RADIUS パケット オブ ディスコネクト

RADIUS パケット オブ ディスコネクト機能は、接続された音声コールを終了させるために使用します。

RADIUS パケット オブ ディスコネクトの前提条件

『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』で説明されているように、AAA を設定します。

RADIUS パケット オブ ディスコネクトの制約事項

以下により、適切に一致する識別情報の通知が行われる必要があります。

- 課金サーバとゲートウェイの設定
- ゲートウェイのオリジナル アカウンティング開始要求
- サーバの POD 要求

RADIUS パケット オブ ディスコネクトに関する情報

パケット オブ ディスコネクト（PoD）は RADIUS access_request パケットであり、RADIUS access_accept パケットによりセッションが承認された後、認証するエージェント サーバがユーザを接続解除するときに使用されるようになっています。

POD が必要な場合

POD が必要な場合としては、少なくとも次の 2 つの状況が考えられます。

- 不正使用の検出。これは、コールを承認後でなければ実行できません。価格構造が複雑でコールを受け入れる前に最大セッション期間を推定できない。ある種のディスカウントが適用されるか、複数のユーザが同じサブスクリプションを同時に使用している場合が、これに当てはまります。
- 認可されていないサーバからユーザが切断されるのを防ぐには、POD パケットを発行する認可エージェントが パケット オブ ディスコネクト要求に 3 つのパラメータを含める必要があります。接続解除されるコールに対して、すべてのパラメータは、ゲートウェイの期待値と一致している必要があります。パラメータが一致しないと、ゲートウェイはパケットオブディスコネクトのパケットを破棄し、エージェントに NACK（否定応答）メッセージを送信します。

POD パラメータ

POD には次のパラメータがあります。

- このコールに対してゲートウェイから受信されたものと同じ内容の h323-conf-id ベンダー固有属性（VSA）
- 対象の区間に対してゲートウェイから受信されたものと同じ内容の h323-call-origin VSA。
- POD 要求の *authentication* フィールドで伝送される 16 バイトの MD5 ハッシュ値。
- Cisco IOS XE ソフトウェアは、RFC 3576 の『*Dynamic Authorization Extensions to RADIUS*』（POD を介してサポートされるディスコネクト メッセージ（DM）および認可変更（CoA）の両方を公式にサポートするために RADIUS 標準を拡張）に基づいて POD コード 50 を音声 POD 要求のコード値として割り当てます。

RFC 3576 では、以下の POD コードを指定します。

-
  - 40：切断要求
  - 41：切断 ACK
  - 42：切断 NAK
  - 43：CoA 要求
  - 44：CoA-ACK
  - 45：CoA-NAK

RADIUS パケット オブ ディスコネクトの設定方法

RADIUS POD の設定

次のタスクを使用して、RADIUS POD を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router (config)# **aaa pod server** [**port** *port-number*] [**auth-type** {**any**| **all**| **session-key**}] **server-key** [*encryption-type*] *string*
4. Router# **end**
5. Router# **show running-configuration**

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： `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	Router (config)# **aaa pod server** [**port** *port-number*] [**auth-type** {**any**| **all**| **session-key**}] **server-key** [*encryption-type*] *string* 例： `Router(config)# aaa pod server server-key xyz123`	次のような特定のセッション属性が提供されると、インバウンド ユーザ セッションを切断できます。 • **port** *port-number* ：（任意）POD 要求に使用されるネットワーク アクセス サーバーのユーザー データグラム プロトコル（UDP）ポート。デフォルト値は 1700 です。 • **auth-type**：（任意）セッションの切断に必要な認証の種類。 • **any**：POD パケット内で送信されたすべての属性と一致するセッションが切断されます。POD パケットには、4 つのキー属性（user-name、framed-IP-address、session-ID、session-key）の 1 つまたは複数が含まれることがあります。

	コマンドまたはアクション	目的
		• **all**：4つの主要属性のすべてに一致するセッションだけが切断されます。 **All** がデフォルトです。 • **session-key**：一致する session-key 属性を持つセッションが切断されます。他のすべての属性は無視されます。 • **server-key--** 共有秘密テキスト文字列を設定します。 • *encryption-type*：（任意）直後のテキストが暗号化されるかどうか、および暗号化される場合は使用される暗号化タイプを定義する 1 桁の数字。定義されている暗号化タイプは、0（直後のテキストは暗号化されない）および 7（テキストはシスコが定義した暗号化アルゴリズムを使用して暗号化される）です。 • *string*：ネットワーク アクセス サーバーとクライアント ワークステーションの間で共有される共有秘密テキスト文字列。この事前共有キーは、両方のシステムで同じである必要があります。
ステップ 4	Router# **end**	グローバル 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。

ステップ 5	Router# **show running-configuration**
	例：
	`Router# show running-configuration`
	例：
	`!`
	例：
	`aaa authentication login h323 group radius`
	例：
	`aaa authorization exec h323 group radius`
	例：
	`aaa accounting update newinfo`
	例：
		ゲートウェイが特権 EXEC モードで正しく設定されていることを確認します。

	コマンドまたはアクション	目的

	`aaa accounting connection h323 start-stop group radius`
	例：
	`aaa pod server server-key cisco`
	例：
	`aaa session-id common`
	例：
	`!`	

トラブルシューティングのヒント

AAA Dead-Server Detection を設定したら、**show running-config** コマンドを使用して、その設定を確認してください。この確認が特に重要になるのは、**no** 形式の **radius-server dead-criteria** コマンドを使用している場合です。**show running-config** コマンドの出力は、**radius-server dead-criteria** コマンドを使用して設定した「Dead Criteria Details」フィールドと同じ値を示している必要があります。

RADIUS POD の設定の確認

RADIUS POD 設定を確認するには、次の例に示すように **show running configuration** 特権 EXEC コマンドを使用します。

```
Router# show running-configuration
!
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting update newinfo
aaa accounting connection h323 start-stop group radius
aaa pod server server-key cisco
aaa session-id common
.
.
.
```

その他の参考資料

次の項で、RADIUS パケット オブ ディスコネクト機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA	『*Cisco IOS XE Security Configuration Guide, Securing User Services*, Release 2』の「Authentication, Authorization, and Accounting (AAA)」
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
CLI 設定	『*Cisco IOS XE Configuration Fundamentals Configuration Guide*, Release 2』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索し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。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『*Remote Authentication Dial-in User Service*』
RFC 3576	『*Dynamic Authorization Extensions to RADIUS*』

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/en/US/support/index.html

RADIUS パケット オブ ディスコネクトの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : RADIUS* パケット オブ ディスコネクトの機能情報

機能名	リリース	機能情報
RADIUS パケット オブ ディスコネクト	Cisco IOS XE Release 2.1	RADIUS パケット オブ ディスコネクト機能は、接続された音声コールを終了させるために使用します。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました。**aaa pod server, debug aaa pod**

用語集

AAA：認証、許可、およびアカウンティングセキュリティ サービスのフレームワークであり、ユーザーの身元確認（認証）、リモート アクセス コントロール（許可）、課金、監査、およびレポートに使用するセキュリティ サーバー情報の収集と送信（アカウンティング）の方式を定めています。

L2TP ：レイヤ 2 トンネル プロトコル。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP アクセス ポイント（POP）にあるネットワーク アクセス サーバ（NAS）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

PE：Provider Edge（プロバイダーエッジ）。サービス プロバイダー ネットワークのエッジ上のネットワーキング デバイス。

RADIUS ：リモート認証ダイヤルイン ユーザー サービス。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。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VPN：Virtual Private Network（仮想プライベートネットワーク）。リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP および L2F を使用し、LAC ではなく、LNS でレイヤ 2 およびより高次のネットワーク接続を終了させます。

VRF：Virtual Route Forwarding（仮想ルーティングおよびフォワーディング）。最初は、ルータにグローバルのデフォルト ルーティング/フォワーディング テーブルは 1 つしかありません。VRF は、複数の分離されたルーティング/フォワーディング テーブルとして表示でき、ユーザのルートには別のユーザのルートとの相互関係はありません。

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