビットに拡張して、拡張インターフェイス情報を表示できるようにします。
ステップ 5	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

NAS-Port 属性の RADIUS 属性への置き換え

各スロットに複数のインターフェイス（ポート）があるプラットフォームの場合、シスコの RADIUS 実装では、インターフェイスを区別できる固有の NAS-Port 属性を提供しません。たとえば、スロット 1 にデュアル PRI がある場合、RADIUS IETF NAS-Port 属性に関連付けられた 16 ビット フィールド サイズ制限により、Serial1/0:1 と Serial1/1:1 の両方でのコールが NAS-Port = 20101 として表示されます。この場合、NAS-Port 属性を VSA（RADIUS IETF 属性 26）に置き換えることができます。シスコのベンダー ID は 9 で、Cisco-NAS-Port 属性はサブタイプ 2 です。VSA を有効にするには、**radius-server vsa send** コマンドを入力します。ベンダー固有属性のポート情報を提供および設定するには、**aaa nas port extended** コマンドを使用します。

標準の NAS-Port 属性（RADIUS IETF 属性 5）が送信されます。この情報を送信しない場合、**no radius-server attribute nas-port** コマンドを使用して停止できます。このコマンドを設定すると、標準の NAS-Port 属性は送信されなくなります。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
4. **aaa nas port extended**
5. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**radius-server vsa send** [**accounting** | **authentication**] 例： `Device(config)# radius-server vsa send`	RADIUS IETF 属性 26 の定義に従って、ネットワーク アクセス サーバがベンダー固有属性を認識および使用できるようにします。
ステップ 4	**aaa nas port extended** 例： `Device(config)# aaa nas port extended`	VSA NAS-Port フィールドのサイズを 16 ビットから 32 ビットに拡張して、拡張インターフェイス情報を表示できるようにします。
ステップ 5	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

RADIUS のモニタリングとメンテナンス

手順の概要

1. **enable**
2. **debug radius**
3. **show radius statistics**
4. **show aaa servers**
5. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**debug radius** 例： `Device# debug radius`	RADIUS 関連の情報を表示します。
ステップ 3	**show radius statistics** 例： `Device# show radius statistics`	アカウンティング パケットと認証パケットについての RADIUS 統計情報を示します。
ステップ 4	**show aaa servers** 例： `Device# show aaa servers`	AAA サーバ MIB によって解釈される、すべてのパブリックおよびプライベート AAA RADIUS サーバとの間で送受信されるパケットのステータスと数を表示します。
ステップ 5	**exit** 例： `Device# exit`	デバイス セッションを終了します。

RADIUS の設定例

例：RADIUS の認証と認可

次に、RADIUS を使用して認証および認可を行うようにデバイスを設定する例を示します。

```
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
```

この RADIUS 認証および認可設定のサンプル行は、次のように定義されます。

- **aaa authentication login use-radius group radius local** コマンドを実行すると、デバイスは、ログイン プロンプトで認証に RADIUS を使用するように設定されます。RADIUS がエラーを返すと、ユーザはローカル データベースを使用して認証されます。この例では、**use-radius** は方式リストの名前であり、RADIUS を指定し、次にローカル認証を指定します。
- **aaa authentication ppp user-radius if-needed group radius** コマンドで、ユーザがまだ認可されていない場合に、CHAP または PAP による PPP を使用する回線に RADIUS 認証を使用するように Cisco ソフトウェアを設定します。EXEC ファシリティによってユーザが認証済みの場合、RADIUS 認証は実行されません。この例では、**user-radius** は、if-needed 認証方式として RADIUS を定義する方式リストの名前です。

- **aaa authorization exec default group radius** コマンドで、EXEC 認可、autocommand、およびアクセス リストに使用する RADIUS 情報を設定します。
- **aaa authorization network default group radius** コマンドを実行すると、ネットワーク認可、アドレス割り当て、アクセス リストに RADIUS が設定されます。

例：RADIUS 認証、許可、アカウンティング

次に、AAA コマンドを設定して RADIUS を使用する一般的な設定例を示します。

```
radius-server host 10.45.1.2
radius-server key myRaDiUSpassWoRd
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem ri-is-cd
interface group-async 1
 encaps ppp
 ppp authentication pap dialins
```

この例の RADIUS 認証、許可、アカウンティングの回線は、次のように定義されます。

- **radius-server host** コマンドは、RADIUS サーバ ホストの IP アドレスを定義します。
- **radius-server key** コマンドは、ネットワーク アクセス サーバと RADIUS サーバ ホストの間の共有秘密テキスト文字列を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、まず RADIUS 認証を指定する認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線でローカル認証が使用されます。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワーク パラメータを RADIUS ユーザに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドは、PPP の使用状況を追跡します。
- **aaa authentication login admins local** コマンドは、ログイン認証に別の方式リスト「admins」を定義します。
- **login authentication admins** コマンドは、ログイン認証に「admins」方式リストを適用します。
- **ppp authentication pap dialins** コマンドは「dialins」方式リストを指定した回線に適用します。

例：ベンダー固有の RADIUS 設定

次に、AAA コマンドを設定してベンダー独自の RADIUS を使用する一般的な設定例を示します。

（注） **radius-server host** コマンドは、Cisco IOS リリース 15.4(2)S 以降では廃止されています。IPv4 または IPv6 RADIUS サーバを設定するには、**radius server** *name* コマンドを使用します。 **radius server** コマンドの詳細については、『*Cisco IOS Security Command Reference: Commands M to R*』を参照してください。

```
radius server myserver
radius server address ipv4 192.0.2.2
non-standard
key 7 any key
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
```

この RADIUS 認証、認可、アカウンティング設定例の行は、次のように定義されます。

- **non-standard** コマンドは、RADIUS サーバ ホストの名前を定義し、この RADIUS ホストがベンダー独自バージョンの RADIUS を使用することを指定します。
- **key** コマンドは、ネットワーク アクセス サーバと RADIUS サーバ ホストの間の共有秘密テキスト文字列を定義します。
- **configure-nas** コマンドは、シスコ デバイスが最初に起動したときに、そのデバイスまたはアクセス サーバがスタティック ルートと IP プール定義について RADIUS サーバに照会するように定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、まず RADIUS 認証を指定する認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線でローカル認証が使用されます。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワーク パラメータを RADIUS ユーザに割り当てます。
- **aaa accounting network default start-stop group radius** コマンドは、PPP の使用状況を追跡します。
- **aaa authentication login admins local** コマンドは、ログイン認証に別の方式リスト「admins」を定義します。

例：同じサーバ IP アドレスを持つ複数の RADIUS サーバ エントリ

次に、同じ IP アドレスを持つ複数の RADIUS ホスト エントリを認識するように、ネットワーク アクセス サーバを設定する例を示します。同じ RADIUS サーバ上にある 2 つのホスト エントリは、同じサービス（認証とアカウンティング）のために設定されています。設定されている 2 番めのホストエントリは、1 番めのエントリのフェールオーバー バックアップとして動作します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2001
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
AAA コマンドと RADIUS コマンド	『*Cisco IOS Security Command Reference*』
RADIUS 属性	『*RADIUS Attributes Configuration Guide*』（Securing User Services Configuration Library の一部）
AAA	『*Authentication, Authorization, and Accounting Configuration Guide*』（Securing User Services Configuration Library の一部）
L2TP、VPN、または VPDN	『*Dial Technologies Configuration Guide*』および『*VPDN Configuration Guide*』
モデムの設定と管理	『*Dial Technologies Configuration Guide*』
PPP の RADIUS ポートの識別	『*Wide-Area Networking Configuration Guide*』

RFC

RFC	タイトル
RFC 2138	『*Remote Authentication Dial In User Service (RADIUS)*』

RFC	タイトル
RFC 2139	『*RADIUS Accounting*』
RFC 2865	『*RADIUS*』
RFC 2867	『*RADIUS Accounting Modifications for Tunnel Protocol Support*』
RFC 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするため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

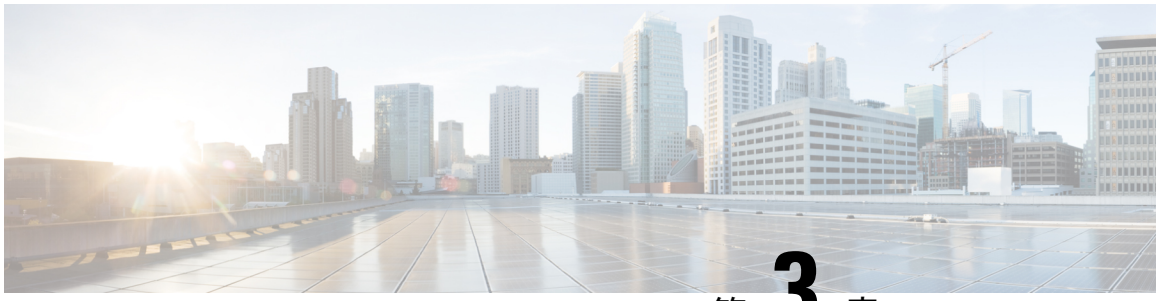
RADIUS の設定に関する機能情報

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 *4 : RADIUS* の設定に関する機能情報

機能名	リリース	機能情報
RADIUS の設定		RADIUS セキュリティ システムは、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。シスコの実装では、RADIUS クライアントはシスコ デバイス上で実行され、すべてのユーザ認証およびネットワーク サービス アクセス情報を持つ中央の RADIUS サーバに認証要求を送信します。
SNMP を介する RADIUS 統計情報		この機能は、RADIUS トラフィックおよびプライベート RADIUS サーバに関連する統計情報を提供します。 次のコマンドが導入または変更されました。**show aaa servers**、**show radius statistics**



第 3 章

複数の UDP ポート用の RADIUS

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。IP アドレスと UDP ポート番号を組み合わせることによって、異なるポートを特定の認証、認可、およびアカウンティング（AAA）サービスを提供する RADIUS ホストとして個別に定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証など）を設定した場合、2 番めに設定されたホストエントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エントリがアカウンティング サービスの提供に失敗すると、ネットワーク アクセス サーバは同じデバイスに設定されている 2 番めのホストエントリを使用してアカウンティング サービスを提供するように試行します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

複数の UDP ポート用の RADIUS の前提条件

シスコ デバイスまたはアクセス サーバで RADIUS を設定するには、次のタスクを実行する必要があります。

- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。RADIUS を使用する予定がある場合、AAA を設定する必要があります。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。

複数の UDP ポート用の RADIUS に関する情報

デバイスと RADIUS サーバの通信

通常、RADIUS ホストは、シスコ（CiscoSecure ACS）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアを実行するマルチユーザ システムです。RADIUS サーバとの通信のためにデバイスを設定するには、次のような要素があります。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- タイムアウト時間
- 再送信回数
- キー文字列

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証など）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エントリがアカウンティング サービスの提供に失敗すると、ネットワーク アクセス サーバは同じデバイスに設定されている 2 番めのホストエントリを使用してアカウンティ

ングサービスを提供するように試行します。（試行されるRADIUSホストエントリの順番は、設定されている順序に従います）。

RADIUSサーバとシスコデバイスは、共有秘密テキスト文字列を使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUSサーバデーモンが稼働するホストと、そのホストがデバイスと共有する秘密テキスト（キー）文字列を指定する必要があります。

タイムアウト値、再送信値、および暗号キー値には、すべてのRADIUSサーバを対象にしたグローバル設定、サーバ別設定、またはグローバル設定とサーバ別設定の組み合わせを使用できます。デバイスと通信するすべてのRADIUSサーバにこのような設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** という 3 つの固有なグローバル コマンドを使用します。特定の RADIUS サーバにこれらの値を適用するには、**radius-server host** コマンドをグローバル コンフィギュレーション モードで使用します。

（注） 同じシスコ製ネットワーク アクセス サーバで、タイムアウト、再送信、およびキー値のコマンドを同時に設定（グローバル設定およびサーバ別設定）できます。デバイスにグローバル機能とサーバ別機能の両方を設定する場合、サーバ別のタイマー、再送信、およびキー値のコマンドが、グローバルのタイマー、再送信、およびキー値のコマンドよりも優先されます。

複数の UDP ポート用の RADIUS を設定する方法

デバイスと RADIUS サーバの通信の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server-name*
4. **address ipv4** *ip-address*
5. **key** {**0** *string* | **7** *string* | *string*}
6. **retransmit** *retries*
7. **timeout** *seconds*
8. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**radius server** *server-name* 例： `Device(config)# radius server rad1`	RADIUS サーバの名前を指定します。
ステップ 4	**address ipv4** *ip-address* 例： `Device(config-radius-server)# address ipv4 10.45.1.2`	RADIUS サーバに IP アドレスを割り当てます。
ステップ 5	**key** {**0** *string* | **7** *string* | *string*} 例： `Device(config-radius-server)# key myRaDIUSpassword`	デバイスと RADIUS サーバの間で使用する共有秘密テキスト文字列を指定します。 （注） この手順では、暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定されます。 • **0** *string* オプションを使用して、暗号化されていない共有秘密を設定します。**7** *string* オプションを使用して、暗号化された共有秘密を設定します。
ステップ 6	**retransmit** *retries* 例： `Device(config-radius-server)# retransmit 25`	デバイスからサーバに対して各 RADIUS 要求を送信する回数の上限を指定します（デフォルトは 3 です）。 （注） この手順では、再送信の値は、すべての RADIUS サーバに対してグローバルに設定されます。
ステップ 7	**timeout** *seconds* 例： `Device(config-radius-server)# timeout 6`	デバイスが RADIUS 要求に対する応答を待機して、要求を再送信するまでの時間（秒数）を指定します。 （注） この手順では、タイムアウト値は、すべての RADIUS サーバに対してグローバルに設定されます。
ステップ 8	**exit** 例：	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
	`Device(config)# exit`	

複数の UDP ポート用の RADIUS の設定例

例：デバイスと RADIUS サーバの通信

次に、固有のタイムアウト、再送信、およびキー値を指定した2つのRADIUSサーバを設定する例を示します。この例では、**aaa new-model** コマンドを使用してデバイス上の AAA サービスを有効化し、特定の AAA コマンドで AAA サービスを定義します。**retransmit** コマンドで、すべてのRADIUSサーバについて、グローバル再送信値を4に変更します。**host** コマンドで、IP アドレスが 172.16.1.1 と 172.29.39.46 の RADIUS サーバ ホストについて、特定のタイムアウト、再送信、およびキーの値を設定します。

```
! Enable AAA services on the device and define those services.
aaa new-model
aaa authentication login default group radius
aaa authentication login console-login none
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
enable password tryit1
!
Device(config)# radius server rad1
Device(config-radius-server)# address ipv4 10.45.1.2
Device(config-radius-server)# key myRaDIUSpassword
Device(config-radius-server)# retransmit 25
Device(config-radius-server)# timeout 6
Device(config)# exit
```

例：サーバ固有の値を指定した RADIUS サーバ

次に、172.31.39.46 という IP アドレスの RADIUS サーバについて、サーバ固有のタイムアウト、再送信、およびキー値を設定する例を示します。

```
radius-server host 172.31.39.46 timeout 6 retransmit 5 key rad123
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	Cisco IOS Master Command List, All Releases

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
AAA	『*Authentication, Authorization, and Accounting Configuration Guide*』（Securing User Services Configuration Library の一部）

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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするため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

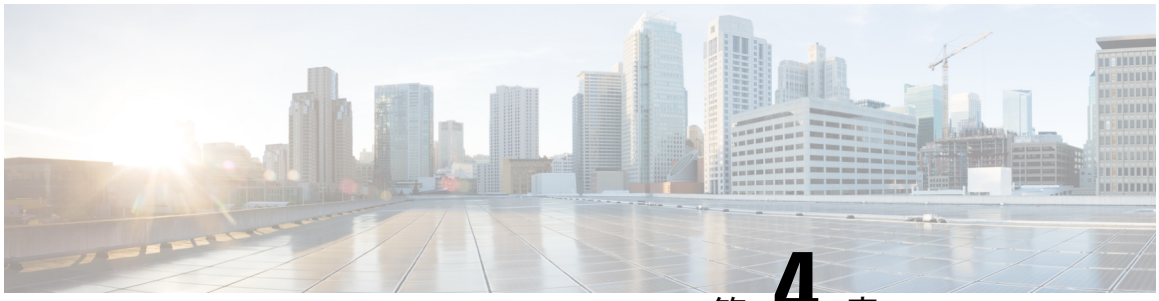
複数の UDP ポート用の RADIUS の機能情報

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 *5 :* 複数の *UDP* ポート用の *RADIUS* の機能情報

機能名	リリース	機能情報
複数の UDP ポート用の RADIUS		RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。 次のコマンドが導入または変更されました。**radius-server host**



第 4 章

許可用の AAA Dialed Number Information Service（DNIS）マップ

許可用の AAA DNIS マップ機能を使用すると、着信番号識別サービス（DNIS）番号を特定の認証、許可、およびアカウンティング（AAA）サーバグループに割り当てることができます。これによって、サーバグループは、そのDNISを使用して、ネットワークにダイヤルインするユーザの認証、許可、アカウンティングの要求を処理できます。すべての電話回線（通常の自宅電話または商用のT1/PRI回線）を、複数の電話番号と関連付けることができます。DNIS番号は、ユーザ宛てに発信された番号を示します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

許可用の AAA DNIS マップの前提条件

- サーバ グループの DNIS に基づいて特定の AAA サーバ グループを選択するようにデバイスを設定する前に、RADIUS サーバ ホストと AAA サーバ グループの一覧を設定する必要があります。
- AAA 事前認証を設定する前に、**aaa new-model** コマンドを設定して、サポートする事前認証アプリケーションが使用中のネットワークの RADIUS サーバで実行されていることを確認する必要があります。

許可用の AAA DNIS マップに関する情報

DNIS に基づく AAA サーバ グループの選択

Cisco ソフトウェアを使用すると、DNIS 番号を特定の AAA サーバ グループに割り当てることができます。これによって、サーバ グループは、その DNIS を使用して、ネットワークにダイヤルインするユーザの認証、認可、アカウンティングの要求を処理できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザ宛てに発信された番号を示します。

たとえば、複数の顧客で同じ電話番号を共有する場合に、電話を受ける前に発信元を知りたいことがあります。DNIS を使用すると、応答するときに発信元の顧客がわかるため、電話に応答する方法をカスタマイズできます。

ISDN または内部モデムと接続するシスコ デバイスは、DNIS 番号を受信できます。この機能を使用すると、顧客ごとに異なる RADIUS サーバ グループを割り当て可能です（つまり、DNIS 番号ごとに異なる RADIUS サーバ）。さらに、サーバ グループを使用して、複数の AAA サービスに同じサーバ グループを指定できます。また、各 AAA サービスに個別のサーバ グループを指定できます。

Cisco ソフトウェアには、認証サービスとアカウンティング サービスを複数の方法で実装できる柔軟性があります。

- グローバル：AAA サービスは、グローバル コンフィギュレーション アクセス リスト コマンドを使用して定義され、特定のネットワーク アクセス サーバ上のすべてのインターフェイスに、全般的に適用されます。
- インターフェイス別：AAA サービスは、インターフェイス コンフィギュレーション コマンドを使用して定義され、特定のネットワーク アクセス サーバに設定されているインターフェイスにだけ適用されます。
- DNIS マッピング：DNIS を使用して、AAA サーバが AAA サービスを提供するように指定します。

このような複数の AAA コンフィギュレーション方式を同時に設定できるため、シスコでは、AAA サービスを提供するサーバまたはサーバ グループを決定するために、優先順位を設定しました。優先順位は次のとおりです。

- DNIS 別：DNIS を使用し、AAA サービスを提供するサーバ グループを指定または決定するようにネットワーク アクセス サーバを設定している場合、この方式がその他の AAA 選択方式よりも優先されます。
- インターフェイス別：サーバから AAA サービスを提供する方法を決定するために、インターフェイス別にネットワーク アクセス サーバを設定してアクセス リストを使用する場合、この方式は、他のグローバル コンフィギュレーション AAA アクセス リストよりも優先されます。
- グローバル：セキュリティ サーバが AAA サービスを提供する方法を決定するために、グローバル AAA アクセス リストを使用してネットワーク アクセス サーバを設定する場合、この方式には最も低い優先度が使用されます。

AAA 事前認証

ISDN PRI または個別線信号方式（CAS）による AAA 事前認証を設定すると、サービス プロバイダーは、既存の RADIUS ソリューションを使用するポートの管理性を改善し、共有リソースの使用を効率的に管理して、各種のサービスレベル契約を提供できるようになります。ISDN PRI または CAS によって、着信コールに関する情報をネットワーク アクセス サーバ（NAS）で使用してから、コールを接続できます。使用できるコール情報は次のとおりです。

- 着信番号識別サービス（DNIS）番号（着信者番号とも呼ばれます）
- 発呼回線 ID（CLID）番号（発番号とも呼ばれます）
- コール タイプ（ベアラ機能とも呼ばれます）

AAA 事前認証の機能を使用すると、Cisco NAS で、DNIS 番号、CLID 番号、またはコール タイプに基づいて着信コールを接続するかどうかを決定することができます。（ISDN PRI を使用する場合、ユーザの認証と認可を行ってから、コールに応答できます。CAS を使用する場合、コールに応答する必要はありますが、事前認証に失敗した場合、コールをドロップできます）。

パブリック ネットワーク スイッチからコールを着信し、まだ接続前の場合、AAA 事前認証によって、NAS から DNIS 番号、CLID 番号、およびコール タイプを RADIUS サーバに送信し、認可を受けることができます。サーバがコールを認可すると、NAS はコールを許可します。サーバがコールを認可しない場合、NAS からパブリック ネットワーク スイッチに接続解除メッセージが送信され、コールが拒否されます。

RADIUS サーバ アプリケーションが使用不能になった場合、または応答が遅くなった場合、NAS でガード タイマーを設定できます。タイマーが期限切れになると、NAS は設定可能なパラメータを使用して、認可されなかった着信コールを許可または拒否します。

AAA 事前認証の機能では、事前認証の動作を指定するために、RADIUS サーバアプリケーションによる属性 44 の使用、および RADIUS 事前認証プロファイルに設定されている RADIUS 属

性の使用がサポートされています。また、これらの属性は、たとえば、以降の認証を実行するかどうか、また実行する場合、どの認証方式を使用するかを指定するためにも使用できます。

ISDN PRI および CAS による AAA 事前認証には、次の制約事項が適用されます。

- 属性 44 は、事前認証またはリソース プーリングをイネーブルにした CAS コールにだけ使用できます。
- マルチシャーシ マルチリンク PPP（MMP）は、ISDN PRI では使用できません。
- AAA 事前認証は、一部のハードウェア プラットフォームでのみ使用できます。
- ISDN PRI は、一部のハードウェア プラットフォームでのみサポートされています。

コール処理のガード タイマー

事前認証要求および認可要求の応答時間はさまざまなので、ガードタイマーを使用してコールの処理を制御できます。ガード タイマーは、DNIS が RADIUS サーバに送信されると開始されます。ガード タイマーが期限切れになる前に NAS が AAA から応答を受信しない場合、タイマーの設定に基づいてコールを許可または拒否します。

許可用の AAA DNIS マップの設定方法

AAA DNIS 事前認証の設定

DNIS 事前認証を使用すると、着信番号に基づいてコール設定時に事前認証を実行できます。DNIS 番号は、コールの着信時にセキュリティ サーバに直接送信されます。コールが AAA によって認証されると、そのコールは許可されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** {**radius** | **tacacs+** | *server-group*}
5. **dnis** [**password** *string*]
6. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**aaa preauthorization** 例： `Device(config)# aaa preauthorization`	AAA 事前認証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	**group** {**radius** | **tacacs+** | *server-group*} 例： `Device(config-preauth)# group radius`	（任意）AAA 事前認証要求に使用するセキュリティ サーバを選択します。 • デフォルトは RADIUS です。
ステップ 5	**dnis** [**password** *string*] 例： `Device(config-preauth)# dnis password dnispass`	DNIS を使用して事前認証をイネーブルにし、必要に応じて Access-Request パケットに使用するパスワードを指定します。
ステップ 6	**end** 例： `Device(config-preauth)# end`	AAA 事前認証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。

DNIS に基づく AAA サーバ グループの選択の設定

サーバ グループの DNIS に基づいて特定の AAA サーバ グループを選択するようにデバイスを設定するには、DNIS マッピングを設定します。DNIS 番号を使用してサーバ グループをグループ名とマッピングするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa dnis map enable**
4. **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*
5. **aaa dnis map** *dnis-number* **authorization network group** *server-group-name*
6. **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*
7. **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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**aaa dnis map enable** 例： `Device(config)# aaa dnis map enable`	DNIS マッピングをイネーブルにします。
ステップ 4	**aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name* 例： `Device(config)# aaa dnis map 7777 authentication ppp group sg1`	DNIS 番号を定義済みの AAA サーバ グループにマッピングします。このサーバ グループのサーバは、認証に使用されます。
ステップ 5	**aaa dnis map** *dnis-number* **authorization network group** *server-group-name* 例： `Device(config)# aaa dnis map 7777 authorization network group sg1`	DNIS 番号を定義済みの AAA サーバ グループにマッピングします。このサーバ グループのサーバは、認可に使用されます。
ステップ 6	**aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name* 例： `Device(config)# aaa dnis map 8888 accounting network stop-only group sg2`	DNIS 番号を定義済みの AAA サーバ グループにマッピングします。このサーバ グループのサーバは、アカウンティングに使用されます。
ステップ 7	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

AAA 事前認証の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa preauthorization**
4. **group** *server-group*
5. **clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
6. **ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
7. **dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]
8. **dnis bypass** *dnis-group-name*
9. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**aaa preauthorization** 例： `Device(config)# aaa preauthorization`	AAA 事前認証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	**group** *server-group* 例： `Device(config-preauth)# group sg2`	事前認証に使用する AAA RADIUS サーバ グループを指定します。
ステップ 5	**clid** [**if-avail**	**required**] [**accept-stop**] [**password** *string*] 例： `Device(config-preauth)# clid required`	CLID 番号に基づいて、コールを事前認証します。
ステップ 6	**ctype** [**if-avail**	**required**] [**accept-stop**] [**password** *string*] 例：	コール タイプに基づいて、コールを事前認証します。

	コマンドまたはアクション	目的
	`Device(config-preauth)# ctype required`	
ステップ 7	**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] 例： `Device(config-preauth)# dnis required`	DNIS 番号に基づいて、コールを事前認証します。
ステップ 8	**dnis bypass** *dnis-group-name* 例： `Device(config-preauth)# dnis bypass group1`	事前認証をバイパスする DNIS 番号のグループを指定します。
ステップ 9	**end** 例： `Device(config-preauth)# end`	事前認証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。

ガード タイマーの設定

RADIUS サーバが認証要求または事前認証要求に応答できなかった場合にコールを許可または拒否するようにガード タイマーを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
5. **call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
6. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* 例： `Device(config)# interface serial 1/0/0:23`	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	**isdn guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] 例： `Device(config-if)# isdn guard-timer 8000 on-expiry reject`	RADIUS サーバが事前認証要求に応答できなかった場合にコールを許可または拒否できる ISDN ガードタイマーを設定します。
ステップ 5	**call guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] 例： `Device(config-if)# call guard-timer 2000 on-expiry accept`	RADIUS サーバが事前認証要求に応答できなかった場合にコールを許可または拒否できる CAS ガードタイマーを設定します。
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。

許可用の AAA DNIS マップの設定例

例：DNIS に基づく AAA サーバ グループの選択

次に、特定の AAA サービスを提供するために、DNIS に基づいて RADIUS サーバ グループを選択する例を示します。

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the RADIUS attributes for each server
! that will be associated with one of the defined server groups.
radius-server host 172.16.0.1 auth-port 1645 acct-port 1646 key cisco1
radius-server host 172.17.0.1 auth-port 1645 acct-port 1646 key cisco2
radius-server host 172.18.0.1 auth-port 1645 acct-port 1646 key cisco3
radius-server host 172.19.0.1 auth-port 1645 acct-port 1646 key cisco4
radius-server host 172.20.0.1 auth-port 1645 acct-port 1646 key cisco5
! The following commands define the sg1 RADIUS server group and associate servers
! with it.
aaa group server radius sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 RADIUS server group and associate a server
```

```
! with it.
aaa group server radius sg2
  server 172.18.0.1
! The following commands define the sg3 RADIUS server group and associate a server
! with it.
aaa group server radius sg3
  server 172.19.0.1
! The following commands define the default-group RADIUS server group and associate
! a server with it.
aaa group server radius default-group
  server 172.20.0.1
! The next set of commands configures default-group RADIUS server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using
! DNIS 7777 are sent to the sg1 server group. The accounting records for these
! connections (specifically, start-stop records) are handled by the sg2 server group.
! Calls with a DNIS of 8888 use server group sg3 for authentication and server group
! default-group for accounting. Calls with a DNIS of 9999 use server group
! default-group for authentication and server group sg3 for accounting records
! (stop records only). All other calls with DNIS other than the ones defined use the
! server group default-group for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

例：AAA 事前認証

次に、事前認証に DNIS 番号を指定する単純な設定を示します。

```
aaa preauthentication
 group radius
 dnis required
```

次に、事前認証に DNIS 番号と CLID 番号の両方を使用する設定の例を示します。DNIS 事前認証が先に実行され、次に CLID 事前認証が実行されます。

```
aaa preauthentication
 group radius
 dnis required
 clid required
```

次に、「dnis-group1」という DNIS グループに指定されている 2 つの DNIS 番号を除き、すべての DNIS 番号について事前認証を実行することを指定する例を示します。

```
aaa preauthentication
 group radius
 dnis required
 dnis bypass dnis-group1
dialer dnis group dnis-group1
 number 12345
 number 12346
```

次に、DNIS 事前認証を使用する AAA 設定の例を示します。

```
aaa new-model
aaa authentication login CONSOLE none
aaa authentication login RADIUS_LIST group radius
aaa authentication login TAC_PLUS group tacacs+ enable
aaa authentication login V.120 none
aaa authentication enable default enable group tacacs+
aaa authentication ppp RADIUS_LIST if-needed group radius
aaa authorization exec RADIUS_LIST group radius if-authenticated
aaa authorization exec V.120 none
aaa authorization network default group radius if-authenticated
aaa authorization network RADIUS_LIST if-authenticated group radius
aaa authorization network V.120 group radius if-authenticated
aaa accounting suppress null-username
aaa accounting exec default start-stop group radius
aaa accounting commands 0 default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting connection default start-stop group radius
aaa accounting system default start-stop group radius
aaa preauthentication
 dnis password Cisco-DNIS
aaa nas port extended
!
radius-server configure-nas
radius-server host 10.0.0.0 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.255.255.255 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 2
radius-server deadtime 1
radius-server attribute nas-port format c
radius-server unique-ident 18
radius-server key MyKey
```

（注） 事前認証を設定するには、RADIUS サーバでも事前認証プロファイルを設定する必要があります。

例：ISDN および CAS のガード タイマー

次に、8,000 ミリ秒に設定された ISDN ガード タイマーの例を示します。事前認証要求に対して RADIUS サーバが応答しないまま、タイマーが期限切れになった場合、コールは拒否されます。

```
interface serial 1/0/0:23
 isdn guard-timer 8000 on-expiry reject
aaa preauthentication
 group radius
 dnis required
```

次に、20,000 ミリ秒に設定された CAS ガード タイマーの例を示します。事前認証要求に対して RADIUS サーバが応答しないまま、タイマーが期限切れになった場合、コールは許可されます。

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
```

```
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept
aaa preauthentication
group radius
dnis required
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	Cisco IOS Master Command List, All Releases
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
AAA	『*Authentication, Authorization, and Accounting Configuration Guide*』（Securing User Services Configuration Library の一部）

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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするため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

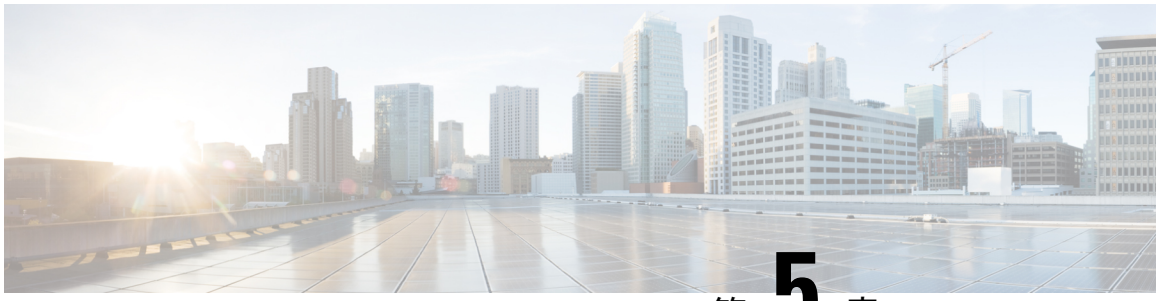
許可用の AAA DNIS マップの機能情報

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 *6 :* 許可用の *AAA DNIS* マップの機能情報

機能名	リリース	機能情報
許可用の AAA Dialed Number Information Service（DNIS）マップ	12.1(1)T 12.2(2)T 12.2(27)SBA Cisco IOS XE Release 2.3	許可用の AAA DNIS マップ機能を使用すると、着信番号識別サービス（DNIS）番号を特定の AAA サーバ グループに割り当てることができます。これによって、サーバ グループは、その DNIS を使用して、ネットワークにダイヤルインするユーザの認証、認可、およびアカウンティングの要求を処理できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザ宛てに発信された番号を示します。 次のコマンドが導入または変更されました。**aaa dnis enable**、**aaa dnis map authentication group**、**aaa dnis map authorization network group**、および **aaa dnis map accounting network**



第 5 章

AAA Server Groups

認証、認可、およびアカウンティング（AAA）サーバ グループを使用するようにデバイスを設定すると、既存のサーバ ホストをグループ化できます。既存のサーバ ホストをグループ化すると、設定したサーバ ホストのサブセットを選択し、それを特定のサービスに使用できます。サーバ グループ内でデッドタイムを設定することで、AAA トラフィックを、異なる動作特性を持つ別のサーバ グループに送信できます。この機能モジュールでは、AAA サーバ グループとデッドタイマーを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

AAA サーバ グループに関する情報

AAA Server Groups

AAA サーバ グループを使用するようにデバイスを設定すると、既存のサーバ ホストをグループ化できます。既存のサーバ ホストをグループ化すると、設定したサーバ ホストのサブセットを選択し、それを特定のサービスに使用できます。サーバ グループは、グローバル サーバ ホストの一覧と一緒に使用されます。サーバ グループには、選択したサーバ ホストの IP アドレスが一覧表示されます。

また、サーバ グループには、各エントリが一意の ID を持っていれば、同一サーバに複数のホスト エントリを組み込むことができます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。この一意の ID により、同じ IP アドレスでサーバの異なる UDP ポートに RADIUS の要求を送ることができるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティングなど）を設定した場合、2 番目に設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エントリがアカウンティング サービスの提供に失敗すると、ネットワーク アクセス サーバは同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように試行します。（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

AAA サーバ グループのデッドタイマー

サーバ名を指定してサーバホストを設定したら、**deadtime** コマンドを使用して、サーバ グループごとに各サーバを設定できます。サーバグループ内でデッドタイムを設定することで、AAA トラフィックを、異なる動作特性を持つ別のサーバ グループに送信できます。

デッドタイムの設定は、グローバル コンフィギュレーションに限定されません。すべてのサーバ グループの各サーバ ホストには、個別のタイマーがあります。そのため、サーバが応答せず、再送信とタイムアウトが何度も発生する場合、そのサーバは動作していない（デッド状態）と見なされます。すべてのサーバ グループの各サーバ ホストに付属するタイマーが開始されます。基本的に、タイマーがチェックされ、サーバに対する以降の要求は（デッド状態と見なされた場合）、（設定されていれば）代替タイマーに送信されます。ネットワーク アクセス サーバがサーバからの応答を受信すると、すべてのサーバ グループのそのサーバに関するすべての設定済みタイマー（実行中の場合）が停止されます。

タイマーが期限切れになると、タイマーが付属しているサーバは応答可能（アライブ状態）と見なされます。このサーバは、タイマーが属するサーバ グループを使用して後で AAA 要求のために試行できる唯一のサーバになります。

（注） 1つのサーバが複数のタイマーを持ち、異なるデッドタイム値がサーバ グループに設定されることがあるため、同時刻の同じサーバでも複数の状態（デッドとアライブ）になる可能性があります。

（注） サーバの状態を変更するには、すべてのサーバ グループですべての設定済みタイマーを起動および終了する必要があります。

新しいタイマーと deadtime 属性が追加されるため、サーバ グループのサイズはやや増えます。構造の全体的な影響は、サーバ グループの数と規模、およびその設定でサーバ グループ内でサーバを共有する方法によって変わります。

AAA サーバ グループの設定方法

AAA サーバ グループの設定

サーバ グループ名を使用してサーバ ホストを定義するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。一覧のサーバは、グローバル コンフィギュレーション モードに存在します。

始める前に

グループの各サーバは、**radius-server host** コマンドを使用して事前に定義する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server-name*
4. **aaa group server** {**radius** | **tacacs+**} *group-name*
5. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**radius server** *server-name* 例： `Device(config)# radius server rad1`	RADIUS サーバの名前を指定します。
ステップ 4	**aaa group server** {**radius** | **tacacs+**} *group-name* 例： `Device(config)# aaa group server radius group1`	グループ名を使用して、AAA サーバ グループを定義します。 • グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS または TACACS+ です。このコマンドを実行すると、デバイスはサーバ グループ RADIUS コンフィギュレーション モードへ移行します。
ステップ 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] 例： `Device(config-sg-radius)# server 172.16.1.1 acct-port 1616`	特定の RADIUS サーバを定義済みのサーバ グループと関連付けます。 • セキュリティ サーバは、IP アドレスと UDP ポート番号で識別されます。 • AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。
ステップ 6	**end** 例： `Device(config-sg-radius)# end`	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、特権 EXEC モードに戻ります。

AAA サーバ グループのデッドタイマーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group*
4. **deadtime** *minutes*
5. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**aaa group server radius** *group* 例： `Device(config)# aaa group server radius group1`	RADIUS タイプ サーバ グループを定義し、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。
ステップ 4	**deadtime** *minutes* 例： `Device(config-sg-radius)# deadtime 1`	デッドタイム値（分）を設定および定義します。 （注） ローカル サーバ グループのデッドタイムは、グローバル コンフィギュレーションよりも優先されます。ローカル サーバ グループ コンフィギュレーションでデッドタイム値を省略した場合は、マスター リストから継承されます。
ステップ 5	**end** 例： `Device(config-sg-radius)# end`	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、特権 EXEC モードに戻ります。

AAA サーバ グループの設定例

例：AAA サーバ グループ

次に、3 つの RADIUS サーバ メンバを持ち、各メンバがデフォルトの認証ポート（1645）とアカウンティング ポート（1646）を使用するサーバ グループ radgroup1 を作成する例を示します。

```
aaa group server radius radgroup1
 server 172.16.1.11
 server 172.17.1.21
 server 172.18.1.31
```

次に、3 つの RADIUS サーバ メンバを持ち、各メンバは IP アドレスは同じでも認証ポートとアカウンティング ポートはそれぞれ異なるサーバ グループ radgroup2 を作成する例を示します。

```
aaa group server radius radgroup2
 server 172.16.1.1 auth-port 1000 acct-port 1001
 server 172.16.1.1 auth-port 2000 acct-port 2001
 server 172.16.1.1 auth-port 3000 acct-port 3001
```

例：AAA サーバ グループを使用する複数の RADIUS サーバ エントリ

次に、2 つの RADIUS サーバ グループを認識するようにネットワーク アクセス サーバを設定する例を示します。一方のグループである group1 には、同じ RADIUS サーバ上に同じサービス用に設定された 2 つのホスト エントリがあります。設定されている 2 番めのホスト エントリは、1 番めのエントリのフェールオーバーバックアップとして動作します各グループのデッドタイムは個々に設定されています。group 1 のデッドタイムは 1 分で、group 2 のデッドタイムは 2 分です。

（注） グローバル コマンドと **server** コマンドの両方を使用する場合、**server** コマンドがグローバル コマンドよりも優先されます。

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS server group and associate servers
! with it and configures a deadtime of one minute.
aaa group server radius group1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 server 10.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
! The following commands define the group2 RADIUS server group and associate servers
! with it and configures a deadtime of two minutes.
aaa group server radius group2
 server 10.2.2.2 auth-port 2000 acct-port 2001
 server 10.3.3.3 auth-port 1645 acct-port 1646
 deadtime 2
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined server groups.
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server host 10.2.2.2 auth-port 2000 acct-port 2001
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
AAA コマンドと RADIUS コマンド	『*Cisco IOS Security Command Reference*』
RADIUS 属性	『*RADIUS Attributes Configuration Guide*』（Securing User Services Configuration Library の一部）
AAA	『*Authentication, Authorization, and Accounting Configuration Guide*』（Securing User Services Configuration Library の一部）
L2TP、VPN、または VPDN	『*Dial Technologies Configuration Guide*』および『*VPDN Configuration Guide*』
モデムの設定と管理	『*Dial Technologies Configuration Guide*』
PPP の RADIUS ポートの識別	『*Wide-Area Networking Configuration Guide*』

RFC

RFC	タイトル
RFC 2138	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC 2139	『*RADIUS Accounting*』
RFC 2865	『*RADIUS*』
RFC 2867	『*RADIUS Accounting Modifications for Tunnel Protocol Support*』
RFC 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするため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

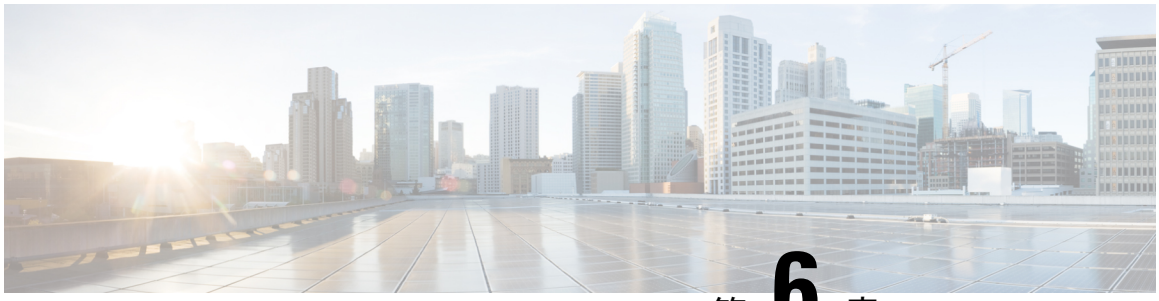
AAA サーバ グループの機能情報

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 *7*: *AAA* サーバ グループの機能情報

機能名	リリース	機能情報
AAA Server Group		AAA サーバ グループを使用するようにデバイスを設定すると、既存のサーバ ホストをグループ化できます。これによって、設定したサーバ ホストのサブセットを選択し、それを特定のサービスに使用できます。サーバ グループは、グローバル サーバ ホストの一覧と一緒に使用されます。サーバ グループには、選択したサーバホストの IP アドレスが一覧表示されます。 次のコマンドが導入または変更されました。**aaa group server radius**、**aaa group server tacacs+**、および **server**（RADIUS）。
AAA サーバ グループの拡張機能		AAA サーバ グループの拡張機能により、サーバ グループ内のサーバの完全な設定が可能です。
AAA サーバ グループ デッドタイマー		サーバ グループ内でデッドタイムを設定することで、AAA トラフィックを、異なる動作特性を持つ別のサーバ グループに送信できます。 次のコマンドが導入または変更されました。**deadtime**



第 6 章

RADIUS アカウンティング内の Framed-Route

RADIUS アカウンティング内の Framed-Route 機能は、RADIUS Accounting-Request アカウンティング レコードに Framed-Route（RADIUS 属性 22）情報を挿入します。Framed-Route 情報は、Accounting-Request パケットで RADIUS サーバに返されます。Framed-Route 情報を使用すれば、ユーザ単位ルートがネットワーク アクセス サーバ（NAS）上の特定の静的 IP 顧客に適用されているかどうかを確認できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RADIUS アカウンティング内の Framed-Route の前提条件

認証、許可、アカウンティング（AAA）、RADIUS サーバ、および RADIUS 属性スクリーニングの設定に精通している必要があります。

RADIUS アカウンティング内の Framed-Route に関する情報

Framed-Route 属性 22

インターネット技術特別調査委員会（IETF）標準の RFC 2865 で属性 22 として定義されている Framed-Route は、NAS 上のユーザに対して設定すべきルーティング情報を提供します。通常、Framed-Route 属性情報は、Access-Accept パケットで RADIUS サーバから NAS に送信されます。この属性は複数挿入できます。

RADIUS アカウンティング パケット内の Framed-Route

RADIUS アカウンティング パケット内の Framed-Route 属性情報は、NAS 上の特定の静的 IP 顧客に適用されたユーザ単位ルートを表します。現在は、Framed-Route 属性情報が Access-Accept パケットで送信されます。Framed-Route 属性情報は、Access-Accept パケットに挿入され、正常に適用されていれば、Accounting-Request パケットでも送信されます。Accounting-Request パケットには、0 個以上の Framed-Route 属性を挿入できます。

（注） Access-Accept パケット内に複数の Framed-Route 属性が存在する場合は、Accounting-Request 内にも複数の Framed-Route 属性を挿入できます。

Framed-Route 情報は、accounting Delay-Start の設定時に、Stop および Interim アカウンティング レコードと Start アカウンティング レコードで返されます。

Frame-Route 属性情報を RADIUS アカウンティング パケットで返すための設定は不要です。

RADIUS アカウンティング内の Framed-Route のモニタ方法

debug radius コマンドを使用して、Framed-Route（属性 22）の情報が RADIUS Accounting-Request パケットで送信されているかどうかをモニタします。

RADIUS アカウンティング内の Framed-Route の設定例

debug radius コマンドの出力例

次の例では、**debug radius** コマンドを使用して、Framed-Route（属性 22）情報が Accounting-Request パケットで送信されているかどうかを確認します（00:06:23: RADIUS: Framed-Route [22] 26 "10.80.0.1 255.255.255.255 10.60.0.1 100" の行を参照）。

```
Router# debug radius
00:06:23: RADIUS:  Send to unknown id 0 10.1.0.2:1645, Access-Request, len 126
00:06:23: RADIUS:  authenticator 40 28 A8 BC 76 D4 AA 88 - 5A E9 C5 55 0E 50 84 37
00:06:23: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
00:06:23: RADIUS:  User-Name           [1]   14  "nari@trw1001"
00:06:23: RADIUS:  CHAP-Password       [3]   19  *
00:06:23: RADIUS:  NAS-Port            [5]   6   1
00:06:23: RADIUS:  Vendor, Cisco       [26]  33
00:06:23: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:23: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
00:06:23: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:06:23: RADIUS:  NAS-IP-Address      [4]   6   12.1.0.1
00:06:23: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:06:23: RADIUS:  Received from id 0 10.1.0.2:1645, Access-Accept, len 103
00:06:23: RADIUS:  authenticator 5D 2D 9F 25 11 15 45 B2 - 54 BB 7F EB CE 79 20 3B
00:06:23: RADIUS:  Vendor, Cisco       [26]  33
00:06:23: RADIUS:  Cisco AVpair        [1]   27  "interface=Virtual-Access1"
00:06:23: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:06:23: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
00:06:23: RADIUS:  Framed-IP-Netmask   [9]   6   255.255.255.255
00:06:23: RADIUS:  Framed-IP-Address   [8]   6   10.60.0.1
00:06:23: RADIUS:  Framed-Route        [22]  26  "10.80.0.1 255.255.255.255 10.60.0.1
100"        <=======
00:06:23: RADIUS:  Received from id 2
00:06:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state
 to up
00:06:25: AAA/AUTHOR:  Processing PerUser AV route
00:06:25: Vi1 AAA/PERUSER/ROUTE: route string: IP route  10.80.0.1 255.255.255.255
10.60.0.1 100
00:06:25: RADIUS/ENCODE(00000002): Unsupported AAA attribute timezone
00:06:25: RADIUS(00000002): sending
00:06:25: RADIUS:  Send to unknown id 1 10.1.0.2:1646, Accounting-Request, len 278
00:06:25: RADIUS:  authenticator E0 CC 99 EB 49 18 B9 78 - 4A 09 60 0F 4E 92 24 C6
00:06:25: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:06:25: RADIUS:  Tunnel-Server-Endpoi[67]  12  00:"10.1.1.1"
00:06:25: RADIUS:  Tunnel-Client-Endpoi[66]  12  00:"10.1.1.2"
00:06:25: RADIUS:  Tunnel-Assignment-Id[82]  15  00:"from_isdn101"
00:06:25: RADIUS:  Tunnel-Type         [64]  6   00:L2TP                   [3]
00:06:25: RADIUS:  Acct-Tunnel-Connecti[68]  12  "2056100083"
00:06:25: RADIUS:  Tunnel-Client-Auth-I[90]  10  00:"isdn101"
00:06:25: RADIUS:  Tunnel-Server-Auth-I[91]  6   00:"lns"
00:06:25: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
00:06:25: RADIUS:  Framed-Route        [22]  39  "10.80.0.1 255.255.255.255 10.60.0.1
100"         <========
00:06:25: RADIUS:  Framed-IP-Address   [8]   6   10.60.0.1
00:06:25: RADIUS:  Vendor, Cisco       [26]  35
00:06:25: RADIUS:  Cisco AVpair        [1]   29  "connect-progress=LAN Ses Up"
00:06:25: RADIUS:  Authentic           [45]  6   RADIUS                    [1]
00:06:25: RADIUS:  User-Name           [1]   14  "username1@example.com"
```

```
00:06:25: RADIUS:  Acct-Status-Type     [40]  6   Start                       [1]
00:06:25: RADIUS:  NAS-Port             [5]   6   1
00:06:25: RADIUS:  Vendor, Cisco        [26]  33
00:06:25: RADIUS:  Cisco AVpair         [1]   27  "interface=Virtual-Access1"
00:06:25: RADIUS:  NAS-Port-Type        [61]  6   Virtual                     [5]
00:06:25: RADIUS:  Service-Type         [6]   6   Framed                      [2]
00:06:25: RADIUS:  NAS-IP-Address       [4]   6   10.1.0.1
00:06:25: RADIUS:  Acct-Delay-Time      [41]  6   0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ 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、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』
RADIUS	「Configuring RADIUS」機能モジュール。

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、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
RFC 2865	『Remote Authentication Dial In User Service (RADIUS)』

RFC	タイトル
RFC 3575	『IANA Considerations for RADIUS (Remote Authentication Dial In User Service)』

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/cisco/web/support/index.html

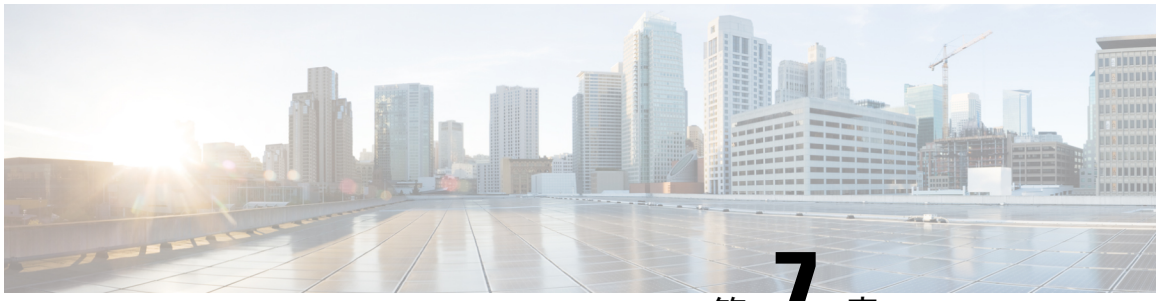
RADIUS アカウンティング内の Framed-Route の機能情報

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 *8 : RADIUS* アカウンティング内の *Framed-Route* の機能情報

機能名	リリース	機能情報
RADIUS アカウンティング内の Framed-Route	Cisco IOS XE Release 2.1	RADIUS アカウンティング内の Framed-Route 機能は、RADIUS Accounting-Request アカウンティング レコードに Framed-Route（RADIUS 属性 22）情報を挿入します。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。



第 7 章

RFC-2867 RADIUS トンネル アカウンティング

RFC-2867 RADIUS トンネル アカウンティングは、6 つの新しい RADIUS アカウンティング タイプを導入しています。これらのタイプは、アカウンティング要求がユーザ サービスの始まり（開始）と終わり（終了）のどちらを表しているかを示す、RADIUS アカウンティング属性の Acct-Status-Type（属性 40）と一緒に使用されます。

また、この機能は、ユーザによる VPDN セッション イベントのトラブルシューティングを支援する 2 つの新しい仮想プライベート ダイヤルアップ ネットワーク（VPDN）コマンドを導入しています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RFC-2867 RADIUS トンネル アカウンティングの制約事項

RADIUS トンネル アカウンティングは、L2TP トンネル サポートがなければ動作しません。

RFC-2867 RADIUS トンネル アカウンティングに関する情報

RFC-2867 RADIUS トンネル アカウンティングの利点

ユーザが tunnel-link ステータスの変化を判断できるようにするネットワーク アカウンティングを使用した VPDN では、RADIUS トンネル アカウンティングがサポートされていないため、使用可能なすべての属性がアカウンティング レコード ファイルに書き込まれませんでした。現在は使用可能なすべての属性を表示できるため、ユーザはアカウンティング レコードをインターネット サービス プロバイダー（ISP）に確認しやすくなりました。

RADIUS トンネル アカウンティングのための RADIUS 属性サポート

以下の表に、ダイヤルアップ ネットワーク内の Compulsory Tunneling のプロビジョンをサポートするように設計された新しい RADIUS アカウンティング タイプの概要を示します。これらの属性タイプを使用すると、トンネル ステータスの変化をより適切に追跡できます。

（注） アカウンティング タイプは 2 つのトンネル タイプに分けられるため、ユーザは、トンネル タイプが必要なのか、tunnel-link タイプが必要なのか、両方のアカウンティング タイプが必要なのかを判断できます。

表 *9 : Acct-Status-Type* 属性用の *RADIUS* アカウンティング タイプ

タイプ名	ケース	説明	追加属性[1]
Tunnel-Start	9	別のノードとのトンネル セットアップの始まりを示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Stop	10	別のノードへの、または別のノードからのトンネル接続の終わりを示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Input-Octets（42）：AAA から • Acct-Output-Octets（43）：AAA から • Acct-Session-Id（44）：AAA から • Acct-Session-Time（46）：AAA から • Acct-Input-Packets（47）：AAA から • Acct-Output-Packets（48）：AAA から • Acct-Terminate-Cause（49）：AAA から • Acct-Multi-Session-Id（51）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから • Acct-Tunnel-Packets-Lost（86）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Reject	11	別のノードとのトンネル セットアップの拒否を示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Terminate-Cause（49）：クライアントから • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから
Tunnel-Link-Start	12	トンネル リンクの構築を示します。一部のトンネル タイプ（レイヤ 2 トランスポート プロトコル（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • NAS-Port（5）：AAA から • Acct-Delay-Time（41）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Link-Stop	13	トンネル リンクの終わりを示します。一部のトンネル タイプ（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • NAS-Port（5）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Input-Octets（42）：AAA から • Acct-Output-Octets（43）：AAA から • Acct-Session-Id（44）：AAA から • Acct-Session-Time（46）：AAA から • Acct-Input-Packets（47）：AAA から • Acct-Output-Packets（48）：AAA から • Acct-Terminate-Cause（49）：AAA から • Acct-Multi-Session-Id（51）：AAA から • Event-Timestamp（55）：AAA から • NAS-Port-Type（61）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから • Acct-Tunnel-Packets-Lost（86）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Link-Reject	14	既存のトンネル内の新しいリンクに対するトンネル セットアップの拒否を示します。一部のトンネル タイプ（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Terminate-Cause（49）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

[1] 指定されたトンネル タイプが使用されている場合は、これらの属性もアカウンティング要求パケットに含める必要があります。

RADIUS トンネル アカウンティングの設定方法

トンネル タイプ アカウンティング レコードの有効化

このタスクを使用して、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバに送信するように LAC を設定します。

vpdn セッション アカウンティング ネットワーク（tunnel-link-type レコード）と vpdn トンネル アカウンティング ネットワーク（tunnel-type レコード）という 2 つの新しいコマンドライン インターフェイス（CLI）が、次のイベントの特定を支援するためにサポートされています。

- VPDN トンネルが構築または破壊された。
- VPDN トンネルの作成要求が拒否された。
- VPDN トンネル内のユーザ セッションが起動または停止された。
- ユーザ セッション作成要求が拒否された。

（注） 最初の 2 つのイベントは、tunnel-type アカウンティング レコードです。認証、許可、アカウンティング（AAA）が、Tunnel-Start、Tunnel-Stop、または Tunnel-Reject アカウンティング レコードを RADIUS サーバに送信します。次の 2 つのイベントは、tunnel-link-type アカウンティング レコードです。AAA が、Tunnel-Link-Start、Tunnel-Link-Stop、または Tunnel-Link-Reject アカウンティング レコードを RADIUS サーバに送信します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa accounting network default** *list-name*} {**start-stop** | **stop-only** | **wait-start** | **none group** *groupname*
4. Router(config)# **vpdn enable**
5. Router(config)# **vpdn tunnel accounting network** *list-name*
6. Router(config)# **vpdn session accounting network** *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。 • 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： `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	Router(config)# **aaa accounting network default** *list-name*} {**start-stop**	**stop-only**	**wait-start**	**none group** *groupname* 例： 例： 例： 例： 例：	ネットワーク アカウンティングを有効にします。 • **default** ：デフォルトのネットワーク アカウンティングの方式リストが設定され、インターフェイス上でどの追加のアカウンティング設定も有効になっていない場合は、デフォルトで、ネットワーク アカウンティングが有効になります。 **vpdn session accounting network** コマンドまたは **vpdn tunnel accounting network** コマンドが **default** 方式リストにリンクされている場合、すべてのトンネルおよびトンネルリンク アカウンティング レコードが、これらのセッションで有効になります。

	コマンドまたはアクション	目的
	例： 例： 例： 例： 例： 例： `Router(config)# aaa accounting network m1 start-stop group radius`	• *list-name* ：**aaa accounting** コマンドで定義された *list-name* は、VPDN コマンドで定義された *list-name* と同一である必要があります。そうでない場合、アカウンティングは発生しません。
ステップ 4	Router(config)# **vpdn enable** 例： `Router(config)# vpdn enable`	ルータ上のバーチャル プライベート ダイヤルアップ ネットワーキングを有効にして、ルータにローカル データベースとリモート認可サーバ（該当する場合）上でトンネル定義を検索するように指示します。
ステップ 5	Router(config)# **vpdn tunnel accounting network** *list-name* 例： `Router(config)# vpdn tunnel accounting network m1`	Tunnel-Start、Tunnel-Stop、および Tunnel-Reject アカウンティング レコードを有効にします。 • *list-name* ：*list-name* は、**aaa accounting** コマンドで定義された *list-name* と一致している必要があります。そうでない場合、ネットワーク アカウンティングは発生しません。
ステップ 6	Router(config)# **vpdn session accounting network** *list-name* 例： `Router(config)# vpdn session accounting network m1`	Tunnel-Link-Start、Tunnel-Link-Stop、および Tunnel-Link-Reject アカウンティング レコードを有効にします。 • *list-name* ：*list-name* は、**aaa accounting** コマンドで定義された *list-name* と一致している必要があります。そうでない場合、ネットワーク アカウンティングは発生しません。

次の作業

RADIUS トンネル アカウンティングを有効にしたら、次のオプション タスク「RADIUS トンネル アカウンティングの確認」で設定を確認できます。

RADIUS トンネル アカウンティングの確認

次のオプション手順のどちらかまたは両方を使用して、RADIUS トンネルアカウンティング設定を確認します。

手順の概要

1. **enable**
2. Router# **show accounting**
3. Router# **show vpdn** [**session**] [**tunnel**]

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。 • パスワードを入力します（要求された場合）。
ステップ 2	Router# **show accounting** 例： `Router# show accounting`	ネットワーク上でアクティブなアカウント可能イベントを表示して、アカウンティング サーバ上でのデータ消失イベント時の情報収集を支援します。
ステップ 3	Router# **show vpdn** [**session**] [**tunnel**] 例： 例： 例： 例： `Router# show vpdn session`	VPDN 内のアクティブな L2TP トンネルとメッセージ識別子に関する情報を表示します。 • **session** ：すべてのアクティブなトンネルのステータス サマリーを表示します。 • **tunnel** ：すべてのアクティブな L2TP トンネルに関する情報をサマリー形式で表示します。

RADIUS トンネル アカウンティングの設定例

LAC 上での RADIUS トンネル アカウンティングの設定例

次の例は、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバに送信するように L2TP アクセス コンセントレータ（LAC）を設定する方法を示しています。

```
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$IDjH$iL7puCja1RMlyOM.JAeuf/
enable password lab
!
username ISP_LAC password 0 tunnelpass
!
!
resource-pool disable
!
!
ip subnet-zero
ip cef
no ip domain-lookup
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.1.26.71
 local name ISP_LAC
!
mta receive maximum-recipients 0
!
interface GigabitEthernet0/0/0
 ip address 10.1.27.74 255.255.255.0
 no ip mroute-cache
 duplex half
 speed auto
 no cdp enable
!
interface FastEthernet0/0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip default-gateway 10.1.27.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.27.254
no ip http server
ip pim bidir-enable
!
no cdp run
!
!
radius-server host 172.19.192.26 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
```

```
call rsvp-sync
!
```

LNS 上での RADIUS トンネル アカウンティングの設定例

次の例は、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバに送信するように L2TP ネットワーク サーバ（LNS）を設定する方法を示しています。

```
aaa new-model
!
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@cisco.com password 0 lab
username user2@cisco.com password 0 lab
spe 1/0 1/7
 firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
 firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 172.24.80.28 10.47.0.0
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname ISP_LAC
 local name ENT_LNS
!
mta receive maximum-recipients 0
!
interface Loopback0
 ip address 192.168.70.101 255.255.255.0
!
interface Loopback1
 ip address 192.168.80.101 255.255.255.0
!
interface FastEthernet0/0/0
 ip address 10.1.26.71 255.255.255.0
 no ip mroute-cache
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool vpdn-pool1
 ppp authentication chap
```

```
!
interface Virtual-Template2
 ip unnumbered Loopback1
 peer default ip address pool vpdn-pool2
 ppp authentication chap
!
interface FastEthernet0/0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip local pool vpdn-pool1 192.168.70.1 192.168.70.100
ip local pool vpdn-pool2 192.168.80.1 192.168.80.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 10.90.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
no cdp run
!
radius-server host 172.19.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
```

その他の参考資料

次の項で、RFC-2867 RADIUS トンネル アカウンティングに関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUS 属性	『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』の「RADIUS Attributes Overview and RADIUS IETF Attributes」
VPDN	『*Cisco IOS XE VPDN Configuration Guide* , Release 2』
ネットワーク アカウンティング	『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』の「Configuring Accounting」
コマンド	• 『*Cisco IOS Security Command Reference*』 • 『*Cisco IOS VPDN Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
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規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ 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
RFC 2867	『*RADIUS Accounting Modifications for Tunnel Protocol Support*』

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/en/US/support/index.html

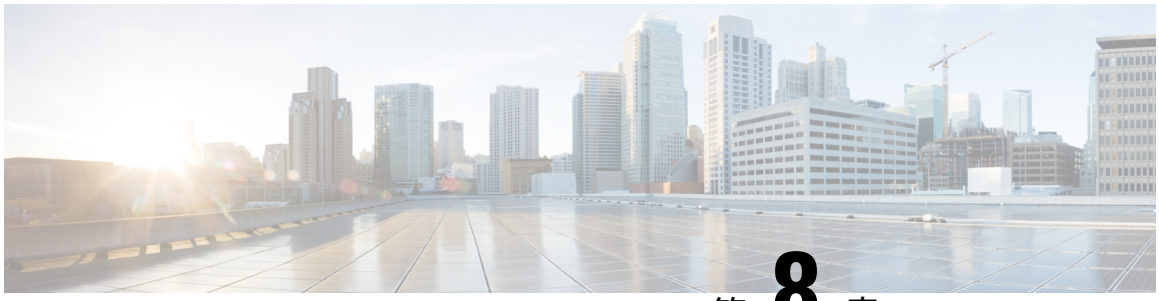
RFC-2867 RADIUS トンネル アカウンティングの機能情報

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 *10 : RFC-2867 RADIUS* トンネル アカウンティングの機能情報

機能名	リリース	機能情報
RFC-2867 RADIUS トンネル アカウンティング	Cisco IOS XE Release 2.1	RFC-2867 RADIUS トンネル アカウンティングは、6 つの新しい RADIUS アカウンティング タイプを導入しています。これらのタイプは、アカウンティング要求がユーザ サービスの始まり（開始）と終わり（終了）のどちらを表しているかを示す、RADIUS アカウンティング属性の Acct-Status-Type（属性 40）と一緒に使用されます。 また、この機能は、ユーザによる VPDN セッション イベントのトラブルシューティングを支援する 2 つの新しい仮想プライベート ダイヤルアップ ネットワーク（VPDN）コマンドを導入しています。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました。**aaa accounting**、**vpdn session accounting network**、**vpdn tunnel accounting network**



第 8 章

RADIUS 論理回線 ID

論理回線 ID（LLID）ブロッキング機能としても知られる RADIUS 論理回線 ID 機能を使用すれば、管理者は、顧客コールが発信された物理回線に基づいて顧客を追跡できます。管理者は、顧客が物理回線を移動しても変化しない仮想ポートを使用します。この仮想ポートは、管理者の顧客プロファイルデータベースのメンテナンスを容易にし、管理者が顧客に対して追加のセキュリティ チェックを実施できるようにします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RADIUS 論理回線 ID の前提条件

この機能は任意の RADIUS サーバと一緒に使用できますが、RADIUS サーバによっては、Access-Accept メッセージで Calling-Station-ID 属性を返せるようにディレクトリ ファイルを変更する必要があります。たとえば、「ATTRIBUTE Calling-Station-Id 31 string (*, *)」のようにディクショナリを変更しなければ、Merit RADIUS サーバで LLID ダウンロードはサポートされません。

RADIUS 論理回線 ID の制約事項

RADIUS 論理回線 ID 機能は RADIUS のみをサポートしています。TACACS+ はサポートしていません。

この機能は、PPP over Ethernet over ATM（PPPoEoATM）コールと PPP over Ethernet over VLAN（PPPoEoVLAN）（Dot1Q）コールにしか適用できません。ISDN などのその他のコールは使用できません。

RADIUS 論理回線 ID に関する情報

事前認可

LLID は、加入者線の論理識別を表す英数字文字列です（1 ～ 253 文字にする必要があります）。また、LLID は、RADIUS サーバ上の顧客プロファイルデータベース上に保存されます。顧客プロファイル データベースがアクセス ルータから事前認可要求を受け取ると、RADIUS サーバが LLID を Calling-Station-ID 属性（属性 31）としてルータに送信します。

レイヤ 2 トンネリング プロトコル（L2TP）アクセス コンセントレータ（LAC）が、事前認可用に設定されている場合に、事前認可要求を顧客プロファイル データベースに送信します。**subscriber access** コマンドを使用して、LAC を事前認可用に設定します。

（注） LLID のダウンロードは「事前認可」と呼ばれています。これは、サービス（ドメイン）認可またはユーザ認証および認可の前に実施されるためです。

RADIUS サーバ上の顧客プロファイルデータベースは、ルータに接続された物理ネットワーク アクセス サーバ（NAS）ごとのユーザ プロファイルで構成されています。各ユーザ プロファイルには、ルータ上の物理ポートを表すユーザ名（属性 1）と一致したプロファイルが格納されています。ルータは、事前認可用に設定されている場合に、接続先の物理 NAS ポートの代表ユーザ名を使用して顧客プロファイル データベースに問い合わせます。顧客プロファイル データベース内で一致するものが見つかると、顧客プロファイル データベースが、ユーザ プ

ロファイル内の LLID を含む Access-Accept メッセージを返します。LLID は、Calling-Station-ID 属性として Access-Accept レコード内に定義されています。

事前認可プロセスは、認証に使用される実際のユーザ名を RADIUS サーバに提供することもできます。物理 NAS ポート情報がユーザ名（属性 1）として使用されるため、RADIUS 属性 77（Connect-Info）を認証ユーザ名を含めるように設定できます。この設定によって、RADIUS サーバは、LLID をルータに返す前に、選択した認可要求に対して追加の検証（プライバシールールに対するユーザ名の分析など）を実施できます。

RADIUS 論理回線 ID の設定方法

事前認可の設定

LLID をダウンロードして、LAC を事前認可用に設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *interface-name*
4. **subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id** [**default** | *list-name*] [**send username**]

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。 • 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： `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 radius source-interface** *interface-name* 例： 例：	事前認可要求用のユーザ名の IP アドレス部分を指定します。

	コマンドまたはアクション	目的
	`Router (config)# ip radius source-interface Loopback1`	
ステップ 4	**subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id** [**default** | *list-name*] [**send username**] 例： 例： `Router (config)# subscriber access pppoe pre-authorize nas-port-id mlist_llid send username`	LLID のダウンロードを可能にして、ルータを事前認可用に設定できるようにします。 **send username** オプションは、Access-Request メッセージ内の Connect-Info（属性 77）にセッションの認証ユーザ名を含めるように指定します。

RADIUS ユーザ プロファイル内の LLID の設定

ユーザ プロファイルを事前認可用に設定するには、顧客プロファイル データベースに NAS ポート ユーザを追加して、ユーザ プロファイルに RADIUS インターネット技術特別調査委員会（IETF）属性 31（Calling-Station-ID）を追加します。

手順の概要

1. UserName=nas_port: ip-address:slot/module/port/vpi.vci
2. User-Name=nas-port: ip-address:slot/module/port/vlan-id
3. Calling-Station-Id = “string (*,*)”

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	UserName=nas_port: ip-address:slot/module/port/vpi.vci	（任意）PPPoE over ATM NAS ポート ユーザを追加します。
ステップ 2	User-Name=nas-port: ip-address:slot/module/port/vlan-id	（任意）PPPoE over VLAN NAS ポート ユーザを追加します。
ステップ 3	Calling-Station-Id = “string (*,*)”	ユーザ プロファイルに属性 31 を追加します。 • String：ユーザがかけてきた電話番号を含む 1 つ以上のオクテット。

論理回線 ID の確認

機能を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **debug radius**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug radius** 例： `Router# debug radius`	RADIUS 属性 31 が、LAC 上の Accounting-Request と、LNS 上の Access-Request および Accounting-Request 内の LLID であることを確認します。

RADIUS 論理回線 ID の設定例

事前認可用の LAC 設定例

次の例は、LLID をダウンロードすることによって、LAC を事前認可用に設定する方法を示しています。

```
aaa new-model
aaa group server radius sg_llid
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_water
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg_water
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_water password 0 lab
vpdn enable
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain example.com
 domain example.com#184
 initiate-to ip 10.1.1.1
 local name s7200_2
 l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
```

```
 accept dialin
  protocol pppoe
  virtual-template 1
!
!
Enable the LLID to be downloaded.
subscriber access pppoe pre-authorize nas-port-id mlist_llid send username
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet1/0/0
 ip address 10.1.1.8 255.255.255.0 secondary
 ip address 10.0.58.111 255.255.255.0
 no cdp enable
!
interface ATM4/0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0/0.1 point-to-point
 pvc 1/100
  encapsulation aa15snap
  protocol pppoe
!
interface virtual-template1
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.31.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.31.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1
```

LLID 用の RADIUS ユーザ プロファイルの例

次の例は、ユーザ プロファイルを PPPoEoVLAN および PPPoEoATM に対する LLID 問い合わせ用に設定する方法と属性 31 の追加方法を示しています。

```
pppoeovlan
----------
nas-port:10.1.0.3:6/0/0/0    Password = "password1",
    Service-Type = Outbound,
    Calling-Station-ID = "cat-example"
pppoeoa
--------
nas-port:10.1.0.3:6/0/0/1.100    Password = "password1",
    Service-Type = Outbound,
    Calling-Station-ID = "cat-example"
```

その他の参考資料

次の項で、RADIUS EAP サポート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA を使用した ppp 認証の設定	「Configuring Authentication」モジュール。
RADIUS の設定	「Configuring RADIUS」モジュール。
PPP の設定	「Configuring Asynchronous SLIP and PPP」モジュール。
ダイヤルテクノロジー コマンド	『*Cisco IOS Dial Technologies Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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
RFC 2284	『*PPP Extensible Authentication Protocol (EAP)*』
RFC 1938	『*A One-Time Password System*』
RFC 2869	『*RADIUS Extensions*』

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/en/US/support/index.html

RADIUS 論理回線 ID 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 *11 : RADIUS* 論理回線 *ID* の機能情報

機能名	リリース	機能情報
RADIUS 論理回線 ID	Cisco IOS XE Release 2.1	論理回線 ID（LLID）ブロッキング機能としても知られる RADIUS 論理回線 ID 機能を使用すれば、管理者は、顧客コールが発信された物理回線に基づいて顧客を追跡できます。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 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。**subscriber access**

機能名	リリース	機能情報
発信側ステーション ID 属性 31	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
LLID ブロッキング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

用語集

attribute ：RADIUS Internet Engineering Task Force（IETF）属性は、クライアントとサーバの間で認証、認可、およびアカウンティング（AAA）情報を通信するために使用される 255 個の標準属性からなるオリジナル セットの 1 つです。IETF 属性は標準であるため、属性データは事前定義されてその内容も認識されています。このため、IETF 属性を介して AAA 情報を交換するすべてのクライアントとサーバは、属性の厳密な意味や各属性値の一般的な限界などの属性データを一致させる必要があります。

CHAP ：チャレンジ ハンドシェイク認証プロトコル。PPP カプセル化を使用した回線上でサポートされ、不正アクセスを防止するセキュリティ機能。CHAPそれ自体が不正アクセスを防止するわけではなく、単に、リモートエンドを識別するだけです。その後で、ルータまたはアクセス サーバがそのユーザのアクセスを許可するかどうかを決定します。

EAP ：拡張認証プロトコル。認証フェーズ（Link Control Protocol（LCP）フェーズではなく）でネゴシエートされる複数の認証メカニズムをサポートする PPP 認証プロトコル。EAP を使用すれば、汎用のインターフェイスを介して、サードパーティ製の認証サーバと PPP 実装の間でデータのやり取りができます。

LCP ：リンク制御プロトコル。PPP で使用するためのデータ リンク接続を確立して、設定し、テストするプロトコル。

MD5 (HMAC variant) ：Message Digest 5。パケット データの認証に使用するハッシュ アルゴリズム。HMAC は、メッセージ認証用の重要なハッシングです。

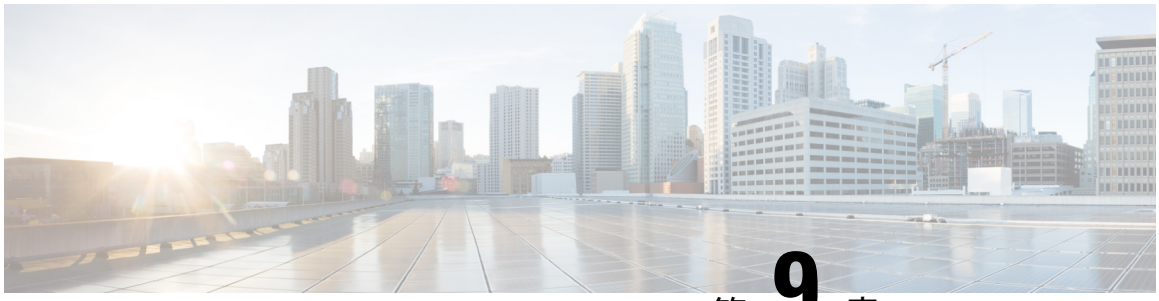
NAS ：ネットワーク アクセス サーバ。公衆電話交換網（PSTN）などのリモート アクセス ネットワーク上でユーザにローカル ネットワーク アクセスを提供するデバイス。

PAP ：パスワード認証プロトコル。PPP ピアの相互認証を可能にする認証プロトコル。ローカル ルータに接続を試みているリモート ルータは、認証要求を送信するように要求されます。CHAP と違って、PAP はパスワードとホスト名またはユーザ名をクリア テキスト（暗号化なし）で渡します。PAP それ自体が不正アクセスを防止するわけではなく、単に、リモート エンドを識別するだけです。ルータまたはアクセス サーバがそのユーザのアクセスを許可するかどうかを決定します。PAP は、PPP 回線上でのみサポートされます。

PPP ：ポイントツーポイント プロトコル。ポイントツーポイント リンク上でネットワーク層プロトコル情報をカプセル化するプロトコル。PPP は RFC 1661 で規定されています。

RADIUS ：リモート認証ダイヤルイン ユーザ サービス。モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。



第 9 章

RADIUS ルート ダウンロード

RADIUS ルート ダウンロード機能を使用すれば、RADIUS 認可を転送するようにネットワーク アクセス サーバ（NAS）を設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RADIUS ルート ダウンロードの前提条件

この機能でタスクを実行する前に、AAA ネットワーク セキュリティを有効にする必要があります。

RADIUS ルート ダウンロードに関する情報

RADIUS ルート ダウンロード機能を使用すれば、RADIUS 認可を転送するようにネットワーク アクセス サーバ（NAS）を設定できます。ユーザは、NAS から認証、許可、アカウンティング（AAA）に送信されるスタティック ルート ダウンロード要求用として、もう一つの名前付き方式リスト（デフォルトの方式リストに加えて）を設定できます。

この機能以前は、スタティック ルート ダウンロード要求用の RADIUS 認可が、デフォルトの方式リストで指定された AAA サーバにのみ送信されていました。

この機能では、AAA サーバへのスタティック ルート ダウンロード要求の転送に使用される方式リストの名前を指定できるように **aaa route download** コマンドの機能が拡張されています。**aaa route download** コマンドは、スタティック ルートをダウンロードするためのもう 1 つの方式リストを指定するために使用できます。この方式リストは、**aaa authorization configuration** コマンドを使用して追加できます。

RADIUS ルート ダウンロードの設定方法

RADIUS ルート ダウンロードの設定

名前付き方式リストで指定されたサーバにスタティック ルート ダウンロード要求を送信するように NAS を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaa authorization configuration** *method-name* **[radius | tacacs+ | group** *group-name* **]**
2. Router(config)# **aaa route download** [*time*] [**authorization** *method-list*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaa authorization configuration** *method-name* **[radius | tacacs+ | group** *group-name* **]**	RADIUS を使用して AAA サーバからスタティック ルート設定情報をダウンロードします。
ステップ 2	Router(config)# **aaa route download** [*time*] [**authorization** *method-list*]	スタティック ルート ダウンロード機能を有効にします。**authorization** *method-list* 属性を使用して、スタティック ルート ダウンロード用の RADIUS 認可要求が送信される名前付き方式リストを指定します。

RADIUS ルート ダウンロードの確認

インストールされているルートを確認するには、EXEC モードで **show ip route** コマンドを使用します。

RADIUS に関連付けられた情報を表示するには、特権 EXEC モードで **debug radius** コマンドを使用します。

RADIUS ルート ダウンロードの設定例

RADIUS ルート ダウンロード設定例

次の例は、スタティック ルート ダウンロード要求を「list1」という名前の方式リストで指定されたサーバに送信するように NAS を設定する方法を示しています。

```
aaa new-model
aaa group server radius rad1
server 10.2.2.2 auth-port 1645 acct-port 1646
!
aaa group server tacacs+ tac1
server 172.17.3.3
!
aaa authorization configuration default group radius
aaa authorization configuration list1 group rad1 group tac1
aaa route download 1 authorization list1
tacacs-server host 172.17.3.3
tacacs-server key cisco
tacacs-server administration
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

その他の参考資料

次の項で、RADIUS ルート ダウンロードに関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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、Cisco IOS XE ソフトウェア リリース、およびフィーチャ 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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

テクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/en/US/support/index.html

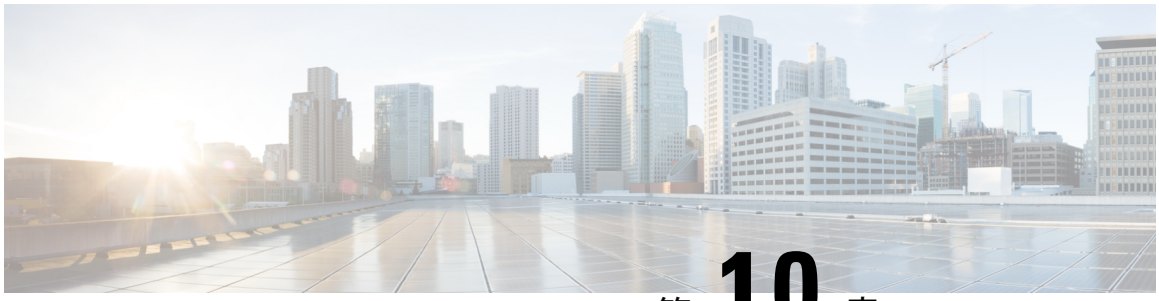
RADIUS ルート ダウンロードの機能情報

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 *12 : RADIUS* ルート ダウンロードの機能情報

機能名	リリース	機能情報
RADIUS ルート ダウンロード	Cisco IOS XE Release 2.1	RADIUS ルート ダウンロード機能を使用すれば、RADIUS 認可を転送するようにネットワーク アクセス サーバ（NAS）を設定できます。ユーザは、NAS から認証、許可、アカウンティング（AAA）に送信されるスタティック ルート ダウンロード要求用として、もう一つの名前付き方式リスト（デフォルトの方式リストに加えて）を設定できます。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズアグリゲーション サービス ルータに導入されました。 次のコマンドが導入されました。 **aaa route download**



第 10 章

RADIUS サーバ ロード バランシング

RADIUS サーバ ロード バランシング機能は、認証、認可、およびアカウンティング（AAA）の認証トランザクションとアカウンティング トランザクションをサーバ グループ内のRADIUS サーバに分配します。これらのサーバは、AAA トランザクションの負荷を共有することで、着信要求に迅速に応答できるようになります。

このモジュールでは、RADIUS サーバ ロード バランシング機能について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RADIUS サーバ ロード バランシングの前提条件

- 認証、認可、およびアカウンティング（AAA）を RADIUS サーバに設定する必要があります。
- AAA RADIUS サーバ グループを設定する必要があります。
- 認証、アカウンティング、スタティック ルート ダウンロードなどの機能用に RADIUS を設定する必要があります。

RADIUS サーバ ロード バランシングの制約事項

- パケット オブ ディスコネクト（POD）要求などの着信 RADIUS 要求はサポートされていません。

RADIUS サーバ ロード バランシングに関する情報

RADIUS サーバ ロード バランシングの概要

ロード バランシングは、トランザクションのバッチをサーバ グループ内の RADIUS サーバに分配します。ロードバランシングにより、トランザクションの各バッチは、キュー内の未処理トランザクション数が最も少ないサーバに割り当てられます。トランザクションのバッチの割り当てプロセスは次のとおりです。

1. 最初のトランザクションが新しいバッチとして受信されます。
2. すべてのサーバ トランザクション キューがチェックされます。
3. 最小番号の未処理トランザクションを持つサーバが特定されます。
4. 特定されたサーバが、トランザクションの次のバッチに割り当てられます。

バッチ サイズはユーザ設定のパラメータです。バッチ サイズを変更すると、CPU の負荷やネットワークのスループットに影響する可能性があります。バッチ サイズが大きくなるほど、CPU の負荷が減少し、ネットワークのスループットが増加します。ただし、バッチ サイズが大きくても、使用可能なすべてのサーバ リソースが使い果たされることはありません。バッチ サイズが小さくなるほど、CPU の負荷が増加し、ネットワークのスループットが減少します。

（注） 大きなバッチ サイズまたは小さなバッチ サイズに関する設定数はありません。50 を超えるトランザクションを含むバッチは大きいと見なされ、25 より少ないトランザクションを含むバッチは、小さいと見なされます。

（注） サーバ グループに 10 以上のサーバが含まれている場合、CPU の負荷を軽減するために高いバッチ サイズを設定することを推奨します。

RADIUS サーバ グループ全体のトランザクションのロード バランシング

名前付き RADIUS サーバ グループごとに、またはグローバル RADIUS サーバ グループに対してロード バランシングを設定できます。ロード バランシング サーバ グループは、認証、認可、およびアカウンティング（AAA）方式リストで「radius」として参照される必要があります。RADIUS サーバ グループの一部であるすべてのパブリック サーバは、その後、ロード バランシングされます。

同じ RADIUS サーバを使用するか、または別のサーバを使用するように認証およびアカウンティングを設定できます。1 つのサーバをセッションの事前認証、認証、またはアカウンティング トランザクションに使用することもできます。内部設定であり、デフォルトとして設定される優先サーバが、サーバ コストに関係なく、セッションの開始レコードと終了レコードに対して同じサーバを使用するよう AAA に指示します。優先サーバ設定を使用する場合は、初期トランザクション（認証など）に使用されるサーバ、つまり優先サーバが、以降のトランザクション（アカウンティングなど）に使用される他のサーバ グループにも属するようにします。

優先サーバは、次のいずれかの条件が真である場合は使用されません。

- **load-balance method least-outstanding ignore-preferred-server** コマンドが使用されている。
- 優先サーバが停止中である。
- 優先サーバが隔離中である。
- 必要サーバ フラグがセットされている場合は、優先サーバ設定が無効になります。

内部設定である必要サーバ フラグは、サーバ コストに関係なく、マルチステージ トランザクションのすべてのステージに対して同じサーバを使用する必要がある場合に使用されます。必要サーバが使用できない場合は、トランザクションが失敗します。

次のいずれかの設定がある場合、**load-balance method least-outstanding ignore-preferred-server** コマンドを使用できます。

- 専用の認証サーバと別の専用のアカウンティング サーバ
- 開始レコードと終了レコード、および別のサーバに保存されたレコードなど、すべての通話レコード統計情報と通話レコード詳細を追跡可能なネットワーク

認証サーバをアカウンティング サーバのスーパーセットとして設定している場合、優先サーバは使用されません。

RADIUS サーバ ステータスと自動テスト

RADIUS サーバ ロード バランシング機能では、バッチを割り当てるときにサーバ ステータスを考慮します。トランザクションのバッチは、稼働中のサーバのみに送信されます。あまり使用されていないサーバ（バックアップ サーバなど）を含む、すべての RADIUS ロード バランシング サーバのステータスをテストすることを推奨します。

停止中としてマークされたサーバにはトランザクションが送信されません。隔離状態になったサーバは、タイマーが切れるまで停止中としてマークされます。RADIUS 自動テスタ機能によって動作中であることが確認されるまでサーバは隔離中になります。

サーバが稼働中でトランザクションを処理できるかどうかを確認するために、RADIUS 自動テスターは、テスト ユーザ ID で要求を定期的にサーバに送信します。サーバが Access-Reject メッセージを返した場合、サーバは稼働中です。それ以外の場合、サーバは停止中または隔離中です。

未応答のサーバに送信されたトランザクションは、未応答のサーバが停止中としてマークされる前に、次の使用可能なサーバにフェールオーバーされます。失敗したトランザクションには再試行順序変更モードを使用することを推奨します。

RADIUS 自動テスターを使用する場合、認証、認可、およびアカウンティング（AAA）サーバが、ネットワーク アクセス サーバ（NAS）によって送信されるテスト パケットに応答していることを確認します。サーバが正しく設定されていない場合は、パケットが破棄され、サーバが誤って停止中としてマークされる可能性があります。

注意 RADIUS サーバ上で定義されていないテストユーザを RADIUS サーバ自動テストに使用して、テストユーザが正しく設定されていない場合に発生するセキュリティ上の問題を解決することを推奨します。

（注） ロード バランシング トランザクションを確認するには、**test aaa group** コマンドを使用します。

RADIUS サーバ ロード バランシングの設定方法

名前付き RADIUS サーバ グループのロード バランシングの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group-name*

4. **server ip-address [auth-port port-number] [acct-port port-number]**
5. **load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]
6. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**aaa group server radius** *group-name* 例： `Device(config)# aaa group server radius rad-sg`	サーバ グループ コンフィギュレーション モードに入ります。
ステップ 4	**server ip-address [auth-port port-number] [acct-port port-number]** 例： `Device (config-sg-radius)server 192.0.2.238 auth-port 2095 acct-port 2096`	グループ サーバ用の RADIUS サーバの IP アドレスを設定します。
ステップ 5	**load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] 例： `Device(config-sg-radius)# load-balance method least-outstanding batch-size 30`	名前付きサーバ グループに対して最小未処理ロード バランシングを有効にします。
ステップ 6	**end** 例： `Device(config-sg)# end`	サーバ グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

グローバル RADIUS サーバ グループのロード バランシングの有効化

グローバル RADIUS サーバ グループは、認証、認可、およびアカウンティング（AAA）方式リストで「radius」として参照されます。

手順の概要

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

3. **radius-server host** {*hostname* | *ip-address*} [**test username** *name*] [**auth-port** *number*] [**ignore-auth-port**] [**acct-port** *number*] [**ignore-acct-port**] [**idle-time** *seconds*]
4. **radius-server load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]
5. **load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]
6. **end**

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： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**radius-server host** {*hostname* | *ip-address*} [**test username** *name*] [**auth-port** *number*] [**ignore-auth-port**] [**acct-port** *number*] [**ignore-acct-port**] [**idle-time** *seconds*] 例： `Device(config)# radius-server host 192.0.2.1 test username test1 idle-time 1`	RADIUS 自動テストを有効にします。
ステップ 4	**radius-server load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] 例： `Device(config)# radius-server load-balance method least-outstanding`	グローバル RADIUS サーバ グループに対して最小未処理ロード バランシングを有効にし、サーバ グループ コンフィギュレーション モードを開始します。 • デフォルトのバッチ サイズは 25 です。バッチ サイズの範囲は 1 ～ 2147483647 です。
ステップ 5	**load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**] 例： `Device(config-sg)# load-balance method least-outstanding batch-size 5`	グローバル名前付きサーバ グループに対して最小未処理ロード バランシングを有効にします。
ステップ 6	**end** 例： `Device(config-sg)# end`	サーバ グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

RADIUS サーバ ロード バランシングのトラブルシューティング

RADIUS サーバ ロード バランシング機能を設定した後は、アイドル タイマー、デッド タイマー、ロードバランシング サーバの選択をモニタしたり、手動テスト コマンドを使用してサーバ ステータスを確認したりできます。

手順の概要

1. **debug aaa test** コマンドを使用して、アイドル タイマーやデッド タイマーが期限切れになった日時、テスト パケットが送信された日時、およびサーバ ステータスを特定し、サーバの状態を確認します。
2. **debug aaa sg-server selection** コマンドを使用して、ロード バランシング用に選択されたサーバを特定します。
3. **test aaa group** コマンドを使用して、RADIUS ロード バランシング サーバのステータスを手動で確認します。

手順の詳細

ステップ 1 **debug aaa test** コマンドを使用して、アイドル タイマーやデッド タイマーが期限切れになった日時、テスト パケットが送信された日時、およびサーバ ステータスを特定し、サーバの状態を確認します。

アイドル タイマーは、サーバ ステータスのチェックに使用され、着信要求の有無に関係なく更新されます。アイドル タイマーをモニタすると、未応答のサーバが存在するかどうかを判断し、RADIUS サーバのステータスを最新の状態に保つことができるため、利用可能なリソースを効率的に利用できます。たとえば、アイドル タイマーが更新されていれば、着信要求が動作中のサーバに送信されていることを簡単に確認できます。

デッド タイマーは、サーバが停止中であることを特定したり、停止中のサーバのステータスを適切に更新したりするために使用します。

サーバの選択をモニタすると、サーバの選択が変更される頻度を特定するのに役立ちます。サーバの選択は、ボトルネック、つまり、キュー内に大量の要求が存在するかどうかや、特定のサーバのみが着信要求を処理しているかどうかを分析するのに有効です。

debug aaa test コマンドの次のサンプル出力は、アイドル タイマーが期限切れになった日時を示しています。

例：

```
Device# debug aaa test

Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) quarantined.
Jul 16 00:07:01: AAA/SG/TEST: Sending test request(s) to server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Sending 1 Access-Requests, 1 Accounting-Requests in current batch.
Jul 16 00:07:01: AAA/SG/TEST(Req#: 1): Sending test AAA Access-Request.
Jul 16 00:07:01: AAA/SG/TEST(Req#: 1): Sending test AAA Accounting-Request.
Jul 16 00:07:01: AAA/SG/TEST: Obtained Test response from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Obtained Test response from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Necessary responses received from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) marked ALIVE. Idle timer set for 60
sec(s).
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) removed from quarantine.
```

ステップ 2 **debug aaa sg-server selection** コマンドを使用して、ロード バランシング用に選択されたサーバを特定します。

debug aaa sg-server selection コマンドの次のサンプル出力は、5 つのアクセス要求がバッチ サイズ 3 のサーバ グループに送信されていることを示しています。

例：

```
Device# debug aaa sg-server selection

Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [3] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [2] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [1] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: No more transactions in batch. Obtaining a new server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining a new least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[0] load: 3
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[1] load: 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[2] load: 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Selected Server[1] with load 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [3] transactions remaining in batch.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [2] transactions remaining in batch. Reusing server.
```

ステップ 3 **test aaa group** コマンドを使用して、RADIUS ロード バランシング サーバのステータスを手動で確認します。

次のサンプル出力は、ユーザ名「test」がユーザ プロファイルと一致しない場合の動作中の RADIUS ロード バランシング サーバからの応答を示しています。**test aaa group** コマンドを使用して生成された認証、認可、およびアカウンティング（AAA）パケットに対し、サーバが Access-Reject 応答を発行する場合、そのサーバは動作中であることが確認されます。

例：

```
Device# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6 on-for-login-auth"
 is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS:  authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS:  User-Password       [2]   18  *
00:06:07: RADIUS:  User-Name           [1]   6   "test"
00:06:07: RADIUS:  NAS-IP-Address      [4]   6   192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS:  authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS:  Reply-Message       [18]  24
00:06:07: RADIUS:   41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66  [Authentication f]
00:06:07: RADIUS:   61 69 6C 75 72 65                               [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
```

RADIUS サーバ ロード バランシングの設定例

例：グローバル RADIUS サーバ グループのロード バランシングの有効化

次の例は、グローバル RADIUS サーバ グループのロード バランシングを有効化する方法を示しています。これらの例は、RADIUS コマンド出力の現在の設定、デバッグ出力、認証、認可、およびアカウンティング（AAA）サーバのステータス情報という 3 つの部分からなります。区切り文字を使用して、設定の関連する部分を表示できます。

次の例は、関連する RADIUS 設定を示しています。

```
Device# show running-config | include radius

aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa authentication ppp** コマンドは RADIUS を使用してすべての PPP ユーザを認証します。
- **aaa accounting** コマンドは、クライアントが認証された後に **start-stop** キーワードを使用して切断されたときに、すべてのアカウンティング要求を AAA サーバに送信できるようにします。
- **radius-server host** コマンドは、指定された認可ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバ ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバ グループのロード バランシングを有効化します。

下の **show debug** サンプル出力は、設定に関する優先サーバの選択と要求の処理を示しています。

```
Device# show debug

General OS:
  AAA server group server selection debugging is on
#
<sending 10 pppoe requests>
Device#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now
being used as preferred server.
```

show aaa servers コマンドの次のサンプル出力は、グローバル RADIUS サーバ グループ設定に対する AAA サーバのステータスを示しています。

このサンプル出力は、2 つの RADIUS サーバのステータスを示しています。両方のサーバが稼働しており、最後の 2 分間に次の要求が正常に処理されました。

- 6 件の認証要求のうち 5 件
- 5 件のアカウンティング要求のうち 5 件

```
Device# show aaa servers

RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3303ms
```

```
            Transaction:success 5, failure 0
        Elapsed time since counters last cleared:2m
RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
        State:current UP, duration 3175s, previous duration 0s
        Dead:total time 0s, count 0
        Quarantined:No
        Authen:request 6, timeouts 1
                Response:unexpected 1, server error 0, incorrect 0, time 1955ms
                Transaction:success 5, failure 0
        Author:request 0, timeouts 0
                Response:unexpected 0, server error 0, incorrect 0, time 0ms
                Transaction:success 0, failure 0
        Account:request 5, timeouts 0
                Response:unexpected 0, server error 0, incorrect 0, time 3247ms
                Transaction:success 5, failure 0
        Elapsed time since counters last cleared:2m
```

例：サーバ設定とグローバル RADIUS サーバ グループに対するロード バランシングの有効化

次の例は、関連する RADIUS 設定を示しています。

```
Device# show running-config | include radius

aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa authentication ppp** コマンドは RADIUS を使用してすべての PPP ユーザを認証します。
- **aaa accounting** コマンドは、クライアントが認証された後に **start-stop** キーワードを使用して切断されたときに、すべてのアカウンティング要求を認証、認可、およびアカウンティング（AAA）サーバに送信できるようにします。
- **radius-server host** コマンドは、指定された認可ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバ ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバ グループのロード バランシングを有効化します。

例：グローバル RADIUS サーバ グループのデバッグ出力

下の **debug** コマンドの出力は、設定に関する優先サーバの選択と要求の処理を示しています。

```
Device# show debug

General OS:
  AAA server group server selection debugging is on
#
<sending 10 pppoe requests>
Device#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now
being used as preferred server.
```

例：グローバル RADIUS サーバ グループのサーバ ステータス情報

show aaa server コマンドの次のサンプル出力は、グローバル RADIUS サーバ グループ設定に対する AAA サーバのステータスを示しています。

```
Device# show aaa server

RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
```

```
             Response:unexpected 0, server error 0, incorrect 0, time 3303ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1955ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3247ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
```

このサンプル出力は、2 つの RADIUS サーバのステータスを示しています。両方のサーバが稼働しており、最後の 2 分間に次の要求が正常に処理されました。

- 6 つの認証要求のうち 5 つ
- 5 つのアカウンティング要求のうち 5 つ

例：名前付き RADIUS サーバ グループのロード バランシングの有効化

次の例は、名前付き RADIUS サーバ グループで有効化されたロード バランシングを示しています。これらの例は、RADIUS コマンド出力の現在の設定、デバッグ出力、認証、認可、およびアカウンティング（AAA）サーバのステータス情報という 3 つの部分からなります。

次のサンプル出力は、関連する RADIUS 設定を示しています。

```
Device# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
Device(config-sg-radius)# load-balance method least-outstanding batch-size 30
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa group server radius** コマンドは、2 つのメンバー サーバからなるサーバ グループの設定を表示します。
- **load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバ グループのロード バランシングを有効化します。
- **aaa authentication ppp** コマンドは RADIUS を使用してすべての PPP ユーザを認証します。

- **aaa accounting** コマンドは、クライアントが認証された後に **start-stop** キーワードを使用して切断されたときに、すべてのアカウンティング要求を AAA サーバに送信できるようにします。

下の show debug サンプル出力は、前の設定に関する優先サーバの選択と要求の処理を示しています。

```
Device# show debug

*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

show aaa servers コマンドの次のサンプル出力は、名前付き RADIUS サーバ グループ設定に対する AAA サーバのステータスを示しています。

このサンプル出力は、2 つの RADIUS サーバのステータスを示しています。両方のサーバが動作中ですが、カウンタが 0 分前にクリアされて以降は、どの要求も処理されていません。

```
Device# show aaa servers

RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
```

例：サーバ設定と名前付き RADIUS サーバ グループに対するロード バランシングの有効化

次のサンプル出力は、関連する RADIUS 設定を示しています。

```
Device# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa group server radius** コマンドは、2 つのメンバー サーバからなるサーバ グループの設定を表示します。

- **load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバ グループのロード バランシングを有効化します。
- **aaa authentication ppp** コマンドは RADIUS を使用してすべての PPP ユーザを認証します。
- **aaa accounting** コマンドは、クライアントが認証された後に **start-stop** キーワードを使用して切断されたときに、すべてのアカウンティング要求を AAA サーバに送信できるようにします。

例：名前付き RADIUS サーバ グループのデバッグ出力

下のデバッグ サンプル出力は、上の設定に関する優先サーバの選択と要求の処理を示しています。

```
Device# show debug

*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
 server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
```

```
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

例：名前付き RADIUS サーバ グループのサーバ ステータス情報

show aaa servers コマンドの次のサンプル出力は、名前付き RADIUS サーバ グループ設定に対する AAA サーバのステータスを示しています。

```
Device# show aaa servers

RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
```

このサンプル出力は、2 つの RADIUS サーバのステータスを示しています。両方のサーバが動作中ですが、カウンタが 0 分前にクリアされて以降は、どの要求も処理されていません。

例：アイドル タイマーのモニタリング

次の例は、名前付き RADIUS サーバ グループに対して有効にされたロード バランシングに関するアイドル タイマーと関連するサーバ状態を示しています。RADIUS コマンド出力と debug コマンド出力の現在の設定も表示されます。

次のサンプル出力は、関連する RADIUS 設定を示しています。

```
Device# show running-config | include radius
```

```
aaa group server radius server-group1
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 test username junk1 idle-time
 1 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 test username junk1 idle-time
 1 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa group server radius** コマンドは、サーバ グループの設定を表示します。
- **radius-server host** コマンドは、指定された認可ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバ ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定された RADIUS サーバのロード バランシングを有効化します。

下の **show debug** サンプル出力は、サーバに送信されるテスト要求を示しています。サーバに送信されたテスト要求に対する応答が受信され、必要に応じて、隔離からサーバが除外され、サーバが動作中としてマークされてから、アイドル タイマーがリセットされます。

```
Device# show debug

*Feb 28 13:52:20.835:AAA/SG/TEST:Server (192.0.2.238:2015,2016) quarantined.
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending test request(s) to server (192.0.2.238:2015,2016)
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending 1 Access-Requests, 1 Accounting-Requests in
current batch.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Access-Request.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Accounting-Request.
*Feb 28 13:52:21.087:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Necessary responses received from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) marked ALIVE. Idle timer
 set for 60 secs(s).
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) removed from quarantine.
.
.
.
```

例：サーバ設定とアイドル タイマー モニタリングに対するロード バランシングの有効化

次のサンプル出力は、関連する RADIUS 設定を示しています。

```
Device# show running-config | include radius

aaa group server radius server-group1
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 test username junk1 idle-time
 1 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 test username junk1 idle-time
 1 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記の RADIUS コマンド出力のうち、現在の設定に関する行は次のように定義されます。

- **aaa group server radius** コマンドは、サーバ グループの設定を表示します。

- **radius-server host** コマンドは、指定された認可ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバ ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定された RADIUS サーバのロード バランシングを有効化します。

例：アイドル タイマー モニタリングのデバッグ出力

下の **debug** コマンドの出力は、サーバに送信されるテスト要求を示しています。サーバに送信されたテスト要求に対する応答が受信され、必要に応じて、隔離からサーバが除外され、動作中としてマークされてから、アイドル タイマーがリセットされます。

```
Device# show debug
*Feb 28 13:52:20.835:AAA/SG/TEST:Server (192.0.2.238:2015,2016) quarantined.
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending test request(s) to server (192.0.2.238:2015,2016)
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending 1 Access-Requests, 1 Accounting-Requests in
current batch.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Access-Request.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Accounting-Request.
*Feb 28 13:52:21.087:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Obtained Test response from server (192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Necessary responses received from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) marked ALIVE. Idle timer
 set for 60 secs(s).
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) removed from quarantine.
.
.
.
```

例：認証サーバと認可サーバが同じ優先サーバの設定

次の例は、サーバの 209.165.200.225 と 209.165.200.226 を共有する認証サーバ グループと認可サーバ グループを示しています。両方のサーバ グループで優先サーバ フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
aaa group server radius accounting-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
```

あるセッションで優先サーバが選択されると、そのセッションのすべてのトランザクションでオリジナルの優先サーバの使用が継続されます。サーバの 209.165.200.225 と 209.165.200.226 は、トランザクションではなく、セッションに基づいてロード バランシングされます。

例：認証サーバと認可サーバが別々の優先サーバの設定

次の例は、サーバの 209.165.200.225 と 209.165.200.226 を使用する認証サーバ グループとサーバの 209.165.201.1 と 209.165.201.2 を使用する認可サーバ グループを示しています。両方のサーバ グループで優先サーバ フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
aaa group server radius accounting-group
   server 209.165.201.1 key radkey3
   server 209.165.201.2 key radkey4
```

認証サーバ グループとアカウンティング サーバ グループはどの共通サーバも共有しません。アカウンティング トランザクションでは優先サーバは検出されないため、認証サーバとアカウンティング サーバはトランザクションに基づいてロードバランシングされます。1 つのセッションで開始レコードと終了レコードが同じサーバに送信されます。

例：認証サーバと認可サーバが重複している優先サーバの設定

次の例は、サーバの 209.165.200.225、209.165.200.226、および 209.165.201.1 を使用する認証サーバ グループとサーバの 209.165.201.1 と 209.165.201.2 を使用する認可サーバ グループを示しています。両方のサーバ グループで優先サーバ フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3
aaa group server radius accounting-group
   server 209.165.201.1 key radkey3
   server 209.165.201.2 key radkey4
```

すべてのサーバのトランザクション処理能力が同じ場合は、すべての認証トランザクションの 1/3 がサーバの 209.165.201.1 に転送されます。したがって、すべてのアカウンティング トランザクションの 1/3 もサーバの 209.165.201.1 に転送されます。アカウンティング トランザクションの残りの 2/3 は、サーバの 209.165.201.1 と 209.165.201.2 の間で均等にロード バランシングされます。サーバの 209.165.201.1 に未処理のアカウンティング トランザクションがあるため、サーバの 209.165.201.1 が受信する認証トランザクション数は減少します。

例：認証サーバが認可サーバのサブセットである優先サーバの設定

次の例は、サーバの 209.165.200.225 と 209.165.200.226 を使用する認証サーバ グループと、サーバの 209.165.200.225、209.165.200.226、および 209.165.201.1 を使用する認可サーバ グループを示しています。両方のサーバ グループで優先サーバ フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
aaa group server radius accounting-group
  server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3
```

すべての認証トランザクションの半分がサーバの 209.165.200.225 に送信され、残りの半分がサーバの 209.165.200.226 に送信されます。サーバの 209.165.200.225 と 209.165.200.226 は、認証およびアカウンティング トランザクションの優先サーバです。そのため、認証およびアカウンティング トランザクションは、サーバの 209.165.200.225 と 209.165.200.226 に均等に分配されます。サーバの 209.165.201.1 は相対的に使用されません。

例：認証サーバが認可サーバのスーパーセットである優先サーバの設定

次の例は、サーバの 209.165.200.225、209.165.200.226、および 209.165.201.1 を使用する認証サーバ グループとサーバの 209.165.200.225 と 209.165.200.226 を使用する認可サーバ グループを示しています。両方のサーバ グループで優先サーバ フラグが有効になっています。

```
aaa group server radius authentication-group
   server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
   server 209.165.201.1 key radkey3
aaa group server radius accounting-group
  server 209.165.200.225 key radkey1
   server 209.165.200.226 key radkey2
```

最初に、認証トランザクションの 1/3 が認可サーバ グループ内の各サーバに割り当てられます。追加のセッションに対してアカウンティング トランザクションが生成されますが、優先サーバ フラグがオンになっているため、アカウンティング トランザクションはサーバの 209.165.200.225 と 209.165.200.226 に送信されます。サーバの 209.165.200.225 と 209.165.200.226 がトランザクションの処理を開始しますが、認証トランザクションはサーバの 209.165.201.1 に送信されます。サーバの 209.165.201.1 で認証されたトランザクション要求は、どの優先サーバ設定も含まず、サーバの 209.165.200.225 と 209.165.200.226 に分配されるため、優先サーバ フラグの使用が無効になります。この設定は慎重に使用する必要があります。

RADIUS サーバ ロード バランシングのその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	Cisco IOS Master Command List, All Releases
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
AAA および RADIUS	『*Authentication, Authorization, and Accounting Configuration Guide*』

関連項目	マニュアル タイトル
AAA サーバ グループと RADIUS 設定	『*RADIUS Configuration Guide*』の「Configuring RADIUS」モジュール
フェールオーバー再試行順序変更モード	『*RADIUS Configuration Guide*』の「RADIUS Server Reorder on Failure」モジュール

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/en/US/support/index.html

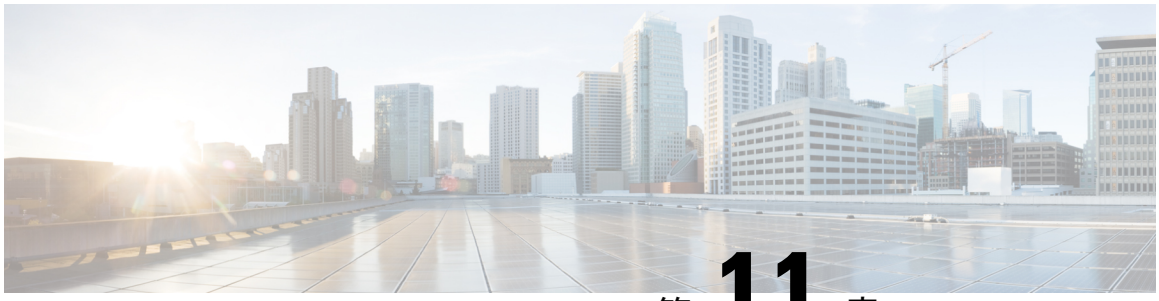
RADIUS サーバ ロード バランシングの機能情報

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 *13 : RADIUS* サーバ ロード バランシングの機能情報

機能名	リリース	機能情報
RADIUS サーバ ロード バランシング	12.2(28)SB 12.4(11)T 12.2(33)SRC	RADIUS サーバ ロード バランシング機能は、認証、認可、およびアカウンティング（AAA）の認証トランザクションとアカウンティング トランザクションをサーバ グループ内のサーバに分配します。これらのサーバは、トランザクションの負荷を分担し、空いているサーバを効率的に使用して着信要求に対するより迅速な応答を実現します。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.4(11)T に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 次のコマンドが導入または変更されました。**debug aaa sg-server selection**、**debug aaa test**、**load-balance (server-group)**、**radius-server host**、**radius-server load-balance**、**test aaa group.**
RADIUS サーバ ロード バランシング ポーティング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。



第 11 章

RADIUS サーバ障害発生時順序変更

RADIUS サーバ障害発生時順序変更機能は、高負荷期間またはサーバで障害が発生した場合に、サーバ グループ内の別のサーバへのフェールオーバーを提供します。障害発生後は、すべての RADIUS トラフィックが新しいサーバに転送されます。新しいサーバからサーバ グループ内の別のサーバにトラフィックが切り替えられるのは、新しいサーバでも障害が発生した場合に限られます。トラフィックが自動的に最初にサーバに戻されることはありません。

RADIUS トランザクションを複数のサーバに分散させることによって、認証要求とアカウンティング要求がより迅速に処理されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RADIUS サーバ障害発生時順序変更の前提条件

- 障害発生時に順序変更を実行するように RADIUS サーバを設定する前に、**aaa new-model** コマンドを使用して、認証、認可、およびアカウンティング（AAA）を有効にする必要があります。
- 認証、アカウンティング、スタティック ルート ダウンロードなどの機能用に RADIUS を設定する必要もあります。

RADIUS サーバ障害発生時順序変更の制約事項

- サーバ グループごとに新しい4バイトのメモリが消費されます。ただし、ほとんどのサーバは少数のサーバ グループのみに設定されているため、追加の4バイトはそれほど性能に影響しない可能性があります。
- ソフトウェア セット内の RADIUS 機能によっては、この機能を使用できない場合があります。RADIUS機能でRADIUSサーバ障害発生時順序変更機能を使用できない場合は、順序変更機能が設定されていないかのようにサーバが動作します。

RADIUS サーバ障害発生時順序変更に関する情報

RADIUS サーバの障害

RADIUSサーバ障害発生時順序変更機能が設定されていない状態でサーバの障害が発生した場合：

1. 新しい RADIUS トランザクションを実行する必要があります。
2. トランザクション用のRADIUSパケットが、グループ内で停止中としてマークされていない（設定されたデッドタイムに従って）最初のサーバに送信され、設定された再送回数だけ再送されます。
3. 再送のすべてがタイムアウトした（設定されたタイムアウトに従って）場合は、ルータがそのパケットをリストで次の非停止中サーバに設定された再送回数だけ送信します。
4. ステップ 3 は、トランザクションごとに指定された最大送信回数に達するまで繰り返されます。最大送信回数に到達する前にリストの最後に到達した場合は、ルータがリストの先頭に戻ってそこから処理を継続します。

このプロセスのどの時点でも、サーバが停止中サーバの検出基準（設定不可。使用されているソフトウェアのバージョンによって異なる）を満たした場合は、設定されたデッドタイムに合わせてサーバが停止中としてマークされます。

RADIUS サーバ障害発生時順序変更機能の動作方法

RADIUSサーバ障害発生時順序変更機能を設定した場合は、次のように、初期サーバとして使用する RADIUS サーバが決定されます。

- ネットワーク アクセス サーバ（NAS）は、トランスミッションが送信される最初のサーバである「フラグ設定された」サーバのステータスを保持します。
- フラグ設定されたサーバにトランスミッションが送信された後は、設定された再送回数だけ、フラグ設置されたサーバにトラフィックが再送されます。
- その後は、NASが、フラグ設定されたサーバの次にリストされたサーバから始めて、設定されたトランザクションの最大再試行回数に到達するか、応答が返されるまで、サーバグループ内の非停止中サーバのリストの順にトランスミッションを送信します。
- 起動時は、**radius-server host** コマンドを使用して設定されたように、フラグ設定されたサーバがサーバ グループ リストで最初のサーバになります。
- フラグ設定されたサーバが停止中としてマークされている場合は（デッドタイムが0の場合でも）、フラグ設定されたサーバの次にリストされた最初の非停止中サーバがフラグ設定されたサーバになります。
- フラグ設定されたサーバが、リスト内の最後のサーバで、停止中としてマークされている場合は、フラグ設定されたサーバがリスト内で停止中としてマークされていない最初のサーバになります。
- すべてのサーバが停止中としてマークされている場合は、トランザクションが失敗して、フラグ設定されたサーバへの変更が実施されません。
- フラグ設定されたサーバが停止中としてマークされており、デッドタイマーが切れた場合は、何も行われません。

（注） トランスミッションのタイプ（チャレンジハンドシェーク認証プロトコル（CHAP）、Microsoft CHAP（MS-CHAP）、拡張可能認証プロトコル（EAP））によっては、1 つのサーバを何度も往復しなければならない場合があります。これらの特別なトランザクションでは、サーバのラウンドトリップの全シーケンスは、1 つのトランスミッションと同じように処理されます。

RADIUS サーバが停止中の場合

次の 1 と 2 の基準が満たされた場合に、サーバを停止中としてマークすることができます。

1. **radius-server transaction max-tries** コマンドで指定された再送信回数を超えてサーバが応答しなかった場合。
2. 設定されたタイムアウトまでどの要求にもサーバが応答しなかった場合。両方の基準（これと上の基準）が満たされた場合にのみ、サーバが停止中としてマークされます。デッドタイムが 0 の場合でも、サーバを停止中としてマークすると、RADIUS サーバの再試行方式順序変更システムに重大な影響を及ぼします。

RADIUS サーバ障害発生時順序変更の設定方法

RADIUS サーバ障害発生時順序変更の設定

このタスクを実行して、サーバグループ内のあるサーバを、最初のサーバで障害が発生した場合に別のサーバにトラフィックを転送するように設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server retry method reorder**
5. **radius-server retransmit** {*retries*}
6. **radius-server transaction max-tries {** *number* **}**
7. **radius-server host { *hostname* | *ip-address* } [key *string*]**
8. **radius-server host { *hostname* | *ip-address* } [key *string*]**

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。 • 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： `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。
ステップ 4	**radius-server retry method reorder** 例： 例： `Router (config)# radius-server retry method reorder`	サーバ グループ内の RADIUS トラフィック エントリの順序変更を指定します。

	コマンドまたはアクション	目的
ステップ 5	**radius-server retransmit** {*retries*} 例： `Router (config)# radius-server retransmit 1`	Cisco IOS XE ソフトウェアが RADIUS サーバ ホストのリストを検索する回数の最大値を指定します。 *retries* 引数は、再送信の最大試行回数です。デフォルトは 3 回に設定されています。
ステップ 6	**radius-server transaction max-tries {** *number* **}** 例： `Router (config)# radius-server transaction max-tries 3`	RADIUS サーバ上で試行可能なトランザクション当たりのトランスミッション数の最大値を指定します。 *number* 引数は、トランザクション当たりのトランスミッション数の総数です。このコマンドが設定されなかった場合のデフォルトは 8 トランスミッションです。 （注） このコマンドは、特定のトランザクションに関係するすべての RADIUS サーバに適用されます。
ステップ 7	**radius-server host** { *hostname* | *ip-address* } **[key** *string* **]** 例： `Router (config)# radius-server host 10.2.3.4 key radi23`	RADIUS サーバ ホストを指定します。 （注） **radius-server key** コマンドを発行することによって、サーバ単位キーが設定されていないすべての RADIUS サーバのグローバル キーを設定することもできます。
ステップ 8	**radius-server host** { *hostname* | *ip-address* } **[key** *string* **]** 例： `Router (config)# radius-server host 10.5.6.7 key rad234`	RADIUS サーバ ホストを指定します。 （注） 少なくとも 2 つのサーバを設定する必要があります。

RADIUS サーバ障害発生時順序変更のモニタリング

ルータ上でサーバ障害発生時順序変更プロセスをモニタするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **debug aaa sg-server selection**
3. **debug radius**

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。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug aaa sg-server selection** 例： `Router# debug aaa sg-server selection`	ルータ内の RADIUS および TACACS+ サーバ グループ システムが特定のサーバを選択している理由に関する情報を表示します。
ステップ 3	**debug radius** 例： `Router# debug radius`	ルータが特定の RADIUS サーバを選択している理由に関する情報を表示します。

例

デバッグ 1

デバッグ 2

次の 2 つのデバッグ出力は、RADIUS サーバ障害発生時順序変更機能の動作を示しています。

次のサンプル出力では、RADIUS サーバ障害発生時順序変更機能が設定されています。サーバの再送は 0（したがって、次に設定されたサーバへのフェールオーバー前に、各サーバが一度だけ試行される）に設定され、トランザクション当たりのトランスミッション数は 4（3 回めのフェールオーバーでトランスミッション終了）に設定されています。サーバ グループ内で 3 番めのサーバ（10.107.164.118）が、3 回めのトランスミッション（2 回めのフェールオーバー）のトランザクションを受け入れています。

```
00:38:35: %SYS-5-CONFIG-I: Configured from console by console
00:38:53: RADIUS/ENCODE(OOOOOOOF) : ask "Username: "
00:38:53: RADIUS/ENCODE (0000000F) : send packet; GET-USER
00:38:58: RADIUS/ENCODE (0000000F) : ask "Password: "
00:38:58: RADIUS/ENCODE(0000000F) : send packet; GET-PASSWORD
00:38:59: RADIUS: AAA Unsupported [152] 4
00:38:59: RADIUS: 7474 [tt]
00:38:59: RADIUS (0000000F) : Storing nasport 2 in rad-db
00:38:59: RADIUS/ENCODE(0000000F) : dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:38:59: RADIUS (0000000F) : Config NAS IP: 0.0.0.0
00:38:59: RADIUS/ENCODE (0000000F) : acct-session-id: 15
00:38:59: RADIUS (0000000F) : sending
00:38:59: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.1.1.1
00:38:59: RAPIUS(0000000F) : Send Access-Request to 10.10.10.10:1645 id 21645/11, len
78
```

```
00:38:59: RADIUS:: authenticator 4481 E6 65 2D 5F 6F OA -lE F5 81 8F 4E 1478 9C
00:38:59: RADIUS: User-Name [1] 7 "username1"
00:38:59: RADIUS: User-Password [2] 18 *
00:38:59: RADIUS: NAS-Port fSl 6 2
00:~8:59: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
00:38:59: RADIUS: Calling-Station-Id [31] 15 "10.19.192.23"
00:39:00: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:39:02: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/11
00:39:02: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.2.2.2
00:39:04: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/11
00:39:04: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 128.107.164.118
00:39:05: RADIUS: Received from id 21645/11 10.107.164.118:1645, Access-Accept, len 26
00:39:05: RADIUS: authenticator 5609 56 F9 64 4E DF 19- F3 A2 DD 73 EE 3F 9826
00:39:05: RADIUS: Service-Type [6] 6 Login [1]
```

次のサンプル出力では、RADIUSサーバ障害発生時順序変更機能が設定されています。サーバの再送は 0 に設定され、トランザクション当たりのトランスミッション数は 8 に設定されています。このトランザクションでは、サーバ10.10.10.0へのトランスミッションが 8 回めで失敗します。

```
00:42:30: RADIUS(00000011): Received from id 21645/13
00:43:34: RADIUS/ENCODE(00000012) : ask "Username: "
00:43:34: RADIUS/ENCODE(00000012) : send packet; GET-USER
00:43:39: RADIUS/ENCODE(00000012) : ask "Password: "
00:43:39: RADIUS/ENCODE(00000012) : send packet; GET-PASSWORD
00:43:40: RADIUS: AAA Unsupported [152] 4
00:43:40: RADIUS: 7474 [tt]
00:43:40: RADIUS(00000012) : Storing nasport 2 in rad-db
00:43:40: RADIUS/ENCODE(00000012): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:43:40: RADIUS(00000012) : Co~fig NAS IP: 0.0.0.0
00:43:40: RADIUS/ENCODE(00000012) : acct-session-id: 18
00:43:40: RADIUS(00000012) : sending
00:43:40: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
 00:43:40: RADIUS(00000012) : Send Access-Request to 10.107.164.118:1645 id 21645/14,
len 78 00:43:40: RADIUS: authenticator B8 OA 51 3A AF A6 0018 -B3 2E 94 5E 07 OB 2A IF
00:43:40: RADIUS: User-Name [1] 7 "username1" 00:43:40: RADIUS: User-Password [2] 18 *
00:43:40: RADIUS: NAS-Port [5] 6 2
00:43:40: RADIUS: NAS-Port-Type [61] 6 Virtual [5] 00:43:40: RADIUS: Calling-Station-]d
 [31] 15 "172.19.192.23" 00:43:40: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:43:42: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:42: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:44: RADius: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:44: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2
00:43:46: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:46: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
 00:43:48: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:48: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:50: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:50: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2
00:43:52: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:52: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
 00:43:54: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:54: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:56: RADIUS: No response from (10.10.10.10:1645,1646) for id 21645/14 00:43:56:
RADIUS/DECODE: parse response no app start; FAIL 00:43:56: RADIUS/DECODE: parse response;
 FAIL
```

RADIUS サーバ障害発生時順序変更の設定例

RADIUS サーバで障害発生時の順序変更を設定する例

次の設定例は、RADIUS サーバが障害発生時に順序変更されるように設定されます。RADIUS サーバ上で試行可能なトランザクション当たりのトランスミッション数の最大値は 6 です。

```
aaa new-model

radius-server retry method reorder

radius-server retransmit 0

radius-server transaction max-tries 6

radius-server host 10.2.3.4 key rad123

radius-server host 10.5.6.7 key rad123
```

RADIUS サーバが停止中の送信順序の決定

起動時に次のように設定し、

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 0
Router(config)# radius-server transaction max-tries 6
Router(config)# radius-server host 10.2.3.4
Router(config)# radius-server host 10.5.6.7
```

両方のサーバがダウンしているが、まだ、停止中としてマークされていない場合は、最初のトランザクションで、次のようなトランスミッションが見られます。

```
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
```

順序変更を次のように設定し、

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 1
Router(config)# radius-server transaction max-tries 3
Router(config)# radius-server host 10.2.3.4
Router(config)# radius-server host 10.4.5.6
```

両方の RADIUS サーバが RADIUS パケットに応答していないが、まだ、停止中としてマークされていない（NASの起動後のため）場合は、最初のトランザクションのトランスミッションが次のようになります。

```
10.2.3.4
10.2.3.4
10.4.5.6
```

以降のトランザクションは、別のパターンに従って転送されます。トランスミッションは、どちらか（または両方）のサーバを停止中としてマークする基準が満たされているかどうかと、前述したサーバのフラグ設定パターンによって異なります。

順序変更を次のように設定し、

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 1
Router(config)# radius-server max-tries-per-transaction 8
Router(config)# radius-server host 10.1.1.1
Router(config)# radius-server host 10.2.2.2
Router(config)# radius-server host 10.3.3.3
Router(config)# radius-server timeout 3
```

RADIUS サーバ 10.1.1.1 が RADIUS パケットに応答していないが、まだ、停止中としてマークされておらず、残りの 2 つの RADIUS サーバが動作中の場合は、次のように表示されます。

最初のトランザクションの場合：

```
10.1.1.1
10.1.1.1
10.2.2.2
```

サーバが停止中としてマークされる前に任意のトランスミッションに対して開始された追加のトランザクションの場合：

```
10.1.1.1
10.1.1.1
10.2.2.2
```

その後開始されたトランザクションの場合：

```
10.2.2.2
```

その後で、サーバの 10.2.2.2 と 10.3.3.3 もダウンした場合は、サーバの 10.2.2.2 と 10.3.3.3 が停止中としてマークされる基準を満たすまで、次のようなトランスミッションが見られます。

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
10.1.1.1
10.2.2.2
10.2.2.2
```

この後に、トランスミッションが失敗し、方式リスト内で次の方式が使用されます（存在する場合）。

サーバの 10.2.2.2 と 10.3.3.3 がダウンしたが、同時に、サーバ 10.1.1.1 が復旧した場合は、次のようになります。

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
```

その後で、サーバの 10.2.2.2 と 10.3.3.3 が停止中としてマークされると、次のようになります。

```
10.1.1.1
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
RADIUS	『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』の「Configuring RADIUS」
AAA コマンドと RADIUS コマンド	『*Cisco IOS Security Command Reference*』
AAA の有効化	『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』の「Authentication, Authorization, and Accounting (AAA)」
セキュリティ コマンド	『*Cisco IOS* セキュリティ コマンド リファレンス』

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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、Cisco IOS XE ソフトウェア リリース、およびフィーチャ 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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC の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。 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。 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。	http://www.cisco.com/en/US/support/index.html

RADIUS サーバ障害発生時順序変更の機能情報

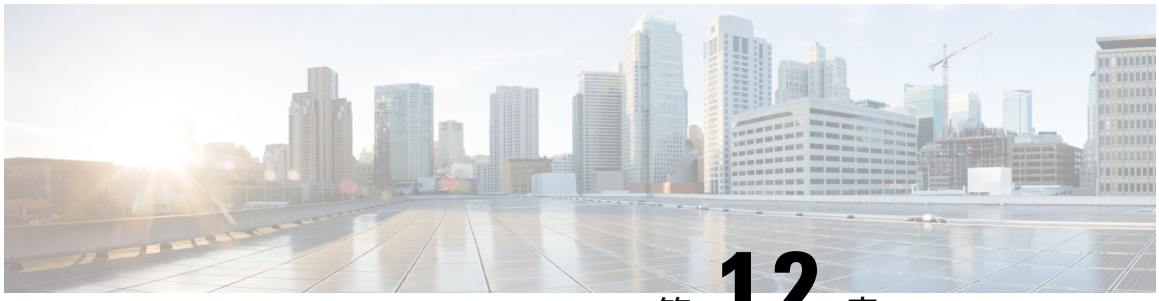
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

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 *14 : RADIUS* サーバ障害発生時順序変更の機能情報

機能名	リリース	機能情報
RADIUS サーバ障害発生時順序変更	Cisco IOS XE Release 2.1	RADIUS サーバ障害発生時順序変更機能は、高負荷期間またはサーバで障害が発生した場合に、サーバ グループ内の別のサーバへのフェールオーバーを提供します。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 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。 **debug aaa sg-server selection, radius-server retry method reorder, radius-server transaction max-tries.**



第 12 章

アカウンティングの RADIUS 個別再送信カウンタ

RADIUS：アカウンティングの個別再送信カウンタ機能を使用すると、指数バックオフ再送信を設定することができます。つまり、標準設定された再送信が再試行された後に、ルータは、設定された最大間隔に達するまで各再送信の失敗時に間隔を2倍にして試行を継続します。この機能により、RADIUS サーバが復旧したときにサーバに負荷をかけすぎることなく、長時間にわたってアカウンティング要求を再送信することができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

アカウンティングの RADIUS 個別再送信カウンタの制約事項

次のタスクでは、ルータのメモリが過剰に消費されます。

- ルータ上でこの機能を高い発信レートで設定。
- **aaa accounting send stop-record authentication failure** コマンドを設定：これにより、RADIUS サーバがダウンしている間、認証に失敗する各ユーザに対してアカウンティング レコードと RADIUS パケットが生成されます。
- 中間アカウンティングの設定：新しいアカウンティング レコードが生成され、ルータに保存されます。

アカウンティングの RADIUS 個別再送信カウンタに関する情報

アカウンティング要求の再送信のしくみ

多くの環境では、認証およびアカウンティングに単一の RADIUS サーバが使用されます。このサーバが約 24 時間にわたってダウンすると、認証、認可、およびアカウンティング（AAA）がすべての再送信を行った後に、ルータ上に保持されているユーザのアカウンティング レコードは失われます。この機能を導入する前に、再送信の再試行が最大 100 回に設定され、タイムアウトが 1,000 秒に設定されている可能性があります。このような設定では、ルータ上のアカウンティング レコードが 24 時間保持されますが、タイムアウトが 1,000 秒の設定は、ネットワークの輻輳が原因で RADIUS サーバに接続できないときに問題が発生するため、適切ではありません。

RADIUS：アカウンティングの個別再送信カウンタ機能を使用すると、指数バックオフ再送信を設定することができます。つまり、標準設定された再送信が再試行された後に、ルータは、設定された最大間隔に達するまで各再送信の失敗時に間隔を 2 倍にして試行を継続します。この機能により、RADIUS サーバが復旧したときにサーバに負荷をかけすぎることなく、長時間にわたってアカウンティング要求を再送信することができます。

この機能は、グローバルに設定（**radius-server backoff exponential** コマンドを使用）、サーバごとに設定（**radius-server host** コマンドを使用）、またはグループごとに設定（**backoff exponential** コマンドを使用）できます。

利点

この機能を使用すると、RADIUS サーバまたはサーバへの接続がダウンし、アカウンティング応答の確認がない場合に、RADIUS クライアント（ルータ）がアカウンティング要求を RADIUS サーバに送信する時間を延長できます。この機能により、アカウンティング レコードを最大 24 時間、ルータ上に保持できます。

アカウンティングの RADIUS 個別再送信カウンタの設定方法

アカウンティングの再送信カウンタのグローバル設定または RADIUS ホストごとの設定

拡張された期間での RADIUS 再送信の指数バックオフをグローバルおよび RADIUS ホストごとに設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **radius-server backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *retransmits*
4. Router(config)# **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **key** *encryption-key* | **max-delay** *minutes*}]

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 モードを開始します。 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： `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	Router(config)# **radius-server backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *retransmits* 例：	アカウンティング要求の指数バックオフ再送信をルータで設定します。

	コマンドまたはアクション	目的
	`Router (config)# radius-server backoff exponential max-delay 60 backoff-retry 32`	
ステップ 4	Router(config)# **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **key** *encryption-key* | **max-delay** *minutes*}] 例： `Router (config)# radius-server host 192.0.2.1 test username test1 auth-port 1645 acct-port 1646`	RADIUS サーバホストを指定し、アカウンティング要求の指数バックオフ再送信を行うように設定します。

アカウンティングの再送信カウンタの RADIUS サーバ グループごとの設定

RADIUS サーバ グループごとに拡張された期間で RADIUS 再送信の指数バックオフを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa group server radius** *group-name*
4. Router(config -sg-radius)# **backoff exponential max-delay** *minutes*] [**backoff-retry** *retransmits*

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 モードを開始します。 • 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： `Router (config)# 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。

	コマンドまたはアクション	目的
ステップ 3	Router(config)# **aaa group server radius** *group-name*	異なる RADIUS サーバ ホストを別々のリストと方式にグループ化し、server-group RADIUS 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	Router(config -sg-radius)# **backoff exponential max-delay** *minutes*] [**backoff-retry** *retransmits*	RADIUS サーバ グループごとのアカウンティング要求の指数バックオフ再送信をルータで設定します。

再送信設定の確認

機能を確認するには、次のいずれかの EXEC コマンドを使用します。

手順の概要

1. **enable**
2. **debug radius**
3. **show accounting**
4. **show radius statistics**

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 モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug radius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。
ステップ 3	**show accounting** 例： `Router# show accounting`	すべてのアクティブセッションを表示し、アカウントがアクティブな機能のすべてのアカウンティングレコードを出力します。
ステップ 4	**show radius statistics** 例： `Router# show radius statistics`	アカウンティング パケットについての RADIUS 統計情報を表示します。

アカウンティングの RADIUS 個別再送信カウンタの設定例

ここでは、次の設定例について説明します。

アカウンティングの再送信カウンタの包括的な設定例

次の例は、ルータでアカウンティング要求の指数バックオフ再送信を設定する方法を示します。この例では、指数バックオフはグローバル（**radius-server backoff exponential** コマンドを使用）およびRADIUS サーバホスト「172.107.164.206」（**radius-server host** コマンドを使用）に設定されています。

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization exec default group radius
aaa authorization network default group radius
aaa accounting send stop-record authentication failure
aaa accounting update periodic 1
aaa accounting network default start-stop group radius
!
radius-server host 172.107.164.206 auth-port 1645 acct-port 1646 backoff exponential
max-delay 60 backoff-retry 32
radius-server backoff exponential max-delay 60 backoff-retry 32
radius-server retransmit 3
radius-server key rad123
end
```

サーバごとの設定例

次に、サーバ単位で指数バックオフ再送信を有効化する例を示します。この例では、再送信は 3 回の再試行に設定され、タイムアウトは 5 秒に設定されると想定します。つまり、RADIUS 要求は 5 秒間の遅延で 3 回送信されます。その後、ルータは、再試行が 32 回になるまで、各再試行時に遅延間隔を 2 倍にして RADIUS 要求の再送信を継続します。ルータは、再送信間隔が設定された 60 分を超えると、間隔を 2 倍にする操作を中止し、その後は 60 分ごとに送信します。

```
radius-server host foo.xyz.com backoff exponential max-delay 60 backoff-retry 32
```

このコマンドを有効にすると、次のように再送信が実行されます（「t」は秒単位）。

```
t = 0 req sent
t = 5 retrans 1
t = 10 retrans 2
t = 15 retrans 3
t = 25 retrans 4
t = 45 retrans 5
t = 85 retrans 6
t = 165 retrans 7
```

```
t = 325 retrans 8
t = 645 retrans 9
t = 1285 retrans 10
t= 2565 retrans 11
t = 5125 retrans 12
t = 8725 retrans 13 (The interval has stabilized to 60 minutes here).
t = 12325 retrans 14 till retransmit 35
```

すべての再送信が完了すると、RADIUS要求は、通常の再送信がすべて完了したときと同じパスに従います。

その他の参考資料

次の項で、RADIUS：アカウンティングの個別再送信カウンタに関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUSおよびAAAアカウンティング設定のタスクとコマンド	• 『*Cisco IOS XE Security Configuration Guide: Configuring User Services* , Release 2』の「Configuring RADIUS」および「Configuring Accounting」の章 • 『Cisco IOS Security Command Reference』

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しいMIBまたは変更されたMIBはありません。またこの機能による既存MIBの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、Cisco IOS XE ソフトウェア リリース、およびフィーチャ 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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

テクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/en/US/support/index.html

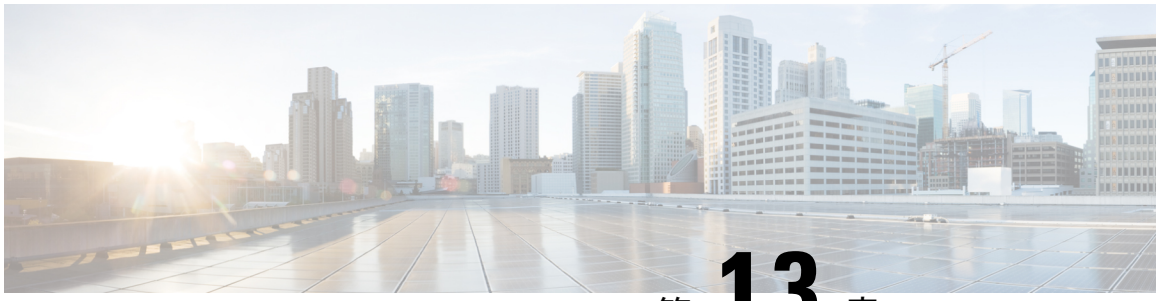
アカウンティングの RADIUS 個別再送信カウンタの機能情報

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 *15 : RADIUS* の機能情報：アカウンティングの個別再送信カウンタ

機能名	リリース	機能情報
RADIUS：アカウンティングの個別再送信カウンタ	Cisco IOS XE Release 2.1	RADIUS：アカウンティングの個別再送信カウンタ機能を使用すると、指数バックオフ再送信を設定することができます。つまり、標準設定された再送信が再試行された後に、ルータは、設定された最大間隔に達するまで各再送信の失敗時に間隔を 2 倍にして試行を継続します。この機能により、RADIUS サーバが復旧したときにサーバに負荷をかけすぎることなく、長時間にわたってアカウンティング要求を再送信することができます。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズアグリゲーションサービスルータに導入されました。 次のコマンドが導入または変更されました。**backoff exponential**、**radius-server host**、**radius-server backoff exponential**



第 13 章

RADIUS VC ロギング

RADIUS 仮想回線（VC）ロギングを使用すると、着信サブスクライバ セッションの仮想パス インターフェイス（VPI）と仮想回線インターフェイス（VCI）を Cisco IOS XE で正確に記録できます。

RADIUS VC ロギングを有効にすると、RADIUS ネットワーク アクセス サーバ（NAS）のポート フィールドが拡張され、VPI/VCI 情報を伝送するように変更されます。この情報は、セッションの起動時に作成された RADIUS アカウンティング レコードに記録されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RADIUS VC ロギングの設定方法

NSP での NME インターフェイス IP アドレスの設定

RADIUS アカウンティング パケットの NAS-IP-Address フィールドには、NME がシャットダウンされた場合でも、ネットワーク サービス プロバイダー（NSP）のネットワーク管理イーサネット（NME）ポートの IP アドレスが含まれています。IP アドレスを取得するためにネットワーク ルート プロセッサ（NRP）で DHCP サーバを使用しない場合、静的 IP アドレスを設定する必要があります。次の手順を実行して、静的に結合された NME IP アドレスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface BVI** *bridge-group*
4. **ip address** *address subnet*
5. **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。 • 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： `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 BVI** *bridge-group* 例： `Router(config)# interface BVI1`	結合されたブリッジグループ仮想インターフェイス（BVI）NME インターフェイスを選択して、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** *address subnet* 例： `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	静的 IP アドレスとサブネットワーク アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config)# exit`	インターフェイス コンフィギュレーション モードを終了します。

NME IP アドレスの設定

結合された NME インターフェイスの代わりに、ギガビット イーサネット ポートを別の NME インターフェイスとして使用できます。次の手順を実行して NME IP アドレスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface GigabitEthernet** *number*
4. **ip address** *address mask*
5. **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。 • 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： `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 GigabitEthernet** *number* 例： `Router(config)# interface GigabitEthernet 0/0/0`	NME インターフェイスを選択します。
ステップ 4	**ip address** *address mask* 例： `Router(config-if)# ip address 209.165.200.225 255.255.255.224`	静的 IP アドレスとサブネットワーク アドレスを設定します。 （注） NRP で PVC を設定する前に、NME IP アドレスを設定する必要があります。そうしないと、RADIUS アカウンティング パケットの NAS-IP-Address フィールドに正しくない IP アドレスが含まれます。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config)# exit`	設定モードを終了します。

NRP での RADIUS VC ロギングの設定

次の手順を実行して RADIUS VC ロギングを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port format d**
4. **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。 • 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： `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	**radius-server attribute nas-port format d** 例： `Router(config)# radius-server attribute nas-port format d`	NAS ポート フィールドに ATM VC（仮想回線）拡張形式を選択します。
ステップ 4	**exit** 例： `Router(config)# exit`	インターフェイス コンフィギュレーション モードを終了します。

NME インターフェイス IP アドレスの確認

NME IP アドレスを確認するには、NSP で **show interface bvi1** または **show interface e0/0/0** EXEC コマンドを入力します。インターネット アドレス ステートメント（矢印で示されます）を確認します。

```
Router# show interface bvi1BVI1 is up, line protocol is up
  Hardware is BVI, address is 0010.7ba9.c783 (bia 0000.0000.0000)
    MTU 1500 bytes, BW 10000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1540 packets input, 302775 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     545 packets output, 35694 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

NRP での RADIUS VC ロギングの確認

RADIUS サーバ上の RADIUS VC ロギングを確認するには、RADIUS アカウンティング パケットを検査します。RADIUS VC ロギングが Cisco IOS XE ソフトウェアで有効になっている場合、RADIUS アカウンティング パケットは次の例のように表示されます。

```
Wed Jun 16 13:57:31 1999
NAS-IP-Address = 192.168.100.192
NAS-Port = 268566560
NAS-Port-Type = Virtual
User-Name = "cisco"
Acct-Status-Type = Start
Service-Type = Framed
Acct-Session-Id = "1/0/0/2.32_00000009"
Framed-Protocol = PPP
Framed-IP-Address = 172.16.7.254
Acct-Delay-Time = 0
```

NAS-Port フィールドは、RADIUS VC ロギングが有効であることを示します。この行が出力に表示されない場合、RADIUS VC ロギングは Cisco IOS XE ソフトウェアで有効になっていません。

また、Acct-Session-Id フィールドでは、着信 NSP インターフェイスと VPI/VCI 情報を次の形式で識別します。

```
Acct-Session-Id = "slot/subslot/port/VPI.VCI_acct-session-id"
```

RADIUS VC ロギングの設定例

NSP での NME インターフェイス IP アドレスの設定例

次に、ブリッジグループ仮想インターフェイスの静的 IP およびサブネットワーク アドレスを設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface BVI1
ip address 209.165.200.225 255.255.255.224
Router(config)# exit
```

NME IP アドレスの設定例

次に、GigabitEthernet インターフェイスを設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 209.165.200.225 255.255.255.224
Router(config)# exit
```

NRP での RADIUS VC ロギングの設定例

次に、NRP で RADIUS VC ロギングを設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# radius-server attribute nas-port format d
Router(config)# exit
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Security Commands List, All Releases*』

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ 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

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/cisco/web/support/index.html

RADIUS VC ロギングの機能情報

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 *16 :* ゾーンベース ポリシー ファイアウォールの機能情報

機能名	リリース	機能の設定情報
RADIUS VC ロギング	Cisco IOS XE Release 3.1S	RADIUS 仮想回線（VC）ロギングを使用すると、着信サブスクライバ セッションの仮想パス インターフェイス（VPI）と仮想回線インターフェイス（VCI）を Cisco IOS XE ソフトウェアで正確に記録できます。

第 14 章

RADIUS 集中型フィルタ管理

RADIUS 集中型フィルタ管理機能は、ACL の設定と管理を容易にするフィルタ サーバを導入しています。このフィルタ サーバは、集中型 RADIUS リポジトリおよび管理ポイントとして機能します。ユーザは、アクセス コントロール リスト（ACL）フィルタを集中的に管理および設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RADIUS 集中型フィルタ管理の前提条件

- 新しい RADIUS VSA をサポートしていないサーバにディレクトリ ファイルを追加しなければならない場合があります。サンプルのディクショナリとベンダー ファイルについて

は、このドキュメントの後半にある「RADIUSディクショナリとベンダーファイルの例」を参照してください。

ディレクトリ ファイルを追加する必要がある場合は、RADIUSサーバが非標準であり、新しく導入された VSA を送信可能であること確認してください。

- リモート ユーザがダイヤルインして IP 接続を確立できるように、RADIUS ネットワーク認証をセットアップすることができます。

RADIUS 集中型フィルタ管理の制約事項

この機能では複数の方式リストがサポートされていません。単一のグローバル フィルタ方式リストが設定できるだけです。

RADIUS 集中型フィルタ管理に関する情報

RADIUS 集中型フィルタ管理機能以前は、ホールセール プロバイダー（ACL などの顧客サービスに対して特別料金を課している）が、顧客の網羅的な ACL の適用を阻止できました。この行為は、ルータの性能や他の顧客に影響を与える可能性があります。この機能では、ACL管理用の集中型管理ポイント（フィルタ サーバ）が導入されます。フィルタ サーバは、ACL 設定用の集中型 RADIUS リポジトリとして機能します。

フィルタ サーバとして使用されている RADIUS サーバがアクセス認証に使用されているサーバと同じかどうかに関係なく、ネットワーク アクセス サーバ（NAS）はフィルタ サーバに対して別のアクセス要求を開始します。設定されていれば、NASは、認証ユーザ名と2つめのアクセス要求用のフィルタ サーバ パスワードとして、フィルタ ID 名を使用します。RADIUS サーバは、フィルタ ID名を認証して、access-accept応答内に必要なフィルタリング設定を返そうとします。

ACL のダウンロードには時間がかかるため、NAS 上でローカル キャッシュが維持されます。ローカル キャッシュ上にACL名が存在する場合は、フィルタ サーバに問い合わせることなくその設定が使用されます。

（注） キャッシュが適切に設定されていれば、遅延は最小限に抑えられるはずです。ただし、フィルタが必要な最初のダイヤルイン ユーザは必ず待たされることになります。これは、初めての場合は、ACL 設定が読み込まれるためです。

キャッシュ管理

グローバル フィルタ キャッシュは最後に ACL をダウンロードした NAS 上で維持されます。そのため、ユーザは、過負荷状態の RADIUS サーバに対して同じ ACL 設定情報を何度も要求

する必要がありません。ユーザは、次の基準が満たされている場合にキャッシュをフラッシュする必要があります。

- エントリが新しいアクティブ コールに関連付けられた後に、そのエントリに関連付けられたアイドル タイマーがリセットされる（そのように設定されている場合）。
- アイドル時間スタンプの期限が切れたエントリが削除される。
- グローバル キャッシュのエントリが指定された最大数に到達した後に、アイドル タイマーがアイドル時間限界に最も近いエントリが削除される。

1 つのタイマーがすべてのキャッシュ エントリの管理に使用されます。このタイマーは、最初のキャッシュ エントリの作成時に開始され、リブートされるまで定期的に実行されます。タイマーの期間は、キャッシュ アイドル タイマーの設定時に指定された最小粒度に対応し、毎分期限切れになります。タイマーが 1 つしかないことによって、ユーザは、キャッシュ エントリごとに別々のタイマーを管理する必要がありません。

（注） 単一のタイマーは、タイマーの期限切れの精度に欠けます。約 50% のタイマー粒度に平均誤差が含まれています。タイマー粒度を下げると平均誤差も下がりますが、性能が低下する可能性があります。キャッシュ管理には正確なタイミングが必要ないため、誤差遅延を受け入れる必要があります。

新しいベンダー固有属性のサポート

この機能は、次の 2 つのカテゴリに分類可能な 3 つの新しいベンダー固有属性（VSA）のサポートを導入しています。

- ユーザ プロファイルの拡張
  - Filter-Required（50）：指定されたフィルタが見つからなかった場合にコールを許可するかどうかを指定します。存在する場合は、この属性が、すべての認証、許可、アカウンティング（AAA）フィルタ方式リストの後に適用されます。
- 疑似ユーザ プロファイルの拡張
  - Cache-Refresh（56）：エントリが新しいセッションから参照されるたびにキャッシュ エントリを更新するかどうかを指定します。この属性は、**cache refresh** コマンドに対応します。
  - Cache-Time（57）：キャッシュ エントリのアイドル タイムアウトを分単位で指定します。この属性は、**cache clear age** コマンドに対応します。

（注） すべての RADIUS 属性が、すべてのコマンドライン インターフェイス（CLI）設定よりも優先されます。

RADIUS 用の集中型フィルタ管理の設定方法

RADIUS ACL フィルタ サーバの設定

RADIUS ACL フィルタ サーバを有効にするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa authorization cache filterserver default methodlist[methodlist2...]`	AAA 認可キャッシュと、RADIUS フィルタ サーバからの ACL 設定のダウンロードを有効にします。 • **default** ：デフォルト認可リスト。 • *methodlist* [*methodlist2...*] : **password** コマンド ページに列挙されたキーワードの 1 つ。

フィルタ キャッシュの設定

この項の次の手順に従って、AAA フィルタ キャッシュを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa cache filter**
4. Router(config-aaa-filter)# **password 0 7**} *password*
5. Router(config-aaa-filter)# **cache disable**
6. Router(config-aaa-filter)# **cache clear age** *minutes*
7. Router(config-aaa-filter)# **cache refresh**
8. Router(config-aaa-filter)# **cache max** *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。 • 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： `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。

	コマンドまたはアクション	目的
ステップ 3	Router(config)# **aaa cache filter**	フィルタ キャッシュ設定を有効にして、AAA フィルタ コンフィギュレーション モードに入ります。
ステップ 4	Router(config-aaa-filter)# **password 0 7**} *password*	（任意）フィルタ サーバ認証要求に使用されるオプション パスワードを指定します。 **0** ：暗号化されていないパスワードが後に続くことを示します。 **7** ：非表示パスワードが後に続くことを示します。 *password*：暗号化されていない（クリア テキスト）パスワード。 （注） パスワードが指定されなかった場合は、デフォルト パスワード（「cisco」）が有効になります。
ステップ 5	Router(config-aaa-filter)# **cache disable**	（任意）キャッシュを無効にします。
ステップ 6	Router(config-aaa-filter)# **cache clear age** *minutes*	（任意）キャッシュ エントリの期限が切れ、キャッシュがクリアされるタイミングを分単位で指定します。 *minutes* ：0 ～ 4294967295 の任意の値。 （注） 時間が指定されなかった場合は、デフォルト（1400 分（1 日））が有効になります。
ステップ 7	Router(config-aaa-filter)# **cache refresh**	（任意）新しいセッションの開始時点でキャッシュ エントリをリフレッシュします。このコマンドは、デフォルトでイネーブルになっています。この機能をディセーブルにするには、**no cache refresh** コマンドを使用します。
ステップ 8	Router(config-aaa-filter)# **cache max** *number*	（任意）キャッシュで特定のサーバ用に維持できるエントリの絶対数を制限します。 *number*：キャッシュに含めることが可能なエントリの最大数。0 ～ 4294967295 の任意の値。 （注） 数値が指定されなかった場合は、デフォルト（100 エントリ）が有効になります。

フィルタ キャッシュの確認

キャッシュ ステータスを表示するには、**show aaa cache filterserver** EXEC コマンドを使用します。次に、**show aaa cache filterserver** コマンドの出力例を示します。

```
Router# show aaa cache filterserver
Filter     Server          Age Expires Refresh Access-Control-Lists
-------------------------------------------------------------------------------
aol        10.2.3.4          0    1440     100 ip in icmp drop
                                               ip out icmp drop
                                               ip out forward tcp dstip 1.2.3...
msn        10.3.3.4        N/A   Never       2 ip in tcp drop
msn2       10.4.3.4        N/A   Never       2 ip in tcp drop
vone       10.5.3.4        N/A   Never       0 ip in tcp drop
```

（注） **show aaa cache filterserver** コマンドは、特定のフィルタが参照またはリフレッシュされた回数を表示します。この機能は、実際に使用されるフィルタを決定するために管理者が使用します。

トラブルシューティングのヒント

フィルタ キャッシュ設定のトラブルシューティングを支援するために、**debug aaa cache filterserver** 特権 EXEC コマンドを使用します。**debug aaa cache filterserver** コマンドのサンプル出力を確認するには、このドキュメントの後半にある「デバッグ出力の例」を参照してください。

フィルタ キャッシュのモニタリングと維持

フィルタ キャッシュをモニタおよび維持するには、次の EXEC コマンドの少なくとも 1 つを使用します。

コマンド	目的
`Router# clear aaa cache filterserver acl [filter-name`	特定のフィルタまたはすべてのフィルタのキャッシュ ステータスをクリアします。
`Router# show aaa cache filterserver`	キャッシュ ステータスを表示します。

RADIUS 集中型フィルタ管理の設定例

NAS の設定例

次の例は、キャッシュ フィルタリング用の NAS の設定方法を示しています。この例では、最初に、サーバ グループの「mygroup」に接続されます。応答がない場合は、デフォルト RADIUS サーバに接続されます。それでも応答がない場合は、ローカル フィルタ ケアに接続されます。最終的に、フィルタが解決できなければ、コールが受け入れられます。

```
aaa authorization cache filterserver group mygroup group radius local none
!
aaa group server radius mygroup
 server 10.2.3.4
 server 10.2.3.5
!
radius-server host 10.1.3.4
!
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
!
```

RADIUS サーバの設定例

次の例は、NAS にダイヤルしているリモート ユーザ「user1」のサンプル RADIUS 設定です。

```
myfilter Password = "cisco"
Service-Type = Outbound,
Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 icmp",
Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 tcp dstport
 = telnet",
Ascend:Ascend-Cache-Refresh = Refresh-No,
Ascend:Ascend-Cache-Time = 15
user1 Password = "cisco"
Service-Type = Framed,
Filter-Id = "myfilter",
Ascend:Ascend-Filter-Required = Filter-Required-Yes,
```

RADIUS ディクショナリとベンダー ファイルの例

次の例は、新しい VSA 用のサンプル RADIUS 辞書ファイルです。この例では、辞書ファイルが Merit サーバ用です。

```
dictionary file:
Ascend.attr Ascend-Filter-Required 50 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Refresh   56 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Time      57 integer (*, 0, NOENCAPS)
Ascend.value Ascend-Cache-Refresh Refresh-No  0
Ascend.value Ascend-Cache-Refresh Refresh-Yes 1
Ascend.value Ascend-Filter-Required  Filter-Required-No  0
```

```
Ascend.value Ascend-Filter-Required  Filter-Required-Yes 1
vendors file:
50     50
56     56
57     57
```

デバッグ出力例

次に、**debug aaa cache filterserver** コマンドの出力例を示します。

```
Router# debug aaa cache filterserver

AAA/FLTSV: need "myfilter" (fetch), call 0x612DAC64
AAA/FLTSV: send req, call 0x612DAC50
AAA/FLTSV: method SERVER_GROUP myradius
AAA/FLTSV: recv reply, call 0x612DAC50 (PASS)
AAA/FLTSV: create cache
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: skip attr "filter-cache-refresh"
AAA/FLTSV: skip attr "filter-cache-time"
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" refresh? no
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" cachetime 15
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: PASS call 0x612DAC64
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (1 entry)
AAA/CACHE: destroy "AAA filtserv cache" entry "myfilter"
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
```

その他の参考資料

次の項で、RADIUS 集中型フィルタ管理に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
認可の設定	「Configuring Authorization」機能モジュール。
RADIUS の設定	「Configuring RADIUS」機能モジュール
認可コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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
なし	--

テクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/en/US/support/index.html

RADIUS 集中型フィルタ管理の機能情報

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 *17 : RADIUS* 集中型フィルタ管理の機能情報

機能名	リリース	機能情報
RADIUS集中型フィルタ管理	Cisco IOS XE Release 3.9S	RADIUS集中型フィルタ管理機能は、ACLの設定と管理を容易にするフィルタ サーバを導入しています。このフィルタ サーバは、集中型RADIUSリポジトリおよび管理ポイントとして機能します。ユーザは、アクセス コントロール リスト（ACL）フィルタを集中的に管理および設定できます。 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。**aaa authorization cache filterserver**、**aaa cache filter, cache clear age, cache disable, cache refresh**、**clear aaa cache filterserver acl**、**debug aaa cache filterserver**、**password**、**show aaa cache filterserver.**

第 15 章

RADIUS EAP サポート

RADIUS EAP サポート機能は、ユーザに PPP 内でのクライアント認証方式（独自の認証を含む）の適用を可能にします。この認証方式は、ネットワーク アクセス サーバ（NAS）ではサポートされない可能性があり、拡張可能認証プロトコル（EAP）を通して実現されます。この機能が導入される前は、PPP接続用のさまざまな認証方式をサポートするために、特別なベンダー固有設定と、クライアントと NAS に対する変更が必要でした。RADIUS EAP サポートを使用すれば、トークン カードや公開キーなどの認証スキームでネットワークに対するエンドユーザとデバイスの認証対象アクセスを補強できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RADIUS EAP サポートの前提条件

クライアント上で EAP RADIUS を有効化する前に、次のタスクを実行する必要があります。

- **interface** コマンドを使用してインターフェイス 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。
- **encapsulation** コマンドを使用して、PPP をカプセル化するためのインターフェイスを設定します。

これらのタスクの実行方法については、「Configuring Asynchronous SLIP and PPP」モジュールを参照してください。

RADIUS EAP サポートの制約事項

EAP がプロキシ モードで動作中に、認証時間が大幅に増加する可能性があります。これは、ピアからのすべてのパケットを RADIUS サーバに送信する必要があり、RADIUS サーバからのすべての EAP パケットをクライアントに送り返す必要があるためです。この追加処理は遅延の原因になりますが、**ppp timeout authentication** コマンドを使用して、デフォルトの認証タイムアウト値を増やすことができます。

RADIUS EAP サポートに関する情報

EAP は、認証フェーズ（Link Control Protocol（LCP）フェーズではなく）でネゴシエートされる複数の認証メカニズムをサポートする PPP 用の認証プロトコルです。EAP を使用すると、汎用のインターフェイスを介して、サードパーティ製の認証サーバと PPP 実装の間でデータのやり取りができます。

EAP のしくみ

デフォルトでは、EAP はプロキシモードで実行されます。このため、EAP では、RADIUS サーバに存在するバックエンド サーバ、または RADIUS サーバを介してアクセスできるバックエンド サーバに対する認証プロセス全体を、NAS によってネゴシエートすることができます。LCP の交換中にクライアントと NAS の間で EAP がネゴシエートされると、その後のすべての認証メッセージは、クライアントとバックエンド サーバの間で透過的に送信されます。NAS は認証プロセスに直接関与しなくなります。つまり、NAS はプロキシとして機能し、リモートピア間で EAP メッセージを送信します。

（注） EAP は、ローカル モードでも実行できます。その場合、セッションは Message Digest 5（MD5）アルゴリズムを使用して認証され、Challenge Handshake Authentication Protocol（CHAP）と同じ認証ルールに従います。プロキシ モードを無効にしてローカルで認証するには、**ppp eap local** コマンドを使用する必要があります。

新しくサポートされた属性

RADIUS EAP サポート機能では、次の RADIUS 属性のサポートが追加されています。

番号	IETF 属性	説明
79	EAP-Message	PPP type、request-id、length、および EAP-type の各フィールドを含む EAP メッセージの 1 つのフラグメントをカプセル化します。
80	Message Authenticator	メッセージの発信元整合性を保証します。無効なチェックサムを伴って受信されたすべてのメッセージは、通知されることなく両端で破棄されます。この属性には、RADIUS 要求または応答メッセージ全体の HMAC-MD5 チェックサムが含まれており、キーとして RADIUS サーバ シークレットが使用されます。

RADIUS EAP サポートの設定方法

EAP の設定

このタスクを実行して、PPP カプセル化用に設定されたインターフェイス上で EAP を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ppp authentication eap**
4. **ppp eap identity** *string*
5. **ppp eap password** [*number*] *string*
6. **ppp eap local**
7. **ppp eap wait**
8. **ppp eap refuse** [**callin**]

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。 • 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： `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	**ppp authentication eap** 例： `Router(config-if)# ppp authentication eap`	認証プロトコルとして EAP を有効にします。
ステップ 4	**ppp eap identity** *string* 例： `Router(config-if)# ppp eap identity user`	（任意）ピアから要求されたときの EAP ID を指定します。
ステップ 5	**ppp eap password** [*number*] *string* 例： `Router(config-if)# ppp eap password 7 141B1309`	（任意）ピア認証用の EAP パスワードを設定します。 このコマンドは、クライアント上でのみ設定する必要があります。
ステップ 6	**ppp eap local** 例： `Router(config-if)# ppp eap local`	（任意）RADIUS バックエンド サーバを使用する代わりにローカルで認証します。これはデフォルトの設定です。 （注） このコマンドは、NAS 上でのみ設定する必要があります。
ステップ 7	**ppp eap wait** 例： `Router(config-if)# ppp eap wait`	（任意）発信者が自分自身を最初に認証するのを待機します。デフォルトでは、クライアントの方が発信者よりも先に自分自身を認証します。 （注） このコマンドは、NAS 上でのみ設定する必要があります。
ステップ 8	**ppp eap refuse** [**callin**] 例： `Router(config-if)# ppp eap refuse`	（任意）EAP を使用した認証を拒否します。**callin** キーワードが有効になっている場合は、着信コールのみが認証されません。

	コマンドまたはアクション	目的
		（注） このコマンドは、NAS 上でのみ設定する必要があります。

EAP の確認

クライアントまたは NAS 上の EAP 設定を確認するには、特権 EXEC コンフィギュレーション モードで次のコマンドの少なくとも 1 つを使用します。

コマンド	目的
`Router# show users`	ルータのアクティブ回線に関する情報を表示します。
`Router# show interfaces`	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。
`Router# show running-config`	使用している設定が実行コンフィギュレーションの一部として表示されていることを確認します。

設定例

クライアント上の EAP ローカル設定例

次の例は、EAP 用に設定されたクライアントのサンプル設定です。

```
interface Ethernet0/0
 ip address 10.1.1.202 255.255.255.0
 no ip mroute-cache
 half-duplex
!
interface BRI0/0
 ip address 192.168.101.100 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 192.168.101.101 56167
 dialer-group 1
 isdn switch-type basic-5ess
 ppp eap identity user
 ppp eap password 7 141B1309
!
!
ip default-gateway 10.1.1.1
ip classless
ip route 192.168.101.101 255.255.255.255 BRI0/0
no ip http server
!
dialer-list 1 protocol ip permit
```

NAS 用の EAP プロキシ設定例

次の例は、EAP プロキシを使用するように設定された NAS のサンプル設定です。

```
aaa authentication login default group radius
aaa authentication login NOAUTH none
aaa authentication ppp default if-needed group radius
aaa session-id common
enable secret 5 $1$x5D0$cfTL/D8Be.34PgTbdGdgl/
!
username dtw5 password 0 lab
username user password 0 lab
ip subnet-zero
no ip domain-lookup
ip host lab24-boot 172.19.192.254
ip host lb 172.19.192.254
!
isdn switch-type primary-5ess
!
controller T1 3
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface Ethernet0
 ip address 10.1.1.108 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface Serial3:23
 ip address 192.168.101.101 255.255.255.0
 encapsulation ppp
 dialer map ip 192.168.101.100 60213
 dialer-group 1
 isdn switch-type primary-5ess
 isdn T321 0
 ppp authentication eap
 ppp eap password 7 011F0706
!
!
ip default-gateway 10.0.190.1
ip classless
ip route 192.168.101.0 255.255.255.0 Serial3:23
no ip http server
!
dialer-list 1 protocol ip permit
!
radius-server host 10.1.1.201 auth-port 1645 acct-port 1646 key lab
radius-server retransmit 3
call rsvp-sync
!
mgcp profile default
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login authentication NOAUTH
line 1 48
line aux 0
ine vty 0 4
lpassword lab
```

その他の参考資料

次の項で、RADIUS EAP サポート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA を使用した ppp 認証の設定	「Configuring Authentication」モジュール。
RADIUS の設定	「Configuring RADIUS」モジュール。
PPP の設定	「Configuring Asynchronous SLIP and PPP」モジュール。
ダイヤルテクノロジー コマンド	『*Cisco IOS Dial Technologies Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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
RFC 2284	『*PPP Extensible Authentication Protocol (EAP)*』
RFC 1938	『*A One-Time Password System*』
RFC 2869	『*RADIUS Extensions*』

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/en/US/support/index.html

RADIUS EAP サポートの機能情報

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 *18 : RADIUS EAP* サポートの機能情報

機能名	リリース	機能情報
RADIUS EAP サポート	Cisco IOS XE Release 3.9S	RADIUS EAP サポート機能は、ユーザに PPP 内でのクライアント認証方式（独自の認証を含む）の適用を可能にします。この認証方式は、ネットワーク アクセス サーバ（NAS）ではサポートされない可能性があり、拡張可能認証プロトコル（EAP）を通して実現されます。この機能が導入される前は、PPP 接続用のさまざまな認証方式をサポートするために、特別なベンダー固有設定と、クライアントと NAS に対する変更が必要でした。RADIUS EAP サポートを使用すれば、トークン カードや公開キーなどの認証スキームでネットワークに対するエンドユーザとデバイスの認証対象アクセスを補強できます。 次のコマンドが導入または変更されました。**ppp authentication**、**ppp eap identity, ppp eap local**、**ppp eap password**、**ppp eap refuse**、**ppp eap wait**

用語集

attribute ：RADIUS Internet Engineering Task Force（IETF）属性は、クライアントとサーバの間で認証、認可、およびアカウンティング（AAA）情報を通信するために使用される 255 個の標準属性からなるオリジナル セットの 1 つです。IETF 属性は標準であるため、属性データは事前定義されてその内容も認識されています。このため、IETF 属性を介して AAA 情報を交換するすべてのクライアントとサーバは、属性の厳密な意味や各属性値の一般的な限界などの属性データを一致させる必要があります。

CHAP ：チャレンジ ハンドシェイク認証プロトコル。PPP カプセル化を使用した回線上でサポートされ、不正アクセスを防止するセキュリティ機能。CHAP それ自体が不正アクセスを防止するわけではなく、単に、リモートエンドを識別するだけです。その後で、ルータまたはアクセス サーバがそのユーザのアクセスを許可するかどうかを決定します。

EAP ：拡張認証プロトコル。認証フェーズ（Link Control Protocol（LCP）フェーズではなく）でネゴシエートされる複数の認証メカニズムをサポートする PPP 認証プロトコル。EAP を使用すれば、汎用のインターフェイスを介して、サードパーティ製の認証サーバと PPP 実装の間でデータのやり取りができます。

LCP ：リンク制御プロトコル。PPP で使用するためのデータ リンク接続を確立して、設定し、テストするプロトコル。

MD5 (HMAC variant) ：Message Digest 5。パケット データの認証に使用するハッシュ アルゴリズム。HMAC は、メッセージ認証用の重要なハッシングです。

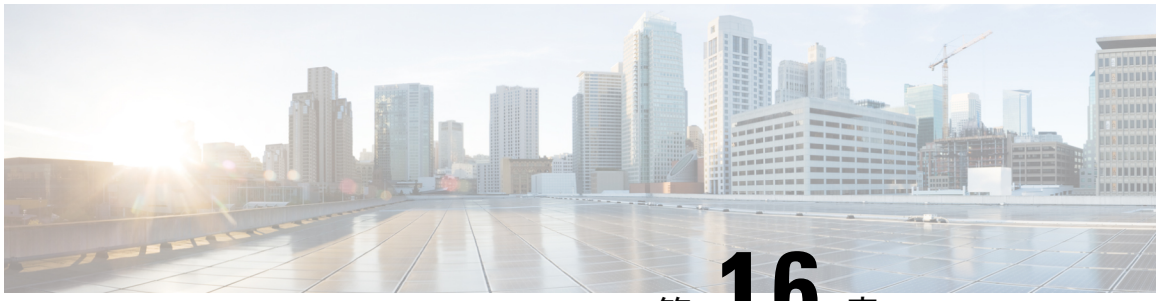
NAS ：ネットワーク アクセス サーバ。公衆電話交換網（PSTN）などのリモート アクセス ネットワーク上でユーザにローカル ネットワーク アクセスを提供するデバイス。

PAP ：パスワード認証プロトコル。PPP ピアの相互認証を可能にする認証プロトコル。ローカル ルータに接続を試みているリモート ルータは、認証要求を送信するように要求されます。CHAP と違って、PAP はパスワードとホスト名またはユーザ名をクリア テキスト（暗号化なし）で渡します。PAP それ自体が不正アクセスを防止するわけではなく、単に、リモート エンドを識別するだけです。ルータまたはアクセス サーバがそのユーザのアクセスを許可するかどうかを決定します。PAP は、PPP 回線上でのみサポートされます。

PPP ：ポイントツーポイント プロトコル。ポイントツーポイント リンク上でネットワーク層プロトコル情報をカプセル化するプロトコル。PPP は RFC 1661 で規定されています。

RADIUS ：リモート認証ダイヤルイン ユーザ サービス。モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。



第 16 章

コール接続時の RADIUS 暫定アップデート

コール接続時の RADIUS 暫定アップデート機能では、課金サーバにコール接続のタイムスタンプを提供する追加のアカウンティング レコードが生成されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

コール接続時の RADIUS 暫定アップデートに関する情報

コール接続時の RADIUS 暫定アップデート機能を有効にすると、Cisco IOS ソフトウェアは、コール レッグが接続されたときに、追加の更新済み中間アカウンティング レコードを生成してアカウンティング サーバに送信します。コール レッグは、Voice over IP（VoIP）ネットワーク内のコール接続の別個のセグメントであり、ルータと、ベアラ チャネルを介したテレフォニー エンドポイントまたはセッション プロトコルを使用した別のエンドポイントとの間の論理的な接続です。コール接続時に使用可能なすべての属性（h323-connect-time や backward-call-indicators など）がこの更新済み中間アカウンティング レコードによって送信されます。

コール接続時の RADIUS 暫定アップデート機能を有効化する方法

次のタスクを実行して、コール レッグが接続されたときに、Cisco IOS で追加の更新済み中間アカウンティング レコードを生成してアカウンティング サーバに送信できるようにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **gw-accounting aaa**
5. **aaa accounting update newinfo**

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。 • 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： `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`	認証、認可、およびアカウンティング（AAA）を有効化します。
ステップ 4	**gw-accounting aaa** 例： `Router(config)# gw-accounting aaa`	AAA システムを通じてアカウンティングを有効化し、コール詳細レコード（CDR）をベンダー固有属性（VSA）の形式でRADIUS サーバに送信します。
ステップ 5	**aaa accounting update newinfo** 例： `Router(config)# aaa accounting update newinfo`	問題のユーザに関する新しいアカウンティング情報が生成されるたびに、一時アカウンティング レコードを定期的にアカウンティング サーバに送信できるようにします。

その他の参考資料

次の項で、コール接続時の RADIUS 暫定アップデート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
認証、許可、アカウンティング（AAA）	「Configuring Authentication」、「Configuring Authorization」、および「Configuring Accounting」モジュール。
RADIUS ベンダー固有属性	「RADIUS Vendor-Proprietary Attributes」モジュール。
ダイナミック プロンプトの設定、アカウンティングテンプレートのカスタマイズ、および音声ゲートウェイへの AAA 要求の転送	『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』および『*Cisco IOS VPDN Configuration Guide* , Release 12.4T』。

標準

標準	タイトル
なし。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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
RFC 2138	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC 2139	『*RADIUS Accounting*』

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/en/US/support/index.html

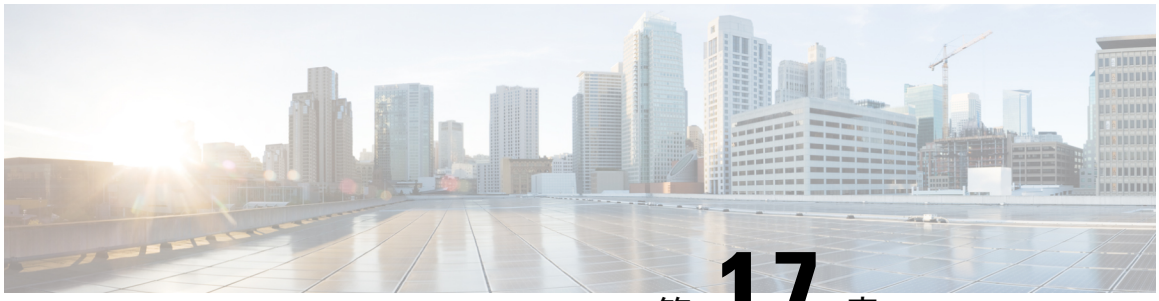
コール接続時の RADIUS 暫定アップデートの機能情報

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 *19 :* コール接続時の *RADIUS* 暫定アップデートの機能情報

機能名	リリース	機能情報
コール接続時の RADIUS 暫定アップデート	Cisco IOS XE Release 3.9S	コール接続時の RADIUS 暫定アップデート機能では、課金サーバにコール接続のタイムスタンプを提供する追加のアカウンティング レコードが生成されます。 次のコマンドが導入または変更されました。 **gw-accounting aaa** および **aaa accounting update**



第 17 章

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、シスコ独自のベンダー固有属性（VSA）を使用せずに、業界標準のロードバランシング機能とフェールオーバー機能を Layer 2 Tunneling Protocol ネットワーク サーバ（LNS）に提供します。この機能は、RFC 2868 で規定されているマルチベンダー ネットワーク環境に使用すべきトンネル属性に適合しているため、複数のベンダーで製造されたネットワーク アクセス サーバ（NAS）間の相互運用性の問題を解決します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

前提条件

VPDN と HGW グループの設定はこのマニュアルの範囲を超えています。詳細については、「関連資料」を参照してください。

制約事項

次の制約および制限が、ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能に適用されます。

- この機能は、VPDN ダイヤルアウト ネットワークをサポートしていません。ダイヤルイン アプリケーション専用に設計されています。
- ネットワーク上で許容される LNS の最大数は、タグ属性グループ当たり 50 ずつの合計 1550 で、タグは 31 までに制限されています。
- この機能には、RFC 2868 をサポートする RADIUS サーバ実装が必要です。

ロードバランシングおよびフェールオーバー用のRADIUS トンネル プリファレンスに関する情報

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、ロード バランシングおよびフェールオーバーの仮想プライベート ダイヤルアップ ネットワーク（VPDN）ホーム ゲートウェイ（HGW）グループを標準化された方式で提供します。この機能は、新しいソフトウェア機能を導入しています。この機能に関連付けられた新しいコマンドはありません。

独自の属性ではなく、業界標準の属性

Cisco IOS Release 12.2(4)T までは、LNS のロード バランシングおよびフェールオーバー機能が、シスコ独自の VSA によって提供されていました。マルチベンダー ネットワーク環境で、RADIUS 上の VSA を使用した場合は、複数のベンダーによって製造された NAS 間で相互運用性の問題が発生する可能性があります。特定の RADIUS サーバ実装が要求元の NAS で解読可能な VSA を送信可能な場合でも、ユーザが同じ目的で複数の VSA をシングル サービス プロファイルに保存しておく必要があります。

マルチベンダー ネットワーク環境で使用すべきトンネル属性に関する合意は RFC 2868 で規定されています。RFC 2868 では、Tunnel-Server-Endpoint と Tunnel-Medium-Type を組み合わせ

て、NAS が新しいセッションを開始すべきアドレスが指定されます。複数の Tunnel-Server-Endpoint 属性が 1 つのタグ付き属性グループ内で定義されている場合は、equal-cost load-balancing HGW として解釈されます。

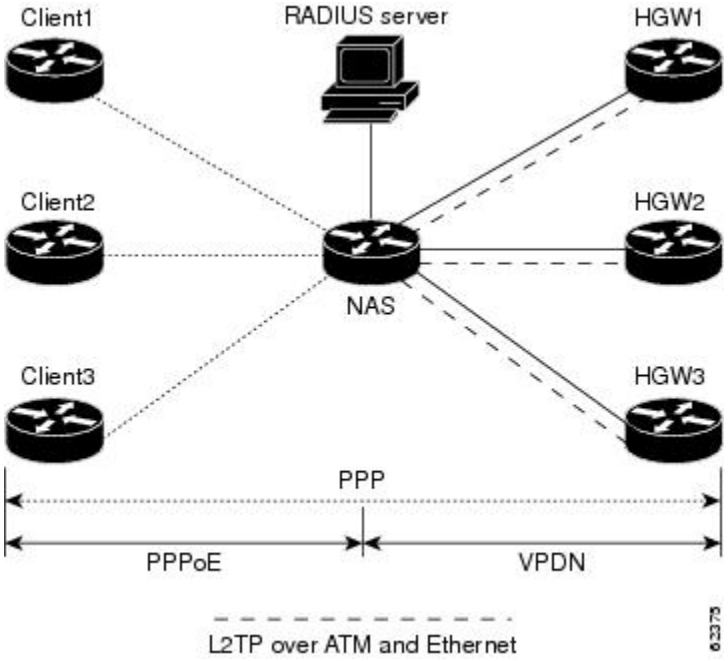
RFC 2868 で規定されている Tunnel-Preference 属性は、ロード バランシングおよびフェールオーバー HGW グループを形成する手段として使用できます。複数のタグ付き属性グループの Tunnel-Preference 値が同じ場合は、他に指定されていなければ、それらの属性グループの Tunnel-Server-Endpoint が同じ優先順位に設定されていると見なされます。一部の属性グループの Tunnel-Preference 値が他の属性グループよりも高い（プリファレンスが低い）場合は、それらの Tunnel-Server-Endpoint 属性の優先順位が上になります。ある属性グループの優先順位値が高い場合は、それより優先順位値が低い属性グループが接続に使用できない場合に、その属性グループがフェールオーバーに使用されます。

Cisco IOS Release 12.2(4)T までは、特別に書式設定された文字列が Cisco VSA の「vpdn:ip-addresses」文字列内で NAS に転送され、HGW のロード バランシングおよびフェールオーバーに使用されていました。たとえば、10.0.0.1 10.0.0.2 10.0.0.3/2.0.0.1 2.0.0.2 は、ロード バランシング用の最初のグループに関する IP アドレスの 10.0.0.1、10.0.0.2、および 10.0.0.3 として解釈されます。新しいセッションは、least-load-first アルゴリズムに基づいて、この 3 つのアドレスに送出されます。このアルゴリズムは、ローカルな知識を利用して、新しいセッションを開始する負荷が最低の HGW を選択します。この例では、2 番めのグループ内のアドレスの 2.0.0.1 と 2.0.0.2 が、優先順位が低く、最初のグループ内で指定されたすべての HGW が新しい接続要求に対する応答に失敗した場合にのみ適用可能になります。そのため、2.0.0.1 と 2.0.0.2 がフェールオーバー アドレスになります。RADIUS トンネル プロファイル内でのこのようなフェールオーバー アドレスを設定する方法の例については、ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスの設定例（179 ページ）を参照してください。

マルチベンダー ネットワークにおけるロード バランシングとフェールオーバー

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、以下の図に示す構成のように、ATM および Ethernet などの WAN リンクを経由して VPDN レイヤ 2 トンネルを使用する大規模なマルチベンダー ネットワーク向けに設計されています。

図 *1:* マルチベンダー ネットワークにおける代表的なロード バランシングとフェールオーバー



上の図に示す構成では、NAS が RADIUS サーバからダウンロードされたトンネル プロファイルを使用して、ロード バランシングおよびフェールオーバー用の VPDN レイヤ 2 トンネルを構築します。Point-to-Point over Ethernet（PPPoE）プロトコルが、PPP セッションを生成するクライアントとして使用されます。

関連機能およびテクノロジー

ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、VPDN で使用されます。加えて、次のテクノロジーとプロトコルに精通していることが求められます。

- ATM
- イーサネット
- L2TP と L2F
- PPP と PPPoE
- RADIUS サーバ

ロードバランシングおよびフェールオーバー用のRADIUS トンネル プリファレンスの設定方法

この機能には新しいコンフィギュレーション コマンドはありません。ただし、RADIUS トンネル プロファイル内でのロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能の実装方法の例については、次の項を参照してください。

ロードバランシングおよびフェールオーバー用のRADIUS トンネル プリファレンスの設定例

次の例は、RADIUS トンネル プロファイルの作成方法を示しています。

```
net3 Password = "cisco" Service-Type = Outbound
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Server-Endpoint = :0:"1.1.3.1",
        Tunnel-Assignment-Id = :0:"1",
        Tunnel-Preference = :0:1,
        Tunnel-Password = :0:"welcome"
        Tunnel-Type = :1:L2TP,
        Tunnel-Medium-Type = :1:IP,
        Tunnel-Server-Endpoint = :1:"1.1.5.1",
        Tunnel-Assignment-Id = :1:"1",
        Tunnel-Preference = :1:1,
        Tunnel-Password = :1:"welcome"
        Tunnel-Type = :2:L2TP,
        Tunnel-Medium-Type = :2:IP,
        Tunnel-Server-Endpoint = :2:"1.1.4.1",
        Tunnel-Assignment-Id = :2:"1",
        Tunnel-Preference = :2:1,
        Tunnel-Password = :2:"welcome"
        Tunnel-Type = :3:L2TP,
        Tunnel-Medium-Type = :3:IP,
        Tunnel-Server-Endpoint = :3:"1.1.6.1",
        Tunnel-Assignment-Id = :3:"1",
        Tunnel-Preference = :3:1,
        Tunnel-Password = :3:"welcome"
```

これらのプロファイル内でフェールオーバー アドレスがどのように選択されるかの詳細については、ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンスに関する情報 （176 ページ）を参照してください。

その他の参考資料

次の項で、ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUS	「Configuring RADIUS」モジュール。
RADIUS 属性	「RADIUS Attributes Overview and RADIUS IETF Attributes」モジュール。
バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）のロードマップ	『*Cisco IOS VPDN Configuration Guide* , Release 15.0』
ダイヤル テクノロジー	『*Cisco IOS Dial Technologies Configuration Guide* , Release 12.4T』
ブロードバンドアクセス：PPP とルーテッド ブリッジ エンカプセレーション	『*Cisco IOS Broadband Access Aggregation and DSL Configuration Guide* , Release 12.4T』

標準

標準	タイトル
なし。	--

MIB

MIB	MIB のリンク
なし。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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
RFC 2868	『RADIUS Attributes for Tunnel Protocol Support』

ロードバランシングおよびフェールオーバー用のRADIUS トンネル プリファレンスの機能情報

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 *20* : ロード バランシングおよびフェールオーバー用の *RADIUS* トンネル プリファレンスの機能情報

機能名	リリース	機能情報
ロードバランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス	Cisco IOS XE Release 3.9S	ロード バランシングおよびフェールオーバー用の RADIUS トンネル プリファレンス機能は、シスコ独自のベンダー固有属性（VSA）を使用せずに、業界標準のロード バランシング機能とフェールオーバー機能を Layer 2 Tunneling Protocol ネットワーク サーバ（LNS）に提供します。この機能は、RFC 2868 で規定されているマルチベンダー ネットワーク環境に使用すべきトンネル属性に適合しているため、複数のベンダーで製造されたネットワーク アクセス サーバ（NAS）間の相互運用性の問題を解決します。

用語集

HGW ：ホーム ゲートウェイ。L2TP などのレイヤ 2 トンネリング プロトコルを終端するゲートウェイ。

home gateway ：「HGW」を参照してください。

L2TP ：レイヤ 2 トンネル プロトコル。PPP のトンネリングを提供する RFC 2661 で規定されたインターネット技術特別調査委員会（IETF）標準トラック プロトコル。L2F と PPTP の最良の機能に基づいて、L2TP が、VPDN を実装するための業界全体で相互運用可能な方式を提供します。

L2TP ネットワーク サーバ：LNS を参照してください。

Layer 2 Tunnel Protocol ：「L2TP」を参照してください。

LNS ：L2TP ネットワーク サーバ。L2TP トンネル エンドポイントの一方の側として機能し、NAS または L2TP アクセス コンセントレータ（LAC）に対するピアであるノード。LNS は、

アクセス サーバによってリモート システムからトンネル化されている PPP セッションの論理的終端点です。レイヤ 2 フォワーディング（L2F）HGW に似ています。

NAS ：ネットワーク アクセス サーバ。パケットの世界（インターネットなど）と回線の世界（公衆電話交換網など）をインターフェイスするシスコプラットフォームまたはプラットフォームの集合。

network access server ：「NAS」を参照してください。

Request for Comments ：「RFC」を参照してください。

RFCs ：コメント要求。インターネット技術特別調査委員会（IETF）によって収集されたインターネットに関する各種規約。1969 年に発足した IETF は、インターネット アーキテクチャの発展に携わっているネットワーク設計者、運営業者、ベンダー、および研究者の大規模でオープンな国際的コミュニティです。RFC は、ネットワーキング プロトコル、手続き、プログラム、および概念に焦点を当てた、コンピュータ通信のさまざまな側面を規定しています。

virtual private dialup network ：「VPDN」を参照してください。

VPDN ：バーチャル プライベート ダイヤルアップ ネットワーク。ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。