



RADIUS の設定

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

- [RADIUS を設定するための前提条件 \(1 ページ\)](#)
- [RADIUS の設定に関する制約事項 \(2 ページ\)](#)
- [RADIUS に関する情報 \(3 ページ\)](#)
- [RADIUS の設定方法 \(24 ページ\)](#)
- [RADIUS の設定例 \(40 ページ\)](#)
- [RADIUS に関する追加情報 \(43 ページ\)](#)
- [RADIUS の機能の履歴 \(44 ページ\)](#)

RADIUS を設定するための前提条件

ここでは、RADIUS による device アクセスの制御の前提条件を示します。

全般：

- この章のいずれかのコンフィギュレーションコマンドを使用するには、RADIUS および認証、許可、ならびにアカウントिंग (AAA) をイネーブルにする必要があります。
- RADIUS は、AAA を介して実装され、AAA コマンドを使用するのみイネーブルにできません。
- **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。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。

- 最低限、RADIUS サーバソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS 認証の方式リストを定義する必要があります。また、任意で RADIUS 許可およびアカウントングの方式リストを定義できます。
- device 上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。
- RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、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が稼働しているマルチユーザシステムです。詳細については、RADIUS サーバのマニュアルを参照してください。
- Change-of-Authorization (CoA) インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。CoA を使用すると、セッションの識別と接続解除要求を実行できます。アップデートは、指定されたセッションにだけ作用します。

RADIUS 操作の場合：

- ユーザは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります（イネーブルに設定されている場合）。

RADIUS の設定に関する制約事項

ここでは、RADIUS による device アクセスの制御の制約事項について説明します。

全般：

- セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。

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、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状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービスモデルにバインドします。

RADIUS に関する情報

RADIUS およびスイッチ アクセス

この項では、RADIUS をイネーブルにし、設定する方法について説明します。RADIUS を使用すると、アカウントの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます。

RADIUS の概要

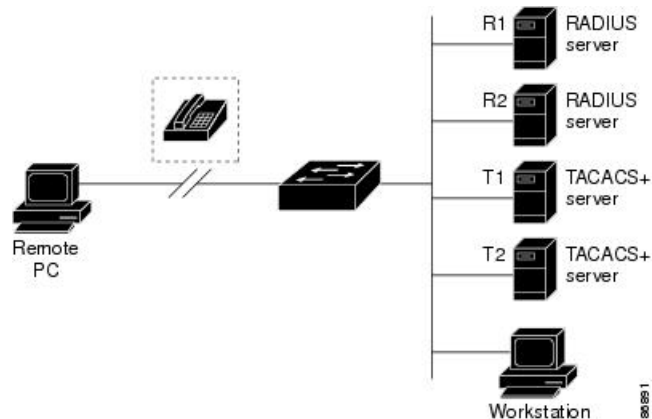
RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバシステムです。RADIUS クライアントは、サポート対象の Cisco ルータおよびスイッチ上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。

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 サーバによるネットワーク。たとえば、複数のベンダーのアクセスサーバが、1つの RADIUS サーバベースセキュリティ データベースを使用します。複数ベンダーのアクセスサーバからなる IP ベースのネットワークでは、ダイヤルインユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティシステムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマートカードアクセス コントロールシステムを使用するアクセス環境。あるケースでは、RADIUS は Enigma のセキュリティカードとともに使用してユーザを確認し、ネットワーク リソースのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。RADIUS クライアント装備のシスコ device をネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。下の図「RADIUS サービスから TACACS+ サービスへの移行」を参照してください。
- ユーザが 1つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1つのホスト、Telnet などの 1つのユーティリティ、または IEEE 802.1x などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、「IEEE 802.1x ポートベース認証の設定」の章を参照してください。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウントリング ソフトウェアのフ

リーウェアバージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

図 1: RADIUS サービスから TACACS+ サービスへの移行



RADIUS の動作

RADIUS サーバによってアクセス コントロールされる device に、ユーザがログインおよび認証を試みると、次のイベントが発生します。

1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
 - ACCEPT : ユーザは認証されます。
 - 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が必要されるか、またはアクセスが拒否されます。
 - CHALLENGE : ユーザに追加データを要求します。
 - CHALLENGE PASSWORD : ユーザは新しいパスワードを選択するように要求されます。

ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 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、およびユーザ タイムアウトを含む)

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

RADIUS サーバホスト

スイッチと RADIUS サーバの通信には、次の要素が関係します。

- 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
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティサーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS ホストとして個々のポートを定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホストエントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番目に設定したホストエントリは、最初に設定したホストエントリのフェールオーバーバックアップとして動作します。この例では、最初のホストエントリがアカウンティング サービスを提供できなかった場合、スイッチは

「%RADIUS-4-RADIUS_DEAD」メッセージを表示し、その後、同じデバイス上で 2 番めに設定されたホストエントリでアカウンティング サービスを試みます（RADIUS ホストエントリは、設定した順序に従って試行されます）。

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

タイムアウト、再送信回数、および暗号キーの値は、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できますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単位での設定を組み合わせることもできます。

RADIUS ログイン認証

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。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ます。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外は、デフォルトの方式リストです。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する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、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから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による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのある時点で認証が失敗した場合（つまり、セキュリティサーバまたはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

AAA サーバグループ

既存のサーバホストを認証用にグループ化するため、AAA サーバグループを使用するようにデバイスを設定できます。設定済みのサーバホストのサブセットを選択して、それを特定のサービスに使用します。サーバグループは、選択されたサーバホストの IP アドレスのリストを含むグローバルなサーバホストリストとともに使用されます。

サーバグループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意的 ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。この一意的 ID を使用することによって、同じ IP アドレスにあるサーバ上の異なる UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウントティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エントリがアカウントティング サービスの提供に失敗すると、ネットワーク アクセス サーバは同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウントティング サービスを提供するように試行します。（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

AAA 許可

AAA 許可によってユーザが利用できるサービスが制限されます。AAA 許可が有効になっていると、デバイスはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザデータベースまたはセキュリティサーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

RADIUS アカウンティング

AAA アカウンティング機能は、ユーザが使用したサービスと、消費したネットワーク リソース量を追跡します。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で 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 レコードにはアカウンティングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティサーバに格納されます。これらのデータは、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後で分析できます。

ベンダー固有の RADIUS 属性

Internet Engineering Task Force (IETF) ドラフト規格に、ベンダー固有の属性 (属性 26) を使用して、デバイスと RADIUS サーバ間でベンダー固有の情報を通信するための方式が定められています。各ベンダーは、Vendor-Specific Attribute (VSA) を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを1つサポートしています。シスコのベンダー ID は9であり、サポート対象のオプションはベンダータイプ1 (名前は *cisco-avpair*) です。この値は、次のフォーマットのストリングです。

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

protocol は、特定の認証タイプに使用するシスコのプロトコル属性の値です。*attribute* および *value* は、シスコの TACACS+ 仕様で定義されている適切な属性値 (AV) ペアです。*sep* は、必須の属性の場合は =、任意指定の属性の場合は * です。TACACS+ 認証で使用できるすべての機能は、RADIUS でも使用できます。

たとえば、次の AV ペアにより、IP 許可時 (PPP のインターネットプロトコル制御プロトコル (IPCP) アドレス割り当て時) に、シスコの複数の名前付き IP アドレスプール機能がアクティブになります。

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

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

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

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

```
cisco-avpair= "shell:priv-lvl=15"
```

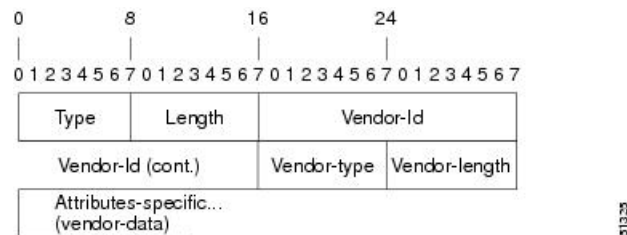
他のベンダーにも、それぞれ独自のベンダー ID、オプション、および対応する VSA があります。ベンダー ID および VSA の詳細については、RFC 2138 『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

属性 26 には、次の3つの要素が含まれています。

- タイプ
- 長さ
- スtring (またはデータ)
 - Vendor-Id
 - Vendor-Type
 - Vendor-Length
 - Vendor-Data

次の図は、属性 26 の「背後で」カプセル化される VSA のパケット形式を示します。

図 2: 属性 26 の背後でカプセル化される VSA



- (注) VSA の形式はベンダーが指定します。Attribute-Specific フィールド (Vendor-Data と呼ばれる) は、ベンダーによるその属性の定義によって異なります。

次の表に、「ベンダー固有 RADIUS IETF 属性テーブル」(次の 2 番目の表) で表示される重要なフィールドを示します。これは、サポート対象のベンダー固有 RADIUS 属性 (IETF 属性 26) を表示します。

表 1: ベンダー固有属性表のフィールドの説明

フィールド	説明
番号	次の表に示されるすべての属性は、IETF 属性 26 の拡張です。
ベンダー固有のコマンドコード	特定のベンダーの識別に使用する定義されたコード。コード 9 は Cisco VSA、311 は Microsoft VSA、529 は Ascend VSA を定義します。
サブタイプ番号	属性 ID 番号。この番号は、属性 26 の背後でカプセル化される「2 番目のレイヤ」の ID 番号であること以外、IETF 属性の ID 番号に似ています。
属性	属性の ASCII スtring 名。
説明	属性の説明。

表 2: ベンダー固有 RADIUS IETF 属性

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
MS-CHAP 属性				
26	311	1	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでしか使用されません。この属性は、PPP CHAP ID と同じです (RFC 2548)
26	311	11	MSCHAP-Challenge	ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャレンジが含まれます。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。(RFC 2548)
VPDN 属性				
26	9	1	l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウサイズを指定します。この値は、トンネルの確立中にピアにアダプティブされます。
26	9	1	l2tp-drop-out-of-order	正しくない順序で受信したデータパケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データパケット上でシーケンス番号が送信されるわけではありません。
26	9	1	l2tp-hello-interval	hello キープアライブインターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	l2tp-hidden-avp	イネーブルにすると、L2TP 制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。
26	9	1	l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。
26	9	1	tunnel-tos-reflect	LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロードパケットの IP ヘッダーからトンネルパケットの IP ヘッダーにコピーします。
26	9	1	l2tp-tunnel-authen	この属性を設定すると、L2TP トンネル認証が実行されます。
26	9	1	l2tp-tunnel-password	L2TP トンネル認証および AVP 隠蔽に使用される共有秘密。
26	9	1	l2tp-udp-checksum	これは認可属性で、L2TP がデータパケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」と「no」です。デフォルトは「no」です。
Store and Forward Fax 属性				
26	9	3	Fax-Account-Id-Origin	mmp aaa receive-id コマンドまたは mmp aaa send-id コマンドについて、システム管理者によって定義されたものとしてアカウント ID の発信元を示します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	4	Fax-Msg-Id=	Store and Forward Fax 機能によって割り当てられた一意のファクスメッセージ識別番号を示します。
26	9	5	Fax-Pages	このファクスセッション中に送信または受信したページ数を示します。このページ数には、カバーページも含まれます。
26	9	6	Fax-Coverpage-Flag	カバーページがこのファクスセッションのオフランプゲートウェイで生成されたかどうかを示します。true はカバーページが生成されたことを示します。false はカバーページが生成されなかったことを意味します。
26	9	7	Fax-Modem-Time	モデムがファクスデータを送信した時間 (x)、およびファクスセッションの合計時間 (y) を秒単位で示します。これには、fax-mail および PSTN 時間が x/y の形式で含まれます。たとえば、10/15 は送信時間が 10 秒で、合計ファクスセッションが 15 秒であったことを示します。
26	9	8	Fax-Connect-Speed	この fax-mail が最初に送信または受信された時点のモデム速度を示します。有効値は、1200、4800、9600、および 14400 です。
26	9	9	Fax-Recipient-Count	このファクス送信の受信者数を示します。Eメールサーバがセッションモードをサポートするまで、この数字は 1 にする必要があります。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	10	Fax-Process-Abort-Flag	ファクスセッションが中断したこと、または正常に終了したことを示します。true はセッションが中断したことを示します。false はセッションが成功したことを示します。
26	9	11	Fax-Dsn-Address	DSN の送信先のアドレスを示します。
26	9	12	Fax-Dsn-Flag	DSN がイネーブルにされているかどうかを示します。true は DSN がイネーブルにされていることを示します。false は DSN がイネーブルにされていないことを示します。
26	9	13	Fax-Mdn-Address	MDN の送信先のアドレスを示します。
26	9	14	Fax-Mdn-Flag	メッセージ配信通知 (MDN) がイネーブルにされているかどうかを示します。true は MDN がイネーブルにされていることを示します。false は MDN がイネーブルにされていないことを示します。
26	9	15	Fax-Auth-Status	このファクスセッションに対する認証が成功したかどうかを示します。このフィールドに対する有効値は、success、failed、bypassed、または unknown です。
26	9	16	Email-Server-Address	オンランプ fax-mail メッセージを処理する E メールサーバの IP アドレスを示します。
26	9	17	Email-Server-Ack-Flag	オンランプ ゲートウェイが fax-mail メッセージを受け入れる E メールサーバから肯定確認応答を受信したことを示します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	18	Gateway-Id	ファクスセッションを処理したゲートウェイの名前を示します。名前は、 hostname.domain-name という形式で表示されます。
26	9	19	Call-Type	ファクスのアクティビティのタイプを、fax receive または fax send のどちらかで記述します。
26	9	20	Port-Used	この fax-mail の送受信いずれかに使用される Cisco AS5300 のスロット/ポート番号を示します。
26	9	21	Abort-Cause	ファクスセッションが中断した場合、中断の信号を送信したシステムコンポーネントを示します。中断する可能性のあるシステムコンポーネントには、FAP (Fax Application Process)、TIFF (TIFF リーダーまたは TIFF ライター)、fax-mail クライアント、fax-mail サーバー、ESMTP クライアント、ESMTP サーバーなどがあります。
H323 属性				
26	9	23	Remote-Gateway-ID (h323-remote-address)	リモートゲートウェイの IP アドレスを示します。
26	9	24	Connection-ID (h323-conf-id)	会議 ID を識別します。
26	9	25	Setup-Time (h323-setup-time)	以前、グリニッジ標準時 (GMT) およびズールタイムと呼ばれていた協定世界時 (UTC) でのこの接続のセットアップ時間を示します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	26	Call-Origin (h323-call-origin)	ゲートウェイに対するコールの発行元を示します。有効値は、 originating および terminating です (回答)。
26	9	27	Call-Type (h323-call-type)	コールのレグタイプを示します。使用可能な値は telephony と VoIP です。
26	9	28	Connect-Time (h323-connect-time)	このコールレグの UTC での接続時間を示します。
26	9	29	Disconnect-Time (h323-disconnect-time)	このコールレグが UTC で接続解除された時間を示します。
26	9	30	Disconnect-Cause (h323-disconnect-cause)	Q.931 仕様によって、接続がオフラインにされた理由を示します。
26	9	31	Voice-Quality (h323-voice-quality)	コールの音声品質に影響する Impairment Factor (ICPIF) を指定します。
26	9	33	Gateway-ID (h323-gw-id)	下位のゲートウェイの名前を示します。
大規模のダイヤルアウト属性				
26	9	1	callback-dialstring	コールバックに使用するダイヤリング文字列を定義します。
26	9	1	data-service	説明はありません。
26	9	1	dial-number	ダイヤルする番号を定義します。
26	9	1	force-56	チャンネルの 64K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56K の部分のみを使用するかどうかを指定します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	map-class	ユーザプロファイルに、ダイヤルアウトするネットワークアクセスサーバ上で同じ名前のマップクラスで設定される情報の参照を許可します。
26	9	1	send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル (PAP または CHAP) を定義します。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	send-name	<p>PPP 名前認証。PAP に適用する場合、インターフェイスで ppp pap sent-name password コマンドは設定しないでください。PAP の場合、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 は発信元のボックスへのチャレンジパッケージに、「preauth:send-name」で定義された名前を使用します。</p> <p>(注) send-name 属性は時間の経過とともに変わっています。最初は、現在 send-name および remote-name 属性の両方で提供されている機能を実行していました。remote-name 属性が追加されたため、send-name 属性は現在の動作に制限されています。</p>

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	send-secret	PPP パスワード認証。ベンダー固有属性 (VSA) の場合、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 アウトバウンドの場合、 「preauth:send-name」と「preauth:send-secret」の両方が応答パケットで使用されます。
26	9	1	remote-name	大規模のダイヤルアウトで使用するリモートホストの名前を提供します。ダイヤラは、大規模のダイヤルアウトのリモート名が認証された名前と一致することを確認し、偶発的なユーザ RADIUS 設定ミスから保護します (有効な電話番号にダイヤルしたが誤ったデバイスに接続されるなどのミスです)。
その他の属性				
26	9	2	Cisco-NAS-Port	NAS-Port アカウンティングに追加的なベンダー固有属性 (VSA) を指定します。追加的な NAS-Port 情報を属性値ペア (AVPair) の形式で指定するには、 radius-server vsa send グローバルコンフィギュレーションコマンドを使用します。 (注) この VSA は、通常アカウンティングで使用されますが認証 (Access-Request) パケットで使用される場合もあります。

番号	ベンダー固有の企業コード	サブタイプ番号	属性	説明
26	9	1	min-links	MLP に対するリンクの最小数を設定します。
26	9	1	proxyacl#<n>	ダウンロード可能なユーザプロフィール（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。
26	9	1	spi	登録中にホームエージェントがモバイルノードの認証で必要とする認証情報を伝送します。この情報は、 ip mobile secure host <addr> コンフィギュレーションコマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーションコマンドはそのまま含まれます。これにはセキュリティパラメータインデックス（SPI）、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。

RADIUS Disconnect-Cause 属性値

Disconnect-cause 属性値は、接続がオフラインにされた理由を指定します。属性値は、アカウント要求パケットで送信されます。セッションの認証が失敗しても、これらの値は、セッションの終了時に送信されます。セッションが認証されないと、属性が開始レコードを生成せずに終了レコードを発生させる可能性があります。

次の表に、Disconnect-Cause（195）属性の原因コード、値、および説明を示します。



- (注) Disconnect-Cause は、RADIUS AVPairs で使用されるごとに 1000 ずつ増分されます。たとえば、disc-cause 4 は 1004 になります。

表 3: Disconnect-Cause 属性値

原因コード	値	説明
0	No-Reason	接続解除の理由は提供されない。
1	No-Disconnect	イベントは接続解除されていない。
2	Unknown	理由は不明。
3	Call-Disconnect	コールが接続解除された。
4	CLID-Authentication-Failure	calling-party 数の認証の失敗。
9	No-Modem-Available	コールへの接続にモデムが使用できない。
10	No-Carrier	キャリアが検出されない。 (注) 最初のモデム接続中に接続解除があると、コード 10、11、および 12 が送信される場合があります。
11	Lost-Carrier	キャリアの喪失。
12	No-Detected-Result-Codes	モデム結果コード検出の失敗。
20	User-Ends-Session	ユーザがセッションを終了した。 (注) コード 20、22、23、24、25、26、27、および 28 は、EXEC セッションに適用されます。
21	Idle-Timeout	ユーザ入力待機中のタイムアウト。 コード 21、100、101、102、および 120 は、すべてのセッションタイプに適用されます。
22	Exit-Telnet-Session	既存の Telnet セッションによる接続解除。
23	No-Remote-IP-Addr	SLIP/PPP への切り替え不能。リモートエンドに IP アドレスがない。
24	Exit-Raw-TCP	既存の raw TCP による接続解除。
25	Password-Fail	間違ったパスワード。
26	Raw-TCP-Disabled	Raw TCP がディセーブルにされた。
27	Control-C-Detected	Control-C が検出された。
28	EXEC-Process-Destroyed	EXEC プロセスが破棄された。
29	Close-Virtual-Connection	ユーザが仮想接続を終了した。
30	End-Virtual-Connection	仮想接続が終了した。

原因コード	値	説明
31	Exit-Rlogin	ユーザが Rlogin を終了した。
32	Invalid-Rlogin-Option	無効な Rlogin オプションが選択された。
33	Insufficient-Resources	不十分なリソース。
40	Timeout-PPP-LCP	PPP LCP ネゴシエーションがタイムアウトした。 (注) コード 40 ~ 49 が PPP セッションに適用されます。
41	Failed-PPP-LCP-Negotiation	PPP LCP ネゴシエーションが失敗した。
42	Failed-PPP-PAP-Auth-Fail	PPP PAP 認証が失敗した。
43	Failed-PPP-CHAP-Auth	PPP CHAP 認証が失敗した。
44	Failed-PPP-Remote-Auth	PPP リモート認証が失敗した。
45	PPP-Remote-Terminate	PPP がリモート エンドから Terminate Request を受信した。
46	PPP-Closed-Event	上位層がセッションの終了を要求した。
47	NCP-Closed-PPP	開いている NCP がなかったため、PPP セッションが終了した。
48	MP-Error-PPP	MP エラーのため、PPP セッションが終了した。
49	PPP-Maximum-Channels	最大チャンネルに達したため、PPP セッションが終了した。
50	Tables-Full	ターミナルサーバテーブルがいっぱいになったため、接続解除された。
51	Resources-Full	内部リソースがいっぱいになったため、接続解除された。
52	Invalid-IP-Address	Telnet ホストに対する IP アドレスが有効でない。
53	Bad-Hostname	ホスト名が検証されていない。
54	Bad-Port	ポート番号が無効または欠落している。
60	Reset-TCP	TCP 接続がリセットされた。 (注) コード 60 ~ 67 は Telnet または raw TCP セッションに適用されます。
61	TCP-Connection-Refused	TCP 接続がホストによって拒否された。
62	Timeout-TCP	TCP 接続がタイムアウトした。
63	Foreign-Host-Close-TCP	TCP 接続が終了した。
64	TCP-Network-Unreachable	TCP ネットワークに到達できない。

原因コード	値	説明
65	TCP-Host-Unreachable	TCP ホストに到達できない。
66	TCP-Network-Admin Unreachable	管理上の理由により、TCP ネットワークに到達できない。
67	TCP-Port-Unreachable	TCP ポートに到達できない。
100	Session-Timeout	セッションがタイムアウトした。
101	Session-Failed-Security	セキュリティ上の理由から、セッションが失敗した。
102	Session-End-Callback	コールバックにより、セッションが終了した。
120	Invalid-Protocol	検出されたプロトコルがディセーブルにされていたため、コールが拒否された。
150	RADIUS-Disconnect	RADIUS 要求による接続解除。
151	Local-Admin-Disconnect	管理上の接続解除。
152	SNMP-Disconnect	SNMP 要求による接続解除。
160	V110-Retries	許可された V.110 リトライを超過した。
170	PPP-Authentication-Timeout	PPP 認証がタイムアウトした。
180	Local-Hangup	ローカルのハングアップによって接続解除された。
185	Remote-Hangup	リモートエンドのハングアップによって接続解除された。
190	T1-Quiesced	T1 回線が休止状態のため接続解除された。
195	Call-Duration	コールの最大継続時間を超過したため、接続解除された。
600	VPN-User-Disconnect	クライアントによってコールが接続解除された (PPP 経由)。 LNS がクライアントから PPP terminate request を受信するとコードが送信されます。
601	VPN-Carrier-Loss	キャリアの喪失。これは回線が物理的に普通になった結果である場合があります。 クライアントがダイヤラを使用してダイヤルアウトできない場合、コードが送信されます。
602	VPN-No-Resources	コールの処理に使用できるリソースがない。 クライアントがメモリを割り当てることができない場合、コードが送信されます (メモリの不足)。

原因コード	値	説明
603	VPN-Bad-Control-Packet	L2TP または L2F 制御パケットが間違っている。 このコードは、必須の属性値ペア (AVP) が欠落しているなど、ピアから受信した制御パケットが無効な場合に送信されます。L2TP を使用すると、コードは 6 回の再送信後に送信されます。L2F を使用すると、再送信の回数はユーザ設定が可能です。 (注) トンネルにアクティブなセッションがある場合は、VPN-Tunnel-Shut が送信されます。
604	VPN-Admin-Disconnect	管理上の接続解除。これは、VPN ソフト シャットダウンの結果である場合があります。これは、クライアントが最大セッション制限に達するか、最大ホップカウントを超過した場合に発生します。 トンネルが、 clear vpdn tunnel コマンドの発行によってダウンした場合に、コードが送信されます。
605	VPN-Tunnel-Shut	トンネルのティアダウン、またはトンネルのセットアップが失敗した。 トンネルにアクティブなセッションがあり、トンネルがダウンした場合にコードが送信されます。 (注) このコードはトンネルの認証が失敗した場合は、送信されません。
606	VPN-Local-Disconnect	LNS PPP モジュールによって、コールが接続解除された。 LNS がクライアントに PPP terminate request を送信するとコードが送信されます。これは通常の PPP 接続解除が LNS によって開始されたことを示します。
607	VPN-Session-Limit	VPN ソフト シャットダウンがイネーブルになった。 前述したソフトシャットダウンの制約事項のいずれかによってコールが拒否されると、コードが送信されます。
608	VPN-Call-Redirect	VPN コールリダイレクトがイネーブルになった。

RADIUS 進捗コード

RADIUS 進捗コード機能は、進捗コードを通してコールが切断される前の接続状態を示す RADIUS 属性 196 (Ascend-Connect-Progress) に新たな進捗コードを追加します。

属性 196 は、ネットワーク、EXEC、およびリソースアカウンティング開始および終了レコード内で送信されます。各進捗コードからコールの接続状態に関連するアカウンティング情報が特定されるため、この属性によってコール失敗のデバッグが容易になります。この属性はデフォルトでアクティブになります。アカウンティング開始または終了アカウンティングレコー

ドが要求されると、認証、許可、およびアカウントिंग（AAA）が、属性 196 を標準属性リストの一部としてレコードに追加します。アカウントिंग開始および終了レコード内で送信される進捗コードがコール失敗のデバッグを容易にするため、属性 196 は有用です。



(注) アカウントिंग開始レコードでは、属性 196 に値はありません。

表 4: 属性 196 で新たにサポートされた進捗コード

コード	説明
10	モデム割り当てとネゴシエーションが完了しています。コールが作動しています。
30	モデムが動作中です。
33	モデムが結果コードを待機しています。
41	最大 TNT が、TCP クリア コールを設定することにより TCP 接続を確立しています。
60	リンク制御プロトコル（LCP）が、PPP および IP Control Protocol（IPCP）ネゴシエーションを伴ってオープンな状態にあります。LAN セッションが動作中です。
65	PPP ネゴシエーションが行われ、初めに、LCP ネゴシエーションが行われます。LCP がオープン状態にあります。
67	オープン状態の LCP を伴う PPP ネゴシエーションが行われた後、IPCP ネゴシエーションが開始されます。



(注) 進捗ステータスコード 33、30、および 67 は、NAS でのデバッグを通して生成され表示されます。他のコードはすべて、RADIUS サーバでのデバッグとアカウントングレコードを通して生成され表示されます。

ベンダー独自仕様の RADIUS サーバ通信

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバ間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS 属性セットを独自に機能拡張しているベンダーもあります。Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

前述したように、RADIUS（ベンダーの独自仕様によるものか、IETF ドラフトに準拠するものかを問わず）を設定するには、RADIUS サーバデーモンが稼働しているホストと、そのホストがスイッチと共有秘密テキスト文字列を指定する必要があります。RADIUS ホストおよび秘密テキスト文字列を指定するには、**radius server** グローバル コンフィギュレーション コマンドを使用します。

拡張テストコマンド

拡張テストコマンド機能を使用すると、発呼回線 ID (CLID) または着信番号識別サービス (DNIS) 属性値を持つ名前付きユーザプロファイルを作成できます。RADIUS サーバがすべての着信コールの CLID または DNIS 属性情報にアクセスできるように、CLID または DNIS 属性値を、ユーザプロファイルとともに送信される RADIUS レコードに関連付けることができます。

RADIUS の設定方法

RADIUS サーバホストの識別

デバイスと通信するすべての RADIUS サーバにこのような設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** という 3 つの固有なグローバルコンフィギュレーションコマンドを使用します。

既存のサーバホストを認証用にグループ化するため、AAA サーバグループを使用するようにデバイスを設定できます。詳細については、次の関連項目を参照してください。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。device の IP アドレス、およびサーバと device の双方で共有するキーストリングなどの設定値です。詳細については、RADIUS サーバのマニュアルを参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、次の手順を実行します。

始める前に

device 上にグローバルな機能とサーバ単位での機能 (タイムアウト、再送信回数、およびキーコマンド) を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、およびキーに関するコマンドは、グローバルに設定したタイムアウト、再送信回数、およびキーに関するコマンドを上書きします。すべての RADIUS サーバに対してこれらの値を設定する方法については、次の関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 :	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
	Device# <code>configure terminal</code>	
ステップ 3	radius server <i>server name</i> 例 : Device(config)# <code>radius server server1</code>	RADIUS サーバーの名前を指定し、RADIUS サーバー 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	address { <i>ipv4</i> <i>ipv6</i> } <i>ip address</i> { auth-port <i>port number</i> acct-port <i>port number</i> } 例 : Device(config-radius-server)# <code>address ipv4 172.2.2.12 auth-port 1612</code>	RADIUS サーバのパラメータを指定します。 auth-port <i>port-number</i> には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1645 です。指定できる範囲は 0 ~ 65536 です。 acct-port <i>port-number</i> には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1646 です。
ステップ 5	key [<i>0</i> <i>6</i> <i>7</i>] <i>string</i> 例 : Device(config-radius-server)# <code>key 0</code>	device と RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。

	コマンドまたはアクション	目的
	<code>cisco123</code>	<p>(注)</p> <ul style="list-style-type: none"> キー 0、6、7 は、それぞれクリアテキストパスワード、タイプ 6 暗号化、タイプ 7 暗号化を示します。キーがタイプ 7 と設定されている場合は、タイプ 7 の有効な暗号化文字列も設定する必要があります。同様に、キータイプ 6 の後に続けてタイプ 6 の暗号化文字列を指定する必要があります。 テキスト文字列は、RADIUS サーバーで使用する暗号化キーと一致させる必要があります。必ず radius server コマンドの最終項目としてキーを設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
ステップ 6	<p>end</p> <p>例 :</p> <p>Device(config)# end</p>	特権 EXEC モードに戻ります。

すべての RADIUS サーバの設定

すべての RADIUS サーバを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	radius-server key string 例 : Device(config)# radius-server key your_server_key Device(config)# key your_server_key	スイッチとすべての RADIUS サーバ間で共有されるシークレット テキスト ストリングを指定します。 (注) キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
ステップ 4	radius-server retransmit retries 例 : Device(config)# radius-server retransmit 5	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ~ 1000 です。
ステップ 5	radius-server timeout seconds 例 : Device(config)# radius-server timeout 3	スイッチが RADIUS 要求に対する応答を待つ、要求を再送信するまでの時間（秒）を指定します。デフォルトは 5 秒です。指定できる範囲は 1 ~ 1000 です。
ステップ 6	radius-server deadtime minutes 例 :	RADIUS サーバが認証要求に回答していない場合、このコマンドはそのサーバに対する要求を停止する時刻を指定しま

	コマンドまたはアクション	目的
	Device (config)# radius-server deadtime 0	す。これにより、要求がタイムアウトするまで待たずとも、次に設定されているサーバを試行することができます。デフォルトは0です。指定できる範囲は1～1440分です。
ステップ7	end 例： Device (config)# end	特権 EXEC モードに戻ります。

RADIUS ログイン認証の設定

RADIUS ログイン認証を設定するには、次の手順を実行します。

始める前に

AAA 方式を使用して HTTP アクセスに対しデバイスのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでデバイスを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しデバイスのセキュリティは確保されません。

手順

	コマンドまたはアクション	目的
ステップ1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	aaa new-model 例： Device (config)# aaa new-model	AAA をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	<p>aaa authentication login {default list-name} method1 [method2...]</p> <p>例 :</p> <pre>Device(config)# aaa authentication login default local</pre>	<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"> • login authentication コマンドに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、default キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • <i>list-name</i> には、作成するリストの名前として使用する文字列を指定します。 • <i>method1...</i> 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。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> • <i>enable</i> : イネーブルパスワードを認証に使用します。この認証方式を使用するには、あらかじめ enable password 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イネーブルパスワードを定義しておく必要があります。 • <i>group radius</i> : RADIUS 認証を使用します。この認証方式を使用するには、あらかじめ RADIUS サーバを設定しておく必要があります。 • <i>line</i> : 回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。 password password ライン コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>local</i> : ローカルユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。 username name password グローバル コンフィギュレーション コマンドを使用します。 • <i>local-case</i> : 大文字と小文字が区別されるローカルユーザ名データベースを認証に使用します。username password 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、ユーザ名情報をデータベースに入力する必要があります。 • <i>none</i> : ログインに認証を使用しません。
ステップ 5	line [console tty vty] line-number <i>[ending-line-number]</i> 例 : Device(config)# line 1 4	ライン コンフィギュレーション 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 6	login authentication {default list-name} 例 : Device(config)# login authentication default	1つの回線または複数回線に認証リストを適用します。 <ul style="list-style-type: none"> • default を指定する場合は、aaa authentication login コマンドで作成したデフォルトのリストを使用します。 • <i>list-name</i> には、aaa authentication login コマンドで作成したリストを指定します。
ステップ 7	end 例 : Device(config)# end	特権 EXEC モードに戻ります。

AAA サーバグループの定義

定義したグループサーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **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することもできます。

AAA サーバグループを定義するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	radius server name 例： Device(config)# radius server ISE	RADIUS サーバの設定の名前を Protected Access Credential (PAC) のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。 deviceは、IPv6 対応の RADIUS をサポートしています。
ステップ 4	address {ipv4 ipv6} {ip-address hostname} auth-port port-number acct-port port-number 例： Device(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646	RADIUS サーバのアカウントिंगおよび認証パラメータの IPv4 アドレスを設定します。
ステップ 5	key [0 6 7] string 例： Device(config-radius-server)# key 0	デバイスと RADIUS サーバとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。

	コマンドまたはアクション	目的
	<pre>cisco123</pre>	<p>(注)</p> <ul style="list-style-type: none"> キー 0、6、7 は、それぞれクリアテキストパスワード、タイプ 6 暗号化、タイプ 7 暗号化を示します。キーがタイプ 7 と設定されている場合は、タイプ 7 の有効な暗号化文字列も設定する必要があります。同様に、キータイプ 6 の後に続けてタイプ 6 の暗号化文字列を指定する必要があります。 テキスト文字列は、RADIUS サーバーで使用する暗号化キーと一致させる必要があります。必ず radius server コマンドの最終項目としてキーを設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
<p>ステップ 6</p>	<pre>end</pre> <p>例 :</p> <pre>Device(config-radius-server)# end</pre>	<p>RADIUS サーバコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。</p>

ユーザイネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定



(注) 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

ユーザ特権アクセスおよびネットワーク サービスに関する RADIUS 許可を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	aaa authorization network radius 例 : Device (config)# aaa authorization network radius	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 許可を受けられるようにデバイスを設定します。
ステップ 4	aaa authorization exec radius 例 : Device (config)# aaa authorization exec radius	ユーザに特権 EXEC のアクセス権限がある場合、ユーザが RADIUS 許可を受けられるように device を設定します。 exec キーワードを指定すると、ユーザ プロファイル情報 (autocommand 情報など) が返される場合があります。
ステップ 5	end 例 : Device (config)# end	特権 EXEC モードに戻ります。

次のタスク

aaa authorization グローバル コンフィギュレーション コマンドと **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

RADIUS アカウンティングの起動

RADIUS アカウンティングを開始するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	aaa accounting network start-stop radius 例： Device (config)# aaa accounting network start-stop radius	ネットワーク関連のあらゆるサービス要求に関して、RADIUS アカウンティングをイネーブルにします。
ステップ 4	aaa accounting exec start-stop radius 例： Device (config)# aaa accounting exec start-stop radius	RADIUS アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	end 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device(config)# end	

属性 196 の確認

RADIUS 進捗コードには設定は必要ありません。アカウント開始および停止記録内の属性 196 を確認するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	debug aaa accounting 例： Device# debug aaa accounting	説明の義務があるイベントが発生したときに、その情報を表示します。
ステップ 3	show radius statistics 例： Device# debug aaa authorization	アカウントリ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。

ベンダー固有の RADIUS 属性を使用するデバイスの設定

ベンダー固有の RADIUS 属性を使用するようにデバイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例：	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
	Device# <code>configure terminal</code>	
ステップ 3	radius-server vsa send [accounting authentication] 例 : Device (config)# <code>radius-server vsa send accounting</code>	<p>device が VSA (RADIUS IETF 属性 26 で定義) を認識して使用できるようにします。</p> <ul style="list-style-type: none"> • (任意) 認識されるベンダー固有属性の集合をアカウントング属性だけに限定するには、accounting キーワードを使用します。 • (任意) 認識されるベンダー固有属性の集合を認証属性だけに限定するには、authentication キーワードを使用します。 <p>キーワードを指定せずにこのコマンドを入力すると、アカウントングおよび認証のベンダー固有属性の両方が使用されます。</p>
ステップ 4	end 例 : Device (config)# <code>end</code>	特権 EXEC モードに戻ります。

ベンダー独自仕様の RADIUS サーバ通信に関するデバイスの設定

ベンダー独自仕様の RADIUS サーバ通信を使用するようにデバイスを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> <code>enable</code>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 :	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
	Device# configure terminal	
ステップ 3	radius server <i>server name</i> 例 : Device(config)# radius server server1	RADIUS サーバ設定の名前を Protected Access Credential (PAC) のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。
ステップ 4	address { <i>ipv4 ipv6</i> } <i>ip address</i> 例 : Device(config-radius-server)# address ipv4 172.2.2.12	(任意) RADIUS サーバの IP アドレスを指定します。
ステップ 5	non-standard 例 : Device(config-radius-server)# non-standard	RADIUS サーバが RADIUS ベンダー独自の実装を使用していることを示します。
ステップ 6	key [<i>0 6 7</i>] <i>string</i> 例 : Device(config-radius-server)# key 0 cisco123	デバイスとベンダー独自仕様の RADIUS サーバとの間で使用される共有秘密タイプと文字列を指定します。デバイスと RADIUS サーバはこれを使用してパスワードを暗号化し、応答を交換します。

	コマンドまたはアクション	目的
		<p>(注)</p> <ul style="list-style-type: none"> • キー 0、6、7 は、それぞれクリアテキストパスワード、タイプ 6 暗号化、タイプ 7 暗号化を示します。キーがタイプ 7 と設定されている場合は、タイプ 7 の有効な暗号化文字列も設定する必要があります。同様に、キータイプ 6 の後に続けてタイプ 6 の暗号化文字列を指定する必要があります。 • テキスト文字列は、RADIUS サーバーで使用する暗号化キーと一致させる必要があります。必ず radius server コマンドの最終項目としてキーを設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
ステップ 7	<p>end</p> <p>例 :</p> <pre>Device(config-radius-server)# end</pre>	特権 EXEC モードに戻ります。

ユーザ プロファイルの設定と RADIUS レコードへの関連付け

ここでは、CLID または DNIS 属性値を持つ名前付きユーザ プロファイルを作成し、RADIUS レコードに関連付ける方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	aaa user profile profile-name 例： Device(config)# aaa user profile profilename1	ユーザ プロファイルを作成します。
ステップ 4	aaa attribute {dnis clid} 例： Device(config)# aaa attribute dnis	DNIS または CLID 属性値をユーザ プロファイルに追加し、AAA ユーザ コンフィギュレーション モードを開始します。
ステップ 5	exit 例： Device(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 6	test aaa group {group-name radius} username password new-code [profile profile-name] 例： Device# test aaa group radius secret new-code profile profilename1	DNIS または CLID の名前付きユーザ プロファイルを、RADIUS サーバに送信するレコードに関連付けます。 (注) <i>profile-name</i> は aaa user profile コマンドで指定するプロファイル名と一致する必要があります。

拡張テスト コマンドの設定の確認

拡張テスト コマンドの設定を確認するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Device# debug radius	RADIUS 関連の情報を表示します。

コマンド	目的
Device# more system:running-config	現在実行されているコンフィギュレーション ファイルの内容を表示します(コマンド more system:running-config が show running-config コマンドに置き換えられていることに注意してください)。

RADIUS の設定例

例：RADIUS サーバホストの識別

次に、1つのRADIUSサーバを認証用に、もう1つのRADIUSサーバをアカウントング用に設定する例を示します。

```
Device# configure terminal
Device(config)# radius server server1
Device(config-radius-server)# address ipv4 172.2.2.12 auth-port 1612
Device(config-radius-server)# key key1
Device(config-radius-server)# exit
Device(config)# radius server server2
Device(config-radius-server)# address ipv4 172.2.2.20 auth-port 1618
Device(config-radius-server)# key key2
Device(config-radius-server)# exit
```

例：AAA サーバグループ

次に、3つのRADIUSサーバメンバを持ち、各メンバがデフォルトの認証ポート（1645）とアカウントングポート（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、各メンバがIPアドレスは同じでも認証ポートとアカウント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
```


RADIUS 進捗コードに関するトラブルシューティングのヒント

次の例は、**debug ppp negotiation** コマンドからのデバッグ出力のサンプルです。このデバッグ出力を使用して、アカウント終了レコードが生成されていることと、属性 196 (Ascend-Connect-Progress) に 65 の値が設定されていることを確認します。

```
Tue Aug 7 06:21:03 2001
  NAS-IP-Address = 10.0.58.62
  NAS-Port = 20018
  Vendor-Specific = ""
  NAS-Port-Type = ISDN
  User-Name = "peer_16a"
  Called-Station-Id = "5213124"
  Calling-Station-Id = "5212175"
  Acct-Status-Type = Stop
  Acct-Authentic = RADIUS
  Service-Type = Framed-User
  Acct-Session-Id = "00000014"
  Framed-Protocol = PPP
  Framed-IP-Address = 172.16.0.2
  Acct-Input-Octets = 3180
  Acct-Output-Octets = 3186
  Acct-Input-Packets = 40
  Acct-Output-Packets = 40
  Ascend-Connect-Pr = 65
  Acct-Session-Time = 49
  Acct-Delay-Time = 0
  Timestamp = 997190463
  Request-Authenticator = Unverified
```

例：ベンダー固有の RADIUS 属性を使用するデバイスの設定

たとえば、次の AV ペアを指定すると、IP 許可時 (PPP の IPCP アドレスの割り当て時) に、シスコの複数の名前付き IP アドレス プール機能が有効になります。

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

次に、デバイスから特権 EXEC コマンドへの即時アクセスが可能となるユーザログインを提供する例を示します。

```
cisco-avpair= "shell:priv-lvl=15"
```

次に、RADIUS サーバデータベース内の許可 VLAN を指定する例を示します。

```
cisco-avpair= "tunnel-type (#64)=VLAN (13)"
cisco-avpair= "tunnel-medium-type (#65)=802 media (6)"
cisco-avpair= "tunnel-private-group-id (#81)=vlanid"
```

次に、この接続中に ASCII 形式の入力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

例：ベンダー独自仕様の RADIUS サーバ通信に関するデバイスの設定

```
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

次に、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

例：ベンダー独自仕様の RADIUS サーバ通信に関するデバイスの設定

次に、ベンダー独自の RADIUS ホストを指定し、デバイスとサーバの間で *rad124* という秘密キーを使用する例を示します。

```
Device# configure terminal
Device(config)# radius server server1
Device(config-radius-server)# address ipv4 172.2.2.12
Device(config-radius-server)# nonstandard
Device(config-radius-server)# key rad124
Device(config-radius-server)# exit
```

例：test aaa group コマンドに関連付けるユーザ プロファイル

次に、*dnis = dnisvalue* ユーザプロファイル *prfl1* を設定し、**test aaa group** コマンドに関連付ける例を示します。この例では、**debug radius** コマンドが有効化され、設定の後に出力が続いています。

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
!
!
!
! debug radius output, which shows that the dnis value has been passed to the radius !
server.
*Dec 31 16:35:48: RADIUS: Sending packet for Unique id = 0
*Dec 31 16:35:48: RADIUS: Initial Transmit unknown id 8 172.22.71.21:1645, Access-Request,
len 68
*Dec 31 16:35:48: RADIUS: code=Access-Request id=08 len=0068
  authenticator=1E CA 13 F2 E2 81 57 4C - 02 EA AF 9D 30 D9 97 90
  T=User-Password[2] L=12 V=*
  T=User-Name[1] L=07 V="test"
  T=Called-Station-Id[30] L=0B V="dnisvalue"
  T=Service-Type[6] L=06 V>Login [1]
  T=NAS-IP-Address[4] L=06 V=10.0.1.81

*Dec 31 16:35:48: RADIUS: Received from id 8 172.22.71.21:1645, Access-Accept, len 38
*Dec 31 16:35:48: RADIUS: code=Access-Accept id=08 len=0038
```

RADIUS に関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst Micro Switches)</i>

標準および RFC

標準/RFC	タイトル
RFC 5176	RADIUS 認可変更 (CoA) の拡張

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィッチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/support</p>

RADIUS の機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS Release 15.2(7)E3k	RADIUS	RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバシステムです。RADIUS クライアントは、サポート対象のシスコデバイス上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。

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 には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。