



Radius パケットの切断

- [マニュアルの変更履歴, on page 1](#)
- [機能説明 \(1 ページ\)](#)
- [要件の概要 \(2 ページ\)](#)
- [認可変更メッセージ \(2 ページ\)](#)
- [メッセージ交換 \(2 ページ\)](#)
- [RADIUS 開始切断メッセージ \(3 ページ\)](#)
- [メッセージ交換 \(3 ページ\)](#)
- [RADIUS 認可変更 NAS-IP-Address 機能の設定 \(3 ページ\)](#)

マニュアルの変更履歴

改訂の詳細	リリース
初版	21.26

機能説明

RADIUS 認可変更は、デバイスの認証後に認可を動的に変更するメカニズムを提供します。ポリシーが変更されると、認可サーバーから RADIUS CoA パケットを送信して認証を再開し、新しいポリシーを適用できます。RADIUS CoA プロセスでは、有線スイッチまたはアクセスポイントが再認証プロセスを開始したり、デバイスが切断して再接続したりするのを待つことなく、必要に応じてすぐにユーザーアクセスを変更できます。

異なる RADIUS サーバーと異なる NAS IP アドレスを使用する複数の APN があるコンテキストにおいて、コンテキストごとに複数の RADIUS 認可変更 (CoA) NAS IP アドレスを定義できるようになりました。

要件の概要

次の表に、既存のアーキテクチャに関する要件の概要を示します。

モジュール	要件
CLI	単一のコンテキストで複数の Radius COA NAS-IP-Address を設定できる必要があります。
SCTRL	単一のコンテキストで複数の Radius CoA NAS-IP-Address を設定できる必要があります。これらの複数の Radius CoA NAS-IP-Address は、SCTRL によってすべての AAAMGR インスタンスにブロードキャストされる必要があります。
AAAMGR	コンテキスト内で複数の NAS-IP-Address ソケットを開くことができるように AAAMGR 設定を変更します。 AAAMGR は、同じコンテキスト内の異なる NAS-IP-Address で CoA または DM メッセージを受信できる必要があります。

認可変更メッセージ

RADIUS dynamic-request サーバーは、RADIUS サーバーからの一方的な認可変更 (CoA) メッセージを受信して処理します。RADIUS 開始 CoA 機能は、RADIUS 要求および応答メッセージで次のコードを使用します。

- CoA-Request (43)
- CoA-ACK (44)
- CoA-NAK (45)

メッセージ交換

RADIUS サーバーとルータの RADIUS dynamic-request サーバーは、UDP を使用してメッセージを交換します。RADIUS サーバーによって送信される COA 要求メッセージの形式は、切断操作で送信される切断要求パケットと同じです。

応答は、COA-ACK または COA-NAK メッセージのいずれかです。

- AAA が認可を正常に変更した場合、応答は COA-ACK メッセージを含む RADIUS 形式のパケットになり、データフィルタがセッションに適用されます。
- AAA が失敗したか、要求の形式が正しくないか、属性がない場合、応答は COA-NAK メッセージを含む RADIUS 形式のパケットになります。

RADIUS 開始切断メッセージ

ここでは、RADIUS dynamic-request サーバーの RADIUS 開始切断機能について説明します。リモートアクセスユーザーの切断を集中制御するには、ルータ上の RADIUS dynamic-request サーバーが RADIUS サーバーからの一方的なメッセージを受信して処理する必要があります。RADIUS 開始切断機能は、RADIUS 切断要求および応答メッセージの既存の形式を使用します。RADIUS 開始切断機能は、RADIUS 要求および応答メッセージで次のコードを使用します。

- Disconnect-Request (40)
- Disconnect-ACK (41)
- Disconnect-NAK (42)

メッセージ交換

RADIUS サーバーとルータの RADIUS dynamic-request サーバーは、User Datagram Protocol (UDP) を使用してメッセージを交換します。RADIUS サーバーによって送信される切断要求メッセージの形式は、認可変更操作で送信される COA 要求パケットと同じです。

切断応答は、Disconnect-ACK または Disconnect-NAK メッセージのいずれかです。

- AAA がユーザーの接続を正常に切断すると、Disconnect-ACK メッセージを含む RADIUS 形式のパケットが応答として返されます。
- AAA がユーザーの接続を切断できないか、要求の形式が正しくないか、リクエストに属性がない場合、応答は Disconnect-NAK メッセージを含む RADIUS 形式のパケットになります。

RADIUS 認可変更 NAS-IP-Address 機能の設定

次の CLI は、RADIUS サーバーから CoA メッセージを受信してサーバーに確認応答を返すように CP を設定します。

```
configure
  context context_name
```

```
radius change-authorize-nas-ip ip_address
  [ encrypted ] key secret
  { port port }
  { no-reverse-path-forward-check }
  { timestamp-window <0-4294967295>}
exit
exit
```

特定のコンテキスト内で **radius change-authorize-nas-ip** CLI コマンドの複数の行を許可します。特定のコンテキスト内で最大 32 の行を設定できます。

show コマンドと出力

ここでは、この機能をサポートするために使用可能な show CLI コマンドについて説明します。特定のコンテキスト内で show コマンドを実行します。

- **show radius counters**
- **show radius info instance**
- **show session subsystem facility aaamgr instance**

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。