CHAPTER 18

RADIUS の設定

この章では、Cisco Nexus 4001I/4005I Switch Module for IBM BladeCenter 上で、Remote Access Dial-In User Service（RADIUS）プロトコルを設定する方法について説明します。

この章で説明する内容は、次のとおりです。

RADIUS について

RADIUS 分散クライアント / サーバ システムを使用すると、不正アクセスからネットワークを保護できます。シスコの実装では、RADIUS クライアントはスイッチで稼動し、すべてのユーザ認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウンティング要求を送信します。

ここでは、次の内容について説明します。

RADIUS ネットワーク環境

RADIUS は、高度なセキュリティを必要とし、同時にリモート ユーザのネットワーク アクセスを維持する必要があるさまざまなネットワーク環境に実装できます。

RADIUS は、アクセス セキュリティを必要とする次のネットワーク環境で使用します。

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク

  たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバ ベースのセキュリティ データベースを使用できます。

- すでに RADIUS を使用しているネットワーク

  RADIUS を使用したスイッチをネットワークに追加できます。この作業は、AAA サーバに移行するときの最初の手順になります。

- リソース アカウンティングを必要とするネットワーク

  RADIUS アカウンティングは、RADIUS 認証または RADIUS 許可とは個別に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。Internet Service Provider（ISP; 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用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。

- 認証プロファイルをサポートするネットワーク

  ネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルをセットアップできます。ユーザごとのプロファイルにより、スイッチは、既存の RADIUS ソリューションを使用してポートを容易に管理できると同時に、共有リソースを効率的に管理してさまざまな service-level agreement（SLA; サービス レベル契約）を提供できます。

RADIUS の操作

ユーザがログインを試行し、RADIUS を使用してスイッチに対する認証を行う際には、次のプロセスが実行されます。

1. ユーザが、ユーザ名とパスワードの入力を求められ、入力します。
2. ユーザ名と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：ユーザが認証されました。
   - REJECT：ユーザは認証されず、ユーザ名とパスワードの再入力を求められるか、アクセスを拒否されます。
   - CHALLENGE：RADIUS サーバによってチャレンジが発行されます。チャレンジは、ユーザから追加データを収集します。
   - CHANGE PASSWORD：RADIUS サーバからユーザに対して新しいパスワードの選択を求める要求が発行されます。

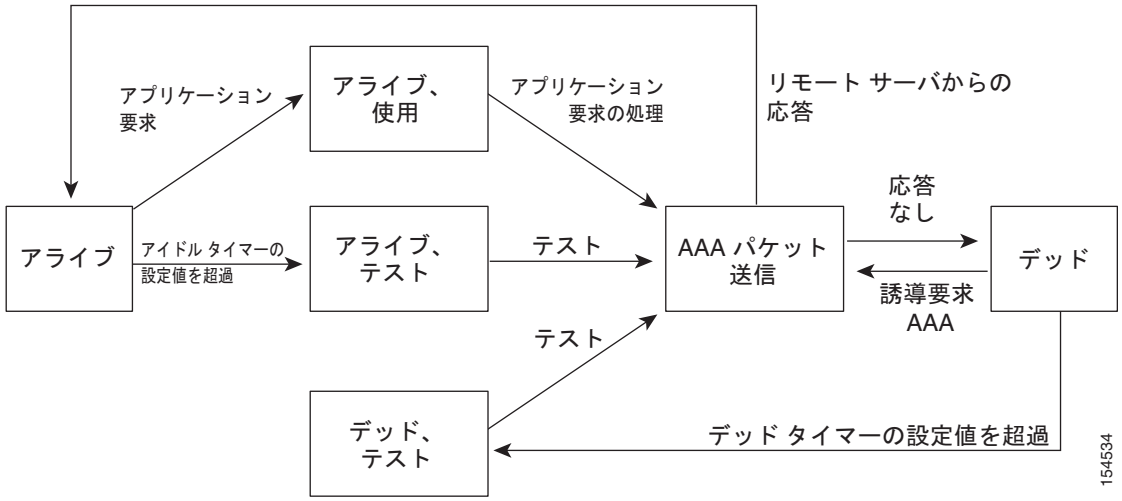
ACCEPT または REJECT 応答には、EXEC またはネットワーク許可に使用される追加データが含まれています。RADIUS 許可を使用するには、まず RADIUS 認証を完了する必要があります。ACCEPT または REJECT パケットに含まれる追加データの内容は次のとおりです。

- ユーザがアクセス可能なサービス（Telnet、rlogin、または local-area transport（LAT; ローカルエリア トランスポート）接続、PPP（ポイントツーポイント プロトコル）、Serial Line Internet Protocol（SLIP; シリアル ライン インターネット プロトコル）、EXEC サービスなど）
- 接続パラメータ（ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセス リスト、ユーザ タイムアウト）

RADIUS サーバのモニタリング

応答を返さない RADIUS サーバがあると、AAA 要求の処理に遅延が発生する可能性があります。AAA 要求の処理時間を節約するため、定期的に RADIUS サーバをモニタリングし、RADIUS サーバが応答を返す（アライブ）かどうかを調べるよう、スイッチを設定できます。スイッチは、応答を返さない RADIUS サーバをデッド（dead）としてマークし、デッド RADIUS サーバには AAA 要求を送信しません。また、定期的にデッド RADIUS サーバをモニタリングし、それらが応答を返したらアライブ状態に戻します。このモニタリング プロセスでは、実際の AAA 要求が送信される前に、RADIUS サーバが稼動状態であることを確認します。RADIUS サーバの状態がデッドまたはアライブに変わると、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップが生成され、スイッチによって、障害が発生したことを知らせるエラー メッセージが表示されます。
図 18-1 を参照してください。

図 18-1　RADIUS サーバの状態



（注）　アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。RADIUS サーバ モニタリングを実行するには、テスト認証要求を RADIUS サーバに送信します。

ベンダー固有属性

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）が、ネットワーク アクセス サーバと RADIUS サーバの間での Vendor-Specific Attribute（VSA; ベンダー固有属性）の通信のための方式を規定する標準を作成しています。IETF は、属性 26 を使用します。VSA を使用するとベンダーは、一般的な用途には適合しない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。値は、次の形式のストリングです。

```
protocol : attribute separator value *
```

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号（=）で、アスタリスク（*）は任意属性を示します。

スイッチでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションが、スイッチでサポートされています。

- Shell：access-accept パケットで、ユーザ プロファイル情報を提供するために使用されます。
- Accounting：accounting-request パケットで使用されます。値にスペースが含まれている場合は、二重引用符で囲む必要があります。

スイッチでは、次の属性がサポートされています。

- roles：ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。
- accountinginfo：標準の RADIUS アカウンティング プロトコルで処理される属性に加えて、アカウンティング情報が格納されます。この属性は、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分だけに送信されます。この属性と共に使用できるのは、アカウンティングの Protocol Data Unit（PDU; プロトコル データ ユニット）だけです。

RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IPv4 または IPv6IP アドレスまたはホスト名を取得していること。
- RADIUS サーバから事前共有キーを取得していること。
- スイッチが、AAA サーバの RADIUS クライアントとして設定されていること。

注意事項と制限事項

スイッチ上に設定できる RADIUS サーバの最大数は 64 です。

RADIUS サーバの設定

RADIUS サーバを設定する手順は、次のとおりです。

ステップ 1　スイッチと RADIUS サーバとの接続を確立します。

「RADIUS サーバ ホストの設定」（P.18-5）を参照してください。

ステップ 2　RADIUS サーバの事前共有秘密キーを設定します。

「グローバルな事前共有キーの設定」（P.18-6）を参照してください。

ステップ 3　必要に応じて、AAA 認証方式用に、RADIUS サーバのサブセットを使用して RADIUS サーバ グループを設定します。

「ログイン時にユーザによる RADIUS サーバの指定を許可」（P.18-9）および第 17 章「AAA の設定」を参照してください。

ステップ 4　必要に応じて、次のオプションのパラメータを設定します。

- デッドタイム間隔

「次に、RADIUS サーバの定期的なモニタリングを設定する例を示します。」（P.18-12）を参照してください。

- ログイン時に RADIUS サーバの指定を許可

  「ログイン時にユーザによる RADIUS サーバの指定を許可」（P.18-9）を参照してください。

- 送信リトライ回数とタイムアウト間隔

  「グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定」（P.18-9）を参照してください。

- アカウンティングおよび認証属性

  「RADIUS サーバのアカウンティングおよび認証属性の設定」（P.18-10）を参照してください。

ステップ 5　必要に応じて、定期的に RADIUS サーバをモニタリングするよう設定します。

「RADIUS サーバの定期的モニタリングの設定」（P.18-11）を参照してください。

次のトピックで、RADIUS の設定手順について詳しく説明します。

- 「RADIUS サーバ ホストの設定」（P.18-5）
- 「グローバルな事前共有キーの設定」（P.18-6）
- 「RADIUS サーバの事前共有キーの設定」（P.18-7）
- 「RADIUS サーバ グループの設定」（P.18-7）
- 「ログイン時にユーザによる RADIUS サーバの指定を許可」（P.18-9）
- 「グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定」（P.18-9）
- 「サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定」（P.18-10）
- 「RADIUS サーバのアカウンティングおよび認証属性の設定」（P.18-10）
- 「RADIUS サーバの定期的モニタリングの設定」（P.18-11）
- 「デッド タイム間隔の設定」（P.18-12）
- 「RADIUS サーバまたはサーバ グループの手動モニタリング」（P.18-13）

RADIUS サーバ ホストの設定

認証に使用する各 RADIUS サーバについて、IP アドレス（IPv4 または IPv6）、またはホスト名を設定する必要があります。すべての RADIUS サーバ ホストは、デフォルトの RADIUS サーバ グループに追加されます。最大 64 の RADIUS サーバを設定できます。

RADIUS サーバ ホストを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	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	`switch(config) #radius-server host {ipv4-address | ipv6-address | host-name}`	RADIUS サーバの IPv4 または IPv6 アドレス、またはホスト名を指定します。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 4	switch# **show radius-server**	（任意）RADIUS サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、RADIUS サーバ ホストを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

グローバルな事前共有キーの設定

スイッチで使用するすべてのサーバについて、グローバル レベルで事前共有キーを設定できます。事前共有キーとは、スイッチと RADIUS サーバ ホスト間の共有秘密テキスト ストリングです。

グローバルな事前共有キーを設定するには、リモートの RADIUS サーバの事前共有キー値を取得した上で、次の作業を行います。

	コマンド	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **radius-server key** [**0** | **7**] *key-value*	すべての RADIUS サーバで使用する事前共有キーを指定します。クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。デフォルトの形式はクリア テキストです。キーの最大長は 63 文字です。 デフォルトでは、事前共有キーは設定されません。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show radius-server**	（任意）RADIUS サーバの設定を表示します。 **（注）** 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、リモートの RADIUS サーバから事前共有キーの値を取得する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 0 QsEfThUkO
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバの事前共有キーの設定

RADIUS サーバの事前共有キーを設定できます。事前共有キーとは、スイッチと RADIUS サーバ ホスト間の共有秘密テキスト ストリングです。

RADIUS サーバの事前共有キーを設定するには、リモートの RADIUS サーバの事前共有キー値を取得した上で、次の作業を行います。

	コマンド	目的
ステップ 1	`switch# configure terminal`	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	`switch(config)# radius-server host {ipv4-address | ipv6-address | host-name} key [0 | 7] key-value`	特定の RADIUS サーバの事前共有キーを指定します。クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。デフォルトの形式はクリア テキストです。キーの最大長は 63 文字です。 この事前共有キーがグローバル共有キーの代わりに使用されます。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show radius-server`	（任意）RADIUS サーバの設定を表示します。 **（注）** 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、RADIUS サーバの事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによる認証を指定できます。グループのメンバーはすべて、RADIUS プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバ グループは随時設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。AAA サービスについては、第 17 章「AAA の設定」を参照してください。

RADIUS サーバ グループを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	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	`switch(config)# aaa group server radius` *group-name*	RADIUS サーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション サブモードを開始します。*group-name* 引数は、最大 127 文字の長さの英数字のストリングで、大文字小文字が区別されます。
ステップ 3	`switch(config-radius)# server` {*ipv4-address* |*ipv6-address* | *server-name*}	RADIUS サーバを、RADIUS サーバ グループのメンバーとして設定します。 **ヒント** 指定した RADIUS サーバが見つからない場合は、**radius-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	`switch(config-radius)# deadtime` *minutes*	（任意）モニタリング デッド タイムを設定します。デフォルトは 0 分です。指定できる範囲は 1 ～ 1440 です。 **（注）** RADIUS サーバ グループのデッド タイム間隔が 0 より大きい場合は、この値がグローバルなデッド タイム値より優先されます。RADIUS サーバの定期的なモニタリングを設定する例を参照してください。
ステップ 5	`switch(config-radius)# exit`	コンフィギュレーション モードを終了します。
ステップ 6	`switch(config) #show radius-server group [GROUP-NAME]`	（任意）RADIUS サーバ グループの設定を表示します。
ステップ 7	`switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、RADIUS サーバ グループを設定する例を示します。

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# deadtime 30
switch(config-radius)# use-vrf management
switch(config-radius)# exit
switch(config)# show radius-server group
switch(config)# copy running-config startup-config
```

ログイン時にユーザによる RADIUS サーバの指定を許可

（注） デフォルトでは、スイッチは、デフォルトの AAA 認証方式に基づいて認証要求を転送します。VRF と認証要求送信先 RADIUS サーバをユーザが指定できるようにスイッチを設定するには、directed-request オプションをイネーブルにします。このオプションをイネーブルにすると、ユーザは *username@hostname* としてログインできます。ここで、*hostname* は設定済みの RADIUS サーバの名前です。ユーザ指定のログインは、Telnet セッションでのみサポートされます。

ユーザがログイン時に RADIUS サーバを指定できるようにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	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	`switch(config)# radius-server directed-request`	ログイン時にユーザが認証要求の送信先となる RADIUS サーバを指定できるようにします。デフォルトはディセーブルです。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show radius-server directed-request`	（任意）directed request の設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定

すべての RADIUS サーバに対するグローバルな再送信リトライ回数とタイムアウト間隔を設定できます。デフォルトでは、スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。タイムアウト間隔は、スイッチがタイムアウト エラーを宣言する前に、RADIUS サーバからの応答を待機する時間を決定します。

グローバルな RADIUS 送信リトライ回数とタイムアウト間隔を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	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	`switch(config)# radius-server retransmit` *count*	すべての RADIUS サーバの再送信回数を指定します。デフォルトの再送信回数は 1 で、範囲は 0 ～ 5 です。
ステップ 3	`switch(config)# radius-server timeout` *seconds*	RADIUS サーバの送信タイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。
ステップ 4	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 5	`switch# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 6	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定

デフォルトでは、スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。スイッチが、タイムアウト エラーを宣言する前に、RADIUS サーバからの応答を待機するタイムアウト間隔も設定できます。

サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	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	`switch(config)# radius-server host {ipv4-address |ipv6-address | host-name} retransmit count`	特定のサーバに対する再送信回数を指定します。デフォルトはグローバル値です。 **（注）** 特定の RADIUS サーバに指定した再送信回数は、すべての RADIUS サーバに指定した再送信回数より優先されます。
ステップ 3	`switch(config)# switch(config)# radius-server host {ipv4-address |ipv6-address | host-name} timeout seconds`	特定のサーバの送信タイムアウト間隔を指定します。デフォルトはグローバル値です。 **（注）** 特定の RADIUS サーバに指定したタイムアウト間隔は、すべての RADIUS サーバに指定したタイムアウト間隔より優先されます。
ステップ 4	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 5	`switch# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 6	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host server1 retransmit 3
switch(config)# radius-server host server1 timeout 10
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバのアカウンティングおよび認証属性の設定

RADIUS サーバをアカウンティング専用、または認証専用に使用するかを指定できます。デフォルトでは、RADIUS サーバはアカウンティングと認証の両方に使用されます。RADIUS のアカウンティングおよび認証メッセージの宛先 UDP ポート番号も指定できます。

RADIUS サーバのアカウンティング属性と認証属性を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	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	`switch(config) #radius-server host {ipv4-address | ipv6-address | host-name} acct-port udp-port`	（任意）RADIUS アカウンティング メッセージ用の UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。指定できる範囲は 0 ～ 65535 です。
ステップ 3	`switch(config)# radius-server host {ipv4-address | ipv6-address | host-name} accounting`	（任意）特定の RADIUS サーバをアカウンティング用にのみ使用することを指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	`switch(config)# radius-server host {ipv4-address | ipv6-address | host-name} auth-port udp-port`	（任意）RADIUS 認証メッセージ用の UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。指定できる範囲は 0 ～ 65535 です。
ステップ 5	`switch(config)# radius-server host {ipv4-address | ipv6-address | host-name} authentication`	（任意）特定の RADIUS サーバを認証用にのみ使用することを指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 6	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 7	`switch(config)# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 8	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、RADIUS サーバのアカウンティング属性と認証属性を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 acct-port 2004
switch(config)# radius-server host 10.10.1.1 accounting
switch(config)# radius-server host 10.10.2.2 auth-port 2005
switch(config)# radius-server host 10.10.2.2 authentication
switch(config)# exit
switch(config)# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバの定期的モニタリングの設定

RADIUS サーバの可用性をモニタリングできます。パラメータとして、サーバに使用するユーザ名とパスワード、およびアイドル タイマーがあります。アイドル タイマーには、RADIUS サーバがどのくらいの期間要求を受信しなかった場合にスイッチがテスト パケットを送信するかを指定します。このオプションを設定することで、サーバを定期的にテストできます。

（注） セキュリティ上の理由から、RADIUS データベース内の既存のユーザ名と同じテスト ユーザ名を設定しないことを推奨します。

テスト アイドル タイマーには、RADIUS サーバがどのくらいの期間要求を受信しなかった場合にスイッチがテスト パケットを送信するかを指定します。

（注） デフォルトのアイドル タイマー値は 0 分です。アイドル時間間隔が 0 分の場合、スイッチは RADIUS サーバの定期的なモニタリングを実行しません。

RADIUS サーバの定期的なモニタリングを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	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	`switch(config)# radius-server host {ipv4-address | ipv6-address | host-name} test {idle-time minutes | password password [idle-time minutes] | username name [password password [idle-time minutes]]}`	サーバ モニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。デフォルトのアイドル タイマー値は 0 分です。指定できる範囲は 0 ～ 1440 分です。 **（注）** RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	`switch(config)# radius-server deadtime minutes`	スイッチが、前回応答しなかった RADIUS サーバをチェックするまでの時間（分）を指定します。デフォルト値は 0 分です。指定できる範囲は 1 ～ 1440 分です。
ステップ 4	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 5	`switch# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 6	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、RADIUS サーバの定期的なモニタリングを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

デッド タイム間隔の設定

すべての RADIUS サーバのデッド タイム間隔を設定できます。デッド タイム間隔には、スイッチが RADIUS サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを判断するためにテスト パケットを送信するまでの間隔を指定します。デフォルト値は 0 分です。

（注）　デッド タイム間隔が 0 分の場合、RADIUS サーバは、応答を返さない場合でも、デットとしてマークされません。RADIUS サーバ グループのデッド タイム間隔を設定することもできます（「RADIUS サーバ グループの設定」（P.18-7）を参照）。

デッド タイム間隔を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	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	`#switch(config)# radius-server deadtime`	デッド タイム間隔を設定します。デフォルト値は 0 分です。指定できる範囲は 1 ～ 1440 分です。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show radius-server`	（任意）RADIUS サーバの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

RADIUS サーバまたはサーバ グループの手動モニタリング

RADIUS サーバまたはサーバ グループにテスト メッセージを手動で送信する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# test aaa server radius {ipv4-address | ipv6-address | server-name} [vrf vrf-name] username password`	RADIUS サーバにテスト メッセージを送信して可用性を確認します。
ステップ 1	`switch# test aaa group group-name username password`	RADIUS サーバ グループにテスト メッセージを送信して可用性を確認します。

次に、RADIUS サーバに手動でテスト メッセージを送信する例を示します。

```
switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group RadGroup user2 As3He3CI
```

RADIUS の設定の確認

RADIUS の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config radius [**all**]	実行コンフィギュレーションの RADIUS 設定を表示します。

コマンド	目的
show startup-config radius	スタートアップ コンフィギュレーションの RADIUS 設定を表示します。
show radius-server [*server-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての RADIUS サーバのパラメータを表示します。

このコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 4000I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*』を参照してください。

RADIUS サーバの統計情報の表示

スイッチが RADIUS サーバのアクティビティについて保持している統計情報を表示する手順は、次のとおりです。

コマンド	目的
switch# switch# **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}	RADIUS 統計情報を表示します。

次に、統計情報を表示する例を示します。

```
switch# show radius-server statistics 10.10.1.1
```

RADIUS の設定例

次に、RADIUS を設定する例を示します。

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
use-vrf management
```

デフォルト設定

表 18-1 に、RADIUS パラメータのデフォルト設定を示します。

表 18-1　デフォルトの RADIUS パラメータ

パラメータ	デフォルト
サーバの役割	認証とアカウンティング
デッド タイマー間隔	0 分
再送信回数	1
再送信タイマー間隔	5 秒

表 18-1　デフォルトの RADIUS パラメータ（続き）

パラメータ	デフォルト
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	test