RADIUS の設定

Remote Authentication Dial-In User Service（RADIUS ）セキュリティ システムは、不正アクセスに対してネットワーク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 Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。RADIUS は完全にオープンなプロトコルであり、ソース コード形式で配布されているため、現在使用できる任意のセキュリティ システムと連携するように変更できます。

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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS の設定に関する機能情報」（P.45）を参照してください。

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

この章の構成

RADIUS の概要

シスコは、AAA セキュリティ パラダイムの下で RADIUS をサポートしています。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 はすべてのシスコ プラットフォームでサポートされていますが、一部の RADIUS 対応機能は特定のプラットフォームでだけ動作します。

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。

- 複数のベンダーのアクセス サーバで構成され、それぞれが RADIUS をサポートするネットワーク。たとえば複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベースのセキュリティ データベースを使用します。複数ベンダーのアクセス サーバがある IP ベースのネットワークの場合、Kerberos セキュリティ システムと連携するようにカスタマイズされた RADIUS サーバを介して、ダイヤルイン ユーザが認証されます。
- Turnkey ネットワーク セキュリティ環境。「スマート カード」コントロール システムを使用するアクセス環境など、アプリケーションが RADIUS プロトコルをサポートする環境です。ある事例では、RADIUS と Enigma のセキュリティ カードを併用してユーザを検証し、ネットワーク リソースに対するアクセス権を付与しています。
- すでに RADIUS を使用しているネットワーク。RADIUS 機能を持つ Cisco ルータをネットワークに追加できます。Terminal Access Controller Access Control System Plus（TACACS+）サーバに移行する場合、これが最初の手順となります。
- 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（Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル））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。
- リソースの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 認証や認可と無関係に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始と終了の時点にデータを送信し、そのセッション中に使用されたリソース（時間、パケット、バイトなど）の量を示すことができます。Internet service provider（ISP; インターネット サービス プロバイダー）は、RADIUS アクセス制御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、セキュリティおよび課金の独自ニーズを満たすこともできます。
- 事前認証のサポートを希望するネットワーク。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 PAD 接続
- ルータ間で接続している環境。RADIUS には双方向認証機能がありません。非 Cisco ルータが RADIUS 認証を必要としている場合、一方のルータから非 Cisco ルータへの接続を認証するために、RADIUS を使用できます。

- 多様なサービスを使用するネットワーク。通常、RADIUS は 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. プロンプトが表示され、ユーザはユーザ名およびパスワードを入力します。
2. ユーザ名と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。
   a. ACCEPT：ユーザが認証されたことを表します。
   b. REJECT：ユーザの認証が失敗し、ユーザ名およびパスワードの再入力を要求されるか、またはアクセスが拒否されます。
   c. CHALLENGE：RADIUS サーバによりチャレンジが送信されます。チャレンジによってユーザから追加データが収集されます。
   d. CHANGE PASSWORD：ユーザは新しいパスワードを選択するように RADIUS サーバから要求が送信されます。

ACCEPT または REJECT 応答には、EXEC 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。ユーザは RADIUS 認証が完了しないうちは RADIUS 許可を使用できません。ACCEPT または REJECT パケットに含まれる追加データには、次のものがあります。

- Telnet、rlogin、または Local-Area Transport（LAT; ローカルエリア トランスポート）、および PPP、Serial Line Internet Protocol（SLIP）、または EXEC サービスなどといった、ユーザがアクセスできるサービス。
- 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 アトリビュート

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 アトリビュートで定義されている 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。サポートされる RADIUS アトリビュートのリストの詳細については、「関連資料」（P.43）を参照してください。

ここでは、次の内容について説明します。

ベンダー固有 RADIUS アトリビュート

RADIUS の Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト規格には、ネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有情報を通信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 アトリビュートを拡張しています。Cisco IOS ソフトウェアは、RADIUS のベンダー固有アトリビュートの一部をサポートしています。詳細については、「関連資料」（P.43）を参照してください。

RADIUS トンネル アトリビュート

RADIUS は、元は Livingston, Inc. が開発した セキュリティ サーバの Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）プロトコルです。RADIUS は Attribute Value（AV; アトリビュート値）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 サーバ間で情報を通信します。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インターネット技術特別調査委員会（IETF）規格の AV ペアの初期セットについて説明しています。2 つのドラフト IETF 規格「RADIUS Attributes for Tunnel Protocol Support」と「RADIUS Accounting Modifications for Tunnel Protocol Support」は、IETF が定義した AV ペアを拡張して、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）に固有のアトリビュートを追加しました。これらのアトリビュートは、RADIUS サーバとトンネル イニシエータ間の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アトリビュートを追加しています。このアトリビュートを使用して、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。

Cisco ルータとアクセス サーバは、新しい RADIUS IETF 規格の VPDN トンネル アトリビュートにサポートしています。詳細については、「関連資料」（P.43）を参照してください。

また、次の設定例も参照してください。

- 「例：RADIUS トンネリング アトリビュートを指定した RADIUS ユーザ プロファイル」（P.38）
- 「例：L2TP アクセス コンセントレータ」（P.39）
- 「例：L2TP ネットワーク サーバ」（P.40）

L2F、L2TP、VPN、または VPDN の詳細については、「関連資料」（P.43）を参照してください。

RADIUS の設定方法

Cisco ルータまたはアクセス 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。**aaa authentication** コマンドの詳細な使用方法については、「Configuring Authentication」モジュールを参照してください。
- **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。詳細については、「Configuring Authentication」モジュールを参照してください。

次の設定タスクは任意です。

- **aaa group server** コマンドを使用して、特定のサービスのために、選択した RADIUS ホストをグループ化できます。**aaa group server** コマンドの詳細な使用方法については、「AAA サーバ グループの設定」（P.14）を参照してください。
- **aaa dnis map** コマンドを使用して、DNIS 番号に基づいて RADIUS サーバ グループを選択できます。このコマンドを使用するには、**aaa group server** コマンドを使用して RADIUS サーバ グループを定義する必要があります。**aaa dnis map** コマンドの詳細な使用方法については、「DNIS に基づく AAA サーバ グループの選択の設定」（P.18）を参照してください。
- **aaa authorization** グローバル コマンドを使用して、特定のユーザ機能を認可できます。**aaa authorization** コマンドの詳細な使用方法については、「Configuring Authorization」モジュールを参照してください。

- **aaa accounting** コマンドを使用して RADIUS 接続のアカウンティングをイネーブルにできます。**aaa accounting** コマンドの詳細な使用方法については、「Configuring Accounting」モジュールを参照してください。
- **dialer aaa** 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、AAA サーバでの発信アトリビュートを含むリモート サイト プロファイルを作成できます。**dialer aaa** コマンドの詳細な使用方法については、「RADIUS アクセス要求のサフィックスとパスワードの設定」（P.30）を参照してください。

ここでは、ネットワークでの認証、認可、およびアカウンティングについて RADIUS を設定する方法について説明します。内容は次のとおりです。

このモジュールのコマンドを使用した RADIUS の設定例については、「RADIUS の設定例」（P.32）を参照してください。

RADIUS サーバと通信するためのルータの設定

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ルータを設定するには、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
- 再送信値
- キー ストリング

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 アドレスおよび特定の UDP ポート番号に基づいて識別されます。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。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト 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。この例の場合、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、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、ネットワーク アクセス サーバが試行します（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 Cisco ルータは、共有秘密テキスト ストリングを使用してパスワードを暗号化し、応答を交換します。RADIUS を設定して AAA セキュリティ コマンドを使用するには、RADIUS サーバ デーモンを実行するホストと、ルータと共有する秘密テキスト（キー）ストリングを指定する必要があります。

タイムアウト値、再送信値、および暗号化キー値には、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。すべての RADIUS サーバとルータとの通信にこのようなグローバル設定を適用するには、**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。ルータ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の方が、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。

サーバごとに RADIUS サーバ通信を設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]
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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] **例：** `Router(config)# radius-server host 10.45.1.2`	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、認証とアカウンティングの宛先ポート番号を割り当てます。**auth-port** *port-number* オプションを使用して、認証専用の RADIUS サーバに固有の UDP ポートを設定します。**acct-port** *port-number* オプションを使用して、アカウンティング専用の RADIUS サーバに固有の UDP ポートを設定します。**alias** キーワードを使用して、RADIUS サーバを参照するときに使用する IP アドレス（最大 8 個）を設定します。 単一の IP アドレスに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ネットワーク アクセス サーバを設定するには、必要な回数、このコマンドを繰り返すだけです。その際、各 UDP を固有の値にします。特定の RADIUS ホストで使用するタイムアウト、再送信、暗号化キーを設定します。 タイムアウトを設定しない場合、グローバル値が使用されます。設定する場合、値の範囲は 1 ～ 1000 です。再送信値を設定しない場合、グローバル値が使用されます。設定する場合、値の範囲は 1 ～ 1000 です。キーストリングを指定しない場合、グローバル値が使用されます。 **（注）** キーはテキスト ストリングで、RADIUS サーバで使用される暗号化キーと一致する必要があります。キーの先頭にあるスペースは無視されますが、キー内のスペースとキー末尾のスペースは使用されるため、キーは常に **radius-server host** コマンド構文の最後のアイテムとして設定してください。キーにスペースを使用する場合、引用符をキーに含める場合を除き、引用符でキーを囲まないでください。
ステップ 4	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。

ルータと RADIUS サーバ間のグローバル通信設定を指定するには、次の **radius-server** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server key** {**0** *string* | **7** *string* | *string*}
4. **radius-server retransmit** *retries*
5. **radius-server timeout** *seconds*
6. **radius-server deadtime** *minutes*

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server key** {**0** *string* | **7** *string* | *string*} **例：** `Router(config)# radius-server key myRaDIUSpassword`	ルータと RADIUS サーバ間に使用する共有秘密テキスト ストリングを指定します。**0** *line* 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** *line* 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 4	**radius-server retransmit** *retries* **例：** `Router(config)# radius-server retransmit retries`	ルータ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）。
ステップ 5	**radius-server timeout** *seconds* **例：** `Router(config)# radius-server timeout 6`	ルータが RADIUS 要求に対する応答を待機して、再送信するまでの時間（秒数）を指定します。
ステップ 6	**radius-server deadtime** *minutes* **例：** `Router(config)# radius-server deadtime 5`	RADIUS 認証要求に応答しない RADIUS サーバが、認証要求の期限切れになるまでの時間（分数）を指定します。
ステップ 7	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。

RADIUS のベンダー固有アトリビュートを使用するためのルータの設定

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間で VSA（Vendor-Specific Attribute; ベンダー固有アトリビュート）（アトリビュート 26）を使用してベンダー固有の情報を伝達する方法が規定されています。ベンダーは、ベンダー固有アトリビュート（VSA）を使用して、汎用ではない拡張のベンダー固有アトリビュートをサポートしています。シスコの RADIUS 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は「cisco-av-pair」です。値は次の形式のストリングです。

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

「Protocol」は、特定の認可タイプを表すシスコの「protocol」アトリビュートです。使用可能なプロトコルには、IP、IPX、VPDN、VOIP、SHELL、RSVP、SIP、AIRNET、OUTBOUND があります。「Attribute」と「value」は、シスコの TACACS+ 仕様に定義されている適切なアトリビュート値

（AV）ペアで、「sep」は必須アトリビュートの場合には「=」、オプションのアトリビュートの場合に「*」を使用します。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS に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、IP を認可している間（PPP の IPCP アドレス割り当てを行っている間）、シスコの「指定された複数の IP アドレス プール」をアクティブにすることができます。

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

「*」を挿入すると、AV ペア「ip:addr-pool=first」はオプションになります。AV ペアはオプションにできることに注意してください。

```
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ベンダー ID、オプション、および関連する VSA があります。ベンダー ID と VSA の詳細については、「RFC」（P.43）を参照してください。

VSA を認識および使用するようにネットワーク アクセス サーバを設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send** [**accounting** | **authentication**]
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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server vsa send** [**accounting** | **authentication**] **例：** `Router(config)# radius-server vsa send`	RADIUS IETF アトリビュート 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	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。

RADIUS アトリビュートの詳細な一覧やベンダー固有アトリビュート 26 の詳細については、「関連資料」（P.43）を参照してください。

ベンダー固有の RADIUS サーバ通信のためのルータの設定

RADIUS のインターネット技術特別調査委員会（IETF）ドラフト規格では、ネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有情報を通信するための方式を規定していますが、一部のベンダーは独自の方法で RADIUS アトリビュートを拡張しています。Cisco IOS ソフトウェアは、RADIUS のベンダー固有アトリビュートの一部をサポートしています。

前述のように、（ベンダー固有か IETF ドラフト準拠かに関係なく）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、シスコ デバイスと共有する秘密テキスト ストリングを指定する必要があります。RADIUS ホストと秘密テキスト ストリングを指定するには、**radius-server** コマンドを使用します。RADIUS サーバが RADIUS のベンダー固有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、ベンダー固有アトリビュートはサポートされません。

ベンダー固有の RADIUS サーバ ホストと共有秘密テキスト ストリングを指定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} **non-standard**
4. **radius-server key** {**0** *string* | **7** *string* | *string*}
5. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} **non-standard** **例：** `Router(config)# radius-server host alcatraz non-standard`	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、RADIUS のベンダー固有実装を使用することを指定します。

	コマンド	目的
ステップ 4	**radius-server key** {**0** *string* | **7** *string* | *string*} **例：** `Router(config)# radius-server key myRaDIUSpassword`	ルータとベンダー固有 RADIUS サーバ間に使用する共有秘密テキスト ストリングを指定します。ルータと RADIUS サーバはこのテキスト ストリング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 5	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。

RADIUS サーバのスタティック ルートと IP アドレスを照会するためのルータの設定

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。

Cisco ルータまたはアクセス サーバが最初に起動したときに、そのデバイスがスタティック ルートと IP プール定義について RADIUS サーバに照会するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server configuration-nas**
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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server configure-nas** **例：** `Router(config)# radius-server configure-nas`	Cisco ルータまたはアクセス 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。
ステップ 4	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。

（注） **radius-server configure-nas** コマンドは Cisco ルータの起動時に実行するため、**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。

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ルータの設定

PPP またはログイン認証が、コールが着信したインターフェイスとは異なるインターフェイスで発生する場合があります。たとえば、V.120 ISDN コールの場合、ログインまたは 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 アトリビュート（RADIUS IETF アトリビュート 5）フィールドのサイズを 32 ビットに拡張します。NAS-Port アトリビュートの上位 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。

NAS-Port アトリビュート フィールドの拡張インターフェイス情報を表示するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port format**
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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server attribute nas-port format** **例：** `Router(config)# radius-server attribute nas-port format`	NAS-Port アトリビュートのサイズを 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 4	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。

（注） このコマンドで **radius-server extended-portnames** コマンドと **radius-server attribute nas-port extended** コマンドが置換されます。

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 RADIUS 実装では、インターフェイスを区別できる固有の NAS-Port アトリビュートを提供しません。たとえば、デュアル PRI インターフェイスがスロット 1 にある場合、Serial1/0:1 および Serial1/1:1 のいずれも NAS-Port = 20101 と表示されます。

繰り返しになりますが、これは、RADIUS IETF の NAS-Port アトリビュートには 16 ビットのフィールド サイズ制限があるためです。この場合の解決策は、ベンダー固有アトリビュート（RADIUS IETF アトリビュート 26）で NAS-Port アトリビュートを置換することです。シスコのベンダー ID は 9 であり、Cisco-NAS-Port アトリビュートはサブタイプ 2 です。ベンダー固有アトリビュート（VSA）を有効にするには、**radius-server vsa send** コマンドを入力します。ベンダー固有アトリビュート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。

NAS-Port アトリビュートを RADIUS IETF アトリビュート 26 で置換し、拡張フィールド情報を表示するには、次のコマンドを使用します。

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server vsa send** [**accounting** | **authentication**] **例：** `Router(config)# radius-server vsa send`	RADIUS IETF アトリビュート 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アトリビュート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：** `Router(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：** `Router(config)# exit`	特権 EXEC モードに戻ります。

標準の NAS-Port アトリビュート（RADIUS IETF アトリビュート 5）は以降も送信されます。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 アトリビュートは送信されなくなります。

PPP の RADIUS アトリビュートと RADIUS ポートの識別については、「関連資料」（P.43）を参照してください。

AAA サーバ グループの設定

AAA サーバ グループを使用するようにルータを設定すると、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 リストと併せて使用されます。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。

サーバ グループには、1 台のサーバに対して複数のホスト エントリを含めることができます。エントリごとに固有の識別情報を設定します。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。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト 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。この例の場合、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、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、ネットワーク アクセス サーバが試行します（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）。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]
4. **aaa group server** {**radius** | **tacacs+**} *group-name*
5. **server ip-address** [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] **例：** `Router(config)# radius-server host 10.45.1.2`	サーバ ホストの IP アドレスを指定および定義してから、AAA サーバ グループを設定します。**radius-server host** コマンドの詳細については、「RADIUS サーバと通信するためのルータの設定」（P.5）を参照してください。
ステップ 4	**aaa group server** {**radius** | **tacacs+**} *group-name* **例：** `Router(config-if)# 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。このコマンドでは、サーバ グループのサブコンフィギュレーション モードにルータを配置します。
ステップ 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **例：** `Router(config-sg)# 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 グループの各 RADIUS サーバについて、この手順を繰り返します。 **（注）** 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。
ステップ 6	**end** **例：** `Router(config-sg)# end`	サーバ グループ コンフィギュレーション モードを終了します。

デッドタイムによる AAA サーバ グループの設定

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します。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なくなりました。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だけが応答可能（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 アトリビュートが追加されるため、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。

サーバ グループ内のデッドタイムを設定するには、次のコマンドを使用します。

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	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 1	**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 1	**aaa group server radius** *group* **例：** `Router(config)# aaa group server radius group1`	RADIUS タイプ サーバ グループを定義します。

	コマンド	目的
ステップ 2	**deadtime** *minutes* **例：** `Router(config-sg)# 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省略すると、値はマスター リストから継承されます。
ステップ 3	**end** **例：** `Router(config-sg)# end`	サーバ グループ コンフィギュレーション モードを終了します。

AAA DNIS 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。AAA によって認証されると、コールは許可されます。

DNIS 認証を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa preauthorization** **例：** `Router(config)# aaa preauth`	AAA 事前認証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 4	**group** {**radius** | **tacacs+** | *server-group*} **例：** `Router(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：** `Router(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：** `Router(config-preauth)# end`	事前認証コンフィギュレーション モードを終了します。

DNIS に基づく AAA サーバ グループの選択の設定

Cisco IOS ソフトウェアを使用すると、Dialed Number Identification Service（DNIS; 着信番号識別サービス）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。

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 Cisco ルータは、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 IOS 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/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、この方式の方がその他の 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。

（注） DNIS に基づく AAA サーバ グループの選択を設定する前に、RADIUS サーバ ホストのリストを設定し、AAA サーバ グループを設定する必要があります。「RADIUS サーバと通信するためのルータの設定」（P.5）および「AAA サーバ グループの設定」（P.14）を参照してください。

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ルータを設定するには、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、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*
4. **aaa dnis map** *dnis-number* **authorization network group** *server-group-name*
5. **aaa dnis map** ***dnis-number*** **accounting network [none | start-stop | stop-only] group** ***server-group-name***
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa dnis map enable** **例：** `Router(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：** `Router(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。

	コマンドまたはアクション	目的
ステップ 5	**aaa dnis map** *dnis-number* **authorization network group** *server-group-name* **例：** `Router(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：** `Router(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：** `Router(config)# exit`	コンフィギュレーション モードを終了します。

AAA 事前認証の設定

サービス プロバイダーが ISDN PRI または Channel-Associated Signalling（CAS）による AAA 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。ISDN PRI または CAS によって、着信コールに関する情報を Network Access Server（NAS; ネットワーク アクセス サーバ）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（着信番号とも呼ばれます）
- Calling Line Identification（CLID; 発呼回線 ID）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）

この機能を使用すると、Cisco NAS は、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します（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。

この機能は、事前認証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アトリビュート 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 アトリビュートの使用をサポートしています。また、これらのアトリビュートは、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。

- アトリビュート 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。

- ISDN PRI では MMP を使用できません。
- AAA 事前認証を使用できるのは、Cisco AS5300、Cisco AS5400、および Cisco AS5800 プラットフォームだけです。

（注） AAA 事前認証を設定する前に、**aaa new-model** コマンドをイネーブルにし、サポートする事前認証アプリケーションが使用ネットワークの RADIUS サーバで実行されている必要があります。

AAA 事前認証を設定するには、次のコマンドを使用します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa preauthorization** **例：** `Router(config)# aaa preauth`	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：** `Router(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：** `Router(config-preauth)# clid required`	CLID 番号に基づいて、コールを事前認証します。

	コマンド	目的
ステップ 6	**ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **例：** `Router(config-preauth)# ctype required`	コール タイプに基づいて、コールを事前認証します。
ステップ 7	**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **例：** `Router(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：** `Router(config-preauth)# dnis bypass hawaii`	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：** `Router(config-preauth)# end`	事前認証コンフィギュレーション モードを終了します。

DNIS 事前認証を設定するには、次のコマンドを使用します。

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	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa preauthorization** **例：** `Router(config)# aaa preauth`	AAA 事前認証モードを開始します。

	コマンド	目的
ステップ 4	**group** {**radius** | **tacacs+** | *server-group*} **例：** `Router(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：** `Router(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：** `Router(config-preauth)# end`	事前認証コンフィギュレーション モードを終了します。

Cisco ルータ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。事前認証プロファイルの設定については、次の項を参照してください。

- 「DNIS または CLID 事前認証の RADIUS プロファイルの設定」（P.23）
- 「コール タイプ事前認証の RADIUS プロファイルの設定」（P.23）
- 「コールバックのために事前認証を強化する RADIUS プロファイルの設定」（P.24）
- 「大規模なダイヤルアウトに使用されるリモート ホスト名の RADIUS プロファイルの設定」（P.24）
- 「モデム管理のための RADIUS プロファイルの設定」（P.25）
- 「後続の認証のための RADIUS の設定」（P.25）
- 「後続の認証タイプのための RADIUS の設定」（P.26）
- 「ユーザ名を含めるための RADIUS プロファイルの設定」（P.26）
- 「双方向認証のための RADIUS プロファイルの設定」（P.26）
- 「認可をサポートするための RADIUS プロファイルの設定」（P.27）

DNIS または CLID 事前認証の RADIUS プロファイルの設定

RADIUS 事前認証プロファイルを設定するには、DNIS または CLID 番号をユーザ名として使用し、**dnis** または **clid** コマンドで定義し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 タイプは必ず「outbound」です。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 サーバに送信される access-request パケットにも含まれます。

コール タイプ事前認証の RADIUS プロファイルの設定

RADIUS 事前認証プロファイルを設定するには、コール タイプ ストリング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。次の表に、事前認証プロファイルで使用できるコール タイプ ストリングを示します。

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 CAS にだけ使用できるコール 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」です。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。

コールバックのために事前認証を強化する RADIUS プロファイルの設定

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 は現在のコールを終了し、発信元にコールバックします。NAS がコールバックを実行すると、発信接続の情報だけが適用されます。事前認証の access-accept メッセージのその他のアトリビュートは破棄されます。

（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 555-1111 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>" は文字列 "andy" を使用し、cisco-avpair = "preauth:send-secret=<string>" はパスワード "cisco" を使用します。

```
5551111 password = ”cisco”, Service-Type = Outbound
    Service-Type = Callback-Framed
    Framed-Protocol = PPP,
    Dialback-No = ”5551212”
    Class = ”ISP12”
    cisco-avpair = ”preauth:send-name=andy”
    cisco-avpair = ”preauth:send-secret=cisco”
```

大規模なダイヤルアウトに使用されるリモート ホスト名の RADIUS プロファイルの設定

次に、前の例に処理を追加して、発信先の番号は有効でもアクセス先のルータが間違っている発信を回避するために、リモートの名前を提供する例を示します。この例は大規模なダイヤルアウトに適しています。

```
5551111 password = "cisco", Service-Type = Outbound
       Service-Type = Callback-Framed
       Framed-Protocol = PPP,
       Dialback-No = "5551212"
       Class = "ISP12"
```

```
cisco-avpair = "preauth:send-name=andy"
cisco-avpair = "preauth:send-secret=cisco"
cisco-avpair = "preauth:remote-name=Router2"
```

モデム管理のための RADIUS プロファイルの設定

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、ベンダー固有アトリビュート（VSA）26 を介して、モデム管理のモデム ストリング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>"
```

VSA のモデム管理ストリングには、次の内容を含めることができます。

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 からモデム管理ストリングを受信すると、その情報は Cisco IOS 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 モデムや新しいテクノロジーだけです。この機能は Microcom モデムではサポートされません。

モデム管理の詳細については、「関連資料」（P.43）を参照してください。

後続の認証のための RADIUS の設定

事前認証に成功すると、事前認証の RADIUS ベンダー固有アトリビュート 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アトリビュート 201 の値が 0 の場合、後続の認証は実行されません。アトリビュート 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。

アトリビュート 201 の構文は次のとおりです。

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

この <*n*> は、アトリビュート 201（つまり 0 または 1）と同じ値の範囲です。

事前認証プロファイルにアトリビュート 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には、事前認証プロファイルに加え、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 の設定

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>"
```

この <*string*> には、次のいずれかを指定できます。

ストリング	説明
chap	PPP 認証の 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 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 はユーザ別のアトリビュートであり、**ppp authentication** インターフェイス コマンドで指定した認証タイプ リストは置換されます。

（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 プロファイルの設定

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 アトリビュート 1（User-Name）または access-accept パケットで返される VSA を介して使用できるユーザ名を提供します。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の方が、RADIUS 事前認証プロファイルに含まれるユーザ名よりも優先されます。ユーザが指定したユーザ名は、認証と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 プロファイルの設定

双方向認証の場合、発信側ネットワーク デバイスが NAS を認証する必要があります。Password Authentication Protocol（PAP; パスワード認証プロトコル）のユーザ名とパスワード、または Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）のユーザ名とパスワードを NAS のローカルで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） **ppp authentication** コマンドを **radius** 方式とともに設定する必要があります。

PAP に適用する場合は、インターフェイス上で **ppp pap sent-name password** コマンドを設定しないでください。Vendor-Specific Attributes（VSA; ベンダー固有アトリビュート）の場合は、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、「preauth:send-name」および「preauth:send-secret」が使用されます。

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、発信側ネットワーキング 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に使用されます。

次に、双方向認証を指定する設定の例を示します。

```
5551111 password = "cisco", Service-Type = Outbound
    Service-Type = Framed-User
    cisco-avpair = "preauth:auth-required=1"
    cisco-avpair = "preauth:auth-type=pap"
    cisco-avpair = "preauth:send-name=andy"
    cisco-avpair = "preauth:send-secret=cisco"
    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 プロファイルの設定

事前認証だけを設定する場合、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 アトリビュートを含めてユーザ別のアトリビュートを適用することで、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 アトリビュートを設定できますが、service-type アトリビュート（アトリビュート 6）という 1 つの例外があります。service-type アトリビュートは、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>"
```

この <*n*> は、アトリビュート 6 に関する標準の RFC 2865 値の 1 つです。使用できる Service-Type 値については、「関連資料」（P.43）を参照してください。

（注） 後続の認証が必要な場合、事前認証プロファイルの authorization アトリビュートは適用されません。

ガード タイマーの設定

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。

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できるガード タイマーを設定するには、次のコマンドのいずれかを使用します。

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	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface serial1/0/0:23`	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：** `Router(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：** `Router(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：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了します。

RADIUS 認証の指定

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。詳細については、「関連資料」（P.43）を参照してください。

RADIUS 認可の指定

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、ワンタイム認可やサービスごとの認可を含むリモート アクセス コントロール用の方式が 1 つ、ユーザ別のアカウント 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、ARA、および Telnet のサポートを備えています。AAA によって RADIUS 認可は容易になるため、認証方式として RADIUS を指定して、**aaa authorization** コマンドを発行する必要があります。詳細については、「認可の設定」の章を参照してください。

RADIUS アカウンティングの指定

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** コマンドを発行する必要があります。詳細については、「アカウンティングの設定」の章を参照してください。

RADIUS Login-IP-Host の設定

ネットワーク アクセス サーバが、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には、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 *joeuser* 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。

```
joeuser       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、ネットワーク アクセス サーバがリストの次ホストに対して接続を試行するまで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、ネットワーク アクセス サーバが access-accept パケットでサポートするのは 3 ホストだけです。

RADIUS プロンプトの設定

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 アトリビュートを設定します。このアトリビュートは、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 アトリビュートの例を示します。この設定で、ユーザの応答はエコーされません。

```
joeuser 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、このアトリビュートを Echo に設定します。Prompt アトリビュートをユーザ 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。

このアトリビュートは、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 アトリビュートを使用するには、access-challenge パケットをサポートするように RADIUS サーバを設定します。

RADIUS アクセス要求のサフィックスとパスワードの設定

大規模なダイヤルアウトでは、すべての宛先の各 NAS でダイヤラ マップを設定する必要はありません。代わりに、AAA サーバで、発信コール アトリビュートを含むリモート サイト プロファイルを作成できます。パケット トラフィックによって、コールをリモート サイトに配置する必要がある場合、NAS によって プロファイルがダウンロードされます。

RADIUS に対する access-request メッセージでユーザ名を設定できます。「-out」というユーザ名のデフォルトのサフィックスが、ユーザ名に付加されます。ユーザ名アトリビュートを構成する形式は、IP アドレスと設定したサフィックスです。

大規模なダイヤルアウトの場合にユーザ名の設定機能を提供するには、**dialer aaa** コマンドを新しい **suffix** および **password** キーワードを指定して実装します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa route download** *min*
5. **aaa authorization configuration default**
6. **interface dialer** *number*
7. **dialer aaa**
8. **dialer aaa suffix** *suffix* **password** *password*
9. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンド	目的
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	**aaa route download** *min* **例：** `Router(config)# aaa route download 450`	ダウンロードのスタティック ルート機能をイネーブルにし、ダウンロードの間隔を設定します。
ステップ 5	**aaa authorization configuration default** **例：** `Router(config)# aaa authorization configuration default`	TACACS+ または 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 6	**interface dialer** *number* **例：** `Router(config)# interface dialer 1`	ダイヤラ ロータリー グループを定義します。
ステップ 7	**dialer aaa** **例：** `Router(config-if)# dialer aaa`	ダイヤラがダイヤル情報のために AAA サーバにアクセスすることを許可します。
ステップ 8	**dialer aaa suffix** *suffix* **password** *password* **例：** `Router(config-if)# dialer aaa suffix @samp password password12`	ダイヤラがダイヤル情報のために AAA サーバにアクセスすることを許可し、認証に使用するサフィックスとデフォルト以外のパスワードを指定します。
ステップ 9	**exit** **例：** `Router(config-if)# 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。

RADIUS のモニタリングとメンテナンス

RADIUS をモニタおよび保守するには、次のコマンドを使用します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug radius** **例：** `Router# debug radius`	RADIUS 関連の情報を表示します。
ステップ 3	**show radius statistics** **例：** `Router# 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	**exit** **例：** `Router# exit`	ルータ セッションを終了します。

RADIUS の設定例

ここでは、RADIUS 設定の例を紹介します。

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ルータ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、ルータは、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、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 IOS 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、および他のアクセス リストについて RADIUS が設定されます。

例：RADIUS 認証、認可、およびアカウンティング

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、認可、および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 ホスト間の共有秘密テキスト ストリングを定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、RADIUS 認証を示す認証方式リスト「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にはローカル認証が使用されます。
- **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。
- **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** コマンドで、PPP の使用状況を追跡します。

- **aaa authentication login admins local** コマンドは、ログイン認証の別の方式リスト「admins」を定義します。
- **login authentication admins** コマンドは、ログイン認証の「admins」方式リストを適用します。

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。

```
radius-server host alcatraz non-standard
radius-server key myRaDiUSpassWoRd
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
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、認可、および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 non-standard** コマンドで、RADIUS サーバ ホストの名前を定義し、この RADIUS ホストがベンダー固有バージョンの RADIUS を使用することを指定します。
- **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 ホスト間の共有秘密テキスト ストリングを定義します。
- **radius-server configure-nas** コマンドは、デバイスが最初に起動したときに、Cisco ルータまたはアクセス 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、RADIUS 認証を示す認証方式リスト「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にはローカル認証が使用されます。
- **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。
- **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** コマンドで、PPP の使用状況を追跡します。
- **aaa authentication login admins local** コマンドは、ログイン認証の別の方式リスト「admins」を定義します。
- **login authentication admins** コマンドは、ログイン認証の「admins」方式リストを適用します。

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
```

例：グローバル値とサーバ固有の値を指定した複数の RADIUS サーバ

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ルータ上の AAA サービスをイネーブルにし、特定の AAA コマンドで AAA サービスを定義します。**radius-server 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。**radius-server 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、およびキー値を設定します。

```
! Enable AAA services on the router 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
!
! Change the global retransmission value for all RADIUS servers.
radius-server retransmit 4
!
! Configure per-server specific timeout, retransmission, and key values.
! Change the default auth-port and acct-port values.
radius-server host 172.16.1.1 auth-port 1612 acct-port 1616 timeout 3 retransmit 3 key
radkey
!
! Configure per-server specific timeout and key values. This server uses the global
! retransmission value.
radius-server host 172.29.39.46 timeout 6 key rad123
```

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 2000
```

例：RADIUS 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 コマンドとサーバ コマンドの両方を使用する場合、サーバ コマンドの方がグローバル 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
```

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 番号を指定するという単純な設定の例を示します。

```
aaa preauth
 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 preauth
 group radius
 dnis required
 clid required
```

次に、「hawaii」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 preauth
 group radius
 dnis required
```

```
 dnis bypass hawaii

dialer dnis group hawaii
 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 preauth
 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：RADIUS トンネリング アトリビュートを指定した RADIUS ユーザ プロファイル

次に、RADIUS トンネリング アトリビュートを含む RADIUS ユーザ プロファイル（Merit Daemon 形式）の例を示します。このエントリは 2 つのトンネルをサポートします。1 つは L2F 用、もう 1 つは L2TP 用です。:1 が指定されたタグ エントリは L2F トンネルをサポートし、:2 が指定されたタグ エントリは L2TP トンネルをサポートします。

```
cisco.com Password = "cisco", Service-Type = Outbound
    Service-Type = Outbound,
    Tunnel-Type = :1:L2F,
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Client-Endpoint = :1:"10.0.0.2",
    Tunnel-Server-Endpoint = :1:"10.0.0.3",
    Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
    Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
    Tunnel-Assignment-Id = :1:"l2f-assignment-id",
```

```
    Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
    Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
    Tunnel-Preference = :1:1,
    Tunnel-Type = :2:L2TP,
    Tunnel-Medium-Type = :2:IP,
    Tunnel-Client-Endpoint = :2:"10.0.0.2",
    Tunnel-Server-Endpoint = :2:"10.0.0.3",
    Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
    Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
    Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
    Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
    Tunnel-Preference = :2:2
```

例：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 serial1/0/0:23
 isdn guard-timer 8000 on-expiry reject

aaa preauth
 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。

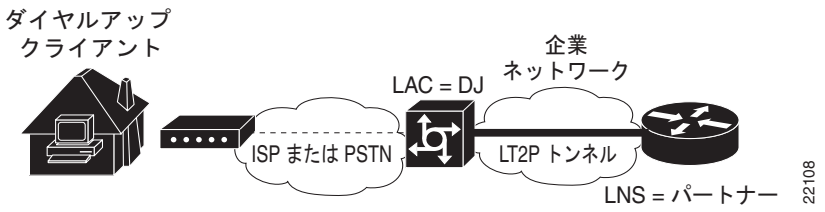
```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept

aaa preauth
group radius
dnis required
```

例：L2TP アクセス コンセントレータ

次に、図 1 に示すトポロジの基本的な L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）を設定する例を示します。ローカル名は定義されていないため、使用されるホスト名はローカル名です。L2TP トンネル パスワードは定義されていないため、ユーザ名パスワードが使用されます。この例では、VPDN が LAC のローカルで設定されます。VPDN は新しい RADIUS トンネル アトリビュートを利用しません。

図 1　設定例のトポロジ




```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
! Define the username as ”DJ.”
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Define VPDN group number 1.
vpdn-group 1
! Allow the LAC to respond to dialin requests using L2TP from IP address 172.21.9.13
! domain ”cisco.com.”
 request dialin
  protocol l2tp
  domain cisco.com
 initiate-ip to 172.21.9.13
 local name nas-1
```

次に、RADIUS トンネル アトリビュートがサポートされる場合、LAC を設定する例を示します。この例では、LAC にローカルの VPDN 設定がありません。代わりに、LAC は、リモート RADIUS セキュリティ サーバを照会するように設定されています。

```
! Enable global AAA securities services.
aaa new-model
! Enable AAA authentication for PPP and list RADIUS as the default method to use
! for PPP authentication.
aaa authentication ppp default group radius local
! Enable AAA (network) authorization and list RADIUS as the default method to use for
! authorization.
aaa authorization network default group radius
! Define the username as ”DJ.”
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Configure the LAC to interface with the remote RADIUS security server.
radius host 171.19.1.1 auth-port 1645 acct-port 1646
radius-server key cisco
```

例：L2TP ネットワーク サーバ

次に、図 1 に示すトポロジの L2TP ネットワーク サーバ（LNS）で基本的な L2TP を設定する例と対応するコメントを示します。

```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
! Define the username as ”partner.”
```

```
username partner password 7 030C5E070A00781B
! Create virtual-template 1 and assign all values for virtual access interfaces.
interface Virtual-Template1
! Borrow the IP address from interface ethernet 1.
 ip unnumbered Ethernet0
! Disable multicast fast switching.
 no ip mroute-cache
! Use CHAP to authenticate PPP.
 ppp authentication chap
! Enable VPDN.
vpdn enable
! Create vpdn-group number 1.
vpdn-group 1
! Accept all dialin l2tp tunnels from virtual-template 1 from remote peer DJ.
 accept dialin l2tp virtual-template 1 remote DJ
  protocol any
  virtual-template 1
 terminate-from hostname nas1
local name hgw1
```

次に、RADIUS トンネリング アトリビュートを使用して、基本的な L2F と L2TP 設定で LNS を設定する例を示します。

```
aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2f-cli-auth-id password 0 l2f-cli-pass
username l2f-svr-auth-id password 0 l2f-svr-pass
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2f
virtual-template 1
terminate-from hostname l2f-cli-auth-id
local name l2f-svr-auth-id
!
vpdn-group 2
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface Ethernet1/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered Ethernet1/0
ppp authentication pap
!
interface Virtual-Template2
ip unnumbered Ethernet1/0
ppp authentication pap
!
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
```

```
radius-server key <deleted>
```

その他の参考資料

ここでは、RADIUS の設定に関する関連資料について説明します。

関連資料

内容	参照先
RADIUS アトリビュート	「RADIUS Attributes Overview and RADIUS IETF Attributes」モジュール
AAA	「Configuring Authentication」モジュール
	「Configuring Authorization」モジュール
	「Configuring Accounting」モジュール
L2F、L2TP、VPN、または VPDN	『*Cisco IOS Dial Technologies Configuration Guide*』および『*Cisco IOS VPDN Configuration Guide*, Release 15.0』
モデムの設定と管理	『*Cisco IOS Dial Technologies Configuration Guide*, Release 15.0』
PPP の RADIUS ポートの識別	『*Cisco IOS Wide-Area Networking Configuration Guide*, Release 15.0』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 2139	「*RADIUS Accounting*」
RFC 2865	「*Remote Authentication Dial-In User Service (RADIUS)*」
RFC 2868	「*RADIUS Attributes for Tunnel Protocol Support*」
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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUS の設定に関する機能情報

表 1 に、この機能のリリース履歴を示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　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	11.1 Cisco IOS XE 3.1.0SG	Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムは、不正アクセスに対してネットワーク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 Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。RADIUS は完全にオープンなプロトコルであり、ソース コード形式で配布されているため、現在使用できる任意のセキュリティ システムと連携するように変更できます。 この機能は、Cisco IOS Release 11.1 で導入されました。
SNMP を介する RADIUS 統計情報	15.1(1)S	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。 この機能については、次の項に説明があります。 「RADIUS のモニタリングとメンテナンス」（P.31） 変更されたコマンド：**show radius statistics**