



## RADIUS と TACACS+ サーバの設定

---

この章では、Remote Authentication Dial-In User Service (RADIUS) と Terminal Access Controller Access Control System Plus (TACACS+) を有効にして設定する方法について説明します。RADIUS と TACACS+ は、認証プロセスと許可プロセスに詳細なアカウント情報と柔軟な管理制御を提供します。RADIUS および TACACS+ は AAA を通じて効率化され、AAA コマンドでのみ有効に設定できます。



(注)

---

この章で使用されるコマンドの完全な構文と使用方法については、『Cisco IOS Security Command Reference for Release 12.2』を参照してください。

---

この章の内容は、次のとおりです。

- [RADIUS の設定と有効化 \(P.11-2\)](#)
- [TACACS+ の設定と有効化 \(P.11-16\)](#)

## RADIUS の設定と有効化

この項では、RADIUS を設定して有効にする方法について説明します。次の各項で RADIUS の設定について説明します。

- RADIUS の概要 (P.11-2)
- RADIUS の操作 (P.11-3)
- RADIUS の設定 (P.11-4)
- RADIUS 設定の表示 (P.11-15)

### RADIUS の概要

RADIUS はネットワークを不正アクセスから保護する、分散型クライアント / サーバシステムです。RADIUS クライアントは RADIUS をサポートするシスコ デバイス上で動作し、中央 RADIUS サーバに認証要求を送信します。RADIUS サーバには、ユーザ認証情報とネットワーク サービス アクセス情報がすべて格納されます。通常、RADIUS ホストは、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 ソフトウェアは、シスコ (Cisco Secure Access Control Server バージョン 3.0)、Livingston、Merit、Microsoft、その他のソフトウェア プロバイダから提供されています。詳細は、RADIUS サーバの資料を参照してください。

RADIUS は、次のようなアクセス セキュリティを必要とするネットワーク環境で使用します。

- それぞれが RADIUS をサポートするマルチベンダー アクセス サーバを含むネットワーク。たとえば、複数のベンダーのアクセス サーバは単一の RADIUS サーバ ベースのセキュリティ データベースを使用します。マルチベンダーのアクセス サーバを使用する IP ベースのネットワークでは、ダイヤルイン ユーザは Kerberos セキュリティ システムを使用するようにカスタマイズされた RADIUS サーバを通じて認証されます。
- 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。これは、スマート カードアクセス制御システムを使用するようなアクセス環境です。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 カードと共に使用されています。
- 既に RADIUS を使用しているネットワーク。ネットワークには、RADIUS クライアントを含むシスコブリッジを追加できます。
- リソース アカウンティングを必要とするネットワーク。RADIUS アカウンティングは、RADIUS 認証または許可とは無関係に使用できます。RADIUS アカウンティング機能により、サービスの開始および終了時に、セッションの間に使用されるリソース (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。インターネット サービス プロバイダは、特別なセキュリティと課金のニーズを満たすために、フリーウェア版の RADIUS アクセス制御およびアカウンティング ソフトウェアを使用することがあります。

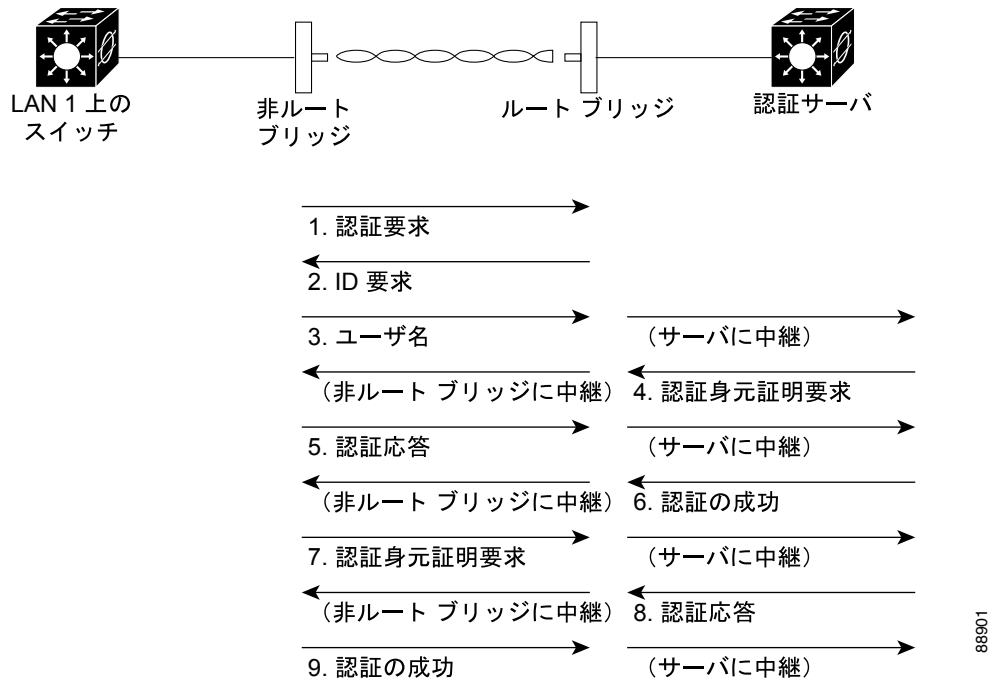
RADISU は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコルアクセス環境。RADIUS は AppleTalk Remote Access (ARA)、NetBIOS Frame Control Protocol (NBFCP)、NetWare Asynchronous Services Interface (NASI)、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間の状況。RADIUS は双方向認証を提供しません。シスコ以外のデバイスが認証を要求する場合、RADIUS を使用してあるデバイスからシスコ以外のデバイスに対して認証を実行できます。
- 各種サービスを使用するネットワーク。一般に RADIUS は、ユーザを 1 つのサービス モデルにバインドします。

## RADIUS の操作

非ルートブリッジが、RADIUS サーバによってアクセス制御されるブリッジへの認証を試行する場合、ネットワークへの認証は [図 11-1](#) に示す手順で実行されます。

図 11-1 EAP 認証のシーケンス



[図 11-1](#) の 1～9 では、有線 LAN 上の非ルートブリッジと RADIUS サーバが 802.1x および EAP を使用して、ルートブリッジ経由で相互認証を実行します。RADIUS サーバは、認証身元証明要求を非ルートブリッジに送信します。非ルートブリッジはユーザが入力したパスワードを一方方向暗号化し、認証身元証明要求に対する応答を生成して RADIUS サーバに送信します。RADIUS サーバは、サーバ自体のユーザデータベースの情報から独自の応答を生成し、それを非ルートブリッジからの応答と比較します。RADIUS サーバが非ルートブリッジを認証すると、同じ処理が逆方向から繰り返され、今度は非ルートブリッジが RADIUS サーバを認証します。

相互認証が終了すると、RADIUS サーバと非ルートブリッジは、非ルートブリッジ固有の WEP キーを特定して、適切なレベルのネットワークアクセスを提供します。これにより、有線のスイッチドセグメントのセキュリティレベルは、個々のデスクトップのレベルまで近付きます。非ルートブリッジはこのキーをロードして、ログオンセッションでの使用に備えます。

ログオンセッションでは、RADIUS サーバがセッションキーと呼ばれる WEP キーを暗号化し、有線 LAN 経由でルートブリッジに送信します。ルートブリッジは、セッションキーを使用してブロードキャストキーを暗号化し、非ルートブリッジに送信します。非ルートブリッジは、送信されてきたキーを、セッションキーを使用して復号化します。非ルートブリッジとルートブリッジが WEP を有効にして、セッションおよびブロードキャスト WEP キーを残りのセッションのすべての通信に使用します。

EAP 認証には複数のタイプがありますが、ルートブリッジはどのタイプについても同じように機能します。すなわち、非ルートブリッジから RADIUS サーバに、RADIUS サーバから非ルートブリッジに、認証メッセージを中継します。RADIUS サーバを使用した認証の設定方法の詳細は、「[SSID への認証タイプの割り当て](#)」の項 (P.10-5) を参照してください。

## RADIUS の設定

この項では、RADIUS をサポートするようブリッジを設定する方法について説明します。ユーザは最低でも、RADIUS サーバソフトウェアを実行するホストを識別し、RADIUS の認証方式リストを定義する必要があります。オプションで、RADIUS 認証とアカウントिंगの方式リストを定義できます。

方式リストは、非ルートブリッジのアカウントの認証、許可、管理に使用される手順と方法を定義します。方式リストを使用して 1 つまたは複数のセキュリティプロトコルを指定できるので、先頭の方式が失敗してもバックアップシステムが確実に機能できます。ソフトウェアは、リストの先頭の方式を使用して非ルートブリッジのアカウントの認証、許可、管理をします。その方式が応答しない場合には、リストの次の方式が選択されます。このプロセスは、リスト内の方式との通信に成功するか、または方式リストをすべて試行するまで続けられます。

ブリッジに RADIUS 機能を設定する前に、RADIUS サーバにアクセスして RADIUS サーバを設定する必要があります。

この項で説明する設定の内容は次のとおりです。

- デフォルトの RADIUS 設定 (P.11-4)
- RADIUS サーバホストの識別 (P.11-4) (必須)
- RADIUS ログイン認証の設定 (P.11-7) (必須)
- AAA サーバグループの定義 (P.11-9) (オプション)
- ユーザ特権アクセスとネットワークサービスの RADIUS 許可の設定 (P.11-11) (オプション)
- RADIUS アカウントिंगの起動 (P.11-12) (オプション)
- すべての RADIUS サーバの設定 (P.11-13) (オプション)
- ベンダー固有の RADIUS 属性を使用するブリッジの設定 (P.11-14) (オプション)
- ベンダー専用の RADIUS サーバ通信用ブリッジの設定 (P.11-15) (オプション)



(注) RADIUS サーバの CLI コマンドは、**aaa new-model** コマンドを入力するまで無効になっています。

### デフォルトの RADIUS 設定

RADIUS と AAA は、デフォルトでは無効になっています。

セキュリティ上の危険を回避するため、ネットワーク管理アプリケーションから RADIUS を設定することはできません。RADIUS を有効にすると、CLI を通じてブリッジにアクセスするユーザを認証できます。

### RADIUS サーバホストの識別

アクセスポイントと RADIUS サーバ間の通信には、次のいくつかのコンポーネントを使用します。

- ホスト名または IP アドレス
- 認証先ポート
- アカウントिंग宛先ポート
- キー文字列
- タイムアウト期間
- 再送信値

RADIUS セキュリティ サーバは、ホスト名と IP アドレス、ホスト名と特定の UDP ポート番号、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 ポート番号の組み合わせから一意の識別子が作成され、異なるポートを特定の 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。この一意の識別子を使用すると、サーバ上の同じ IP アドレスを持つ複数の UDP ポートに RADIUS 要求を送信できます。

同一の RADIUS サーバにアカウントリングなど同じサービスを実行する 2 つのホスト エントリを設定すると、2 番目に設定されたホスト エントリは最初のホスト エントリの故障時のバックアップとして機能します。この例では、最初に設定されたホスト エントリがアカウントリング サービスに失敗すると、ブリッジは同じデバイスに設定された 2 番目のホスト エントリにアカウントリング サービスの提供を求めます (RADIUS ホスト エントリは、設定された順序で試行されます)。

RADIUS サーバとブリッジは、共有の身元証明要求テキスト文字列を使用して、パスワードを暗号化して応答を交換します。AAA セキュリティ コマンドを使用するように RADIUS を設定するには、RADIUS サーバ デーモンを実行するホストと、ブリッジと共有する身元証明要求テキスト (キー) 文字列を指定する必要があります。

タイムアウト、再送信、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することも、またはグローバル設定とサーバ単位の設定を組み合わせることも可能です。ブリッジと通信するすべての RADIUS サーバにこれらの設定をグローバルに適用するには、3 つの一意のグローバル設定コマンド **radius-server timeout**、**radius-server retransmit**、**radius-server key** 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、グローバル設定コマンド **radius-server host** を使用します。




(注)

ブリッジにグローバル機能とサーバ単位の機能 (タイムアウト、再送信、キー コマンド) を同時に設定する場合、サーバ単位のタイマ、再送信、キー値のコマンドが、グローバルなタイマ、再送信、キー値のコマンドより優先されます。すべての RADIUS サーバにこれらの設定を実行する情報は、「すべての RADIUS サーバの設定」の項 (P.11-13) を参照してください。

認証時に AAA サーバ グループを使用して既存のサーバ ホストをグループ化するようにブリッジを設定できます。詳細は、「AAA サーバ グループの定義」の項 (P.11-9) を参照してください。

イネーブル EXEC モードから、次の手順に従ってサーバ単位の RADIUS サーバ通信を設定します。この手順は必須です。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>aaa new-model</b>	AAA を有効にします。

	コマンド	目的
ステップ 3	<code>radius-server host</code> {<ホスト名> <IP アドレス>} [ <code>auth-port</code> <ポート番号>] [ <code>acct-port</code> <ポート番号>] [ <code>timeout</code> <秒数>] [ <code>retransmit</code> <再試行回数>] [ <code>key</code> <文字列>]	<p>リモート RADIUS サーバホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> <li>（オプション）<code>auth-port</code> &lt;ポート番号&gt; には、認証要求の UDP 宛先ポートを指定します。</li> <li>（オプション）<code>acct-port</code> &lt;ポート番号&gt; には、アカウントिंग要求の UDP 宛先ポートを指定します。</li> <li>（オプション）<code>timeout</code> &lt;秒数&gt; には、ブリッジが RADIUS サーバの返答を待ち、再送信するまでの時間を指定します。指定範囲は 1 ~ 1000 です。この設定はグローバル設定コマンド <code>radius-server timeout</code> の設定よりも優先されます。<code>radius-server host</code> コマンドにタイムアウトが設定されていない場合、<code>radius-server timeout</code> コマンドの設定が使用されます。</li> <li>（オプション）<code>retransmit</code> &lt;再試行回数&gt; には、サーバが応答しないか応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。範囲は 1 ~ 1000 です。<code>radius-server host</code> コマンドでこの再送回数を設定しない場合は、グローバル設定コマンド <code>radius-server retransmit</code> の設定が使用されます。</li> <li>（オプション）<code>key</code> &lt;文字列&gt; には、RADIUS サーバで動作する RADIUS デーモンとブリッジの間で使用される認証と暗号キーを指定します。</li> </ul> <p> (注) このキーはテキスト文字列で、RADIUS サーバで使用される暗号キーと一致する必要があります。キーは常に <code>radius-server host</code> コマンドの最後の項目として設定します。先頭の空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないとください。</p> <p>ブリッジが単一の IP アドレスと関連付けられた複数のホストエントリを認識するように設定するには、このコマンドを必要な数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。ブリッジソフトウェアは、指定された順序でホストを検索します。個々の RADIUS ホストで使用するタイムアウト、再送信、暗号キーの値を設定します。</p>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	（オプション）コンフィギュレーションファイルに入力内容を保存します。

指定された RADIUS サーバを削除するには、グローバル設定コマンド `no radius-server host` <ホスト名>|<IP アドレス> を使用します。

次の例は、認証に使用される RADIUS サーバと、アカウントングに使用される別の RADIUS サーバの設定方法を示しています。

```
BR(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
BR(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次の例は、RADIUS サーバとして *host1* を設定して、認証とアカウントングの両方にデフォルトポートを使用する方法を示しています。

```
BR(config)# radius-server host host1
```



(注) RADIUS サーバにはほかにも複数の設定が必要です。その設定には、ブリッジの IP アドレスおよびサーバとブリッジで共有するキー文字列が含まれます。詳細は、RADIUS サーバの資料を参照してください。

## RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外は、デフォルトの方式リスト (名前は、*default*) です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。

方式リストには、ユーザ (この場合は、非ルートブリッジ) の認証時に照会されるシーケンスと認証方式が記述されています。認証に使用するセキュリティプロトコルを1つまたは複数指定できるため、最初の方法が失敗した場合でも認証のバックアップシステムが確実に機能します。ソフトウェアは、まずリストの最初の方法を使用してユーザを認証します。その方式が応答しなければ、方式リストの次の認証方式を選択します。このプロセスは、リスト内の認証方式との通信が成功するか、定義済みの方式をすべて試行するまで続けられます。このサイクルのどの認証にも失敗する場合、つまりセキュリティサーバまたはローカルユーザ名データベースがユーザアクセスの拒否を応答した場合、認証プロセスは停止して、他の認証方式は試行されません。

イネーブル EXEC モードから、次の手順に従ってログイン認証を設定します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA を有効にします。

	コマンド	目的
ステップ 3	<code>aaa authentication login {default  &lt; リスト名 &gt;} &lt;方式 1&gt; [&lt;方式 2...&gt;]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> <li><b>login authentication</b> コマンドで名前付きのリストが指定されていない場合に使用するデフォルトのリストを作成するには、<b>default</b> キーワードの後にデフォルトで使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。リスト名の詳細は、次のリンクをクリックしてください。 <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2</a></li> <li>&lt;方式 1...&gt; には、認証アルゴリズムが試行する実際の方式を指定します。2 番目以降の認証方式が使用されるのは、その前の方式からエラーが返された場合に限られます。前の方式が失敗した場合にはありません。</li> </ul> <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> <li><b>line</b> : 認証に回線パスワードを使用します。この認証方式を使用する前に、回線パスワードを定義する必要があります。回線設定コマンド <b>password</b> &lt;パスワード&gt; を使用します。</li> <li><b>local</b> : 認証にローカル ユーザ名データベースを使用します。データベースにユーザ名情報を入力する必要があります。グローバル設定コマンド <b>username</b> &lt;パスワード&gt; を使用します。</li> <li><b>radius</b> : RADIUS 認証を使用します。この認証方式を使用するには、事前に TACACS+ サーバを設定しておく必要があります。詳細は、「RADIUS サーバホストの識別」の項 (P.11-4) を参照してください。</li> </ul>
ステップ 4	<code>line [console   tty   vty] &lt;回線番号&gt; [&lt;終了回線番号&gt;]</code>	回線設定モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	<code>login authentication {default  &lt;リスト名&gt;}</code>	<p>認証リストを 1 つまたは複数の回線に適用します。</p> <ul style="list-style-type: none"> <li><b>default</b> を指定すると、<b>aaa authentication login</b> コマンドで作成したデフォルトリストを使用します。</li> <li>&lt;リスト名&gt; には、<b>aaa authentication login</b> コマンドで作成したリストを指定します。</li> </ul>
ステップ 6	<code>radius-server attribute 32 include-in-access-req format %h</code>	認証時に NAS_ID 属性でシステム名を送信するようにブリッジを設定します。
ステップ 7	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 8	<code>show running-config</code>	入力内容を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーションファイルに入力内容を保存します。

AAA を無効にするには、グローバル設定コマンド **no aaa new-model** を使用します。AAA 認証を無効にするには、グローバル設定コマンド **no aaa authentication login {default |<リスト名>} <方式 1> [<方式 2...>]** を使用します。ログイン時の RADIUS 認証を無効にするか、デフォルト値に戻すには、回線設定コマンド **no login authentication {default |<リスト名>}** を使用します。



## AAA サーバグループの定義


認証時に AAA サーバグループを使用して既存のサーバホストをグループ化するようブリッジを設定できます。設定されたサーバホストのサブセットを選択して、特定のサービスに使用します。このサーバグループは、グローバルサーバホストリストで使用されます。このリストには、選択されたサーバホストの IP アドレスのリストが示されています。

サーバグループには、各ホストエントリが一意の識別子 (IP アドレスと UDP ポート番号の組み合わせ) を持っていれば、同一サーバに対する複数のホストエントリを含めることも可能で、それによって、特定の AAA サービスを提供する RADIUS ホストとして異なるポートを個別に定義できます。同一の RADIUS サーバにアカウントリングなど同じサービスを実行する 2 つのホストエントリを設定すると、2 番目に設定されたホストエントリは最初のホストエントリの故障時のバックアップとして機能します。

特定のサーバに定義済みグループサーバをアソシエートするには、グループサーバ設定コマンド **server** を使用します。IP アドレスでサーバを特定するか、オプションの **auth-port** および **acct-port** キーワードを使用して複数のホストインスタンスまたはエントリを特定できます。

イネーブル EXEC モードから、次の手順に従って、AAA サーバグループを定義し、特定の RADIUS サーバをそのグループにアソシエートします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA を有効にします。

	コマンド	目的
ステップ 3	radius-server host {<ホスト名> <IP アドレス>} [auth-port <ポート番号>] [acct-port <ポート番号>] [timeout <秒数>] [retransmit <再試行回数>] [key <文字列>]	<p>リモート RADIUS サーバホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> <li>（オプション） <b>auth-port</b> &lt;ポート番号&gt; には、認証要求の UDP 宛先ポートを指定します。</li> <li>（オプション） <b>acct-port</b> &lt;ポート番号&gt; には、アカウント要求の UDP 宛先ポートを指定します。</li> <li>（オプション） <b>timeout</b> &lt;秒数&gt; には、ブリッジが RADIUS サーバの返答を待ち、再送信するまでの時間を指定します。指定範囲は 1 ~ 1000 です。この設定はグローバル設定コマンド <b>radius-server timeout</b> の設定よりも優先されます。<b>radius-server host</b> コマンドにタイムアウトが設定されていない場合、<b>radius-server timeout</b> コマンドの設定が使用されます。</li> <li>（オプション） <b>retransmit</b> &lt;再試行回数&gt; には、サーバが応答しないか応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。範囲は 1 ~ 1000 です。<b>radius-server host</b> コマンドでこの再送回数を設定しない場合は、グローバル設定コマンド <b>radius-server retransmit</b> の設定が使用されます。</li> <li>（オプション） <b>key</b> &lt;文字列&gt; には、RADIUS サーバで動作する RADIUS デーモンとブリッジの間で使用される認証と暗号キーを指定します。</li> </ul> <p> (注) このキーはテキスト文字列で、RADIUS サーバで使用される暗号キーと一致する必要があります。キーは常に <b>radius-server host</b> コマンドの最後の項目として設定します。先頭の空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないでください。</p> <p>ブリッジが単一の IP アドレスと関連付けられた複数のホストエントリを認識するように設定するには、このコマンドを必要な数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。ブリッジソフトウェアは、指定された順序でホストを検索します。個々の RADIUS ホストで使用するタイムアウト、再送信、暗号キーの値を設定します。</p>
ステップ 4	aaa group server radius <グループ名>	<p>AAA サーバグループをグループ名で定義します。</p> <p>このコマンドを実行すると、ブリッジはサーバグループ設定モードへ移行します。</p>
ステップ 5	server <IP アドレス>	<p>特定の RADIUS サーバを定義されたサーバグループにアソシエートします。この手順を、AAA サーバグループの各 RADIUS サーバについて繰り返します。</p> <p>グループ内の各サーバは、手順 2 であらかじめ定義されている必要があります。</p>
ステップ 6	end	イネーブル EXEC モードに戻ります。
ステップ 7	show running-config	入力内容を確認します。

	コマンド	目的
ステップ 8	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。
ステップ 9		RADIUS ログイン認証を有効にします。「 <a href="#">RADIUS ログイン認証の設定</a> 」の項 (P.11-7) を参照してください。

指定された RADIUS サーバを削除するには、グローバル設定コマンド `no radius-server host <ホスト名> | <IP アドレス>` を使用します。設定リストからサーバグループを削除するには、グローバル設定コマンド `no aaa group server radius <グループ名>` を使用します。RADIUS サーバの IP アドレスを削除するには、サーバグループ設定コマンド `no server <IP アドレス>` を使用します。

次の例では、ブリッジは異なる 2 つの RADIUS グループサーバ (*group1* と *group2*) を認識するように設定されます。*group1* には、同じ RADIUS サーバで同じサービス用に設定された異なる 2 つのホストエントリがあります。2 番目のホストエントリは、最初のエントリに対して故障時のバックアップとして機能します。

```
BR(config)# aaa new-model
BR(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
BR(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
BR(config)# aaa group server radius group1
BR(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
BR(config-sg-radius)# exit
BR(config)# aaa group server radius group2
BR(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
BR(config-sg-radius)# exit
```

## ユーザ特権アクセスとネットワーク サービスの RADIUS 許可の設定

AAA 許可は、ユーザが使用できるサービスを制限します。AAA 許可が有効の場合、ブリッジはユーザのプロファイルから取得した情報を使用してユーザのセッションを設定します。ユーザのプロファイルは、ローカルユーザデータベースかセキュリティサーバにあります。ユーザが要求したサービスへのアクセスを許可されるのは、ユーザプロファイル内の情報により許可された場合だけです。



(注) この項では、ブリッジ管理者向けに許可の設定を説明します。

グローバル設定コマンド `aaa authorization` と `radius` キーワードを使用すると、ユーザのネットワークアクセスをイネーブル EXEC モードに制限するパラメータを設定できます。

これらの許可パラメータは、`aaa authorization exec radius local` コマンドで設定します。

- 認証に RADIUS が使用された場合は、イネーブル EXEC アクセス許可に RADIUS を使用します。
- 認証に RADIUS が使用されなかった場合は、ローカルデータベースを使用します。



(注) 許可が設定されている場合でも、CLI からログインする認証ユーザに対しては、許可が省略されます。

## RADIUS の設定と有効化

イネーブル EXEC モードから、次の手順に従ってイネーブル EXEC アクセスとネットワーク サービスに RADIUS 許可を指定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	<code>aaa authorization network radius</code>	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるようにブリッジを設定します。
ステップ 3	<code>aaa authorization exec radius</code>	ユーザの RADIUS 許可でユーザのイネーブル EXEC アクセス権の有無を判断するように、ブリッジを設定します。  <code>exec</code> キーワードにより、ユーザ プロファイル情報 ( <code>autocommand</code> 情報など) が返される場合があります。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

許可を無効にするには、グローバル設定コマンド `no aaa authorization {network | exec} <方式 1>` を使用します。

## RADIUS アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしているサービスと、サービスが消費しているネットワーク リソースの量を追跡します。AAA アカウンティングが有効の場合、ブリッジはアカウンティングの記録の形式でユーザ アクティビティを RADIUS セキュリティ サーバに報告します。各アカウンティングの記録にはアカウンティング属性と値のペア (AV) が含まれており、セキュリティ サーバに保存されます。その後このデータは、ネットワーク管理、クライアントへの課金、または監査のために分析されます。



イネーブル EXEC モードから、次の手順に従って Cisco IOS 特権レベルとネットワーク サービスに RADIUS アカウンティングを有効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	<code>aaa accounting network start-stop radius</code>	ネットワーク関連のすべてのサービス要求に、RADIUS アカウンティングを有効にします。
ステップ 3	<code>ip radius source-interface bvi1</code>	アカウンティングの記録として BVI IP アドレスを <code>NAS_IP_ADDRESS</code> 属性で送信するようにブリッジを設定します。
ステップ 4	<code>aaa accounting update periodic &lt;分数&gt;</code>	アカウンティングの更新間隔を分で入力します。
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	入力内容を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

アカウンティングを無効にするには、グローバル設定コマンド `no aaa accounting {network | exec} {start-stop} <方式 1...>` を使用します。

## すべての RADIUS サーバの設定

イネーブル EXEC モードから、次の手順に従ってブリッジとすべての RADIUS サーバ間のグローバル通信設定を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	<code>radius-server key &lt;文字列&gt;</code>	ブリッジとすべての RADIUS サーバ間で使用する共有の身元証明要求テキスト文字列を指定します。   (注) このキーはテキスト文字列で、RADIUS サーバで使用される暗号キーと一致する必要があります。先頭の空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないでください。
ステップ 3	<code>radius-server retransmit &lt;再試行回数&gt;</code>	ブリッジが RADIUS 要求をサーバに送信して、中止するまでの回数を指定します。デフォルトは 3、範囲は 1 ~ 1000 です。
ステップ 4	<code>radius-server timeout &lt;秒数&gt;</code>	ブリッジが RADIUS 要求を再送する前に、要求への応答を待機する時間を秒数で指定します。デフォルトは 5、範囲は 1 ~ 1000 です。
ステップ 5	<code>radius-server deadtime &lt;分数&gt;</code>	このコマンドは、Cisco IOS ソフトウェアで認証要求に応答しない RADIUS サーバを「dead」とマークして、要求の待機がタイムアウトになる前に、設定された次のサーバを試行する場合に使用します。dead とマークされている RADIUS サーバの場合、またはすべての RADIUS サーバが dead とマークされている場合、指定する時間（分）の間、追加の要求はスキップされます。   (注) 複数の RADIUS サーバを設定した場合、パフォーマンスの最適化のために RADIUS サーバのデッドタイムを設定する必要があります。
ステップ 6	<code>radius-server attribute 32 include-in-access-req format %h</code>	認証時に NAS_ID 属性でシステム名を送信するようにブリッジを設定します。
ステップ 7	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 8	<code>show running-config</code>	設定内容を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

再送信、タイムアウト、デッドタイムをデフォルトの設定に戻すには、それぞれのコマンドで `no` を指定します。

## ベンダー固有の RADIUS 属性を使用するブリッジの設定

Internet Engineering Task Force (IETF) のドラフト規格では、ブリッジと RADIUS サーバ間での、ベンダー固有の属性 (属性 26) を使用した、ベンダー固有の情報の通信方法を指定しています。ベンダーは、Vendor-Specific Attributes (VSA; ベンダー固有の属性) を使用することで、汎用には適していない各社固有の拡張属性に対応できます。シスコの RADIUS 実装では、仕様で推奨される形式を使用することで、ベンダー固有オプションを 1 つサポートします。シスコのベンダー ID は 9 です。サポートされるオプションはベンダータイプ 1 であり、*cisco-avpair* という名前が付けられています。この値は、次の形式の文字列です。

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

*potocol* は特定の許可を受けるためのシスコ プロトコル属性の値です。*attribute* と *value* は、Cisco TACACS+ 仕様で定義された該当 AV ペアです。*sep* の必須属性には = を、オプション属性にはアスタリスク (\*) を指定します。このコマンドにより、TACACS+ 許可で使用できる全機能が RADIUS でも使用できます。

たとえば、次の AV ペアは IP 許可の際 (PPP の IPCP アドレス割り当ての際)、シスコの *multiple named ip address pools* 機能を有効にします。

```
cisco-avpair= "ip:addr-pool=first"
```

次の例は、イネーブル EXEC コマンドへの即時アクセスを使用してユーザがブリッジからログインできるようにする方法を示しています。

```
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。ベンダーの ID と VSA についての詳細は、RFC 2138 「Remote Authentication Dian-In User Service (RADIUS)」を参照してください。

イネーブル EXEC モードから、次の手順に従って、VSA を認識して使用するようブリッジを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	<code>radius-server vsa send [accounting   authentication]</code>	ブリッジが RADIUS IETF 属性 26 で定義された VSA を認識して使用できるようにします。 <ul style="list-style-type: none"> <li>(オプション) 認識されたベンダー固有の属性セットをアカウント属性だけに制限するには、<b>accounting</b> キーワードを使用します。</li> <li>(オプション) 認識されたベンダー固有の属性セットを認証属性だけに制限するには、<b>authentication</b> キーワードを使用します。</li> </ul> キーワードを指定しないでこのコマンドを入力すると、アカウントと認証の両方のベンダー固有属性が使用されます。
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーションファイルに入力内容を保存します。


RADIUS 属性の完全なリスト、または VSA 26 の詳細は、『Cisco IOS Security Configuration Guide for Release 12.2』の付録「RADIUS Attributes」を参照してください。

## ベンダー専用の RADIUS サーバ通信用ブリッジの設定

IETF の RADIUS ドラフト規格では、ブリッジと RADIUS サーバの間でベンダー専用の情報を通信する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 IOS ソフトウェアは、ベンダー専用の RADIUS 属性のサブセットをサポートします。

すでに説明したように、ベンダー専用または IETF ドラフト準拠の RADIUS を設定するには、RADIUS サーバデーモンを実行するホストと、そのホストがブリッジと共有する身元証明要求テキストを指定する必要があります。RADIUS ホストと身元証明要求テキストは、グローバル設定コマンド **radius-server** を使用して指定します。

イネーブル EXEC モードから、次の手順に従ってベンダー専用の RADIUS サーバ ホストおよび共有の身元証明要求テキストを指定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>radius-server host</b> {< ホスト名 > < IP アドレス >} <b>non-standard</b>	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、ホストがベンダー専用の RADIUS 実装を使用していることを識別します。
ステップ 3	<b>radius-server key</b> < 文字列 >	ブリッジとベンダー専用の RADIUS サーバ間で使用する共有の身元証明要求テキスト文字列を指定します。ブリッジと 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。   <b>(注)</b> このキーはテキスト文字列で、RADIUS サーバで使用される暗号キーと一致する必要があります。先頭の空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないでください。
ステップ 4	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	設定内容を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

ベンダー専用の RADIUS ホストを削除するには、グローバル設定コマンド **no radius-server host** {< ホスト名 >|< IP アドレス >} **non-standard** を使用します。キーを無効にするには、グローバル設定コマンド **no radius-server key** を使用します。

次の例は、ベンダー専用の RADIUS ホストを指定して、ブリッジとサーバ間で秘密キー *rad124* を使用する方法を示しています。

```
BR(config)# radius-server host 172.20.30.15 nonstandard
BR(config)# radius-server key rad124
```

## RADIUS 設定の表示

RADIUS 設定を表示するには、**show running-config** イネーブル EXEC コマンドを使用します。

## TACACS+ の設定と有効化

この項で説明する設定の内容は次のとおりです。

- TACACS+ の概要 (P.11-16)
- TACACS+ の操作 (P.11-17)
- TACACS+ の設定 (P.11-17)
- TACACS+ 設定の表示 (P.11-22)

### TACACS+ の概要

TACACS+ は、ブリッジにアクセスしようとするユーザを集中的に検証するセキュリティ アプリケーションです。RADIUS とは異なり、TACACS+ はルートブリッジにアソシエートされた非ルートブリッジを認証しません。

TACACS+ サービスは、通常 UNIX または Windows NT ワークステーションで動作する TACACS+ デーモンのデータベース内で管理されます。ブリッジに TACACS+ 機能を設定する前に、TACACS+ サーバにアクセスして TACACS+ サーバを設定する必要があります。

TACACS+ には独立したモジュール式の認証、許可、およびアカウンティング機能が備わっています。TACACS+ によって、単一のアクセス制御サーバ (TACACS+ デーモン) が、認証、許可、アカウンティングの各サービスを個別に提供できます。各サービスを独自のデータベースと関連付けて、デーモンの機能に応じて、サーバまたはネットワークで使用できる他のサービスを利用することができます。

AAA セキュリティ サービスを通じて管理される TACACS+ は、次のようなサービスを提供します。

- 認証：ログインとパスワードのダイアログ、身元証明要求と応答、メッセージのサポートを通じて管理者の認証を完全に制御します。  
認証機能は、管理者との対話を実行できます (たとえば、ユーザ名とパスワードが入力された後に、自宅住所、母親の旧姓、サービスタイプ、社会保険番号など、複数の質問でユーザの身元を確認します)。また TACACS+ 認証サービスは、管理者の画面にメッセージを送信できます。たとえば、会社のパスワード エージング ポリシーのため、パスワードを変更する必要があります。このことをメッセージで管理者に通知することができます。
- 許可：管理者のセッション期間中の管理機能を詳細に制御します。これには自動コマンドの設定、アクセス制御、セッション期間、またはプロトコルサポートなどが含まれますが、それに限定されません。また、管理者が TACACS+ 許可機能で実行できるコマンドを強制的に制限できます。
- アカウンティング：課金、監査、報告に使用される情報を収集して、TACACS+ デーモンに送信します。ネットワーク マネージャはアカウンティング機能を使用して、セキュリティ監査時に管理者アクティビティを追跡したり、またはユーザの課金時に情報を提供できます。アカウンティングレコードには、管理者 ID、開始時間と終了時間、実行されたコマンド (PPP など)、パケット数、バイト数が含まれます。

TACACS+ プロトコルは、ブリッジと TACACS+ デーモンの間で認証を実行します。ブリッジと TACACS+ デーモンの間で実行されるすべてのプロトコル交換が暗号化されるので、認証の機密性が確保されます。

ブリッジで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアを実行するシステムが必要です。



## TACACS+ の操作

管理者が TACACS+ を使用してブリッジの認証を受け、簡単な ASCII ログインを試行した場合、次のプロセスが発生します。

1. 接続が確立されると、ブリッジは TACACS+ デーモンに連絡してユーザ名プロンプトを取得し、このプロンプトが管理者に表示されます。管理者がユーザ名を入力すると、ブリッジは TACACS+ デーモンに連絡してパスワードプロンプトを取得します。ブリッジは管理者にパスワードプロンプトを表示し、管理者がパスワードを入力すると、パスワードは TACACS+ デーモンに送信されます。

TACACS+ を使用してデーモンと管理者との間で会話が続けられ、デーモンは管理者の認証に必要な情報を取得します。デーモンはユーザ名とパスワードの組み合わせの入力を要求しますが、ユーザの母親の旧姓など、他の項目が含まれる場合があります。

2. ブリッジは最終的に、TACACS+ デーモンから次に示す応答のいずれかを受信します。
  - ACCEPT: 管理者が認証され、サービスが開始します。許可を要求するようにブリッジが設定されている場合、この時点で許可が開始します。
  - REJECT: 管理者は認証されません。管理者は TACACS+ デーモンに従ってアクセスが拒否されるか、ログインシーケンスを再試行するように要求されます。
  - ERROR: デーモンによる認証のある時点、またはデーモンとブリッジ間のネットワーク接続で、エラーが発生しています。ERROR 応答を受信した場合、通常、ブリッジは、別の方法で管理者の認証を試行します。
  - CONTINUE: 管理者は追加の認証情報を要求されます。

認証の後、ブリッジで許可が有効になっている場合、管理者はさらに許可フェーズに進みます。管理者は TACACS+ 許可に進む前に、まず TACACS+ 認証を完了する必要があります。

3. TACACS+ 許可が要求される場合、再び TACACS+ デーモンにアクセスします。TACACS+ デーモンは ACCEPT か REJECT の許可応答を返します。ACCEPT 応答が返された場合、この応答には属性の形でその管理者に EXEC または NETWORK セッションを指示するデータが含まれており、管理者がアクセスできる下記のサービスを決定できます。
  - Telnet、rlogin、またはイネーブル EXEC サービス
  - 接続パラメータ。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、管理者のタイムアウトが含まれます。

## TACACS+ の設定

この項では、TACACS+ をサポートするようブリッジを設定する方法について説明します。ユーザは最低でも TACACS+ デーモンを実行するホストを識別して、TACACS+ 認証の方式リストを定義する必要があります。オプションで、TACACS+ 認証とアカウントングの方式リストを定義できます。方式リストは管理者アカウントの認証、許可、管理に使用される手順と方法を定義します。方式リストを使用して1つまたは複数のセキュリティプロトコルを指定できるので、先頭の方式が失敗してもバックアップシステムが確実に機能できます。ソフトウェアは、リストの先頭の方式を使用して管理者のアカウントの認証、許可、管理をします。その方式が応答しない場合には、リストの次の方式が選択されます。このプロセスは、リスト内の方式との通信に成功するか、または方式リストをすべて試行するまで続けられます。

この項で説明する設定の内容は次のとおりです。

- [デフォルト TACACS+ 設定 \(P.11-18\)](#)
- [TACACS+ サーバホストの識別と認証キーの設定 \(P.11-18\)](#)
- [TACACS+ ログイン認証の設定 \(P.11-19\)](#)
- [イネーブル EXEC アクセスとネットワーク サービスの TACACS+ 許可の設定 \(P.11-21\)](#)
- [TACACS+ アカウンティングの起動 \(P.11-21\)](#)

## デフォルト TACACS+ 設定

TACACS+ と AAA は、デフォルトでは無効になっています。

セキュリティの失効を防止するために、ネットワーク管理アプリケーションを通じて TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI を通じてブリッジにアクセスする管理者を認証できます。

## TACACS+ サーバホストの識別と認証キーの設定

認証時に単一サーバまたは AAA サーバグループを使用して既存のサーバホストをグループ化するようにブリッジを設定できます。サーバをグループ化し、設定されたサーバホストのサブセットを選択して特定のサービスに使用できます。このサーバグループは、グローバルサーバホストリストで使用され、選択されたサーバホストの IP アドレスのリストが含まれます。

イネーブル EXEC モードから、次の手順に従って TACACS+ サーバを実行する IP ホストを識別し、オプションで暗号キーを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	<code>tacacs-server host &lt;ホスト名&gt; [port &lt;整数&gt;] [timeout &lt;整数&gt;] [key &lt;文字列&gt;]</code>	TACACS+ サーバを管理している IP ホストを識別します。このコマンドを数回入力して、優先されるホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 <ul style="list-style-type: none"> <li>• &lt;ホスト名&gt; には、ホストの名前または IP アドレスを指定します。</li> <li>• (オプション) <code>port &lt;整数&gt;</code> には、サーバのポート番号を指定します。デフォルトはポート 49、範囲は 1 ~ 65535 です。</li> <li>• (オプション) <code>timeout &lt;整数&gt;</code> には、タイムアウトになってブリッジがエラーを宣言するまでにデーモンからの応答を待機する時間を秒数で指定します。デフォルト設定は 5 秒です。範囲は 1 ~ 1000 秒です。</li> <li>• (オプション) <code>key &lt;文字列&gt;</code> には、ブリッジと TACACS+ デーモンの間の全トラフィックを暗号化および復号化するための暗号キーを指定します。正常に暗号化するために、同じキーを TACACS+ デーモンに設定する必要があります。</li> </ul>
ステップ 3	<code>aaa new-model</code>	AAA を有効にします。
ステップ 4	<code>aaa group server tacacs+ &lt;グループ名&gt;</code>	(オプション) AAA サーバグループをグループ名で定義します。このコマンドを実行すると、ブリッジはサーバグループサブ設定モードへ移行します。
ステップ 5	<code>server &lt;IP アドレス&gt;</code>	(オプション) 特定の TACACS+ サーバを定義されたサーバグループにアソシエートします。この手順を、AAA サーバグループの各 TACACS+ サーバについて繰り返します。グループ内の各サーバは、手順 2 であらかじめ定義されている必要があります。
ステップ 6	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show tacacs</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーションファイルに入力内容を保存します。

指定された TACACS+ サーバ名またはアドレスを削除するには、グローバル設定コマンド **no tacacs-server host** <ホスト名> を使用します。設定リストからサーバグループを削除するには、グローバル設定コマンド **no aaa group server tacacs+** <グループ名> を使用します。TACACS+ サーバの IP アドレスを削除するには、サーバグループサブ設定コマンド **no server ip-address** を使用します。

## TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外は、デフォルトの方式リスト (名前は、*default*) です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義された方式リストは、デフォルトの方式リストよりも優先されます。

方式リストには、管理者を認証するクエリーのシーケンスと認証方式が記述されています。認証に使用するセキュリティプロトコルを 1 つまたは複数指定できるため、最初の方法が失敗した場合でも認証のバックアップシステムが確実に機能します。ソフトウェアは、まずリストの最初の方法を使用してユーザを認証します。その方式が応答しなければ、方式リストの次の認証方式を選択します。このプロセスは、リスト内の認証方式との通信が成功するか、定義済みの方式をすべて試行するまで続けられます。このサイクルのどの認証にも失敗する場合、つまりセキュリティサーバまたはローカルユーザ名データベースが管理者のアクセスの拒否を応答した場合、認証プロセスは停止して、他の認証方式は試行されません。

イネーブル EXEC モードから、次の手順に従ってログイン認証を設定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>aaa new-model</b>	AAA を有効にします。

	コマンド	目的
ステップ 3	<code>aaa authentication login {default   &lt;リスト名&gt;} &lt;方式 1&gt; [&lt;方式 2...&gt;]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> <li><b>login authentication</b> コマンドで名前付きのリストが指定されていない場合に使用するデフォルトのリストを作成するには、<b>default</b> キーワードの後にデフォルトで使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。</li> <li>&lt;リスト名&gt; には、作成するリストに付ける名前の文字列を指定します。</li> <li>&lt;方式 1...&gt; には、認証アルゴリズムが試行する実際の方式を指定します。2 番目以降の認証方式が使用されるのは、その前の方式からエラーが返された場合に限られます。前の方式が失敗した場合にはありません。</li> </ul> <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> <li><b>line</b> : 認証に回線パスワードを使用します。この認証方式を使用する前に、回線パスワードを定義する必要があります。回線設定コマンド <b>password</b> &lt;パスワード&gt; を使用します。</li> <li><b>local</b> : 認証にローカル ユーザ名データベースを使用します。データベースにユーザ名情報を入力する必要があります。グローバル設定コマンド <b>username</b> &lt;パスワード&gt; を使用します。</li> <li><b>tacacs+</b> : TACACS+ 認証を使用します。この認証方式を使用するには、事前に TACACS+ サーバを設定しておく必要があります。</li> </ul>
ステップ 4	<code>line [console   tty   vty] &lt;回線番号&gt; [&lt;終了回線番号&gt;]</code>	回線設定モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	<code>login authentication {default   &lt;リスト名&gt;}</code>	<p>認証リストを 1 つまたは複数の回線に適用します。</p> <ul style="list-style-type: none"> <li><b>default</b> を指定すると、<b>aaa authentication login</b> コマンドで作成したデフォルトリストを使用します。</li> <li>&lt;リスト名&gt; には、<b>aaa authentication login</b> コマンドで作成したリストを指定します。</li> </ul>
ステップ 6	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

AAA を無効にするには、グローバル設定コマンド **no aaa new-model** を使用します。AAA 認証を無効にするには、グローバル設定コマンド **no aaa authentication login {default | <リスト名>} <方式 1> [<方式 2...>]** を使用します。ログイン時の TACACS+ 認証を無効にするか、デフォルト値に戻すには、回線設定コマンド **no login authentication {default | <リスト名>}** を使用します。

## イネーブル EXEC アクセスとネットワーク サービスの TACACS+ 許可の設定

AAA 許可は、管理者が使用できるサービスを制限します。AAA 許可が有効の場合、ブリッジは管理者のプロファイルから取得した情報を使用して管理者のセッションを設定します。管理者のプロファイルは、ローカル ユーザ データベースかセキュリティ サーバにあります。管理者が要求したサービスへのアクセスが許可されるのは、管理者プロファイル内の情報により許可された場合だけです。

グローバル設定コマンド **aaa authorization** と **tacacs+** キーワードを使用すると、ユーザのネットワーク アクセスをイネーブル EXEC モードに制限するパラメータを設定できます。

これらの許可パラメータは、**aaa authorization exec tacacs+ local** コマンドで設定します。

- 認証に TACACS+ が使用された場合は、イネーブル EXEC アクセス許可に TACACS+ を使用します。
- 認証に TACACS+ が使用されなかった場合は、ローカル データベースを使用する。



(注)

CLI を通してログインした認証済み管理者は、許可が設定されていても許可が省略されます。

イネーブル EXEC モードから、次の手順に従ってイネーブル EXEC アクセスとネットワーク サービスに TACACS+ 許可を指定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>aaa authorization network tacacs+</b>	ネットワーク関連のすべてのサービス要求に対して、管理者が TACACS+ 許可を受けるようにブリッジを設定します。
ステップ 3	<b>aaa authorization exec tacacs+</b>	管理者の TACACS+ 許可で管理者のイネーブル EXEC アクセス権の有無を判断するように、ブリッジを設定します。  <b>exec</b> キーワードにより、ユーザプロファイル情報 ( <b>autocommand</b> 情報など) が返される場合があります。
ステップ 4	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	入力内容を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

許可を無効にするには、グローバル設定コマンド **no aaa authorization {network | exec} <方式 1>** を使用します。

## TACACS+ アカウンティングの起動

AAA アカウンティング機能は、管理者がアクセスしているサービスと、サービスが消費しているネットワーク リソースの量を追跡します。AAA アカウンティングが有効の場合、ブリッジはアカウンティングの記録の形で管理者のアクティビティを TACACS+ セキュリティ サーバに報告します。各アカウンティングの記録にはアカウンティング属性と値のペア (AV) が含まれており、セキュリティ サーバに保存されます。その後このデータは、ネットワーク管理、クライアントへの課金、または監査のために分析されます。

## ■ TACACS+ の設定と有効化

イネーブル EXEC モードから、次の手順に従って Cisco IOS 特権レベルとネットワーク サービスに TACACS+ アカウンティングを有効にします

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	<code>aaa accounting network start-stop tacacs+</code>	ネットワーク関連のすべてのサービス要求に対して、TACACS+ アカウンティングを有効にします。
ステップ 3	<code>aaa accounting exec start-stop tacacs+</code>	TACACS+ アカウンティングを有効にして、イネーブル EXEC プロセスの開始時に <code>start-record</code> アカウンティング通知を送信し、終了時に <code>stop-record</code> アカウンティング通知を送信します。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

アカウンティングを無効にするには、グローバル設定コマンド `no aaa accounting {network | exec} {start-stop} <方式 1...>` を使用します。

## TACACS+ 設定の表示

TACACS+ サーバ統計を表示するには、`show tacacs` イネーブル EXEC コマンドを使用します。