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。

RADIUS の前提条件

シスコ デバイスまたはアクセス サーバーで 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 ユーザー名の検索など、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 ユーザーのネットワーク 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、ユーザー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+ サーバーへの移行の最初のステップとなることもあります。
- ユーザー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）に対するユーザー アクセスを制御できます。たとえば、ユーザーがログインすると、RADIUS は、IP アドレス 10.2.3.4 を使用してそのユーザーが 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サーバーを導入すると、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

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

1. ユーザー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：ユーザーが認証されたことを表します。
   2. CHALLENGE：RADIUSサーバーによってチャレンジが発行されます。チャレンジは、ユーザーから追加データを収集します。
   3. CHANGE PASSWORD：RADIUS サーバーからユーザー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：ユーザーは認証されず、ユーザー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。

- ユーザー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、ユーザー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 サーバーは、各ユーザー 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ーします。

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 サーバーと RADIUS サーバー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 サーバーの 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 サーバーとネットワーク アクセス サーバーの間で通信します。

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 サーバーとトンネル 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、ユーザーはネットワーク アクセス サーバーおよび RADIUS サーバーの認証名を指定できます。

シスコ デバイスとアクセス サーバーでは、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 サーバー上の事前認証

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 サーバー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）の番号をユーザー名として使用し、**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 サーバー（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 タイプのユーザー名と、わかりやすいパスワードを使用してユーザーが 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 サーバーに送信される 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ー名として使用し、**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 ユーザー情報レイヤがある任意のコール。
v.120	V.120 ユーザー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 タイプのユーザー名と、わかりやすいパスワードを使用してユーザーが 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 サーバーに送信された Access-Request パケットにも含まれます。また、RADIUS サーバーがチェックイン 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 ユーザーは、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 サーバー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 サーバー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 サーバー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、通常のユーザー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）のユーザー名とパスワードが必要です。
ms-chap	PPP 認証の MS-CHAP のユーザー名とパスワードが必要です。
pap	PPP 認証の Password Authentication Protocol（PAP）のユーザー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 はユーザー別の属性であり、**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。

ユーザー名を含めるための 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 がユーザー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ー名を提供できます。ユーザー名を指定する VSA の構文は次のとおりです。

```
cisco-avpair = "preauth:username=<
string
>"
```

ユーザー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 番号がユーザー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つのユーザー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ー名と、ユーザーが指定したユーザー名です。この場合、ユーザーが指定したユーザー名は、RADIUS事前認証プロファイルに含まれているユーザー名を上書きします。ユーザーが指定したユーザー名は、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のユーザー名とパスワードやCHAPのユーザー名とパスワードを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ー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ユーザー名と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。ユーザー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ー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 サーバーを指定し、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、ユーザー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、各ユーザーに対するアカウントリストおよびプロファイル、ユーザー 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、ユーザーがアクセスしているサービスや、ユーザー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 サーバー（NAS）が、ダイヤルイン ユーザー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 サーバーのユーザー 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、ユーザー *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 サーバーが 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ーの応答を画面にエコーするかどうかを制御するには、RADIUS サーバーのユーザー 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、ユーザー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
```

ユーザーの応答をエコーするには、この属性を Echo に設定します。Prompt 属性をユーザー 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 サーバーに設定されている **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 サーバーがエコーを表示しないように設定され、個人のユーザー プロファイルではエコーを許可している場合、ユーザー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 サーバー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 サーバーと RADIUS サーバーの間で、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 サーバーのスタティック 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 サーバーの代わりに、ユーザーが RADIUS サーバーのスタティック 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 サーバーは、スタティック ルートと IP プール情報について RADIUS サーバーに照会します。

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 サーバーがスタティック ルートと IP プール定義を RADIUS サーバーに照会するには、**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 サーバー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 サーバーと RADIUS サーバー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 サーバー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 サーバーが 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。

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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 サーバーが 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：	RADIUS サーバーの名前を指定します。

	コマンドまたはアクション	目的
	`Device(config)# radius server rad1`	（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 サーバーを設定するには、**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 サーバーに 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 サーバーが 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 サーバー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 サーバー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 サーバー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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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 サーバーが、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 サーバーに照会するように指定します。 （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：	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`	

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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 サーバー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。

	コマンドまたはアクション	目的
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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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。 （注） RADIUS にエフェメラル送信元ポートを使用する IOS プロセスはほとんどなく、ポート番号は毎回異なる場合があります。
ステップ 4	**show aaa servers** 例：	AAA サーバー 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

	コマンドまたはアクション	目的
	`Device# show aaa servers`	バー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、ユーザーはローカル 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、ユーザー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ーが認証済みの場合、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 サーバー 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 サーバーと RADIUS サーバー 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 サーバーが応答しない場合）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 ユーザー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固有の 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 サーバーを設定するには、**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 サーバー 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 サーバーと RADIUS サーバー 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 サーバーがスタティック ルートと IP プール定義について RADIUS サーバー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 サーバーが応答しない場合）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 ユーザーに割り当てます。
- **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：同じサーバー IP アドレスを持つ複数の RADIUS サーバー 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 サーバーを設定する例を示します。同じ RADIUS サーバー上にある 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 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。 • Catalyst 3850 シリーズ スイッチ • Cisco 5760 Wireless LAN Controller • Catalyst 3650 シリーズ スイッチ

機能名	リリース	機能情報
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 サーバーに関連する統計情報を提供します。 • Catalyst 3850 シリーズ スイッチ • Cisco 5760 Wireless LAN Controller • Catalyst 3650 シリーズ スイッチ 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**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。