



RADIUS の設定

- [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, 2 ページ](#)
- [RADIUS の設定方法, 32 ページ](#)
- [CoA 機能のモニタリング, 48 ページ](#)
- [RADIUS の機能情報, 49 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。

General:

- 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 コマンドを使用してのみイネーブルにできます。
- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。
- **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トिंग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。

General:

- 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

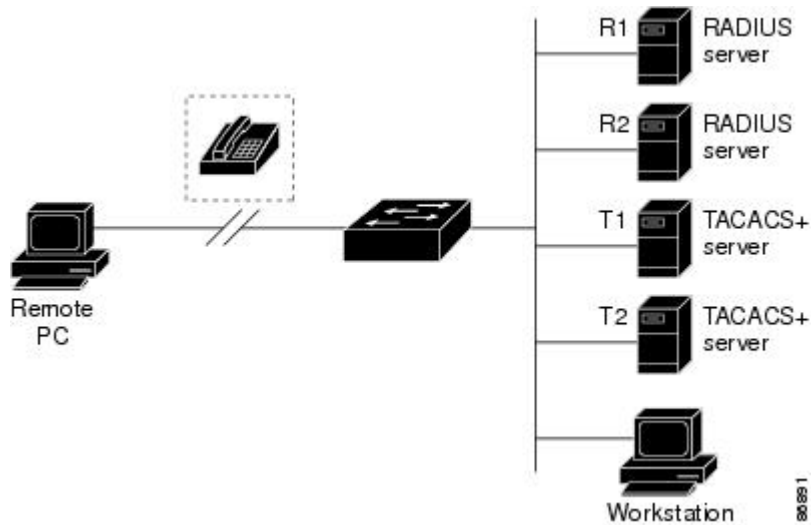
RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバシステムです。RADIUS クライアントは、サポート対象の Cisco ルータおよびスイッチ上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。

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 2 「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、第 11 章 「IEEE 802.1x ポートベース認証の設定」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ティング ソフトウェアのフリーウェア

バージョンを使用して、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 : ユーザが認証されたことを表します。
 - 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 許可の変更

RADIUS 許可の変更（CoA）は、認証、認可、およびアカウントिंग（AAA）セッションの属性を認証された後に変更するためのメカニズムを提供します。AAA でユーザ、またはユーザグループのポリシーが変更された場合、管理者は、AAA サーバから Cisco Secure Access Control Server（ACS）などの RADIUS CoA パケットを送信し、認証を再初期化して新しいポリシーを適用することができます。このセクションでは、使用可能なプリミティブおよびそれらの CoA での使用方法を含む、RADIUS インターフェイスの概要について説明します。

- Change-of-Authorization 要求
- CoA 要求応答コード
- CoA 要求コマンド
- セッション再認証
- セッション強制終了のスタック構成ガイドライン

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプルモデルで使用されます。Catalyst は、RFC 5176 で規定された（通常はプッシュモデルで使用される）RADIUS CoA 拡張機能をサポートし、外部の AAA またはポリシー サーバからのセッションを動的に再設定できるようにします。

は、次のセッション単位の CoA 要求をサポートしています。

- セッション再認証
- セッション終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了

この機能は、Cisco Secure Access Control Server (ACS) 5.1 に統合されています。

Catalyst で、RADIUS インターフェイスはデフォルトでイネーブルに設定されています。ただし、次の属性については、一部の基本的な設定が必要になります。

- セキュリティおよびパスワード：このガイドの「スイッチへの不正アクセスの防止」を参照してください。
- アカウントिंग：このガイドの「スイッチベース認証の設定」の章の「RADIUS アカウントिंगの起動」の項を参照してください。

Cisco IOS ソフトウェアは、RFC 5176 で定義されている RADIUS CoA の拡張をサポートします。この拡張は、一般に、外部 AAA またはポリシー サーバからのセッションのダイナミックな再構成を可能にするプッシュモデルで使用されます。セッションの特定、セッションの終了、ホスト

の再認証、ポートのシャットダウン、およびポートバウンスでは、セッションごとの CoA 要求がサポートされます。このモデルは、次のように、1つの要求 (CoA-Request) と2つの考えられる応答コードで構成されます。

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

要求は CoA クライアント (通常は AAA またはポリシー サーバ) から開始されて、リスナーとして動作するデバイスに転送されます。

次の表は、Identity-Based Networking Services でサポートされている RADIUS CoA コマンドとベンダー固有属性 (VSA) を示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 1: Identity-Based Networking Services でサポートされている RADIUS CoA コマンド

CoA コマンド	シスコの VSA
サービスのアクティブ化	Cisco:Avpair="subscriber:command=activate-service" Cisco:Avpair="subscriber:service-name=<service-name>" Cisco:Avpair="subscriber:precedence=<precedence-number>" Cisco:Avpair="subscriber:activation-mode=replace-all"
Deactivate service	Cisco:Avpair="subscriber:command=deactivate-service" Cisco:Avpair="subscriber:service-name=<service-name>"
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Session query	Cisco:Avpair="subscriber:command=session-query"
Session reauthenticate	Cisco:Avpair="subscriber:command=reauthenticate" Cisco:Avpair="subscriber:reauthenticate-type=last" または Cisco:Avpair="subscriber:reauthenticate-type=rerun"
Session terminate	これは、VSA を必要としない、標準の接続解除要求です。
Interface template	Cisco:AVpair="interface-template-name=<interfacetemplate>"

Change-of-Authorization 要求

Change of Authorization (CoA) 要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。このモデルは、1つの要求 (CoA-Request) と2つの可能な応答コードで構成されています。

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から発信されて、リスナーとして動作するスイッチに送信されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect (POD) とも呼ばれますが、セッション終了に対してスイッチでサポートされています。

次の表に、この機能でサポートされている IETF 属性を示します。

表 2: サポートされている IETF 属性

Attribute Number	属性名 (Attribute Name)
24	状態 (State)
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 3: Error-Cause の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット (無視)
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス

値	説明
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求 (プロキシ)
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチセッションの選択がサポートされていない

CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値 (TLV) 形式の属性から構成されます。属性フィールドは、シスコのベンダー固有属性 (VSA) を送信するために使用します。

セッションの識別

特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

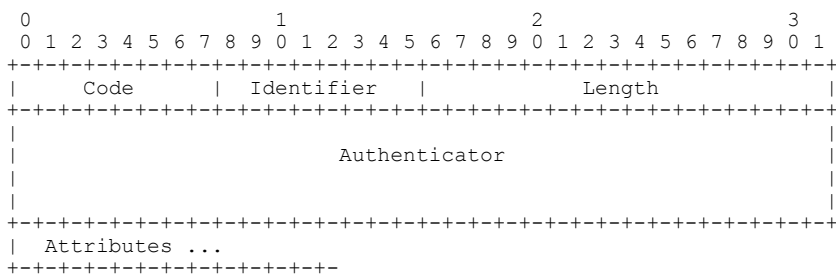
- Acct-Session-Id (IETF 属性 #44)
- Audit-Session-Id VSA (シスコの VSA)
- Calling-Station-Id (ホスト MAC アドレスを含む IETF 属性 #31)
- 次のいずれかの IPv6 属性。
 - Framed-IPv6-Prefix (IETF 属性 #97) および Framed-Interface-Id (IETF 属性 #96) 。ともに RFC 3162 に従った完全な IPv6 アドレスを作成する
 - Framed-IPv6-Address

- プレーン IP アドレス (IETF 属性 #8)

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、スイッチは「Invalid Attribute Value」エラーコード属性を含む Disconnect-NAK または CoA-NAK を返します。

複数のセッション ID 属性がメッセージに含まれる場合は、すべての属性がセッションと一致しなければなりません。そうでない場合は、スイッチが Disconnect-negative acknowledgement (NAK) または CoA-NAK と、「Invalid Attribute Value」エラーコードを返します。

RFC 5176 で定義されている CoA 要求コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値 (TLV) 形式の属性から構成されます。



属性フィールドは、シスコのベンダー固有属性 (VSA) を送信するために使用します。

特定の適用ポリシーを対象とする CoA 要求の場合、上記のセッション ID 属性のいずれかがメッセージに含まれていると、デバイスはエラーコードが「Invalid Attribute Value」の CoA-NAK を返します。

CoA ACK 応答コード

許可状態の変更に成功した場合は、肯定確認応答 (ACK) が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なり、個々の CoA コマンドで検討されます。

CoA NAK 応答コード

否定応答 (NAK) は許可状態の変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。CoA が成功したかを確認するには、**show** コマンドを使用します。

CoA 要求コマンド

表 4: でサポートされる CoA コマンド

コマンド 1	シスコの VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"

コマンド 1	シスコの VSA
Terminate session	これは、VSA を要求しない、標準の接続解除要求です。
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

¹ すべての CoA コマンドには、と CoA クライアント間のセッション識別情報が含まれている必要があります。

セッション再認証

不明な ID または ポスチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファイル（たとえば、ゲスト VLAN）に関連付けられると、AAA サーバは通常、セッション再認証要求を生成します。再認証要求は、クレデンシャルが不明である場合にホストが適切な認証グループに配置されることを許可します。

セッション認証を開始するために、AAA サーバは *Cisco:Avpair="subscriber:command=reauthenticate"* の形式で Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。

現在のセッションステートは、メッセージに対するスイッチの応答を決定します。セッションが現在、IEEE 802.1x によって認証されている場合、スイッチは EAPOL（LAN 経由の拡張認証プロトコル）RequestId メッセージをサーバに送信することで応答します。

現在、セッションが MAC 認証バイパス（MAB）で認証されている場合は、スイッチはサーバにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

スイッチがコマンドを受信したときにセッション認証が実行中である場合は、スイッチはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションがまだ認証されていない、あるいはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認証されている場合は、再認証メッセージがアクセスコントロール方式を再開し、最初に試行されるように設定された方式で開始します。セッションの現在の許可は、再認証によって異なる認証結果になるまで維持されます。

スイッチスタックでのセッションの再認証

スイッチスタックでセッション再認証メッセージを受信すると、次の動作が発生します。

- 確認応答（ACK）を戻す前に、再認証の必要性がチェックされます。
- 適切なセッションで再認証が開始されます。
- 認証が成功または失敗のいずれかで完了すると、再認証をトリガーする信号がスタックメンバから削除されます。

- 認証の完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、再認証が開始されます。
- ACK の送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再転送コマンドが新しいコマンドとして扱われます。

セッションの終了

セッションを終了させる 3 種類の CoA 要求があります。CoA 接続解除要求は、ホストポートをディセーブルにせずにセッションを終了します。このコマンドを使用すると、指定されたホストのオーセンティケータステートマシンが再初期化されますが、そのホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、

Cisco:Avpair="subscriber:command=disable-host-port" VSA の設定で CoA 要求を使用します。このコマンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であり、そのホストに対してネットワーク アクセスをただちにブロックする必要があります。ポートへのネットワークアクセスを復旧する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

プリンタなどのサブリカントを持たないデバイスが新しい IP アドレスを取得する必要がある場合（たとえば、VLAN 変更後）は、ポートバウンスでホストポート上のセッションを終了します（ポートを一時的にディセーブルした後、再びイネーブルにする）。

CoA 接続解除要求

このコマンドは標準の接続解除要求です。セッションが見つからない場合、スイッチは Disconnect-NAK メッセージと「Session Context Not Found」エラーコード属性を返します。セッションがある場合は、スイッチはセッションを終了します。セッションが完全に削除された後、スイッチは接続解除 ACK を返します。

スイッチがクライアントに接続解除 ACK を返す前にスタンバイ スイッチにフェールオーバーする場合は、クライアントから要求が再送信されるたびに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。再送信後もセッションが見つからない場合は、Disconnect-ACK と「Session Context Not Found」エラーコード属性が送信されます。

CoA 要求：ホストポートのディセーブル化

RADIUS サーバの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワークアクセスを即座にブロックする必要がある場合に便利です。ポートのネットワークアクセスを復元するには、非 RADIUS メカニズムを使用して再びイネーブルにします。このコマンドは、次の新しいベンダー固有属性（VSA）が含まれている標準 CoA 要求メッセージで伝達されます。

```
Cisco:Avpair="subscriber:command=disable-host-port"
```

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチは CoA-NAK メッセージと「Session Context Not Found」エラーコード属性を返します。このセッションがある場合は、スイッチはホストポートをディセーブルにし、CoA-ACK メッセージを返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブスイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブスイッチ上でその動作が再開されます。



(注) 再送信コマンドの後に接続解除要求が失敗すると、（接続解除ACKが送信されていない場合に）チェンジオーバー前にセッションが正常終了し、または元のコマンドが実行されてスタンバイスイッチがアクティブになるまでの間に発生した他の方法（たとえば、リンク障害）によりセッションが終了することがあります。

CoA 要求 : バウンス ポート

RADIUS サーバの CoA bounce port が RADIUS サーバから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

```
Cisco:Avpair="subscriber:command=bounce-host-port"
```

このコマンドはセッション指向であるため、1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチは CoA-NAK メッセージと「Session Context Not Found」エラーコード属性を返します。このセッションがある場合は、スイッチはホストポートを 10 秒間ディセーブルし、再びイネーブルにし（ポートバウンス）、CoA-ACK を返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブスイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブスイッチ上でその動作が再開されます。

セッション強制終了のスタック構成ガイドライン

スイッチスタックでは、CoA 接続解除要求メッセージに必要な特別な処理はありません。

CoA 要求バウンス ポートのスタック構成 ガイドライン

bounce-port コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

スタック マスターで **Auth Manager** コマンドハンドラが有効な **bounce-port** コマンドを受信すると、CoA-ACK メッセージを返す前に次の情報が確認されます。

- ポート バウンスの必要性
- ポート ID (ローカルセッション コンテキストで検出された場合)

スイッチで、ポートバウンスが開始されます (ポートが 10 秒間ディセーブルになり、再びイネーブルにされます)。

ポートバウンスが正常に実行された場合、ポートバウンスをトリガーした信号がスタンバイスタック マスターから削除されます。

ポートバウンスの完了前にスタック マスターに障害が発生すると、(後で削除される) 元のコマンドに基づいたスタック マスターの切り替え後、ポートバウンスが開始されます。

CoA-ACK メッセージの送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再送信コマンドが新しいコマンドとして扱われます。

CoA 要求ディセーブル ポートのスタック構成 ガイドライン

disable-port コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

スタック マスターにある **Auth Manager** コマンドハンドラで、有効な **disable-port** コマンドを受信した場合、CoA-ACK メッセージを返す前に次の情報が検証されます。

- ポート ディセーブルの必要性
- ポート ID (ローカルセッション コンテキストで検出された場合)

スイッチで、ポートをディセーブルする操作が試行されます。

ポートをディセーブルする操作が正常に実行された場合、ポートをディセーブルする操作をトリガーした信号がスタンバイスタック マスターから削除されます。

ポートをディセーブルする操作の完了前にスタック マスターに障害が発生すると、(後で削除される) 元のコマンドに基づいたスタック マスターの切り替え後、ポートがディセーブルにされます。

CoA-ACK メッセージの送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再送信コマンドが新しいコマンドとして扱われます。

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。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、共有するシークレットテキストストリングを使用して、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シークレットテキスト（キー）ストリングを指定する必要があります。

タイムアウト、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。この処理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スイッチを設定できます。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、各エントリが一意の 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（たとえばアカウントिंग）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トिंगサービスを提供できなかった場合、ネットワークアクセスサーバは同じデバイス上でアカウントिंगサービス用に設定されている 2 番めのホストエントリを試行します。（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使用できるサービスが制限されます。AAA 許可をイネーブルにすると、スイッチは（ローカルユーザデータベースまたはセキュリティサーバ上に存在する）ユーザのプロファイルから取得した情報を使用して、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 アカウントिंग

AAA アカウントिंग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 アカウントिंग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トिंगレコードの形式で RADIUS セキュリティサーバに報告します。各アカウントिंगレコードにはアカウントिंग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、スイッチと 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、該当の属性値 (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 認証中 (PPP の IPCP アドレス割り当て中) には、シスコの「multiple named IP address pools」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」はオプションになります。AV ペアはオプションにすることが可能である、ということに注意してください。

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

次に、ネットワークアクセスサーバからユーザがログインしたらすぐに EXEC コマンドが実行されるようにする方法の例を示します。

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

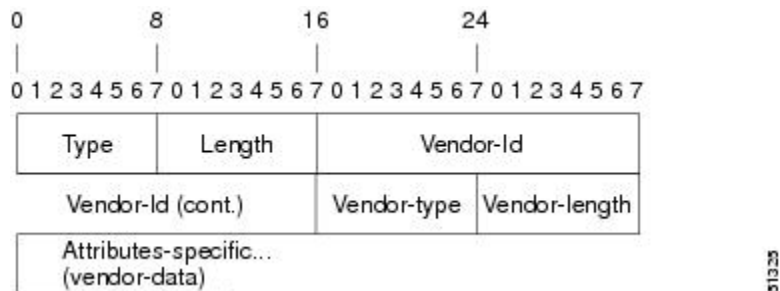
他のベンダーにも、それぞれ独自のベンダー ID、オプション、および関連する VSA があります。ベンダー ID および VSA の詳細については、RFC 2138 『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

属性 26 には、次の 3 つの要素が含まれています。

- タイプ (Type)
- 長さ
- ストリング (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 のパッケージ形式を示します。

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 5: 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 (Number)	次の表に示されるすべての属性は、IETF 属性 26 の拡張です。
Vendor-Specific Command Codes	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。
Sub-Type Number	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 (Attribute)	属性の ASCII スtring 名。
説明	属性の説明。

表 6: ベンダー固有 RADIUS IETF 属性

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	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 立中にピアにアダバタ イズされます。
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。

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
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。
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。

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
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	mmpipaaareceive-id コマンドまたは mmpipaaasend-id コマンドについて、アカウント ID の発信元がシステム管理者によって定義されたものとして示します。
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。

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
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 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	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	18	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。

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
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。
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。

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
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、ESMTPクライアント、ESMTPサーバなどがあります。
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。
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)。

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
26	9	27	Call-Type (h323-call-type)	コールのレグタイプを示します。有効値は、 telephony および VoIP です。
26	9	36	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	チャネルの 64 K 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 56 K の部分のみを使用するかどうかを指定します。

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	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 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
26	9	1	send-name	

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
				<p>PPP 名前認証。PAP に適用する場合は、インターフェイス上で ppppasent-namepassword コマンドを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ケットに、 「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</p>

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
				ため、 send-name 属 性は現在の動 作に制限され ています。
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 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				

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
26	9	2	Cisco-NAS-Port	<p>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-servervsasend 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。</p> <p>(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。</p>
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 プロファイル (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。

番号 (Number)	Vendor-Specific 企業コード	Sub-Type Number	属性 (Attribute)	説明
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、 ipmobility 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、およびプレイ保護タイムスタンプ範囲が含まれています。

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するシークレットテキストストリングを指定する必要があります。RADIUS ホストおよびシークレットテキストストリングを指定するには、**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。

RADIUS の設定方法

RADIUS サーバホストの識別

これらの設定を Device と通信するすべての RADIUS サーバに適用するために使用する固有のグローバル コンフィギュレーション コマンドは、**radius-server timeout**、**radius-server retransmit**、**radius-server key** の 3 つです。

認証時に AAA サーバグループを使用して既存のサーバホストをグループ化するように Device 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。これらの設定値としては、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 ストリングがあります。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。

はじめる前に

デバイス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： 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 server name 例： Device(config)# radius server rsim	

	コマンドまたはアクション	目的
ステップ 4	<p>address {ipv4 ipv6} <i>ip address</i> { auth-port <i>port number</i> acct-port <i>port number</i>}</p> <p>例 :</p> <pre>Device(config-radius-server) # address ipv4 124.2.2.12 auth-port 1612</pre>	<p>(任意) RADIUS サーバのパラメータを指定します。</p> <p>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。</p> <p>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。</p>
ステップ 5	<p>key <i>string</i></p> <p>例 :</p> <pre>Device(config-radius-server) # key rad123</pre>	<p>(任意) key <i>string</i> には、RADIUS サーバ上で動作する RADIUS デーモンと Device の間で使用する認証および暗号キーを指定します。</p> <p>(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。キーは常に radius server コマンドの最後のアイテムとして設定してください。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>retransmit <i>value</i></p> <p>例 :</p> <pre>Device(config-radius-server) # retransmit 10</pre>	<p>(任意) サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ~ 100 です。この設定は、radius-server retransmit グローバルコンフィギュレーション コマンドによる設定を上書きします。</p>
ステップ 7	<p>timeout 秒</p> <p>例 :</p> <pre>Device(config-radius-server) # timeout 60</pre>	<p>(任意) Device が要求を再送信する前に RADIUS サーバからの応答を待機する時間間隔を指定します。指定できる範囲は 1 ~ 1000 です。この設定は、radius-server timeout グローバルコンフィギュレーション コマンドによる設定を上書きします。</p>
ステップ 8	<p>end</p> <p>例 :</p> <pre>Device(config) # end</pre>	<p>特権 EXEC モードに戻ります。</p>

	コマンドまたはアクション	目的
ステップ 9	show running-config 例： Device# show running-config	入力を確認します。
ステップ 10	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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。

はじめる前に

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しません。

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	configureterminal 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。

	コマンドまたはアクション	目的
ステップ 3	aaa new-model 例 : <pre>Device (config) # aaa new-model</pre>	AAA をイネーブルにします。
ステップ 4	aaa authentication login {default list-name} method1 [method2...] 例 : <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 コマンドに名前付きリストが指定されなかった場合に使用され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す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。 • list-name 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。 • method1... 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"> ◦ enable : 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。 ◦ group radius : 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。 ◦ line : 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。 ◦ local : 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 namepassword 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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> ° <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] <i>line-number</i> <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。
ステップ 8	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 9	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

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関連付けるには、**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、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	configureterminal 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 名前 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。 デバイスは、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ing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	end string 例： Device (config-radius-server)# key	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
	<code>cisco123</code>	
ステップ 6	end 例： Device (config-radius-server) # end	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。
ステップ 7	show running-config 例： Device# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

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。

	コマンドまたはアクション	目的
ステップ 2	configureterminal 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 許可を受けるようにデバイスを設定します。 exec キーワードを指定すると、ユーザプロフィール情報 (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。
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

次の作業

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	configureterminal 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： Device(config)# end	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
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

次の作業

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。このコマンドは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

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	configureterminal 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 2	radius-server key string 例： Device(config)# radius-server	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tring を指定します。

	コマンドまたはアクション	目的
	key your_server_key Device (config) # key your_server_key	(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 3	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 4	radius-server timeout 秒 例 : Device (config) # radius-server timeout 3	スイッチが RADIUS 要求に対する応答を待って、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 5	radius-server deadtime 分 例 : Device (config) # radius-server deadtime 0	RADIUS サーバが認証要求に応答していない場合、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 0 ~ 1440 分です。
ステップ 6	end 例 : Device (config) # end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例 : Device# copy running-config	(任意) コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	<code>startup-config</code>	

ベンダー固有の RADIUS 属性を使用するデバイス設定

ベンダー固有仕様の 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	configureterminal 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 vsa send [accounting authentication] 例： Device (config)# radius-server vsa send accounting	デバイスが 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。 <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。 キーワードを指定せずにこのコマンドを入力すると、アカウントおよび認証のベンダー固有属性の両方が使用されます。
ステップ 4	end 例： Device (config)# end	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
ステップ 5	show running-config 例： Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

ベンダー独自の RADIUS サーバとの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	configureterminal 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 server name 例： Device(config)# radius server rsim	RADIUS サーバを指定します。

	コマンドまたはアクション	目的
ステップ 4	address { ipv4 ipv6 } ip address 例 : Device (config-radius-server) # address ipv4 172.24.25.10	(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 string 例 : Device (config-radius-server) # key rad123	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テキスト文字列を指定します。デバイスと RADIUS サーバはこのテキスト文字列を使用してパスワードを暗号化し、応答を交換します。
ステップ 7	end 例 : Device (config) # end	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 9	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

デバイス上での CoA の設定

CoA をデバイスで設定するには、次の手順を実行します。この手順は必須です。

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	configureterminal 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。
ステップ 4	aaa server radius dynamic-author 例： Device (config)# aaa server radius dynamic-author	デバイスを認証、許可、アカウントिंग (AAA) サーバに設定し、外部ポリシーサーバとの相互作用を実行します。
ステップ 5	client {ip-address name} [vrf vrfname] [server-key string]	ダイナミック許可ローカルサーバコンフィギュレーションモードを開始し、デバイスが CoA を受け取り、要求を取り外す RADIUS クライアントを指定します。
ステップ 6	server-key [0 7] string 例： Device (config-sg-radius)# server-key your_server_key	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 7	port port-number 例： Device (config-sg-radius)# port 25	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。

	コマンドまたはアクション	目的
ステップ 8	auth-type {any all session-key} 例 : Device (config-sg-radius) # auth-type any	デバイスが RADIUS クライアントに使用する許可のタイプを指定します。 クライアントは、許可用に設定されたすべての属性と一致していなければなりません。
ステップ 9	ignore session-key	(任意) セッションキーを無視するようにデバイスを設定します。 ignore コマンドの詳細については、Cisco.com 上の『 <i>Cisco IOS Intelligent Services Gateway Command Reference</i> 』を参照してください。
ステップ 10	ignore server-key 例 : Device (config-sg-radius) # ignore server-key	(任意) サーバキーを無視するようにデバイスを設定します。 ignore コマンドの詳細については、Cisco.com 上の『 <i>Cisco IOS Intelligent Services Gateway Command Reference</i> 』を参照してください。
ステップ 11	authentication command bounce-port ignore 例 : Device (config-sg-radius) # authentication command bounce-port ignore	(任意) CoA 要求を無視して、セッションをホスティングするポートを一時的にディセーブルにするようにデバイスを設定します。ポートを一時的にディセーブルにする目的は、VLAN の変更が発生しても、その変更を検出するサブリカントがエンドポイント上にない場合に、ホストから DHCP 再ネゴシエーションを行わせることです。
ステップ 12	authentication command disable-port ignore 例 : Device (config-sg-radius) # authentication command disable-port ignore	(任意) セッションをホスティングしているポートを管理上のシャットダウン状態にすることを要求する非標準コマンドを無視するようにデバイスを設定します。ポートをシャットダウンすると、セッションが終了します。 ポートを再びイネーブルにするには、標準の CLI または SNMP コマンドを使用します。
ステップ 13	end 例 : Device (config-sg-radius) # end	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
ステップ 14	show running-config 例： Device# show running-config	入力を確認します。
ステップ 15	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

CoA 機能のモニタリング

表 7: 特権 EXEC 表示コマンド

コマンド	目的
show aaa attributes protocol radius	RADIUS コマンドの AAA 属性を表示します。

表 8: グローバルトラブルシューティングコマンド

コマンド	目的
debug radius	RADIUS のトラブルシューティングを行うための情報を表示します。
debug aaa coa	CoA 処理のトラブルシューティングを行うための情報を表示します。
debug aaa pod	POD パケットのトラブルシューティングを行うための情報を表示します。
debug aaa subsys	POD パケットのトラブルシューティングを行うための情報を表示します。
debug cmdhd [detail error events]	コマンドヘッダーのトラブルシューティングを行うための情報を表示します。

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

RADIUS 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 リリースのみを示しています。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 Cisco 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 9: RADIUS の機能情報

機能名	リリース	機能情報
RADIUS	Cisco IOS XE Everest 16.5.1a	<p>自動 ID 機能は、一連の組み込みポリシーをグローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードで提供します。この機能は、Class-Based Policy Language (CPL) コントロール ポリシーと同等な新しいスタイルのモードでのみ使用できます。</p> <p>この機能は、次のプラットフォームに実装されていました。</p> <ul style="list-style-type: none"> • Cisco Catalyst 9300 シリーズ スイッチ <p>次のコマンドが導入または変更されました。 source-template</p>

