SIP AAA 機能の設定

この章では、次の SIP Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）機能を設定する方法について説明します。

- 設定可能なスクリーニング インジケータ（このマニュアルでは、SIP - ゲートウェイの拡張課金サポートの一部として扱います）
- 音声コールの Remote Authentication Dial In User Service（RADIUS）事前認証
- SIP：ゲートウェイの拡張課金サポート
- SIP：ゲートウェイ HTTP 認証ダイジェスト

設定可能なスクリーニング インジケータ機能の履歴[1]

リリース	変更点
12.2(2)XB	この機能が導入されました。
12.2(8)T	この機能がこのリリースに統合されました。

音声コールの RADIUS 事前認証機能の履歴

リリース	変更点
12.2(11)T	この機能が導入されました。

SIP - SIP ゲートウェイの拡張課金サポート機能の履歴

リリース	変更点
12.2(2)XB	この機能が導入されました。
12.2(8)T	この機能がこのリリースに統合されました。
12.2(11)T	この機能が追加のプラットフォームに実装されました。

SIP：ゲートウェイ HTTP 認証ダイジェスト機能の履歴

リリース	変更点
12.3(8)T	この機能が導入されました。

1. Resource Reservation Protocol（RSVP; リソース予約プロトコル）と Telephone Uniform Resource Locator（TEL URL）の SIP ゲートウェイ サポート機能の一部として導入されました。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の検索

プラットフォーム サポートと Cisco IOS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザ名やパスワードを忘れた場合は、ログイン ダイアログボックスで [Cancel] をクリックし、表示される説明に従ってください。

この章の構成

SIP AAA の前提条件

すべての SIP AAA 機能

- 運用 IP ネットワークを確立します。IP の設定に関する詳細については、『*Cisco IOS IP Command Reference*』（リリース 12.3）を参照してください。
- VoIP を設定します。VoIP の設定の詳細については、次のドキュメントを参照してください。
  - 『*Cisco IOS Voice Configuration Library*』（リリース 12.4T）
  - 『*Cisco IOS Voice Command Reference*』
  - 『Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms』
- ゲートウェイで SIP の音声機能が設定されていることを確認します。

音声コールの RADIUS 事前認証機能

- 事前認証をサポートしているアプリケーションを所有していることを確認します。
- 事前認証プロファイルをセットアップして、ネットワーク内の RADIUS ベースの Port Policy Management（PPM）サーバで実行します。
- **gw-accounting** コマンドを使用して、ゲートウェイ アカウンティングをイネーブルにします。すべてのコール アカウンティング情報は、事前認証を実行しているサーバに転送する必要があります。コールがゲートウェイから切断されたときにコールの課金が終了するように、アカウンティング終了パケットをこのサーバに送信する必要があります。また、Virtual Private Dial-up Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）など、その他の機能をイネーブルにするには、認証とアカウンティング開始のパケットが必要です。

（注） 事前認証プロファイルをセットアップする方法については、『*Cisco IOS Security Command Reference*』を参照してください。

Cisco Resource Policy Management System（RPMS）の詳細については、『*Cisco Resource Policy Management System 2.0*』を参照してください。

RADIUS ベースの PPM サーバをサポートしている標準については、『RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*』を参照してください。

SIP：ゲートウェイ HTTP 認証ダイジェスト機能

- SIP をサポートしている Cisco IOS SIP ゲートウェイを実装します。
- SIP をサポートしている設定を実装します。
- ゲートウェイが送信した要求に対する認証確認に応答できるように、認証設定を実装します。

SIP AAA に関する制約事項

すべての SIP AAA 機能

- Cisco Resource Policy Management System（RPMS）を RADIUS ベースの PPM サーバとして使用する場合は、バージョン 2.0 以降のリリースを使用する必要があります。
- SIP 環境で、Cisco SIP Proxy Server（Cisco SPS）によって事前認証クエリーを生成する場合は、Cisco SPS 2.0 以降のバージョンを実行する必要があります。

SIP：SIP User Agent（UA; ユーザ エージェント）使用のゲートウェイ HTTP 認証ダイジェスト機能

- SIP 登録がサポートされるのは、デジタル トランク タイプのポートを備えたプラットフォーム上だけです。

SIP AAA の概要

SIP の AAA 機能には次の利点があります。

- RADIUS 事前認証によって、ホールセール事業者は、コールが接続される前にコールを受け入れる、または拒否することによって、Service Level Agreement（SLA; サービス レベル契約）を実施できるので、ゲートウェイのリソースを節約できます。
- コール アドミッション制御によって、リソースが使用できない場合はコールを接続しないようにすることができます。
- 拡張ダイヤル プラン機能によって、コール サービス タイプを事前認証要求データから判断でき、ダイヤル プランのエントリを簡素化できます。
- ユニバーサル ゲートウェイには次の利点があります。
  - 新しいサービスの展開、ビジネス環境の変化への適応を柔軟に実行できます。
  - 各種サービスを提供するのに必要なポートの合計数を減らすことによって、コストを削減できます。
  - オフピーク時にサポートするサービスの数を増やすことによってアクセス インフラストラクチャの使用率を最適化します。

– ダイヤルと音声両方の処理にダイヤル インフラストラクチャを利用することによって、アクセス ネットワーク エンジニアリングに柔軟性をもたらします。

SIP の AAA 機能を設定するには、次の概念を理解しておく必要があります。

- 「音声コールの RADIUS 事前認証」（P.4）
- 「SIP - ゲートウェイの拡張課金サポート」（P.7）
- 「SIP：ゲートウェイ HTTP 認証ダイジェスト」（P.9）

音声コールの RADIUS 事前認証

ここでは、RADIUS 事前認証を実行するためにユニバーサル ゲートウェイと RADIUS ベースの PPM サーバとの間に AAA RADIUS 通信リンクを設定する方法について説明します。

着信コールに関する情報は、そのコールが接続される前にゲートウェイを経由してネットワーク内の RADIUS ベースの PPM サーバに中継されます。RADIUS ベースの PPM サーバでは、コール情報を SLA に定義されている契約パラメータ レベルに照らして評価することによって、ポート ポリシー管理と事前認証を行います。コールが SLA 制限の範囲に収まる場合は、サーバはコールを事前認証し、ユニバーサル ゲートウェイはコールを受け入れます。サーバがコールを認可しない場合、ユニバーサル ゲートウェイは、切断メッセージを公衆網スイッチに送信して、コールを拒否します。使用できるコール情報は、次の 1 つまたは複数の項目です。

- Dialed Number Identification Service（DNIS; 着信番号識別サービス）番号（送信先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）。
- 発信元ドメインの IP アドレス。
- Interzone ClearToken（IZCT）情報。このトークンには、ドメイン内コールの発信ゲートキーパー ゾーン名またはドメイン内コールの起点ドメイン ボーダー ゲートキーパー ゾーン名が格納されます。IZCT 情報は、使用できる場合は必ず、レッグ 3 H.323 VoIP コールの事前認証を行うときに使用されます。

（注） IZCT をイネーブルにするには、ゲートキーパーで、**security izct password** コマンドを使用します。複数のゲートキーパー ゾーンの場合は、**lrq forward-queries** コマンドを使用します。

IZCT の設定の詳細については、『*Inter-Domain Gatekeeper Security Enhancement, Release 12.2(4)T*』を参照してください。

RADIUS ベースの PPM サーバ アプリケーションが応答できないまたは応答が遅い場合に備えて、タイマーによって事前認証クエリーを監視します。受け入れまたは拒否が実行される前にタイマーの期限が切れた場合、ユニバーサル ゲートウェイはコールを拒否します。

RADIUS Pre-authentication for Voice Calls 機能では、RADIUS 事前認証プロファイルに設定する RADIUS アトリビュートを使用して、事前認証の動作を指定することをサポートしています。たとえば、これらのアトリビュートを使用して、後続の認証を実行するかどうかを指定したり、実行する場合に使用する認証方式を指定できます。

このセクションに記載されているコマンドは、レッグ 1 のコール（Public Switched Telephone Network（PSTN; 公衆電話交換網）から着信（発信側）ゲートウェイに移動するコール）とレッグ 3 のコール（IP ネットワークを出て発信（着信側）ゲートウェイに移動するコール）の両方に対して使用されます。オプション コマンドの使用は、各ネットワーク要素によって異なります。

（注） AAA 事前認証を設定する前に、Cisco RPMS など、事前認証をサポートしているアプリケーションがネットワーク内の RADIUS ベースの PPM サーバで実行されていることを確認する必要があります。また、事前認証プロファイルを RADIUS ベースの PPM サーバにセットアップする必要があります。AAA の詳細については、『*Cisco IOS Security Configuration Guide*』を参照してください。

音声コールの RADIUS 事前認証機能を使用すると、ユニバーサル ゲートウェイで受信した音声コールとダイヤル コール両方のコール セットアップ要求を評価し、受け入れるか拒否することができます。このプロセスを事前認証といいます。この機能では、必要に応じて音声コールの評価をバイパスできます。

ユニバーサル ゲートウェイを使用している場合、音声の顧客とダイヤルの顧客は、同じゲートウェイ リソースを利用します。このことは、Internet Service Provider（ISP; インターネット サービス プロバイダー）、Internet Telephony Service Provider（ITSP; インターネット テレフォニー サービス プロバイダー）、Telephony Application Service Provider（T-ASP; テレフォニー アプリケーション サービス プロバイダー）など、さまざまな顧客に IP サービスをリースしている IP サービスのホールセール事業者にとって問題となる場合があります。ホールセール事業者には、提供を保証する接続、パフォーマンス、および可用性のレベルを規定したサービス レベル契約（SLA）を実装して、実施する手段が必要です。RADIUS Pre-authentication for Voice Calls 機能によって、ホールセール事業者は、コールの終端にゲートウェイ リソースを使用する前に、そのコールが SLA 制限の範囲内であるかどうかを判断できます。

RADIUS 事前認証をイネーブルにすると、オーバーサブスクライブ サービス プロバイダーを利用する最終顧客は、SLA でそのサービス プロバイダーに割り当てられた数を超えるポートを使用できなくなります。コールが事前認証段階で受け入れられた場合、そのコールは、完全なダイヤル認証と認可、または音声ダイヤル ピア マッチングと音声セッション アプリケーション認証と認可に進みます。

RADIUS 事前認証では、Cisco Resource Policy Management System（RPMS）などの RADIUS ベースの Port Policy Management（PPM）サーバを使用して、ユニバーサル PPM と事前認証 SLA を解釈し、実施します。RADIUS は、PPM サーバとユニバーサル ゲートウェイの間に通信リンクを提供します。

顧客プロファイルは、SLA の情報を使用して PPM サーバで定義します。コールがユニバーサル ゲートウェイで受信されると、サーバは、そのコールに関連付けられている情報に基づいて、そのコールに適用する顧客の SLA ポリシーを決定します。たとえば、コールは、送信先番号（着信番号識別サービス（DNIS）番号とも呼ばれます）に基づいて、ダイヤルと音声のどちらであるかを識別できます。PPM サーバは、一定数のダイヤル コールだけを許可するように設定されている場合があります。新しいダイヤル コールを受信し、そのコールをカウントに追加すると、SLA に規定されているダイヤル コール数を超える場合は、そのコールを拒否します。

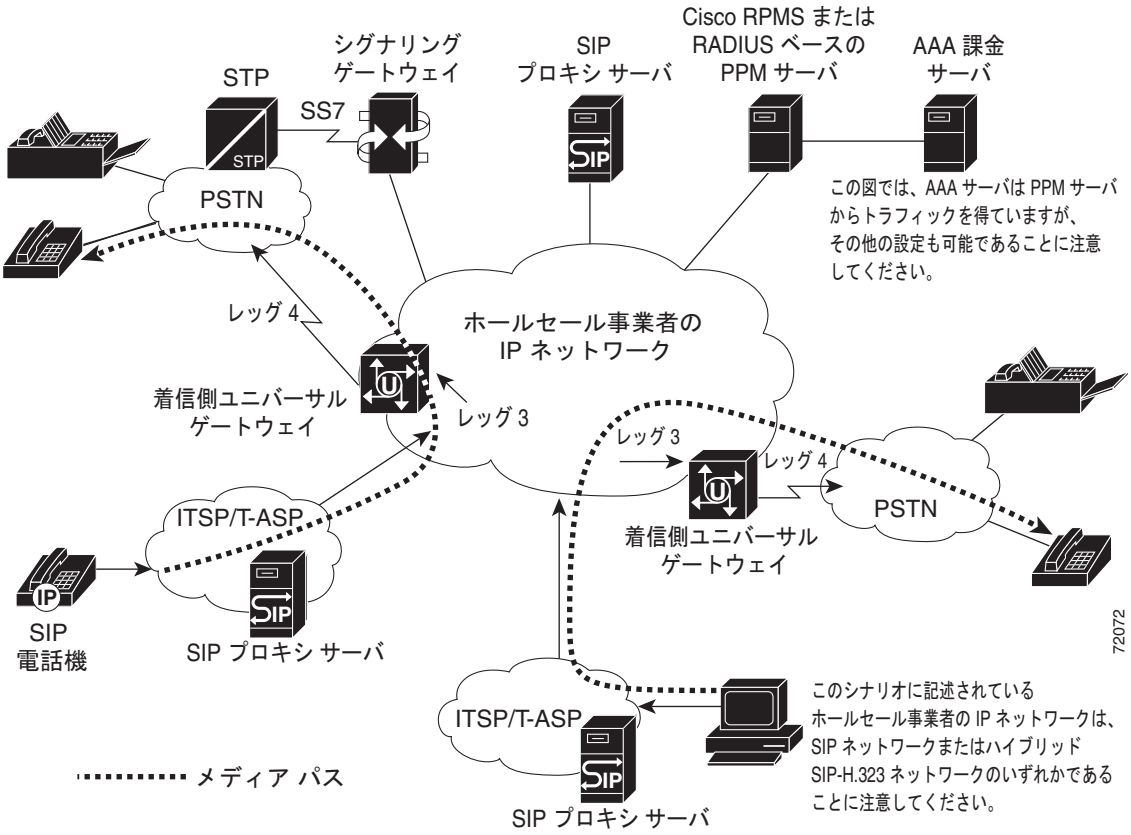
PPM サーバによって受け入れられたコールは、事前認証後、通常のコール セットアップ シーケンスに進みます。PPM サーバからの応答は、ISDN または SIP コール シグナリング インターフェイスなど、発信エンティティに返されます。その後、通常のコール フローに進みます。PPM サーバによって拒否されたコールは、指定のコール モデルに従い、シグナリング エンティティで指定されたエラー コードと拒否理由が適用されます。

SIP ベースの音声インターフェイス

図 1 では、SIP 電話機または SIP 端末からの音声コールが ITSP からホールセール事業者に送信されます。Cisco SIP Proxy Server（Cisco SPS）が、独自のルーティング メカニズムに基づいて SIP INVITE を転送する適切なユニバーサル ゲートウェイを選択します。手順 3 で、Cisco SPS は、RPMS ベースの PPM サーバに事前認証クエリーを実行します。Cisco SPS は、RPMS ベースの PPM サーバによって拒否されたコールをロックアウトします。手順 5 で、ユニバーサル ゲートウェイは、事前認証予約の要求を RPMS ベースの PPM サーバに送信します。このサーバで、コールを処理するリソースが決定されます。

（注） このシナリオには Cisco SPS 2.0 が必要です。

図 1　　SIP ベースの音声インターフェイス



コール フローは次のとおりです。

1. SIP INVITE がエンド ユーザの PC から ITSP SIP プロキシ サーバに送信されます。
2. ITSP の SIP プロキシ サーバは、SIP INVITE をホールセール事業者または ISP 側にある Cisco SPS に転送します。
3. 事前認証。Cisco SPS は、事前認証クエリーを RADIUS ベースの PPM サーバに送信します。PPM サーバは、該当する SLA を見つけ、コールが SLA 制限の範囲内であることを確認します。コールが制限の範囲外である場合、コールは拒否され、Cisco SPS は、「エラー コード 480 - Temporarily not available」メッセージで送信元に応答します。Cisco SPS と RADIUS ベースの PPM サーバの対話は、省略可能です。この対話には、Cisco SPS バージョン 2.0 以降のリリースが必要です。Cisco SPS 2.0 を使用していない場合、ゲートウェイが RADIUS ベースの PPM サーバに対して事前認証クエリーを実行します（ゲートウェイでクエリーを実行するように設定されている場合）。
4. ゲートウェイの選択。事前認証要求が受け入れられた場合、Cisco SPS はルーティング ロジックを使用して、INVITE を転送するのに適切な着信側ユニバーサル ゲートウェイを決定します。
5. コール アドミッション制御。事前認証要求が受け入れられた場合、着信側ユニバーサル ゲートウェイは設定されているコール アドミッション制御の制限を確認します。コールがその制限の範囲外である場合は、コールは拒否されます。

6. 認証と認可。ユニバーサル ゲートウェイはポートを予約し、認証、認可、アカウンティング（AAA）アカウンティング開始パケットを RADIUS ベースの PPM サーバに送信します。
7. 発信側とユニバーサル ゲートウェイの間の接続が成立します（コール レッグ 3）。
8. 発信側は PSTN に接続されます（コール レッグ 4）。
9. アカウンティング終了。発信側が電話を切るか、発信側が切断された後に、着信側ユニバーサル ゲートウェイは、アカウンティング終了パケットを RADIUS ベースの PPM サーバに送信します。PPM サーバは、このアカウンティング終了パケットを使用して、SLA に対するそのコールのカウントを消去します。

SIP - ゲートウェイの拡張課金サポート

ここでは、SIP - ゲートウェイの拡張課金サポート機能について説明します。Cisco SIP ゲートウェイでの認証、認可、アカウンティング（AAA）レコードおよび Remote Authentication Dial-In User Service（RADIUS）の実装の変更点について説明します。これらの変更は、お客様とパートナーが SIP ネットワーク上に転送されるトラフィックの課金を効率的に行うことができるようにするために導入されました。

ここでは、次の内容について説明します。

ユーザ名アトリビュート

ユーザ名アトリビュートは、すべての AAA レコードに格納されていて、課金システムでエンド ユーザを識別するための第一の方法です。パスワード アトリビュートは、着信 VoIP コール レッグの認証と認可のメッセージに格納されます。

ほとんどの実装で SIP ゲートウェイは、FROM: ヘッダーの発番号を使用して SIP INVITE 要求のユーザ名アトリビュートにデータを入力し、ヌルまたは Interactive Voice Response（IVR; 自動音声応答）スクリプトのデータを使用してパスワード アトリビュートにデータを入力します。Proxy-Authorization ヘッダーがある場合、このヘッダーは無視されます。**aaa username** コマンドによって、ユーザ名アトリビュートに入力される情報が決まります。

ユーザの認証を行い、ユーザを識別する Microsoft Passport 認証サービスでは、Passport User ID（PUID; Passport ユーザ ID）が使用されます。PUID とパスワードは、SIP INVITE 要求の Proxy-Authorization ヘッダーを使用して 1 つの Base 64 符号化文字列として Microsoft 社のネットワークからインターネット テレフォニー サービス プロバイダー（ITSP）のネットワークに渡されます。例を次に示します。

```
Proxy-Authorization: basic MDAwMzAwMDA4MDM5MzJlNjou
```

aaa username コマンドを使用すると、Proxy-Authorization ヘッダーの解釈、PUID とパスワードのデコード、ユーザ名アトリビュートへの PUID の入力、およびパスワード アトリビュートへのデコードしたパスワードの入力を実行できます。Microsoft Network（MSN）はこの時点よりも前にユーザの認証を行うので、デコードしたパスワードは、通常、1 つの「.」です。例を次に示します。

```
Username = "123456789012345"
Password = "Z\335\304\326KU\037\301\261\326GS\255\242\002\202"
```

上記の例のパスワードは、暗号化された 1 つの「.」で、すべてのユーザで同じパスワードです。

SIP コール ID

SIP コール ID は、SIP INVITE 要求の Call ID ヘッダーから抽出され、シスコ Vender -Specific Attribute（VSA; ベンダー固有アトリビュート）にアトリビュート値ペア *call-id=string* として入力されます。この値ペアを使用して、Cisco SIP ゲートウェイの RADIUS レコードと、プロキシなどの他の SIP ネットワーク要素の RADIUS レコードを関連付けることができます。

（注） このアトリビュート値ペアの詳細については、『*RADIUS* Vendor-Specific Attributes Voice Implementation Guide』を参照してください。

セッション プロトコル

セッション プロトコルは、コールが SIP と H.323 のどちらをシグナリング プロトコルとして使用しているのかを示すアトリビュート値ペアです。

（注） このアトリビュート値ペアの詳細については、『*RADIUS Vendor-Specific* Attributes Voice Implementation Guide』を参照してください。

サイレント認証スクリプト

SIP - SIP ゲートウェイの拡張課金サポート機能の一部として、Tool Command Language（TCL; ツール コマンド言語）自動音声応答（IVR）2.0 サイレント認可スクリプトが開発されました。サイレント認可スクリプトを使用すると、ユーザが個別にユーザ名またはパスワードをシステムに入力しなくても、ユーザを認可することができます。スクリプトは、自動的に Passport ユーザ ID（PUID）とパスワードを SIP INVITE 要求から抽出し、RADIUS 認証と認可のレコードを使用してその情報の認証を行います。このスクリプトは、発信側にも着信側にもプロンプトが聞こえないことから、*サイレント*と呼ばれます。

（注）
- CCO Software Center からスクリプトの最新バージョンにアップグレードできます。app_passport_silent.2.0.0.0.tcl スクリプトは、http://www.cisco.com/cgi-bin/tablebuild.pl/tclware からダウンロードできます。これらのファイルにログインし、アクセスできるのは、CCO の登録ユーザだけです。
- Tcl IVR API 2.0 の詳細については、『*Tcl IVR API Version 2.0 Programmer's Guide*』を参照してください。

Tcl サイレント認可スクリプトをお使いの開発者は、Cisco Developer Support Program に参加することを推奨します。このプログラムで信頼できる安定したサポートを得ながら、開発プロジェクトでシスコのインターフェイスを活用することができます。また、このプログラムには、Cisco.com を経由して簡単に問題を報告、更新、および追跡できる方法が用意されています。シスコの Web サイトは、Cisco オンライン問題追跡ツールを使用するための主要な通信手段です。このプログラムに参加するには、Developer Support Agreement に署名する必要があります。詳細およびこの契約書については、http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html を参照するか、developer-support@cisco.com までご連絡ください。

設定可能なスクリーニング インジケータ

Screening Indicator（SI; スクリーニング インジケータ）は、着信コールの認可メカニズムとして使用できる ISDN SETUP メッセージのオクテット 3a にあるシグナリング関連情報の要素です。Tcl IVR 2.0 コマンド セットによって、SIP 着信側ゲートウェイは、Tcl スクリプトを使用して特定の値をスクリーニング インジケータに割り当てることができます。

スクリーニング インジケータには、次の 4 つの値のいずれかを割り当てることができます。

- User provided, not screened
- User provided, verified and passed
- User provided, verified and failed
- Network provided

（注）

- どのシナリオでも、ゲートウェイ アカウンティングをイネーブルにし、コール アカウンティング情報を、事前認証を実行するサーバに転送する必要があります。コールがゲートウェイから切断されたときにコールの課金が終了するように、アカウンティング終了パケットをこのサーバに送信する必要があります。また、バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）など、その他の機能をイネーブルにするには、認証とアカウンティング開始のパケットが必要です。
- Tcl IVR スクリプトを使用して、スクリーニング インジケータを設定および取得する方法については、『*Tcl IVR API Version 2.0 Programmer's Guide*』を参照してください。

SIP：ゲートウェイ HTTP 認証ダイジェスト

SIP：ゲートウェイ HTTP 認証ダイジェスト機能は、共通の SIP スタックのクライアント側でダイジェスト アクセスを使用して認証を実装します。ゲートウェイは、認証サーバ、プロキシ サーバ、または User Agent Server（UAS; ユーザ エージェント サーバ）から送信される認証確認に応答します。この機能では、認証をすでにサポートしているシスコのゲートウェイ、プロキシ サーバ、および SIP 電話機の間でパリティを管理します。

この機能の利点は次のとおりです。

- SIP ゲートウェイは、認証プロキシ サーバまたはユーザ エージェント サーバ（UAS）から送信される認証確認に応答することができます。サポートされる認証方式は、ダイジェスト認証です。ダイジェスト認証は最も良い方式ではありませんが、基本レベルのセキュリティが備わっています。

  （注） 認証確認を行うとき、UAS は 401 応答、プロキシ サーバは 407 応答を使用します。これらのサーバは、認証確認と応答を発行してレルムに適切な認証クレデンシャルを見つけようとします。ゲートウェイは、プロキシ サーバと UAS 両方からの認証確認を処理できます。

- Plain Old Telephone Service（POTS; 一般電話サービス）ダイヤル ピアでの宛先パターンの登録は、すべての PSTN インターフェイスに適用されます。

（注） プロキシ サーバは、以前は、SIP 電話機に対してだけ認証を行っていました。

以前のリリースの SIP Survivable Remote Site Telephony（SRST）機能には、Foreign Exchange Station（FXS）（アナログ電話の音声ポート）と Extended Foreign Exchange Station（EFXS; 拡張 FXS）（IP 電話の仮想音声ポート）の E.164 番号を外部の SIP レジストラに登録するためのサポートが追加されました。この機能は、Primary Rate Interface（PRI; 1 次群速度インターフェイス）パイプなど、PSTN トランクに設定された番号をゲートウェイが登録できるように拡張されました。

ここでは、次の内容について説明します。

ダイジェスト アクセス認証

SIP は、ダイジェスト アクセスに基づく認証にステートレス チャレンジ/レスポンス方式を提供します。要求を受信した UAS またはプロキシ サーバは、要求の発信側に識別情報を示すように指示します。User Agent Client（UAC; ユーザ エージェント クライアント）は、認証確認とそのパスワードに対して Message Digest 5（MD5）チェックサムを実行して、応答を生成します。応答は、次の要求で認証確認の発信側に渡されます。

次の 2 つの認証モードがあります。

- プロキシ サーバ認証
- UAS 認証

この機能は、ゲートウェイでの複数のプロキシ認証もサポートしています。ゲートウェイは、UAC として機能するゲートウェイと UAS の間のシグナリング パスで最大 5 つの異なる認証確認に応答できます。

UAC と UAS の間の認証

UAS は、UAC からクレデンシャルのない要求を受信すると、WWW-Authenticate ヘッダーを含んだ 401 Unauthorized 応答でその要求を拒否し、クレデンシャルを示すように発信側に指示します。ヘッダー フィールドの値は、次のように、ダイジェスト方式に適切な引数で構成されます。

- realm：ユーザに表示される文字列。この文字列によってユーザは、使用するユーザ名とパスワードを決定できます。
- nonce：サーバ指定のデータ文字列。この文字列は、401 応答を生成するたびに一意に生成する必要があります。

このヘッダー フィールドには次のオプションの引数が使用される可能性があります。

- opaque：サーバが指定するデータ文字列。クライアントは、後続の要求の Authentication ヘッダーにこの文字列をそのまま変更せずに格納し、同じ保護領域に Uniform Resource Identifier（URI; ユニフォーム リソース識別子）を格納して、送信する必要があります。
- stale：クライアントからの前の要求が拒否されたのは、ナンス値が古いことが理由であるかどうかを示すフラグ。
- algorithm：ダイジェストとチェックサムを生成するのに使用するアルゴリズムのペアを示す文字列。
- qop-options：サーバによってサポートされる「保護の品質」の値を示す、1 つ以上のトークンで構成される文字列。
- auth-param：今後の拡張用に用意されているディレクティブ。

UAC は、Authorization ヘッダー フィールドに適切なクレデンシャルを格納して要求を再び生成します。Authorization ヘッダー フィールドの値は、次の認証情報と引数で構成されます。

- username：指定されたレルムのユーザ名。この値は、ダイヤル ピアまたはグローバル レベルでの設定から取得されます。
- digest-uri：要求の request uri と同じ。
- realm、nonce：WWW-Authenticate ヘッダーに指定された値。

Message Digest 5（MD5）は次のように計算されます。

```
MD5(concat(MD5(A1),(unquoted)nonce-value":"nc-value":"
(unquoted)cnonce-value ":"(unquoted)qop-value":"MD5(A2)))
```

A1 =（引用符なし）ユーザ名値 ":" （引用符なし）レルム値 ":" パスワード

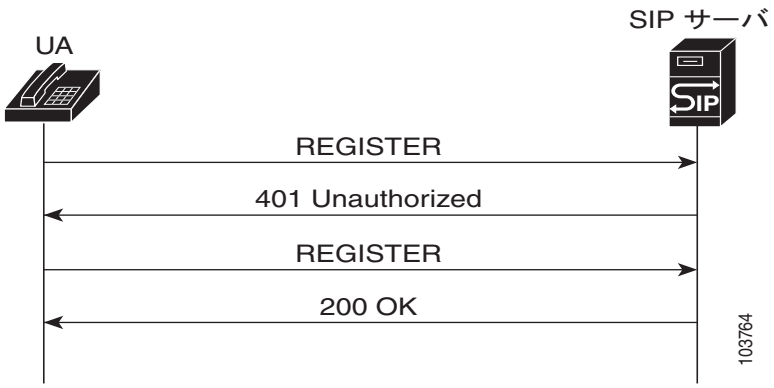
```
A2 = Method ":" request-uri if qop is "auth"
& A2 = Method ":" request-uri ":" MD5(entity-body) if qop is "auth-int".
```

- nc-value は、要求の数の 16 進値です（クライアントが、この要求のナンス値を使用して送信した現在の要求も数に含まれます）。
- cnonce-value は、クライアントとサーバの相互認証のためにクライアントが提供する opaque 文字列です。
- qop-value は、保護の品質ディレクティブで、"auth" または "auth-int" です。

UAC と UAS の間のコール フロー（Register メッセージ使用）

このコール フロー（図 2 を参照）では、UA は、Authorization ヘッダーなしで Register メッセージ要求を送信し、SIP サーバから 401 ステータス コード メッセージ応答の認証確認を受信します。UA は、Authorization ヘッダーに適切なクレデンシャルを格納して要求を再び送信します。

図 2　　UA と UAS の間のコール フロー（Register メッセージ使用）



UA は、CSeq を 1 に初期化して、Register メッセージ要求を SIP サーバに送信します。

```
REGISTER sip:172.18.193.187:5060 SIP/2.0
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK200B
From: "36602" <sip:36602@172.18.193.120>;tag=98AS-87RT
To: <sip:36602@172.18.193.187>
Call-ID: A9EEC728-495E11D6-8003AD63-F55A9C4
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 1 REGISTER
Contact: <sip:36602@172.18.193.120:5060>;user=phone
Expires: 60
Content-Length: 0
```

SIP サーバは、401 Unauthorized 認証確認で UA に応答します。

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK200B
From: "36602" <sip:36602@172.18.193.120>;tag=98AS-87RT
To: <sip:36602@172.18.193.187>;tag=3046583040568302
Call-ID: A9EEC728-495E11D6-8003AD63-F55A9C4
CSeq: 1 REGISTER
WWW-Authenticate: Digest realm="example.com", qop="auth",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", stale=FALSE, algorithm=MD5
Content-Length: 0
```

UA は、認可情報を追加し、CSeq の数を増やして、Register メッセージ要求を再び SIP サーバに送信します。

```
REGISTER sip:172.18.193.187:5060 SIP/2.0
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK1DEA
From: "36602" <sip:36602@172.18.193.120>;tag=98AS-89FD
To: <sip:36602@172.18.193.187>
Call-ID: A9EEC728-495E11D6-8003AD63-F55A9C4
User-Agent: Cisco-SIPGateway/IOS-12.x
Authorization: Digest username="36602", realm="example.com",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", uri="sip:172.18.193.187",
response="dfe56131d1958046689d83306477ecc"
CSeq: 2 REGISTER
Contact: <sip:36602@172.18.193.120:5060>;user=phone
Expires: 60
Content-Length: 0
```

SIP サーバは、200 OK メッセージ応答で UA に応答します。

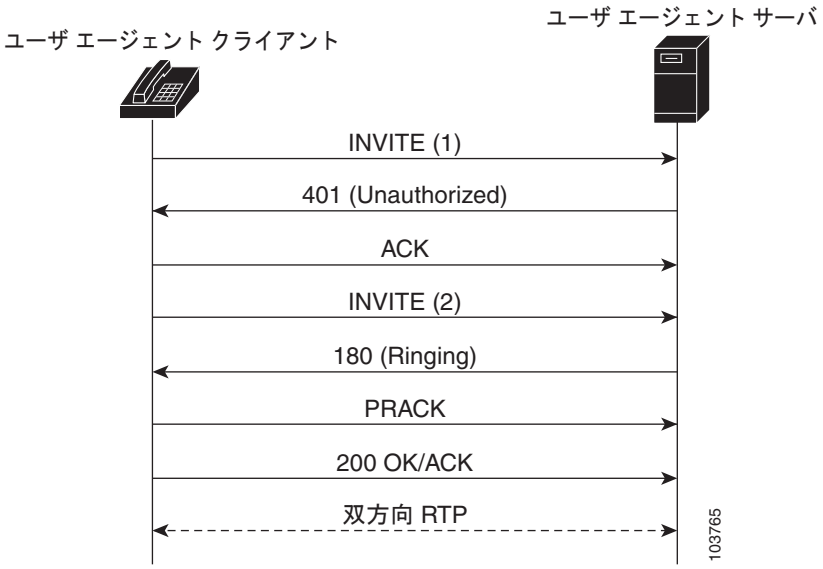
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.18.193.120:5060;received=172.18.193.120;branch=z9hG4bK1DEA
Call-ID: A9EEC728-495E11D6-8003AD63-F55A9C4
From: "36602" <sip:36602@172.18.193.120>;tag=98AS-89FD
To: <sip:36602@172.18.193.187>;tag=1q92461294
CSeq: 2 REGISTER
Contact: <sip:36602@172.18.193.120:5060>;expires="Wed, 02 Jul 2003 18:18:26 GMT"
Expires: 60
Content-Length: 0
```

（注） SIP サーバは、ACK と CANCEL 要求メッセージ以外のすべての要求に対して認証確認を送信できます。ACK メッセージ要求に対して応答は返信しません。また、CANCEL メッセージ要求は再送信できません。UA は、INVITE メッセージ要求と同じクレデンシャルを ACK メッセージ要求で使用します。

UAC と UAS の間のコール フロー（INVITE メッセージ使用）

このコール フロー（図 3 を参照）では、UAC は適切なクレデンシャルなしで INVITE メッセージ要求を UAS に送信し、401 Unauthorized メッセージ応答で認証確認を受信します。正しいクレデンシャルが追加された新しい INVITE メッセージ要求が送信されます。これで、コールが成立します。

図 3　　UAC と UAS の間のコール フロー（INVITE メッセージ使用）



UAS は、401 Unauthorized メッセージ応答を送信して、ユーザ クレデンシャルを示すように UAC に指示します。

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK45TGN
From: "36602" <sip:36602@172.18.193.120>;tag=98AS-87RT
To: <sip:36602@172.18.193.187>;tag=3046583040568302
Call-ID: A9EEC728-495E11D6-8003AD63-F55A9C4
CSeq: 101 INVITE
WWW-Authenticate: Digest realm="example.com", qop="auth",
nonce="ea9c8e8809345gf1cec4341ae6cgh5a359", opaque=""
Content-Length: 0
```

UAC は、Authorization ヘッダーに適切なクレデンシャルを格納して要求を再び送信します。

```
INVITE sip:36601@172.18.193.187:5060 SIP/2.0
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK8DF8H
From: "36602"<sip:36602@172.18.193.120>;tag=50EB48-383
To: <sip:36601@172.18.193.187>
Call-ID: A9EEC728-495E11D6-8003AD63-F55A9C4
CSeq: 102 INVITE
Authorization: Digest username="36602", realm="example.com",
nonce="ea9c8e8809345gf1cec4341ae6cgh5a359", opaque="", uri="sip:36601@172.18.193.187",
response="42ce3cef44b22f50c02350g6071bc8"
.
.
.
```

UAC は、このダイアログの後続の要求では、同じクレデンシャルを使用します。

```
PRACK sip:36601@172.18.193.187:5060 SIP/2.0
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK8YH5790
From: "36602"<sip:36602@172.18.193.120>;tag=50EB48-383
To: <sip:36601@172.18.193.187>;tag=AG09-92315
Call-ID: A9EEC728-495E11D6-8003AD63-F55A9C4
CSeq: 103 PRACK
Authorization: Digest username="36602", realm="example.com",
nonce="ea9c8e8809345gf1cec4341ae6cgh5a359", opaque="", uri="sip:36601@172.18.193.187",
response="42ce3cef44b22f50c02350g6071bc9"
Content-Length: 0
```

プロキシ サーバと UA の間の認証

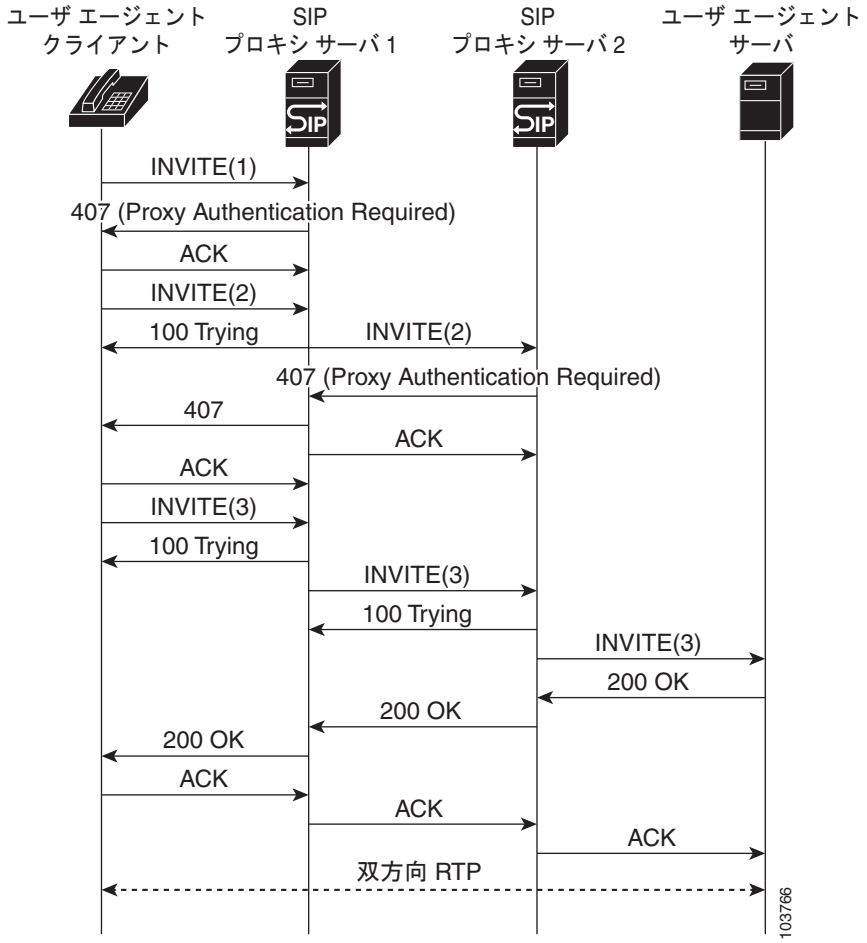
UA が適切なクレデンシャルなしでプロキシ サーバに要求を送信すると、プロキシ サーバは、407 メッセージ応答（Proxy Authentication Required）で要求を拒否することによって送信元の認証を行い、Proxy-Authenticate ヘッダー フィールドに要求されたリソースのプロキシ サーバに該当する値を格納します。UAC は、「UAC と UAS の間の認証」（P.10）で説明した手順と同じ手順に従い、レルムの適切なクレデンシャルを取得して、そのクレデンシャルを Proxy-Authorization ヘッダーに格納して要求を再び送信します。

（注） realm：ユーザに表示される文字列。この文字列によってユーザは、使用するユーザ名とパスワードを決定できます。

プロキシ サーバと UA の間の認証コール フロー

このコール フローでは、UAC は、2 つのプロキシ サーバ（PS 1 または PS 2）を使用して、UAS へのコールを成立させます（図 4 を参照）。UAC は、両方のドメインで有効なクレデンシャルを持っています。最初の INVITE メッセージ要求には、プロキシ サーバ 1 に必要な認可クレデンシャルが格納されていないので、認証確認情報を含んだ 407 Proxy Authorization メッセージ応答が送信されます。正しいクレデンシャルが格納された新しい INVITE メッセージ要求が送信され、プロキシ サーバ 2 が認証確認を送信し、有効なクレデンシャルを受信した後に、コールは次の段階に進みます。

図 4　プロキシ サーバと UA の間のコール フロー



プロキシ サーバ 1 は、UAC に認証確認を送信します。

```
SIP/2.0 407 Proxy Authorization Required
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK207H
From: <sip:36602@172.18.193.120>;tag=50EB48-383
To: <sip:36601@172.18.193.187>;tag=929523858000835
Call-ID: D61E40D3-496A11D6-80070030-9426ED30@172.18.193.120
CSeq: 101 INVITE
Proxy-Authenticate: Digest realm="proxy1.example.com", qop="auth”,
nonce="wf84f1cczx41ae6cbeaea9ce88d359", opaque="", stale=FALSE, algorithm=MD5
Content-Length: 0
```

UAC は、認証クレデンシャルを使用して INVITE メッセージ要求を再び送信して、これに応答します。同じコール ID を使用するので、CSeq の値を増やします。

```
INVITE sip:36601@172.18.193.187:5060 SIP/2.0
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bKEE1
From: <sip:36602@172.18.193.120>;tag=50EB48-383
To: <sip:36601@172.18.193.187>
Call-ID: D61E40D3-496A11D6-80070030-9426ED30@172.18.193.120
CSeq: 102 INVITE
Proxy-Authorization: Digest username="36602", realm="proxy1.example.com",
nonce="wf84f1ceczx41ae6cbe5aea9c8e88d359", opaque="", uri="sip:36601@172.18.193.187",
response="42ce3cef44b22f50c6a6071bc8"
Contact: <sip:172.18.193.120:5060>
.
.
.
```

プロキシ サーバ 2 は、UAC INVITE メッセージ要求に対し、認証確認を送信します。これは、プロキシ サーバ 1 から UAC に転送される 407 認証メッセージ応答です。

```
SIP/2.0 407 Proxy Authorization Required
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bKEE1
From: <sip:36602@172.18.193.120>;tag=50EB48-383
To: <sip:36601@172.18.193.187>;tag=083250982545745
Call-ID: D61E40D3-496A11D6-80070030-9426ED30@172.18.193.120
Proxy-Authenticate: Digest realm="proxy2.example.com", qop="auth",
nonce="c1e22c41ae6cbe5ae983a9c8e88d359", opaque="", stale=FALSE, algorithm=MD5
Content-Length: 0
```

UAC は、プロキシ サーバ 1 とプロキシ サーバ 2 に対する認証クレデンシャルを使用して INVITE メッセージ要求を再び送信して、応答します。

```
INVITE sip:36601@172.18.193.187:5060 SIP/2.0
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK8GY
From: <sip:36602@172.18.193.120>;tag=50EB48-383
To: <sip:36601@172.18.193.187>
Call-ID: D61E40D3-496A11D6-80070030-9426ED30@172.18.193.120
CSeq: 103 INVITE
Proxy-Authorization: Digest username="36602", realm="proxy1.example.com",
nonce="wf84f1ceczx41ae6cbe5aea9c8e88d359", opaque="", uri="sip:36601@172.18.193.187",
response="42ce3cef44b22f50c6a6071bc8"
Proxy-Authorization: Digest username="36602", realm="proxy2.example.com",
nonce="c1e22c41ae6cbe5ae983a9c8e88d359", opaque="", uri="sip:36601@172.18.193.187",
response="f44ab22f150c6a56071bce8"
.
.
.
```

ゲートウェイでの SIP 登録サポートの拡張

SIP：ゲートウェイ HTTP 認証ダイジェスト機能では、機能を拡張して、Cisco IOS SIP ゲートウェイが、すべてのポートに対する運用中の POTS ダイヤル ピアにある宛先パターンによって指定されたすべてのアドレスを登録できるようにしました。これにより、PRI インターフェイスを介してゲートウェイに接続されている Private Branch Exchange（PBX; 構内交換機）の背後に存在するユーザを登録し、認証を行うことができます。FXS ポートを使用するゲートウェイが各 E.164 アドレスを登録する方法に変更はありません。

この機能では、ダイヤル ピアを利用して、登録と認証の細かさを作成します。ただし、ダイヤル ピアは、ワイルドカード（たとえば、.919T。終端子 [T] を指定すると、ゲートウェイは、完全なダイヤル文字列を受信するまで待機します）と番号の範囲（たとえば、.919392...。... は、0000 ～ 9999 の範囲の番号を示します）を使用して作成できます。このような宛先パターンは、To ヘッダーと Contact ヘッダーのユーザ部分に 1 つのワイルドカード文字を使用して登録されます。表 1 に、さまざまなゲートウェイのダイヤル プランとその登録の間のマッピングを示します。

表 1　SIP Cisco IOS ゲートウェイのダイヤル ピアと登録のマッピング[1]

Cisco IOS SIP GW 設定	対応する登録
dial-peer voice 919 pots	REGISTER sip:proxy.example.com SIP/2.0
destination-pattern 919.....	To: <sip:919.....@172.18.193.120>
port 0:D	From: <sip:172.18.192.120>;tag=ABCD
	Contact: <sip:919.....@172.18.193.120>;user=phone
dial-peer voice 555 pots	REGISTER sip:proxy.example.com SIP/2.0
destination-pattern 555T	To: <sip:555*@172.18.193.120>
port 0:D	From: <sip:172.18.192.120>;tag=ABCD
	Contact: <sip:555*@172.18.193.120>;user=phone
dial-peer voice 5550100 pots	REGISTER sip:proxy.example.com SIP/2.0
destination-pattern 5550100	To: <sip:5550100@172.18.193.120>
port 0:D	From: <sip:5550100@172.18.192.120>;tag=ABCD
	Contact: <sip:5550100@172.18.193.120>;user=phone

1. ワイルドカード パターンまたは範囲が指定された宛先パターンのコールを正しくルーティングするように、プロキシ/レジストラの動作を変更する必要があります。ワイルドカード パターンまたは範囲が指定された宛先パターンに適合しないプロキシ サーバまたはレジストラは、その特定の要求で無視する必要があります。

SIP AAA 機能の設定方法

ここでは、次の各手順について説明します。

音声コールの RADIUS 事前認証の設定

ここでは、次の手順について説明します。

RADIUS グループ サーバの設定

RADIUS グループ サーバを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius**
5. **server**
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 new-model** **例：** `Router(config)# aaa new-model`	認証、認可、アカウンティング 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 group server radius** *groupname* **例：** `Router(config-sg-radius)# aaa group server radius radgroup1`	（任意）さまざまな RADIUS サーバ ホストを個別のリストと個別の方式にグループ化します。引数は次のとおりです。 • *groupname*：サーバのグループに名前を付けるために使用する文字列。

	コマンドまたはアクション	目的
ステップ 5	**server** *ip-address* [**auth-port** *port*] [**acct-port** *port*] **例：** `Router(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001`	（**aaa group server** コマンドを使用する場合は必須）グループ サーバ用に RADIUS サーバの IP アドレスを設定します。キーワードと引数は次のとおりです。 • *ip-address* : RADIUS サーバ ホストの IP アドレス。 • **auth-post** *port-number* : 認証要求の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）宛先ポート。この値を 0 に設定した場合、ホストは認証に使用されません。デフォルトは 1645 です。 • **acct-port** *port-number* : アカウンティング要求の UDP 宛先ポート。この値を 0 に設定した場合、ホストはアカウンティング サービスに使用されません。デフォルトは 1646 です。
ステップ 6	**exit** **例：** `Router(config-sg-radius)# exit`	現在のモードを終了します。

アクセスと認証の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authentication login h323 group**
4. **aaa authentication ppp default group**
5. **aaa authorization exec group**
6. **aaa authorization network default group**
7. **aaa authorization reverse-access default local**
8. **aaa accounting suppress null-user-name**
9. **aaa accounting send stop-record authentication failure**
10. **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	**aaa authentication login h323 group** *groupname* **例：** `Router(config)# aaa authentication billson h323 group 123`	ログイン時の認証、認可、アカウンティングを設定します。キーワードと引数は次のとおりです。 • **h323**：認証に H.323 を使用します。 • **group** *groupname*：**aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドによって定義されたとおりに、RADIUS サーバまたは Terminal Access Controller Access Control System Plus（TACACS+）サーバのサブセットを認証に使用します。
ステップ 4	**aaa authentication ppp default group** *groupname* **例：** `Router(config)# aaa authentication ppp default group 123`	(PPP ダイヤルイン方式を事前認証に使用する場合は必須）PPP を実行しているシリアル インターフェイスで使用する 1 つ以上の認証、認可、アカウンティングの認証方式を指定します。キーワードと引数は次のとおりです。 • **default**：この引数の後に指定した認証方式のリストを、ユーザがログインしたときの方式のデフォルト リストとして使用します。 • **group** *groupname*：**aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドによって定義されたとおりに、RADIUS サーバまたは TACACS+ サーバのサブセットを認証に使用します。
ステップ 5	**aaa authorization exec** *list-name* **group** *groupname* **例：** `Router(config)# aaa authorization exec billson group 123`	(任意）ネットワークへのユーザ アクセスを制限するパラメータを設定します。キーワードと引数は次のとおりです。 • **exec**：認可を実行して、EXEC シェルを実行することがユーザに許可されているかどうかを確認します。この機能では、autocommand の情報など、ユーザ プロファイルの情報が返される場合があります。 • *list-name*：認可方式のリストに名前を付けるために使用する文字列。 • **group** *groupname*：**aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドによって定義されたとおりに、RADIUS サーバまたは TACACS+ サーバのサブセットを認証に使用します。

	コマンドまたはアクション	目的
ステップ 6	**aaa authorization network default group** {**radius** | **rpms**} **if-authenticated** **例：** `Router(config)# aaa authorization network default group radius if-authenticated`	（任意）ネットワークへのユーザ アクセスを制限するパラメータを設定します。キーワードは次のとおりです。 • **network**：シリアル ライン インターネット プロトコル、ポイントツーポイント プロトコル、PPP ネットワーク コントロール プログラム、Apple Talk Remote Access を含む、すべてのネットワーク関連のサービス要求に対して認可を実行します。 • **default**：この引数の後に指定した認可方式のリストを認可方式のデフォルト リストとして使用します。 • **group radius**：**aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドによって定義されたとおりに、RADIUS サーバまたは TACACS+ サーバのサブセットを認証に使用します。 • **group rpms**：**aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドによって定義されたとおりに、RADIUS サーバまたは TACACS+ サーバのサブセットを認証に使用します。 • **if-authenticated**：ユーザが認証された場合は、ユーザが要求した機能にアクセスすることを許可します。
ステップ 7	**aaa authorization reverse-access default local** **例：** `Router(config)# aaa authorization reverse-access default local`	（任意）リバース Telnet セッションを確立することをユーザに許可する前にセキュリティ サーバに認可情報を要求するようにネットワーク アクセス サーバを設定します。キーワードは次のとおりです。 • **default**：この引数の後に指定した認可方式のリストを認可方式のデフォルト リストとして使用します。 • **local**：ローカル データベースを認可に使用します。
ステップ 8	**aaa accounting suppress null-user-name** **例：** `Router(config)# aaa accounting suppress null-username`	（任意）ユーザ名の文字列がヌルであるユーザのアカウンティング レコードを Cisco IOS ソフトウェアが送信しないようにします。
ステップ 9	**aaa accounting send stop-record authentication failure** **例：** `Router(config)# aaa accounting send stop-record authentication failure`	（Cisco RPMS を使用している場合は必須）ログイン時またはセッション ネゴシエーション時に認証に失敗したユーザのアカウント「終了」レコードを生成します。
ステップ 10	**exit** **例：** `Router(config)# exit`	現在のモードを終了します。

アカウンティングの設定

（注） **aaa accounting** コマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting delay-start**
4. **aaa accounting update periodic**
5. **aaa accounting exec default start-stop group**
6. **aaa accounting exec start-stop group**
7. **aaa accounting network default start-stop group**
8. **aaa accounting connection h323 start-stop group**
9. **aaa accounting system default start-stop group**
10. **aaa accounting resource default start-stop-failure group**
11. **gw-accounting aaa**
12. **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 accounting delay-start** **例：** `Router(config)# aaa accounting delay-start`	（任意）ユーザの IP アドレスが確立されるまでアカウンティング「開始」レコードの生成を遅らせます。
ステップ 4	**aaa accounting update** [**periodic** *number*] **例：** `Router(config)# aaa accounting update periodic 30`	（任意）アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。キーワードと引数は次のとおりです。 • **periodic** *number*：中間アカウンティング レコードは、引数 *number*（分単位）によって定義されたとおりに、アカウンティング サーバに定期的に送信されます。

	コマンドまたはアクション	目的
ステップ 5	**aaa accounting exec default start-stop group** *groupname* **例：** `Router(config)# aaa accounting exec default start-stop group joe`	（任意）課金のため、あるいは RADIUS または TACACS+ を使用して、シェル セッションを実行するときのセキュリティのために、要求したサービスの認証、認可、アカウンティングをイネーブルにします。キーワードと引数は次のとおりです。 • **exec**：EXEC シェル セッションのアカウンティングを実行します。このキーワードを指定すると、**autocommand** コマンドによって生成される情報など、プロファイル情報が返される場合があります。 • **default**：この引数の後に指定したアカウンティング方式のリストをアカウンティング サービスの方式のデフォルト リストとして使用します。 • **start-stop**：プロセスの開始時に「開始」アカウンティング通知を送信し、プロセスの終了時に「終了」アカウンティング通知を送信します。「開始」アカウンティング レコードはバックグラウンドで送信されます。要求したユーザ プロセスは、「開始」アカウンティング通知がアカウンティング サーバによって受信されたかどうかに関係なく、開始されます。 • **group** *groupname*：server **group** *groupname* によって定義されたとおりに、RADIUS サーバまたは TACACS+ サーバのサブセットをアカウンティングに使用します。
ステップ 6	**aaa accounting exec** *list-name* **start-stop group** *groupname* **例：** `Router(config)# aaa accounting exec joe start-stop group tacacs+`	（任意）課金のため、あるいは RADIUS または TACACS+ を使用して、方式名を指定するときのセキュリティのために、要求したサービスの認証、認可、アカウンティングをイネーブルにします。キーワードと引数は次のとおりです。 • **exec**：EXEC シェル セッションのアカウンティングを実行します。このキーワードを指定すると、**autocommand** コマンドによって生成される情報など、プロファイル情報が返される場合があります。 • *list-name*：1 つ以上のアカウンティング方式で構成されるリストに名前を付けるために使用する文字列。 • **start-stop**：プロセスの開始時に「開始」アカウンティング通知を送信し、プロセスの終了時に「終了」アカウンティング通知を送信します。「開始」アカウンティング レコードはバックグラウンドで送信されます。要求したユーザ プロセスは、「開始」アカウンティング通知がアカウンティング サーバによって受信されたかどうかに関係なく、開始されます。 • **group** *groupname*：server **group** *groupname* によって定義されたとおりに、RADIUS サーバまたは TACACS+ サーバのサブセットをアカウンティングに使用します。

	コマンドまたはアクション	目的
ステップ 7	**aaa accounting network default start-stop group** *groupname* **例：** `Router(config)# aaa accounting network default start-stop group tacacs+`	(PPP ダイヤルイン方式を事前認証に使用する場合は必須）課金のため、あるいは RADIUS または TACACS+ を使用するときのセキュリティのために、要求したネットワーク サービスの認証、認可、アカウンティングをイネーブルにします。キーワードと引数は次のとおりです。 • **network**：シリアル ライン インターネット プロトコル、ポイントツーポイント プロトコル、PPP ネットワーク コントロール プロトコル、Apple Talk Remote Access Protocol を含む、すべてのネットワーク関連のサービス要求に対してアカウンティングを実行します。 • **default**：この引数の後に指定したアカウンティング方式のリストをアカウンティング サービスの方式のデフォルト リストとして使用します。 • **start-stop**：プロセスの開始時に「開始」アカウンティング通知を送信し、プロセスの終了時に「終了」アカウンティング通知を送信します。「開始」アカウンティング レコードはバックグラウンドで送信されます。要求したユーザ プロセスは、「開始」アカウンティング通知がアカウンティング サービスによって受信されたかどうかに関係なく、開始されます。 • **group** *groupname*：次の中から 1 つ以上を使用します。 – **group radius**：**aaa group server radius** コマンドによって定義されたとおりにすべての RADIUS サーバのリストを認証に使用します。 – **group-tacacs+**：**aaa group server tacacs+** コマンドによって定義されたとおりにすべての TACACS+ サーバのリストを認証に使用します。 – **group** *groupname*：server group *groupname* によって定義されたとおりに、RADIUS サーバまたは TACACS+ サーバのサブセットをアカウンティングに使用します。

	コマンドまたはアクション	目的
ステップ 8	**aaa accounting connection h323 start-stop group** *groupname* **例：** `Router(config)# aaa accounting connection h323 start-stop group tacacs+`	（音声コール アカウンティングの場合は必須）課金のため、あるいは RADIUS または TACACS+ を使用して、接続情報を取得するときのセキュリティのために、要求したサービスのアカウンティングをイネーブルにします。キーワードと引数は次のとおりです。 • **connection**：Telnet、LAT、TN3270、PAD、rlogin など、ネットワーク アクセス サーバから行われるすべてのアウトバウンド接続に関する情報を指定します。 • **h323**：1 つ以上のアカウンティング方式で構成されるリストに名前を付けるために使用する文字列。**h323** をアカウンティングに使用します。 • **start-stop**：プロセスの開始時に「開始」アカウンティング通知を送信し、プロセスの終了時に「終了」アカウンティング通知を送信します。「開始」アカウンティング レコードはバックグラウンドで送信されます。要求したユーザ プロセスは、「開始」アカウンティング通知がアカウンティング サービスによって受信されたかどうかに関係なく、開始されます。 • **group** *groupname*：次の中から 1 つ以上を使用します。 – **group radius**：**aaa group server radius** コマンドによって定義されたとおりにすべての RADIUS サーバのリストを認証に使用します。 – **group-tacacs+**：**aaa group server tacacs+** コマンドによって定義されたとおりにすべての TACACS+ サーバのリストを認証に使用します。 – **group** *groupname*：server group *groupname* によって定義されたとおりに、RADIUS サーバまたは TACACS+ サーバのサブセットをアカウンティングに使用します。

	コマンドまたはアクション	目的
ステップ 9	**aaa accounting system default start-stop group** *groupname* **例：** `Router(config)# aaa accounting system default start-stop group tacacs+`	（任意）課金のため、および RADIUS または TACACS+ を使用して、システムレベルのイベントのアカウンティングを行うときのセキュリティのために、要求したサービスのアカウンティングをイネーブルにします。キーワードと引数は次のとおりです。 • **system**：リロードなど、ユーザに関連付けられていないすべてのシステムレベルのイベントに対してアカウンティングを実行します。 • **default**：この引数の後に指定したアカウンティング方式のリストをアカウンティング サービスの方式のデフォルト リストとして使用します。 • **start-stop**：プロセスの開始時に「開始」アカウンティング通知を送信し、プロセスの終了時に「終了」アカウンティング通知を送信します。「開始」アカウンティング レコードはバックグラウンドで送信されます。要求したユーザ プロセスは、「開始」アカウンティング通知がアカウンティング サービスによって受信されたかどうかに関係なく、開始されます。 • **group** *groupname*：次の中から 1 つ以上を使用します。 – **group radius**：**aaa group server radius** コマンドによって定義されたとおりにすべての RADIUS サーバのリストを認証に使用します。 – **group-tacacs+**：**aaa group server tacacs+** コマンドによって定義されたとおりにすべての TACACS+ サーバのリストを認証に使用します。 – **group** *groupname*：server group *groupname* によって定義されたとおりに、RADIUS サーバまたは TACACS+ サーバのサブセットをアカウンティングに使用します。
ステップ 10	**aaa accounting resource default start-stop-failure group** *groupname* **例：** `Router(config)# aaa accounting resource default start-stop-failure group tacacs+`	（任意）完全なリソース アカウンティングをイネーブルにします。この場合、コール セットアップ時に「開始」レコードが生成され、コール終了時に「終了」レコードが生成されます。キーワードと引数は次のとおりです。 • **default**：この引数の後に指定したアカウンティング方式のリストをアカウンティング サービスの方式のデフォルト リストとして使用します。 • **group** *groupname*：アカウンティング サービスに使用するサーバ グループ。有効値は次のとおりです。 – *string*：サーバ グループに名前を付けるために使用する文字列。 – **radius**：すべての RADIUS ホストのリストを使用します。 – **tacacs+**：すべての TACACS+ ホストのリストを使用します。

	コマンドまたはアクション	目的
ステップ 11	**gw-accounting aaa** **例：** `Router(config)# gw-accounting aaa`	VoIP ゲートウェイ固有のアカウンティングをイネーブルにし、アカウンティング方式を定義します。
ステップ 12	**exit** **例：** `Router(config)# exit`	現在のモードを終了します。

事前認証の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa preauth**
4. **group**
5. **clid**
6. **ctype**
7. **dnis**
8. **dnis bypass**
9. **filter voice**
10. **timeout leg3**
11. **service-type call-check**
12. **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 preauth** **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。

	コマンドまたはアクション	目的
ステップ 4	**group** {**radius** | *groupname*} **例：** `Router(config-preauth)# group radius`	事前認証に使用する認証、認可、アカウンティング RADIUS サーバ グループを指定します。キーワードと引数は次のとおりです。 • **radius**：認証に RADIUS サーバを使用します。 • *groupname*：認証に使用するサーバ グループの名前。
ステップ 5	**clid** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **例：** `Router(config-preauth)# clid required`	（任意）発呼回線 ID（CLID）番号に基づいてコールの事前認証を行います。キーワードと引数は次のとおりです。 • **if-avail**：スイッチがデータを提供する場合、事前認証が成功するためには RADIUS が到達可能で、文字列を受け入れる必要があります。スイッチがデータを提供しない場合は、事前認証は成功します。 • **required**：事前認証が成功するためには、スイッチは関連するデータを提供する必要があり、RADIUS は到達可能で、文字列を受け入れる必要があります。この 3 つの条件が満たされない場合、事前認証は失敗します。 • **accept-stop**：1 つのコール要素に対して事前認証が成功したら、**ctype**、**dnis** など、後続の事前認証要素に対して事前認証が行われないようにします。 • **password** *string*：事前認証要素のパスワードを定義します。
ステップ 6	**ctype** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **例：** `Router(config-preauth)# ctype required`	（任意）コール タイプに基づいてコールの事前認証を行います。キーワードと引数は上記のとおりです。
ステップ 7	**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*] **例：** `Router(config-preauth)# dnis required`	（任意）Dialed Number Identification Service（DNIS）番号に基づいてコールの事前認証を行います。キーワードと引数は上記のとおりです。
ステップ 8	**dnis bypass** {*dnis-groupname*} **例：** `Router(config-preauth)# dnis bypass abc123`	（任意）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。引数は次のとおりです。 • *dnis-groupname*：定義された DNIS グループの名前。
ステップ 9	**filter voice** **例：** `Router(config-preauth)# filter voice`	（任意）音声コールが、認証、認可、およびアカウントの事前認証をバイパスすることを指定します。
ステップ 10	**timeout leg3** *time* **例：** `Router(config-preauth)# timeout leg3 100`	（任意）レッグ 3 AAA 事前認証要求のタイムアウト値を設定します。引数は次のとおりです。 • *time*：レッグ 3 事前認証のタイムアウト値（ミリ秒単位）。範囲：100 ～ 1000。デフォルト：100。

	コマンドまたはアクション	目的
ステップ 11	**service-type call-check** **例：** `Router(config-preauth)# service-type call-check`	（任意）AAA サーバへの事前認証要求を識別します。
ステップ 12	**exit** **例：** `Router(config-preauth)# exit`	現在のモードを終了します。

RADIUS 通信の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server host**
4. **radius-server retransmit**
5. **radius-server attribute 6 support-multiple**
6. **radius-server attribute 44 include-in-access-req**
7. **radius-server attribute nas-port format c**
8. **radius-server key**
9. **radius-server vsa send accounting**
10. **radius-server vsa send authentication**
11. **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：** `radius-server host jimname`	RADIUS サーバ ホストを指定します。キーワードと引数は次のとおりです。 • *hostname*：RADIUS サーバ ホストの DNS 名。 • *ip-address*：RADIUS サーバ ホストの IP アドレス。 • **auth-port** *port-number*：認証要求用の UDP 宛先ポート。0 に設定した場合、ホストは認証に使用されません。デフォルトは 1645 です。 • **acct-port** *port-number*：アカウンティング要求用の UDP 宛先ポート。0 に設定した場合、ホストはアカウンティングに使用されません。デフォルトは 1646 です。 • **timeout**：ルータが再送信する前に RADIUS サーバからの応答を待機する時間間隔（秒単位）。この設定は、**radius-server timeout** コマンドのグローバル値を上書きします。範囲は 1 ～ 1000 です。タイムアウト値を指定しなかった場合は、グローバル値が使用されます。 • **retransmit** *retries*：サーバが応答しない、または応答が遅い場合に、そのサーバに RADIUS 要求を再送信する回数。この設定は、**radius-server retransmit** コマンドのグローバル設定を上書きします。範囲は 1 ～ 100 です。再送信の値を指定しなかった場合は、グローバル値が使用されます。 • **key** *string* ：この RADIUS サーバで実行している RADIUS デーモンとルータの間で使用する認証と暗号キー。このキーは、**radius-server key** コマンドのグローバル設定を上書きします。キー文字列を指定しなかった場合は、グローバル値が使用されます。 キーは、テキスト文字列で、RADIUS サーバで使用されている暗号キーに一致する必要があります。キーは、必ず **radius-server host** コマンド構文の最後の項目として設定します。これは、先行するスペースは無視され、キーに含まれるスペースおよびキーの最後のスペースは使用されるためです。キーにスペースを使用する場合は、キーを引用符で囲まないでください。ただし、引用符がキーの一部である場合を除きます。 • **alias**：任意の RADIUS サーバについて 1 行につき最大 8 個のエイリアスを指定できます。
ステップ 4	**radius-server retransmit** *retries* **例：** `Router(config)# radius-server retransmit 1`	（任意）Cisco IOS ソフトウェアが RADIUS サーバ ホストのリストを検索する回数を指定します。引数は次のとおりです。 • *retries*：再送信を実行する最大回数。デフォルト：3。

	コマンドまたはアクション	目的
ステップ 5	**radius-server attribute 6 support-multiple** **例：** `Router(config)# radius-server attribute 6 support-multiple`	（任意）RADIUS プロファイルで、RADIUS アトリビュート 6（Service-Type）の値のオプションを設定します。キーワードは次のとおりです。 • **support-multiple**：各 RADIUS プロファイルで、複数のサービス タイプ値をサポートします。
ステップ 6	**radius-server attribute 44 include-in-access-req** **例：** `Router(config)# radius-server attribute 44 include-in-access-req`	ユーザ認証（事前認証の要求も含む）の前にアクセス要求パケットで RADIUS アトリビュート 44（Accounting Session ID）を送信します。 **（注）** RADIUS アトリビュートの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。
ステップ 7	**radius-server attribute nas-port format c** **例：** *Router(config)#* ***radius-server attribute nas-port format c***	（Cisco RPMS を使用している場合は必須）RADIUS アカウンティング機能に使用する NAS-Port フォーマットを選択します。
ステップ 8	**radius-server key** {**0** *string* | **7** *string* | *string*} **例：** `Router(config)# radius-server key ncmmekweisnaowkakskiiw`	（任意）ルータと RADIUS デーモン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設置します。キーワードと引数は次のとおりです。 • **0** *string*：暗号化されていない（クリアテキスト）共有キーを *string* に指定します。 • **7** *string*：非表示の共有キーを *string* に指定します。 • *string*：暗号化されていない（クリアテキスト）共有キー。
ステップ 9	**radius-server vsa send accounting** **例：** `Router(config)# radius-server vsa send accounting`	（任意）ベンダー固有アトリビュートを認識および使用するようにネットワーク アクセス サーバを設定します。
ステップ 10	**radius-server vsa send authentication** **例：** `Router(config)# radius-server vsa send authentication`	（任意）ベンダー固有アトリビュートを認識および使用するようにネットワーク アクセス サーバを設定します。
ステップ 11	**exit** **例：** `Router(config)# exit`	現在のモードを終了します。

SIP - ゲートウェイの拡張課金サポートの設定

SIP - ゲートウェイの拡張課金サポート機能を設定するには、次の手順を実行します。

手順の概要

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

3. **sip-ua**
4. **aaa username**
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	**sip-ua** **例：** `Router(config)# sip-ua`	SIP ユーザ エージェント 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	**aaa username** {**calling-name** | **proxy-auth**} **例：** `Router(config-sip-ua)# aaa username calling-name`	AAA 課金レコードのユーザ名アトリビュートに入力する情報を指定します。キーワードは次のとおりです。 • **calling-number**：SIP INVITE の FROM: ヘッダーを使用します（デフォルト）。このキーワードは、ほとんどの実装で使用されています。このキーワードはデフォルトです。 • **proxy-auth**：Proxy-Authorization ヘッダーを解析します。Microsoft Passport ユーザ ID（PUID）とパスワードをデコードし、PUID をユーザ名アトリビュートに、「.」をパスワード アトリビュートに入力します。 ユーザはすでに認証されているので、ユーザ名アトリビュートは課金に使用され、「.」はパスワードに使用されます。
ステップ 5	**exit** **例：** `Router(config-sip-ua)# exit`	現在のモードを終了します。

SIP：ゲートウェイ HTTP 認証ダイジェストの設定

ここでは、次の各手順について説明します。

- 「SIP：ダイヤル ピア使用のゲートウェイ HTTP 認証ダイジェストの設定」（P.32）（必須）
- 「SIP：SIP UA 使用のゲートウェイ HTTP 認証ダイジェストの設定」（P.33）（必須）

SIP：ダイヤル ピア使用のゲートウェイ HTTP 認証ダイジェストの設定

SIP：ダイヤル ピア使用のゲートウェイ HTTP 認証ダイジェスト機能を設定するには、次の手順を実行します。

（注）
- この設定では、POTS ダイヤル ピアで定義されているとおりに機能を設定します。
- この機能は、POTS ダイヤル ピアと SIP ユーザ エージェントで設定します。ダイヤル ピアでの設定が SIP ユーザ エージェントでの設定に優先します。

手順の概要

1. **enable**
2. **configure terminal**
3. dial-peer voice pots
4. authentication
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	**dial-peer voice** *tag* **pots** **例：** `Router(config)# dial-peer voice 100 pots`	特定の POTS ダイヤル ピアで、ダイヤル ピア 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	**authentication username** *username* **password** *password* [**realm** *realm*] **例：** `Router(config-sip-ua)# authentication username user1 password password1 realm example.com`	SIP ダイジェスト認証モードを開始します。キーワードと引数は次のとおりです。 • **username** *username*：認証を行っているユーザのユーザ名を表す文字列。 • **password** *password*：認証用のパスワードを表す文字列。 • **realm** *realm*：適切なクレデンシャルを表す文字列。
ステップ 5	**exit** **例：** `Router(config-sip-ua)# exit`	現在のモードを終了します。

SIP：SIP UA 使用のゲートウェイ HTTP 認証ダイジェストの設定

SIP：SIP UA 使用のゲートウェイ HTTP 認証ダイジェスト機能を設定するには、次の手順を実行します。

（注） この機能は、各ダイヤル ピアで個別に設定することも、SIP ユーザ エージェント コンフィギュレーション モードですべての POTS ダイヤル ピアに対してグローバルに設定することもできます。SIP ユーザ エージェント コンフィギュレーション モードと各ダイヤル ピアの両方で認証を設定した場合、各ダイヤル ピアの設定が優先されます。

制約事項

- SIP 登録がサポートされるのは、デジタル トランク タイプのポートを備えたプラットフォーム上だけです。

手順の概要

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. registrar
5. **authentication**
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	**sip-ua** **例：** `Router(config)# sip-ua`	SIP ユーザ エージェント 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 4	**registrar {dns:***address* **| ipv4:***destination-address***}** **expires** *seconds* [**tcp**] [**secondary**] **例：** `Router(config-sip-ua)# registrar ipv4:10.1.1.6 expires 60`	アナログ電話機の音声ポート（FXS）および IP Phone の仮想音声ポート（EFXS）の代わりに、外部 SIP プロキシ サーバまたは SIP レジストラ サーバに E.164 番号を登録します。キーワードと引数は次のとおりです。 • **dns:***address*：コールを受信するダイヤル ピアの名前を解決するドメイン ネーム サーバ。 • **ipv4:***destination address*：コールを受信するダイヤル ピアの IP アドレス。 • **expires** *seconds*：デフォルトの登録時間（秒単位）。 • **tcp**：トランスポート レイヤ プロトコルは、TCP です。デフォルトは UDP です。 • **secondary**：冗長性を確保するためにセカンダリ SIP プロキシまたはレジストラへの登録を指定します。 **（注）** レジストラがプロビジョニングされている場合、ゲートウェイは、`1..` で登録を送信します。
ステップ 5	**authentication username** *username* **password** *password* [**realm** *realm*] **例：** `Router(config-sip-ua)# authentication username user1 password password1 realm example.com`	SIP ダイジェスト認証モードを開始します。キーワードと引数は次のとおりです。 • **username** *username*：認証を行っているユーザのユーザ名を表す文字列。 • **password** *password*：認証用のパスワードを表す文字列。 • **realm** *realm*：適切なクレデンシャルを表す文字列。
ステップ 6	**exit** **例：** `Router(config-sip-ua)# exit`	現在のモードを終了します。

SIP の AAA 機能の確認

AAA 機能の設定を確認するには、必要に応じて次の手順を実行します（コマンドは、アルファベット順に示しています）。

手順の概要

1. **show call active voice**
2. **show radius statistics**
3. **show rpms-proc counters**
4. **show running-config**
5. **show sip-ua register status**

手順の詳細

ステップ 1 **show call active voice**

このコマンドを使用して、アクティブ音声コールの発信者情報を表示します。これにより、ユーザ名アトリビュートを確認できます。

次の出力例では、**proxy-auth** パラメータが選択されていることがわかります。

```
Router# show call active voice

Total call-legs: 2
   GENERIC:
  SetupTime=1551144 ms
    .
    . (snip)
    .
  ReceiveBytes=63006
  VOIP:
  ConnectionId[0x220A95B7 0x6B3611D5 0x801DBD53 0x8F65BA34]
    .
    . (snip)
    .
  CallerName=
  CallerIDBlocked=False
  Username=1234567890123456             <-- PUID from Proxy-Auth header
```

次の出力例では、**calling-number** パラメータが選択されていることがわかります。

```
Router# show call active voice

Total call-legs: 2

   GENERIC:
  SetupTime=1587000 ms
    .
    . (snip)
    .
  ReceiveBytes=22762
  VOIP:
  ConnectionId[0xF7C22E07 0x6B3611D5 0x8022BD53 0x8F65BA34]
    .
    . (snip)
    .
  CallerName=
  CallerIDBlocked=False
  Username=1234                         <-- calling-number
```

ステップ 2　show radius statistics

このコマンドを使用して、アカウンティング パケットと認証パケットに関する RADIUS 統計情報を表示します。

ステップ 3　show rpms-proc counters

このコマンドを使用して、レッグ 3 の事前認証要求の数、成功した数、および拒否された数を表示します。

（注） **clear rpms-proc counters** コマンドを使用すると、**show rpms-proc counters** コマンドによって表示される統計情報を記録しているカウンタがリセットされます。

ステップ 4　show running-config

現在の設定を表示するには、このコマンドを使用します。

ステップ 5　show sip-ua register status

SIP ユーザ エージェントの登録ステータスを確認するには、このコマンドを使用します。

```
Router# show sip-ua register status

Line  peer    expires(sec)  registered
4001  20001   596           no
4002  20002   596           no
5100  1       596           no
9998  2       596           no

where:
line=phone number to register
peer=registration destination number
expires (sec)=amount of time, in seconds, until registration expires
registered=registration status
```

トラブルシューティングのヒント

（注） 一般的なトラブルシューティングのヒント、および重要な **debug** コマンドについては、「一般的なトラブルシューティングのヒント」（P.18）を参照してください。

- 音声コールを行うことができることを確認します。
- ゲートウェイが認証確認に応答しない場合は、適切なドメインのユーザ クレデンシャルが設定されていることを確認します。
- ゲートウェイが POTS ダイヤル ピアで宛先パターンを登録する場合は、レジストラが設定されていることを確認します。
- **debug aaa authentication** コマンドを使用して、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）ログイン関連の高レベル診断を表示します。
- **debug cch323 preauth** コマンドを使用して、事前認証の H.323 Service Provider Interface（SPI; サービス プロバイダー インターフェイス）に対するデバッグ トレースをイネーブルにします。
- **debug ccsip** コマンド ファミリを使用して、SIP デバッグ機能をイネーブルにします。具体的には、次のコマンドを使用します。
  - **debug ccsip all** コマンドおよび **debug ccsip events** コマンドを使用して、SIP - ゲートウェイの拡張課金サポート機能に固有の出力を表示します。
  - **debug ccsip preauth** コマンドを使用して、事前認証の SIP サービス プロバイダー インターフェイス（SPI）に対するデバッグ トレースをイネーブルにします。
- **debug radius** コマンドを使用して、Remote Access Dial-In User Service（RADIUS）アトリビュートのデバッグ トレースをイネーブルにします。
- **debug rpms-proc preauth** コマンドを使用して、H.323 コール、SIP コール、または H.323 コールと SIP コールの両方の Resource Policy Management System（RPMS; リソース ポリシー管理システム）プロセスで、デバッグ トレースをイネーブルにします。

これらのコマンドの一部について、次に出力例を示します。

- 「debug ccsip コマンドの出力例」（P.37）
- 「debug ccsip events コマンドの出力例」（P.40）
- 「debug radius コマンドの出力例」（P.40）

debug ccsip コマンドの出力例

```
Router# debug ccsip messages

*Oct 11 21:40:26.175://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Sent:
INVITE sip:5550123@172.18.193.187:5060 SIP/2.0 ! Invite request message (command sequence
101)
Via:SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK6ED
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>
Date:Fri, 11 Oct 2002 21:40:26 GMT
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
Supported:100rel,timer
Min-SE: 1800
Cisco-Guid:3787171507-3700953558-2147913662-199702180
User-Agent:Cisco-SIPGateway/IOS-12.x
Allow:INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE, NOTIFY, INFO,
UPDATE, REGISTER
CSeq:101 INVITE
Max-Forwards:70
Remote-Party-ID:"36602" <sip:36602@172.18.193.120>;party=calling;screen=no;privacy=off
Timestamp:1034372426
Contact:<sip:36602@172.18.193.120:5060>
Expires:180
Allow-Events:telephone-event
Content-Type:application/sdp
Content-Length:244

v=0
o=CiscoSystemsSIP-GW-UserAgent 6603 1568 IN IP4 172.18.193.120
s=SIP Call
c=IN IP4 172.18.193.120
t=0 0
m=audio 17978 RTP/AVP 18 19
c=IN IP4 172.18.193.120
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:19 CN/8000
a=ptime:20

*Oct 11 21:40:26.179://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 100 Trying! 100 Trying response message (command sequence 101)
Via:SIP/2.0/UDP 172.18.193.120:5060;received=172.18.193.120;branch=z9hG4bK6ED
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>
CSeq:101 INVITE
Content-Length:0

*Oct 11 21:40:26.179://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 407 Proxy Authentication Required ! 407 proxy authentication required response
message (command sequence 101)
Via:SIP/2.0/UDP 172.18.193.120:5060;received=172.18.193.120;branch=z9hG4bK6ED
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>;tag=214b-70c4
CSeq:101 INVITE
Proxy-Authenticate:DIGEST realm="example.com", nonce="405729fe", qop="auth", algorithm=MD5
Content-Length:0

*Oct 11 21:40:26.183://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
```

```
Sent:
ACK sip:5550123@172.18.193.187:5060 SIP/2.0 ! ACK request message (command sequence 101)
Via:SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK6ED
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>;tag=214b-70c4
Date:Fri, 11 Oct 2002 21:40:26 GMT
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
Max-Forwards:70
CSeq:101 ACK
Content-Length:0

*Oct 11 21:40:26.183://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Sent:
INVITE sip:5550123@172.18.193.187:5060 SIP/2.0 ! Invite message request (command sequence
102)
Via:SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK8BA
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>
Date:Fri, 11 Oct 2002 21:40:26 GMT
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
Supported:100rel,timer
Min-SE: 1800
Cisco-Guid:3787171507-3700953558-2147913662-199702180
User-Agent:Cisco-SIPGateway/IOS-12.x
Allow:INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE, NOTIFY, INFO,
UPDATE, REGISTER
CSeq:102 INVITE
Max-Forwards:70
Remote-Party-ID:"36602" <sip:36602@172.18.193.120>;party=calling;screen=no;privacy=off
Timestamp:1034372426
Contact:<sip:36602@172.18.193.120:5060>
Expires:180
Allow-Events:telephone-event
Proxy-Authorization:Digest
username="36602",realm="example.com",uri="sip:172.18.193.187",response="404feee07cc7d3081d
04b977260efef5",nonce="405729fe",cnonce="AD7E41C1",qop=auth,algorithm=MD5,nc=00000001
Content-Type:application/sdp
Content-Length:244

v=0
o=CiscoSystemsSIP-GW-UserAgent 6603 1568 IN IP4 172.18.193.120
s=SIP Call
c=IN IP4 172.18.193.120
t=0 0
m=audio 17978 RTP/AVP 18 19
c=IN IP4 172.18.193.120
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:19 CN/8000
a=ptime:20

*Oct 11 21:40:26.187://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 100 Trying ! 100 Trying response message (command sequence 102)
Via:SIP/2.0/UDP 172.18.193.120:5060;received=172.18.193.120;branch=z9hG4bK8BA
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>
CSeq:102 INVITE
Content-Length:0

*Oct 11 21:40:26.439://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 180 Ringing ! 180 Ringing response message (command sequence 102)
```

```
Via:SIP/2.0/UDP 172.18.193.120:5060;received=172.18.193.120;branch=z9hG4bK8BA
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>;tag=003094c2e56a035d4326b6a1-292418c6
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
CSeq:102 INVITE
Server:CSCO/4
Contact:<sip:5550123@172.18.197.182:5060>
Record-Route:<sip:5550123@172.18.193.187:5060;maddr=172.18.193.187>
Content-Length:0

*Oct 11 21:40:28.795://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 200 OK ! 200 OK response message (command sequence 102)
Via:SIP/2.0/UDP 172.18.193.120:5060;received=172.18.193.120;branch=z9hG4bK8BA
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>;tag=003094c2e56a035d4326b6a1-292418c6
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
CSeq:102 INVITE
Server:CSCO/4
Contact:<sip:5550123@172.18.197.182:5060>
Record-Route:<sip:5550123@172.18.193.187:5060;maddr=172.18.193.187>
Content-Type:application/sdp
Content-Length:146
v=0
o=Cisco-SIPUA 21297 9644 IN IP4 172.18.197.182
s=SIP Call
c=IN IP4 172.18.197.182
t=0 0
m=audio 28290 RTP/AVP 18
a=rtpmap:18 G729/8000

*Oct 11 21:40:28.799://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Sent:
ACK sip:5550123@172.18.193.187:5060;maddr=172.18.193.187 SIP/2.0 ! ACK request message
(command sequence 102)
Via:SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK20A5
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>;tag=003094c2e56a035d4326b6a1-292418c6
Date:Fri, 11 Oct 2002 21:40:26 GMT
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
Route:<sip:5550123@172.18.197.182:5060>
Max-Forwards:70
CSeq:102 ACK
Proxy-Authorization:Digest
username="36602",realm="example.com",uri="sip:172.18.193.187",response="cc865e13d766426fb6
5f362c4f569334",nonce="405729fe",cnonce="9495DEBD",qop=auth,algorithm=MD5,nc=00000002
Content-Length:0

*Oct 11 21:40:32.891://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Sent:
BYE sip:5550123@172.18.193.187:5060;maddr=172.18.193.187 SIP/2.0 ! BYE request message
(command sequence 103)
Via:SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK6AF
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>;tag=003094c2e56a035d4326b6a1-292418c6
Date:Fri, 11 Oct 2002 21:40:26 GMT
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
User-Agent:Cisco-SIPGateway/IOS-12.x
Max-Forwards:70
Route:<sip:5550123@172.18.197.182:5060>
Timestamp:1034372432
CSeq:103 BYE
Reason:Q.850;cause=16
```

```
Proxy-Authorization:Digest
username="36602",realm="example.com",uri="sip:172.18.193.187",response="9b4d617d59782aeaf8
3cd49d932d12dd",nonce="405729fe",cnonce="22EB1F32",qop=auth,algorithm=MD5,nc=00000003
Content-Length:0

*Oct 11 21:40:32.895://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 100 Trying ! 100 Trying response message (command sequence 103)
Via:SIP/2.0/UDP 172.18.193.120:5060;received=172.18.193.120;branch=z9hG4bK6AF
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>;tag=003094c2e56a035d4326b6a1-292418c6
CSeq:103 BYE
Content-Length:0

*Oct 11 21:40:32.963://-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 200 OK ! 200 OK response message (command sequence 103)
Via:SIP/2.0/UDP 172.18.193.120:5060;received=172.18.193.120;branch=z9hG4bK6AF
From:"36602" <sip:36602@172.18.193.120>;tag=3E948-4C5
To:<sip:5550123@172.18.193.187>;tag=003094c2e56a035d4326b6a1-292418c6
Call-ID:E35DBEB1-DC9811D6-80098FBE-BE736A4@172.18.193.120
CSeq:103 BYE
Server:CSCO/4
Content-Length:0
```

debug ccsip events コマンドの出力例

この例は、Proxy-Authorization ヘッダーがどのようにデコード済みのユーザ名およびパスワードに分解されているのかを示します。

```
Router# debug ccsip events

CCSIP SPI: SIP Call Events tracing is enabled

21:03:21: sippmh_parse_proxy_auth: Challenge is 'Basic'.
21:03:21: sippmh_parse_proxy_auth: Base64 user-pass string is 'MTIzNDU2Nzg5MDEyMzQ1Njou'.
21:03:21: sip_process_proxy_auth: Decoded user-pass string is '1234567890123456:.'.
21:03:21: sip_process_proxy_auth: Username is '1234567890123456'.
21:03:21: sip_process_proxy_auth: Pass is '.'.
21:03:21: sipSPIAddBillingInfoToCcb: sipCallId for billing records =
10872472-173611CC-81E9C73D-F836C2B6@172.18.192.19421:03:21: ****Adding to UAS Request
table
```

debug radius コマンドの出力例

```
Router# debug radius

Radius protocol debugging is on
Radius protocol brief debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius packet retransmission debugging is off
Radius server fail-over debugging is off

Jan 23 14:30:25.421:RADIUS/ENCODE(00071EBF):acct_session_id:742769
Jan 23 14:30:25.421:RADIUS(00071EBF):sending
Jan 23 14:30:25.421:RADIUS:Send to unknown id 25 192.168.41.57:1812, Access-Request, len
179
Jan 23 14:30:25.421:RADIUS: authenticator 88 94 AC 32 89 84 73 6D - 71 00 50 6C D0 F8 FD
11
Jan 23 14:30:25.421:RADIUS: User-Name           [1]   9   "2210001"
Jan 23 14:30:25.421:RADIUS: User-Password       [2]   18  *
Jan 23 14:30:25.421:RADIUS: Vendor, Cisco       [26]  32
```

```
Jan 23 14:30:25.421:RADIUS: Cisco AVpair        [1]   26  "resource-service=reserve"
Jan 23 14:30:25.421:RADIUS: Service-Type        [6]   6   Call Check    [10]
Jan 23 14:30:25.421:RADIUS: Vendor, Cisco       [26]  19
Jan 23 14:30:25.421:RADIUS:  cisco-nas-port     [2]   13  "Serial6/0:0"
Jan 23 14:30:25.425:RADIUS: NAS-Port            [5]   6   6144
Jan 23 14:30:25.425:RADIUS: Vendor, Cisco       [26]  29
Jan 23 14:30:25.425:RADIUS:  Cisco AVpair       [1]   23  "interface=Serial6/0:0"
Jan 23 14:30:25.425:RADIUS: Called-Station-Id   [30]  9   "2210001"
Jan 23 14:30:25.425:RADIUS: Calling-Station-Id  [31]  9   "1110001"
Jan 23 14:30:25.425:RADIUS: NAS-Port-Type       [61]  6   Async [0]
Jan 23 14:30:25.425:RADIUS: NAS-IP-Address      [4]   6   192.168.81.101
Jan 23 14:30:25.425:RADIUS: Acct-Session-Id     [44]  10  "000B5571"
Jan 23 14:30:25.429:RADIUS:Received from id 25 192.168.41.57:1812, Access-Accept, len 20
Jan 23 14:30:25.429:RADIUS: authenticator 2C 16 63 18 36 56 18 B2 - 76 EB A5 EF 11 45 BE
F4
Jan 23 14:30:25.429:RADIUS:Received from id 71EBF
Jan 23 14:30:25.429:RADIUS/DECODE:parse response short packet; IGNORE
Jan 23 14:30:25.433:RADIUS/ENCODE(00071EBF):Unsupported AAA attribute start_time
Jan 23 14:30:25.433:RADIUS/ENCODE(00071EBF):Unsupported AAA attribute timezone
Jan 23 14:30:25.433:RADIUS/ENCODE:format unknown; PASS
Jan 23 14:30:25.433:RADIUS(00071EBF):sending
Jan 23 14:30:25.433:RADIUS:Send to unknown id 26 192.168.41.57:1813, Accounting-Request,
len 443
Jan 23 14:30:25.433:RADIUS: authenticator DA 1B 03 83 20 90 11 39 - F3 4F 70 F0 F5 8C CC
75
Jan 23 14:30:25.433:RADIUS: Acct-Session-Id     [44]  10  "000B5571"
Jan 23 14:30:25.433:RADIUS: Vendor, Cisco       [26]  56
Jan 23 14:30:25.433:RADIUS:  h323-setup-time    [25]  50 "h323-setup-time=14:30:25.429 GMT
Wed Jan 23 2002"
Jan 23 14:30:25.433:RADIUS: Vendor, Cisco       [26]  26
Jan 23 14:30:25.433:RADIUS:  h323-gw-id         [33]  20  "h323-gw-id=OrigGW."
Jan 23 14:30:25.433:RADIUS: Vendor, Cisco       [26]  56
Jan 23 14:30:25.433:RADIUS:  Conf-Id            [24]  50  "h323-conf-id=931C146B 0F4411D6
AB5591F0 CBF3D765"
Jan 23 14:30:25.433:RADIUS: Vendor, Cisco       [26]  31
Jan 23 14:30:25.437:RADIUS:  h323-call-origin   [26]  25  "h323-call-origin=answer"
Jan 23 14:30:25.437:RADIUS: Vendor, Cisco       [26]  32
Jan 23 14:30:25.437:RADIUS:  h323-call-type     [27]  26  "h323-call-type=Telephony"
Jan 23 14:30:25.437:RADIUS: Vendor, Cisco       [26]  65
Jan 23 14:30:25.437:RADIUS:  Cisco AVpair       [1]   59 "h323-incoming-conf-id=931C146B
0F4411D6 AB5591F0 CBF3D765"
Jan 23 14:30:25.437:RADIUS: Vendor, Cisco       [26]  30
Jan 23 14:30:25.437:RADIUS:  Cisco AVpair       [1]   24  "subscriber=RegularLine"
Jan 23 14:30:25.437:RADIUS: User-Name           [1]   9   "1110001"
Jan 23 14:30:25.437:RADIUS: Acct-Status-Type    [40]  6   Start             [1]
Jan 23 14:30:25.437:RADIUS: Vendor, Cisco       [26]  19
Jan 23 14:30:25.437:RADIUS:  cisco-nas-port     [2]   13  "Serial6/0:0"
Jan 23 14:30:25.437:RADIUS: NAS-Port            [5]   6   0
Jan 23 14:30:25.437:RADIUS: Vendor, Cisco       [26]  29
Jan 23 14:30:25.437:RADIUS:  Cisco AVpair       [1]   23  "interface=Serial6/0:0"
Jan 23 14:30:25.437:RADIUS: Called-Station-Id   [30]  9   "2210001"
Jan 23 14:30:25.437:RADIUS: Calling-Station-Id  [31]  9   "1110001"
Jan 23 14:30:25.437:RADIUS: NAS-Port-Type       [61]  6   Async [0]
Jan 23 14:30:25.437:RADIUS: Service-Type        [6]   6   Login [1]
Jan 23 14:30:25.437:RADIUS: NAS-IP-Address      [4]   6   192.168.81.101
Jan 23 14:30:25.437:RADIUS: Event-Timestamp     [55]  6   1011796225
Jan 23 14:30:25.437:RADIUS: Delay-Time          [41]  6   0
Jan 23 14:30:25.441:RADIUS/ENCODE(00071EC0):Unsupported AAA attribute start_time
Jan 23 14:30:25.441:RADIUS/ENCODE(00071EC0):Unsupported AAA attribute timezone
Jan 23 14:30:25.441:RADIUS(00071EC0):sending
Jan 23 14:30:25.441:RADIUS:Send to unknown id 27 192.168.41.57:1813, Accounting-Request,
len 411
Jan 23 14:30:25.441:RADIUS: authenticator 15 83 23 D8 0B B2 3A C2 - 1D 8C EF B4 18 0F 1C
65
```

```
Jan 23 14:30:25.441:RADIUS: Acct-Session-Id     [44]  10  "000B5572"
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  56
Jan 23 14:30:25.441:RADIUS:  h323-setup-time    [25]  50 "h323-setup-time=14:30:25.441 GMT
Wed Jan 23 2002"
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  26
Jan 23 14:30:25.441:RADIUS:  h323-gw-id         [33]  20  "h323-gw-id=OrigGW."
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  56
Jan 23 14:30:25.441:RADIUS:  Conf-Id            [24]  50  "h323-conf-id=931C146B 0F4411D6
AB5591F0 CBF3D765"
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  34
Jan 23 14:30:25.441:RADIUS:  h323-call-origin   [26]  28  "h323-call-origin=originate"
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  27
Jan 23 14:30:25.441:RADIUS:  h323-call-type     [27]  21  "h323-call-type=VoIP"
Jan 23 14:30:25.441:RADIUS: Vendor, Cisco       [26]  65
```

SIP AAA 機能の設定例

ここでは、次の設定例について説明します。

- 「SIP - ゲートウェイの拡張課金サポートの例」（P.42）
- 「SIP：ゲートウェイ HTTP 認証ダイジェストの例」（P.45）

SIP - ゲートウェイの拡張課金サポートの例

次の設定例では、完全な機能を実行するために最低限必要な設定オプションを強調表示しています。このマニュアルで説明している **aaa username** コマンドを設定すると、ゲートウェイは、SIP Authorization ヘッダーで受信した情報を使用し、その情報を AAA サービスおよび Tcl IVR サービスで使用できるようにします。通常、この機能に含まれるすべての機能を使用する予定の場合は、AAA と Tcl IVR を事前に設定しておきます。

```
Router# show running-config

Building configuration...
Current configuration : 4017 bytes
!
version 12.3
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname 3640-1
!
logging rate-limit console 10 except errors
! Need the following aaa line
aaa new-model
!
! Need the following four aaa lines
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting connection h323 start-stop group radius
aaa session-id common
enable password lab
!
memory-size iomem 15
clock timezone GMT 0
voice-card 2
!
```

```
ip subnet-zero!
ip domain-name example.sip.com
ip name-server 172.18.192.154
ip name-server 10.10.1.5
!
no ip dhcp-client network-discovery
isdn switch-type primary-5ess
isdn voice-call-failure 0
!
voice service voip
sip
rel1xx disable
!
fax interface-type fax-mail
mta receive maximum-recipients 0
call-history-mib retain-timer 500
!
controller E1 1/0
!
controller E1 1/1
!
controller T1 2/0
framing esf
linecode b8zs
pri-group timeslots 1-24
!
controller T1 2/1
framing sf
linecode ami
!
! Need the following three lines
gw-accounting h323
gw-accounting h323 vsa
gw-accounting voip
!
interface Ethernet0/0
ip address 10.10.1.4 255.255.255.0
half-duplex
ip rsvp bandwidth 7500 7500
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Ethernet0/2
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
no ip address
shutdown
half-duplex
!
interface FastEthernet1/0
ip address 172.18.192.197 255.255.255.0
duplex auto
speed auto
ip rsvp bandwidth 75000 75000
!
interface Serial2/0:23
no ip address
no logging event link-status
```

```
isdn switch-type primary-5ess
isdn incoming-voice modem
isdn T306 200000
isdn T310 200000
no cdp enable
!
ip classless
ip route 10.0.0.0 255.0.0.0 172.18.192.1
ip route 172.18.0.0 255.255.0.0 172.18.192.1
no ip http server
!
ip radius source-interface FastEthernet1/0
logging source-interface FastEthernet1/0
!
! Need the following radius-server lines for accounting/authentication
radius-server host 172.18.192.154 auth-port 1645 acct-port 1646
radius-server retransmit 1
radius-server key lab
radius-server vsa send accounting
radius-server vsa send authentication
call rsvp-sync
!
! Need the following call application lines in order to enable
! tcl scripting feature.
call application voice voice_billing tftp://172.18.207.15/app_passport_silent.2.0.0.0.tcl
!
voice-port 2/0:23
!
voice-port 3/0/0
!
voice-port 3/0/1
!
voice-port 3/1/0
!
voice-port 3/1/1
!
mgcp profile default
dial-peer cor custom
!
dial-peer voice 3640110 pots
destination-pattern 3640110
port 3/0/0
!
dial-peer voice 3640120 pots
destination-pattern 3640120
port 3/0/1
!
dial-peer voice 3660110 voip
destination-pattern 3660110
session protocol sipv2
session target ipv4:172.18.192.194
codec g711ulaw
!
dial-peer voice 3660120 voip
destination-pattern 3660120
session protocol sipv2
session target ipv4:172.18.192.194
codec g711ulaw
!
dial-peer voice 222 pots
huntstop
application session
destination-pattern 222
no digit-strip
```

```
direct-inward-dial
port 2/0:23
!
! Need to add the application line below to enable the tcl script
dial-peer voice 999 voip
application voice_billing
destination-pattern ...
session protocol sipv2
session target ipv4:10.10.1.2:5061
codec g711ulaw
!
! Need to add the aaa line below in order to enable proxy-authorization
! header processing
sip-ua
aaa username proxy-auth
!
line con 0
exec-timeout 0 0
length 0
line aux 0
line vty 0 4
!
!end
```

SIP：ゲートウェイ HTTP 認証ダイジェストの例

ここでは、次の設定例について説明します。

- 「SIP：ゲートウェイ HTTP 認証ダイジェスト機能：ディセーブル」（P.45）
- 「SIP：ゲートウェイ HTTP 認証ダイジェスト機能：イネーブル」（P.48）

SIP：ゲートウェイ HTTP 認証ダイジェスト機能：ディセーブル

```
Router# show running-config

Building configuration...
Current configuration :4903 bytes
!
version 12.3
no parser cache
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Fyay$DfmV/uLXX.X94CoaRy569.
enable password lab
!
voice-card 3
!
aaa new-model
!
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting connection h323 start-stop group radius
aaa session-id common
```

```
ip subnet-zero
ip tcp path-mtu-discovery
!
ip cef
ip domain name example.sip.com
ip name-server 172.18.192.48
!
ip dhcp pool 1
host 172.18.193.173 255.255.255.0
client-identifier 0030.94c2.5d00
  option 150 ip 172.18.193.120
  default-router 172.18.193.120
!
voice call carrier capacity active
!
voice service pots
!
voice service voip
sip
  rel1xx disable
!
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
 codec preference 5 g726r16
 codec preference 6 g726r24
 codec preference 7 g726r32
 codec preference 8 g723ar53
 codec preference 9 g723ar63
!
voice class codec 2
 codec preference 1 g711ulaw
 codec preference 2 g729r8
 codec preference 5 g726r16
 codec preference 6 g726r24
!
fax interface-type fax-mail
!
translation-rule 100
!
interface FastEthernet0/0
 ip address 172.18.193.120 255.255.255.0
 ip mtu 900
 duplex auto
 speed auto
 no cdp enable
 ip rsvp bandwidth 75000 75000
!
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip route 10.0.0.0 255.0.0.0 172.18.193.1
ip route 172.18.0.0 255.255.0.0 172.18.193.1
!
ip radius source-interface FastEthernet0/0
logging source-interface FastEthernet0/0
```

```
dialer-list 1 protocol ip permit
snmp-server engineID local 000000090200003094 26F6D0
snmp-server community public RO
snmp-server community private RW
snmp-server packetsize 4096
snmp-server enable traps tty
!
tftp-server flash:XMLDefault.cnf.xml
!
radius-server host 172.18.192.108 auth-port 1645 acct-port 1646
radius-server retransmit 1
radius-server key lab
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
voice-port 2/0/0
 station-id name 36602
 station-id number 36602
!
voice-port 2/0/1
!
mgcp
mgcp sdp simple
!
dial-peer cor custom
!
dial-peer voice 1 pots
 application session
 destination-pattern 36602
 port 2/0/0
!
dial-peer voice 5 voip
 application session
 destination-pattern 5550123
 session protocol sipv2
 session target ipv4:172.18.193.187
!
dial-peer voice 81 voip
 application session
 destination-pattern 3100801
 session protocol sipv2
 session target ipv4:172.18.193.100
 req-qos controlled-load
 acc-qos controlled-load
!
dial-peer voice 41 voip
 application session
 destination-pattern 333
 session protocol sipv2
 session target ipv4:10.102.17.80
 dtmf-relay rtp-nte
!
dial-peer voice 7 voip
 application session
```

```
 destination-pattern 999
 session protocol sipv2
 session target ipv4:172.18.193.98
 incoming called-number 888
!
dial-peer voice 38 voip
 application session
 destination-pattern 3100802
 voice-class codec 1
 session protocol sipv2
 session target ipv4:172.18.193.99
!
dial-peer voice 88 voip
 preference 1
 destination-pattern 888
 session protocol sipv2
 session target ipv4:172.18.193.187
!
dial-peer voice 123 voip
 destination-pattern 222
 session protocol sipv2
 session target ipv4:10.102.17.80
!
dial-peer voice 6 voip
 destination-pattern 36601
 session protocol sipv2
 session target ipv4:172.18.193.98
 session transport udp
 incoming called-number 36602
!
gateway
 timer receive-rtp 1200
!
sip-ua
 retry invite 1
 retry bye 2
 timers expires 60000
!
rtr responder
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 password lab
 transport preferred all
 transport input all
 transport output all
!
end
```

SIP：ゲートウェイ HTTP 認証ダイジェスト機能：イネーブル

```
Router# show running-config

Building configuration...
Current configuration :5087 bytes
!
version 12.3
no parser cache
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Fyay$DfmV/uLXX.X94CoaRy569.
enable password lab
!
voice-card 3
!
aaa new-model
!
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting connection h323 start-stop group radius
aaa session-id common
ip subnet-zero
ip tcp path-mtu-discovery
!
ip cef
ip domain name example.sip.com
ip name-server 172.18.192.48
!
ip dhcp pool 1
  host 172.18.193.173 255.255.255.0
  client-identifier 0030.94c2.5d00
  option 150 ip 172.18.193.120
  default-router 172.18.193.120
!
voice call carrier capacity active
!
voice service pots
!
voice service voip
 sip
  rel1xx disable
!
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
 codec preference 5 g726r16
 codec preference 6 g726r24
 codec preference 7 g726r32
 codec preference 8 g723ar53
 codec preference 9 g723ar63
!
voice class codec 2
 codec preference 1 g711ulaw
 codec preference 2 g729r8
 codec preference 5 g726r16
 codec preference 6 g726r24
!
fax interface-type fax-mail
!
translation-rule 100
!
interface FastEthernet0/0
ip address 172.18.193.120 255.255.255.0
 ip mtu 900
```

```
 duplex auto
 speed auto
 no cdp enable
 ip rsvp bandwidth 75000 75000
!
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip route 10.0.0.0 255.0.0.0 172.18.193.1
ip route 172.18.0.0 255.255.0.0 172.18.193.1
!
ip radius source-interface FastEthernet0/0
logging source-interface FastEthernet0/0
dialer-list 1 protocol ip permit
snmp-server engineID local 00000009020000309426F6D0
snmp-server community public RO
snmp-server community private RW
snmp-server packetsize 4096
snmp-server enable traps tty
!
tftp-server flash:XMLDefault.cnf.xml
!
radius-server host 172.18.192.108 auth-port 1645 acct-port 1646
radius-server retransmit 1
radius-server key lab
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
voice-port 2/0/0
 station-id name 36602
 station-id number 36602
!
voice-port 2/0/1
!
mgcp
mgcp sdp simple
!
dial-peer cor custom
!
dial-peer voice 1 pots
 application session
 destination-pattern 36602
 port 2/0/0
 authentication username user1 password password1 realm example1.com ! authentication
xample 1
 authentication username user2 password password2 realm example2.com ! authentication
```

```
xample 2
!
dial-peer voice 5 voip
 application session
 destination-pattern 5550123
 session protocol sipv2
 session target ipv4:172.18.193.187
!
dial-peer voice 81 voip
 application session
 destination-pattern 3100801
 session protocol sipv2
 session target ipv4:172.18.193.100
 req-qos controlled-load
 acc-qos controlled-load
!
dial-peer voice 41 voip
 application session
 destination-pattern 333
 session protocol sipv2
 session target ipv4:10.102.17.80
 dtmf-relay rtp-nte
!
dial-peer voice 7 voip
 application session
 destination-pattern 999
 session protocol sipv2
 session target ipv4:172.18.193.98
 incoming called-number 888
!
dial-peer voice 38 voip
 application session
 destination-pattern 3100802
 voice-class codec 1
 session protocol sipv2
 session target ipv4:172.18.193.99
!
dial-peer voice 88 voip
 preference 1
 destination-pattern 888
 session protocol sipv2
 session target ipv4:172.18.193.187
!
dial-peer voice 123 voip
 destination-pattern 222
 session protocol sipv2
 session target ipv4:10.102.17.80
!
dial-peer voice 6 voip
 destination-pattern 36601
 session protocol sipv2
 session target ipv4:172.18.193.98
 session transport udp
 incoming called-number 36602
!
gateway
 timer receive-rtp 1200
!
sip-ua
 authentication username user3 password password3 ! authentication example 3
 retry invite 1
 retry bye 2
 timers expires 60000
 registrar ipv4:172.18.193.187 expires 100 ! registrar example
```

```
!
rtr responder
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 password lab
 transport preferred all
 transport input all
 transport output all
!
end
```

その他の参考資料

一般的な SIP 参考資料

- 「SIP 機能のロードマップ」（P.1）：Cisco Feature Navigator にアクセスする手順について説明します。また、Cisco IOS リリース別に、そのリリースの SIP 機能を示して説明します。
- 「SIP の概要」（P.1）：基本的な SIP テクノロジーのほか、関連資料、規格、MIB、RFC、および技術サポートを受ける方法のリストが掲載されています。

この章で言及した参考資料（アルファベット順）

- 『*Cisco IOS IP Command Reference*』（http://www.cisco.com/）
- 『*Cisco IOS Security Command Reference*』（http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html）
- 『*Cisco IOS Security Configuration Guide*』（リリース 12.4T）（http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/12_4T/sec_securing_user_services_12.4t_book.html）
- 『*Cisco IOS SIP Configuration Guide*』（リリース 12.4T）（http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html）
- 『*Cisco IOS Tcl IVR and VoiceXML Application Guide*』（http://www.cisco.com/en/US/docs/ios/voice/ivr/configuration/guide/tcl_c.html）
- 『*Cisco Resource Policy Management System 2.0*』（http://www.cisco.com/en/US/products/sw/netmgtsw/ps2074/tsd_products_support_eol_series_home.html）
- 『*Cisco Tcl IVR API Programmer's Guide*』（http://www.cisco.com/en/US/docs/ios/voice/tcl/developer/guide/tclivrv2.html）
- 『*Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms*』（http://www.cisco.com/en/US/docs/ios/12_2t/12_2t11/feature/guide/ftsipgv1.html）
- 『*Inter-Domain Gatekeeper Security Enhancement*』（Cisco IOS リリース 12.2(4)T）（http://www.cisco.com/en/US/docs/ios/12_2/12_2x/12_2xa/feature/guide/ft_ctoke.html）
- 『*RADIUS Vendor-Specific Attributes Voice Implementation Guide*』（http://www.cisco.com/en/US/docs/ios/voice/vsa/developer/guide/vsaig3.html）