CHAPTER 19

ML シリーズ カードのセキュリティ設定

この章では、ML シリーズ カードのセキュリティ機能について説明します。

この章の主な内容は次のとおりです。

セキュリティの概要

ML シリーズ カードには、いくつかのセキュリティ機能が含まれています。これらの機能の中には、ML シリーズ カードが取り付けられている ONS ノードから独立して動作するものがあります。それ以外の機能は、Cisco Transport Controller（CTC）または Transaction Language One（TL1）を使用して設定されます。

Cisco IOS で設定されるセキュリティ機能は、以下のとおりです。

- Cisco IOS ログイン強化
- Secure Shell（SSH; セキュア シェル）接続
- Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）/Remote Authentication Dial-In User Service（RADIUS）（AAA/RADIUS）スタンドアロン モード
- Cisco IOS 基本パスワード（Cisco IOS 基本パスワード設定の詳細については、「パスワード」[p.3-9] を参照してください）

CTC または TL1 で設定されるセキュリティ機能は、以下のとおりです。

- ディセーブルのコンソール ポート
- AAA/RADIUS リレー モード

ML シリーズ カードの コンソール ポートのディセーブル化

コンソール ポート（カードの前面にある RJ-11 シリアル ポート）へ直接接続するなど、ML カード上で動作している Cisco IOS にアクセスする方法には数種類あります。ユーザは、このようなデフォルトでイネーブルになっている直接接続をディセーブルにすることでセキュリティを強化できます。これにより、Cisco IOS エラー メッセージなどのコンソール ポート出力を妨げずにコンソール ポート入力を防ぐことができます。

CTC または TL1 を使用してコンソール ポートへのアクセスをディセーブルにできます。CTC を使用してこれをディセーブルにするには、ML シリーズ カードのカードレベル ビューで、**IOS** タブの下をクリックして、**Enable Console Port Access** ボックスをオフにして、**Apply** をクリックします。ユーザは、Superuser レベルでログインしてこのタスクを完了する必要があります。

TL1 を使用してこれをディセーブルにするには、『*Cisco ONS SONET TL1 Command Guide*』を参照してください。

ML シリーズ カードへのセキュアなログイン

ML シリーズ カードは、Cisco IOS Release 12.2(25)S に統合され、Cisco IOS Release 12.3(4)T に導入された Cisco IOS ログイン強化をサポートしています。この強化により、ユーザは Telnet、SSH、HTTP などの仮想接続を確立するときに ML シリーズ カードのセキュリティを強化できます。セキュアなログイン機能では、ML シリーズ カードの vty セッション（監査証跡）に対するログイン試行の成功および失敗を記録します。これらの機能は、Cisco IOS CLI（コマンドライン インターフェイス）を使用して設定されます。

詳細な設定例などの詳細な情報については、http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guides_list.html にある Cisco IOS Release 12.2(25)S 機能ガイド モジュール「Cisco IOS Login Enhancements」を参照してください。

ML シリーズ カードの SSH

このセクションでは、SSH 機能の設定方法について説明します。

以下のセクションがあります。

SSH の設定例については、『*Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*』の「Configuring Secure Shell」の章にある「SSH Configuration Examples」を参照してください。次の URL にあります。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf.htm

（注）　このセクションで使用されている全構文と使用方法の情報については、次の URL にある Cisco IOS Release 12.2 のコマンド リファレンスを参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

SSH の概要

ML シリーズ カードは、SSH のバージョン 1（SSH v1）およびバージョン 2（SSHv2）の両方をサポートしています。SSHv2 は、SSHv1 のセキュリティ面を改善したもので、ML シリーズ カードではデフォルトで選択されています。

SSH には、SSH サーバおよび SSH クライアントの 2 種類のアプリケーションがあります。ML シリーズ カードは、SSH サーバのみをサポートし、SSH クライアントはサポートしていません。Cisco IOS ソフトウェアの SSH サーバは、公的および商用で利用可能な SSH クライアントと連動します。

SSH サーバにより、着信 Telnet 接続と同様ですがよりセキュリティが強化された ML シリーズ カードへの接続が可能になります。SSH が登場するまで、セキュリティは Telnet 固有のセキュリティに限定されていました。SSH により、Cisco IOS ソフトウェア認証が使用できるようになり、セキュリティ面が改善されました。

ONS ノードも SSH をサポートしています。SSH が ONS ノードでイネーブルの場合、Cisco IOS CLI セッションで、SSH を使用して ML シリーズ カードに接続します。

（注）　SSH がイネーブルの場合には、ML シリーズ カードへの Telnet アクセスが自動的にディセーブルになりません。ユーザは、**transport input ssh** vty ライン コンフィギュレーション コマンドを使用して Telnet アクセスをディセーブルにできます。

SSH の設定

ここでは、次の設定情報について説明します。

設定の注意事項

ML シリーズ カードを SSH サーバとして設定する場合には、以下の注意事項に従ってください。

- AAA の新規モデルおよび AAA ログイン方式をイネーブルにする必要があります。まだイネーブルでない場合は、「AAA ログイン認証の設定」（p.19-13）の手順を完了してください。
- SSHv1 サーバで生成された Rivest, Shamir, and Adelman（RSA）キー ペアを SSH v2 サーバで使用することも、またその逆も可能です。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力したあとに CLI エラー メッセージを取得した場合、RSA キー ペアが生成されていません。ホスト名とドメインを再設定して、**crypto key generate rsa** コマンドを入力します。詳細については、「SSH を実行するための ML シリーズ カードの設定」（p.19-4）を参照してください。
- RSA キー ペアを生成する際に、`No host name specified` メッセージが表示される場合があります。表示される場合は、**hostname** 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ホスト名を設定する必要があります。
- RSA キー ペアを生成する際に、`No domain specified` メッセージが表示される場合があります。表示される場合は、**ip domain-name** 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 IP ドメイン名を設定する必要があります。

SSH を実行するための ML シリーズ カードの設定

SSH サーバとして動作するように ML シリーズ カードを設定するには、以下の手順を実行します。

1. ML シリーズ カードのホスト名と IP ドメイン名を設定します。
2. ML シリーズ カードの RSA キー ペアを生成します。これで、SSH が自動的にイネーブルになります。
3. ローカルまたはリモート アクセス用のユーザ認証を設定します。この手順は必須です。

ホスト名と IP ドメイン名を設定して RSA キー ペアを生成するには、特権 EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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 2	`Router (config)# hostname` *hostname*	ML シリーズ カードのホスト名を設定します。
ステップ 3	`Router (config)# ip domain-name` *domain_name*	ML シリーズ カードのホスト ドメインを設定します。
ステップ 4	`Router (config)# crypto key generate rsa`	ML シリーズ カードでローカルおよびリモート認証用の SSH サーバをイネーブルにして、RSA 鍵ペアを生成します。 RSA 鍵を生成する際に、モジュラス長を入力するように要求されます。デフォルトのモジュラス長は 512 ビットです。モジュラス長が長いほど安全ですが、生成や使用の際により時間がかかります。

	コマンドの説明	目的
ステップ 5	`Router (config)# ip ssh timeout seconds`	タイムアウト時間を秒単位で指定します。デフォルトは 120 秒です。範囲は、0 ～ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続の確立後、ML シリーズ カードはデフォルトの CLI ベース セッションのタイムアウト値を使用します。 デフォルトで、ネットワーク上で複数の CLI ベース セッションに対して 5 つまでの同時暗号化 SSH 接続が可能です（セッション 0 ～ 4）。実行シェルの開始後、CLI ベース セッションのタイムアウト値がデフォルトの 10 分に戻ります。
ステップ 6	`Router (config)# ip ssh authentication-retries number`	クライアントがサーバの再認証を受けられる回数を指定します。デフォルトは 3 です。範囲は 0 ～ 5 です。
ステップ 7	`Router (config)# end`	特権 EXEC モードに戻ります。

ステップ 8	`Router # show ip ssh`
	
	または
	
	`Router # show ssh`
		使用している SSH サーバのバージョンおよび設定情報を表示します。
		
		ML シリーズ カードの SSH サーバのステータスを表示します。

ステップ 9	`Router # show crypto key mypubkey rsa`	この ML シリーズ カードに関連付けられた生成済み RSA 鍵ペアを表示します。
ステップ 10	`Router # copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

RSA 鍵ペアを削除するには、**crypto key zeroize rsa** 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。RSA 鍵ペアが削除されると、SSH サーバも自動的に削除されます。

SSH サーバの設定

SSH 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。

	コマンドの説明	目的
ステップ 1	`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 2	`Router (config)# ip ssh version [1 | 2]`	（任意）SSH バージョン 1 または SSH バージョン 2 を実行するように ML シリーズ カードを設定します。 • **1 —** SSH バージョン 1 を実行するように ML シリーズ カードを設定します。 • **2 —** SSH バージョン 2 を実行するように ML シリーズ カードを設定します。 このコマンドを入力しなかったりキーワードを指定しなかったりした場合、SSH サーバは SSH クライアントでサポートされている最新の SSH バージョンを選択します。例えば、SSH クライアントが SSHv1 および SSHv2 をサポートしている場合、SSH サーバは SSHv2 を選択します。

	コマンドの説明	目的
ステップ 3	`Router (config)# ip ssh timeout seconds`	タイムアウト時間を秒単位で指定します。デフォルトは 120 秒です。範囲は、0 ～ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続の確立後、ML シリーズ カードはデフォルトの CLI ベース セッションのタイムアウト値を使用します。 デフォルトで、ネットワーク上で複数の CLI ベース セッションに対して 5 つまでの同時暗号化 SSH 接続が可能です（セッション 0 ～ 4）。実行シェルの開始後、CLI ベース セッションのタイムアウト値がデフォルトの 10 分に戻ります。
ステップ 4	`Router (config)# ip ssh authentication-retries number`	クライアントがサーバの再認証を受けられる回数を指定します。デフォルトは 3 です。範囲は 0 ～ 5 です。
ステップ 5	`Router (config)# end`	特権 EXEC モードに戻ります。

ステップ 6	`Router # show ip ssh`
	
	または
	
	`Router # show ssh`
		使用している SSH サーバのバージョンおよび設定情報を表示します。
		
		ML シリーズ カードの SSH サーバの接続ステータスを表示します。

ステップ 7	`Router # copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

デフォルトの SSH 制御パラメータに戻すには、**no ip ssh** {**timeout** | **authentication-retries**} 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。

SSH 設定およびステータスの表示

SSH サーバの設定とステータスを表示するには、表 19-1 に示す 1 つまたは複数のイネーブル EXEC コマンドを使用します。

表 19-1　SSH 設定およびステータスを表示するコマンド

コマンドの説明	目的
`show ip ssh`	SSH サーバのバージョンおよび設定情報を表示します。
`show ssh`	SSH サーバのステータスを表示します。

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference, Cisco IOS Release 12.2*』の「Other Security Features」の章にある「Secure Shell Commands」を参照してください。次の URL にあります。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/fothercr.htm

ML シリーズ カード上の RADIUS

RADIUS は、無許可アクセスに対してネットワークをセキュリティ保護する分散型クライアント / サーバ システムです。クライアントは、中央 RADIUS サーバに認証要求を送信します。これには、すべてのユーザ認証およびネットワーク サービス アクセス情報が含まれています。RADIUS ホストは、通常 Cisco や他のソフトウェア プロバイダーから RADIUS サーバ ソフトウェアを実行するマルチユーザ システム です。

ONS 15454、ONS 15454 SDH、ONS 15327、ONS 15310-CL、ONS 15600 など、多くの Cisco 製品で RADIUS がサポートされています。ML シリーズ カードでも、RADIUS をサポートしています。

ML シリーズ カードは、RADIUS リレー モードまたは RADIUS スタンド アロン モード（デフォルト）のいずれかで動作できます。いずれのモードでも、ML シリーズ カードからの RADIUS メッセージは、ONS ノードの管理に使用される Data Communication Network（DCN; データ通信ネットワーク）上にある RADIUS サーバに渡されます。

RADIUS リレー モード

RADIUS リレー モードでは、ML シリーズ カードの RADIUS は CTC または TL1 によって設定され、ML シリーズ カードを含む ONS 15454 または ONS 15454 SDH ノードの AAA/RADIUS 機能を使用します。RADIUS リレー モードと RADIUS スタンドアロン モードとの間の相互作用はありません。ONS ノード セキュリティの詳細については、ONS ノードのリファレンス マニュアルにある「Security」の章を参照してください。

RADIUS リレー モードで動作している ML シリーズ カードは、クライアントとして RADIUS エントリに指定する必要がありません。RADIUS サーバは、ML シリーズ カードのプロキシとして ONS ノードのクライアント エントリを使用します。

リレー モードをイネーブルにすると、AAA/RADIUS を設定するのに使用される Cisco IOS CLI コマンドがディセーブルになります。ユーザは、AAA/RADIUS に関連しない Cisco IOS CLI コマンドはそのまま使用できます。

リレー モードでは、ML シリーズ カードは、実際にはアクティブな Timing, Communications, and Control カード（TCC2/TCC2P）の内部 IP アドレスである IP アドレスに RADIUS サーバ ホストが表示されます。ML シリーズ カードが実際に RADIUS パケットをこの内部アドレスに送信すると、TCC2/TCC2P が RADIUS パケット 宛先を RADIUS サーバの実際の IP アドレスに変換します。スタンドアロン モードでは、ML シリーズ カードが RADIUS サーバの実際の IP アドレスを表示します。

複数の RADIUS サーバ ホストを使用した ML シリーズ カードがリレー モードの場合、ML シリーズ カード IOS CLI の **show run** 出力もアクティブな TCC2/TCCP カードの内部 IP アドレスを表示します。単一の IP アドレスで複数のホストを表しているので、個々のホストを識別するために異なるポート番号と IP アドレスがペアになっています。1860 ～ 1869 のポートには各認証サーバ ホストが設定されていて、1870 ～ 1879 のポートには各アカウンティング サーバ ホストが設定されています。

IP アドレスの 1 つは、CTC で示されるホスト IP アドレスとは一致しません。CTC では RADIUS サーバ ホストの実際のアドレスを使用しているためです。これらの実際の同一 IP アドレスは、ML シリーズ カードがスタンドアロン モードのときに、ML シリーズ カード IOS CLI **show run** 出力で表示されます。

（注）　ユーザは、認証またはアカウンティング アプリケーションのいずれかに対して最大で 10 のサーバを設定でき、1 つのサーバ ホストで認証アプリケーションとアカウンティング アプリケーションの両方を実行できます。

RADIUS リレー モードの設定

この機能は、CTC または TL1 でオンにします。CTC を使用して RADIUS リレー モードをイネーブルにするには、ML シリーズ カードのカードレベル ビューで、**Enable RADIUS Relay** チェック ボックスをオンにして、**Apply** をクリックします。ユーザは、Superuser レベルでログインしてこのタスクを完了する必要があります。

TL1 を使用してこれをイネーブルにするには、『*Cisco ONS SONET TL1 Command Guide*』を参照してください。

注意　ML シリーズ カードを RADIUS リレー モードに切り替えると、Cisco IOS コンフィギュレーション ファイルの AAA/RADIUS に関連した設定が消去されます。クリアされた AAA/RADIUS 設定は、ML シリーズ カードがスタンドアロン モードに戻った場合でも Cisco IOS コンフィギュレーション ファイルに復元されません。

注意　ML シリーズ カードがリレー モードのときに Cisco IOS コマンド **copy running-config startup-config** **を使用しないでください。このコマンドは、RADIUS リレーがイネーブルの Cisco IOS コンフィギュレーション ファイルを保存します。リブート時に、CTC の** Enable RADIUS Relay **チェック ボックスがオンになっていなくても、ML シリーズ カードが RADIUS リレー モードで起動します。このような状態が発生した場合、ユーザは Enable RADIUS Relay** チェック ボックスをオンにして **Apply** をクリックしてから、**Enable RADIUS Relay** チェック ボックスをオフにして **Apply** をクリックします。これを行うと、ML シリーズ カードがスタンドアロン モードに設定されて、ML シリーズ カードの設定から RADIUS リレーがクリアされます。

RADIUS スタンドアロン モード

スタンドアロン モードでは、ML シリーズ カードの RADIUS は、Cisco Catalyst スイッチの RADIUS と同じ一般的な方法で Cisco IOS CLI を使用して設定されます。

ここでは、ML シリーズ カードで RADIUS スタンドアロン モードのイネーブルおよび設定方法について説明します。スタンドアロン モードの RADIUS は、AAA 経由で機能し、AAA コマンドでイネーブルになります。

（注）　この章ではこれ以降、RADIUS とは、ML シリーズ カードがスタンドアロン モードのときに利用可能な Cisco IOS RADIUS のことを指します。RADIUS リレー モードのことは指しません。

（注）　ここで使用されている全構文と使用方法の情報については、『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

ここでは、以下の設定情報について説明します。

RADIUS の概要

RADIUS サーバによってアクセス コントロールされるユーザが ML シリーズ カードにログインして認証を受けようとする場合に、次のイベントが発生します。

1. ユーザはユーザ名やパスワードを入力するように求められます。
2. ユーザ名と暗号化されたパスワードがネットワークを通じて RADIUS サーバへ送信されます。
3. ユーザは RADIUS サーバから以下のいずれかの応答を受信します。
   a. ACCEPT — ユーザが認証されます。
   b. REJECT — ユーザが認証されずにユーザ名とパスワードの再入力を求められるか、アクセスが拒否されました。

ACCEPT および REJECT 応答には、イネーブル EXEC またはネットワーク許可で使用される追加データが付いています。RADIUS がイネーブルの場合に、ユーザは RADIUS 許可の前にまず RADIUS 認証を正常に完了させる必要があります。ACCEPT および REJECT パケットに含まれる追加データには、以下の項目があります。

- Telnet、SSH、rlogin、およびイネーブル EXEC サービス
- ホストまたはクライアント IP アドレスなどの接続パラメータ、アクセス リスト、およびユーザ タイムアウト

RADIUS の設定

ここでは、RADIUS をサポートするように ML シリーズ カードを設定する方法について説明します。少なくとも、RADIUS サーバ ソフトウェアが稼働するホスト（複数可）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。また認証を行うインターフェイスに方式リストを定義する必要があります。ML シリーズ カードの場合、これは vty ポートです。任意で RADIUS 許可およびアカウンティングの方式リストを定義することもできます。

ML シリーズ カードに RADIUS 機能を設定する前に、RADIUS サーバにアクセスして設定を行う必要があります。

ここでは、以下の設定情報について説明します。

- RADIUS のデフォルト設定（p.19-10）
- RADIUS サーバ ホストの特定（p.19-10）（必須）
- AAA ログイン認証の設定（p.19-13）（必須）
- AAA サーバ グループの定義（p.19-15）（任意）
- ユーザ イネーブル アクセスおよびネットワーク サービス用の RADIUS 許可の設定（p.19-17）（任意）
- RADIUS アカウンティングの開始（p.19-18）（任意）
- RADIUS パケット内の nas-ip-address の設定（p.19-19）（任意）
- すべての RADIUS サーバに対する設定（p.19-20）（任意）
- ベンダー固有の RADIUS 属性用の ML シリーズ カードの設定（p.19-20）（任意）
- ベンダー固有の RADIUS サーバ通信用の ML シリーズ カードの設定（p.19-22）（任意）

RADIUS のデフォルト設定

RADIUS と AAA は、デフォルトで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使用して RADIUS を設定することはできません。RADIUS は、イネーブルに設定されている場合 Cisco IOS CLI を使用して、ML シリーズ カードにアクセスするユーザを認証できます。

RADIUS サーバ ホストの特定

ML シリーズ カードと RADIUS サーバ間の通信には、次の要素が含まれています。

- ホスト名または IP アドレス
- 認証宛先ポート
- アカウンティング宛先ポート
- キー文字列
- タイムアウト時間
- 再送信値

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 ポート番号で識別されます。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識別子が作成され、特定の AAA サービスを提供する RADIUS ホストとしてさまざまなポートを個別に定義できます。この一意の識別子によって、サーバ上の複数の UDP ポートに同じ IP アドレスで RADIUS 要求を送信できるようになります。

同一の RADIUS サーバ上の 2 つの異なるホスト エントリが同じサービス（たとえば、アカウンティング）を設定している場合、設定された 2 番めのホスト エントリは、最初のエントリのフェールオーバー バックアップとして機能します。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い場合は、ML シリーズ カードは、同じ装置上に設定された 2 番めのホスト エントリでアカウンティング サービスを試行します。

AAA セキュリティ コマンドを使用するように RADIUS を設定するには、RADIUS サーバ デーモンが稼働するホストと、その ML シリーズ カードと共有するシークレット（鍵）文字列を指定する必要があります。RADIUS サーバ、ONS ノード、および ML シリーズ カードは、共有するシークレッ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。システムでは、ML シリーズ カードの共有シークレット鍵が NE の共有シークレット鍵と一致することを保証しています。

（注）　スイッチにグローバルおよびサーバ単位の両方の機能（タイムアウト、再送信回数、および キー コマンド）を設定すると、サーバ単位のタイマー、再送信回数、および キー値コマンドは、グローバルのタイマー、再送信回数、および キー値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には、「すべての RADIUS サーバに対する設定」（p.19-20）を参照してください。

（注）　再送信回数およびタイムアウト時間値は、スタンドアロン モードの ML シリーズ カードに設定されます。これらの値は、リレー モードの ML シリーズ カードには設定できません。

認証用に既存のサーバ ホストをグループ化するために、AAA サーバ グループを使用するように ML シリーズ カードを設定できます。詳細については、「AAA サーバ グループの定義」（p.19-15）を参照してください。

サーバ単位での RADIUS サーバ通信を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンドの説明	目的
ステップ 1	`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 2	`Router (config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	**Router (config)# radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、RADIUS サーバが応答するのを待ってスイッチが再送信するまでの時間を指定します。この範囲は 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 コマンド設定を上書きします。**radius-server host** コマンドでタイムアウトが設定されていない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しないか、応答が遅い場合に、RADIUS 要求をそのサーバに再送信する回数を指定します。この範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信値が設定されていない場合は、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、スイッチと RADIUS サーバ上で稼働する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。 **（注）** 鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要のある文字列です。鍵は、必ず **radius-server host** コマンドの最後の項目として設定します。先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。 1 つの IP アドレスに関連付けられた複数のホスト エントリをスイッチが認識するように設定するには、必要な回数だけこのコマンドを入力し、それぞれの UDP ポート番号が必ず異なるようにしてください。スイッチ ソフトウェアは、指定された順序でホストを検索します。特定の RADIUS ホストで使用するタイムアウト、再送信回数、および暗号化鍵の値を設定します。
ステップ 4	`Router (config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Router# show running-config`	エントリを確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

特定の RADIUS サーバを削除するには、**no radius-server host** *hostname* | *ip-address* 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。

次の例では、ある RADIUS サーバを認証用に、別の RADIUS サーバをアカウンティング用に設定する方法を示します。

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次の例では、RADIUS サーバとして *host1* を設定し、認証およびアカウンティングの両方にデフォルト ポートを使用する方法を示します。

```
Switch(config)# radius-server host host1
```

（注）　さらに、RADIUS サーバでいくつかの設定を行う必要があります。この設定とは、スイッチの IP アドレス、およびサーバとスイッチで共有するキー文字列です。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。

AAA ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義してから、さまざまな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、*default* という名前の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が明示的に定義されたポートを除いて、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順序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方式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すまで続きます。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 ログインの詳細については、『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Authentication, Authorization, and Accounting（AAA）」の章を参照してください。次の URL にあります。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

ログイン認証を設定にするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンドの説明	目的
ステップ 1	`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 2	`Router (config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	`Router (config)# aaa authentication login {default | list-name} method1 [method2...]`	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定されていない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。 次のいずれかの方式を選択します。 — **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、**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 パスワードをあらかじめ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、RADIUS サーバをあらかじめ設定しておく必要があります。詳細については、「RADIUS サーバ ホストの特定」（p.19-10）を参照してください。 — **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、回線パスワードをあらかじめ設定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** *name* **password** グローバル コンフィギュレーション コマンドを使用します。 — **local-case** — 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、データベースにユーザ名情報を入力する必要があります。 — **none** — ログインに認証を使用しません。
ステップ 4	`Router (config)# line [console | tty | vty] line-number [ending-line-number]`	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。

	コマンドの説明	目的
ステップ 5	`Router (config-line)# login authentication {default | list-name}`	回線または回線セットに対して、認証リストを適用します。 • **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。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを使用します。
ステップ 6	`Router (config)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Router# show running-config`	エントリを確認します。
ステップ 8	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 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。ログイン用の RADIUS 認証をディセーブルにするかデフォルト値に戻す場合は、**no login authentication** {**default** | *list-name*} ライン コンフィギュレーション コマンドを使用します。

AAA サーバ グループの定義

認証用に既存のサーバ ホストをグループ化するために、AAA サーバ グループを使用するように ML シリーズ カードを設定できます。設定済みサーバ ホストのサブセットを選択し、特定のサービスに使用できます。サーバ グループには、グローバル サーバ ホスト リストを使用します。このリストは、選択したサーバ ホストの IP アドレスのリストです。

サーバ グループには、各エントリが一意の識別子（IP アドレスと UDP ポート番号の組み合わせ）を持っていれば、同じサーバに対して複数のホスト エントリを組み込むことができます。また、アカウンティングなどの特定の AAA サービスを提供する RADIUS ホストとして、さまざまなポートを個別に定義できます。同じサービスに対して、同一 RADIUS サーバ上に 2 つの異なるホスト エントリを設定すると、設定された 2 番めのホスト エントリは、最初のエントリのフェールオーバー バックアップとして機能します。

定義済みのグループ サーバに特定のサーバを対応付けるには、**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。IP アドレスでサーバを特定したり、任意の **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識別することもできます。

AAA サーバ グループを定義してそれを特定の RADIUS サーバに対応付けるには、特権 EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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 2	`Router (config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	`Router (config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]`	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、RADIUS サーバが応答するのを待ってスイッチが再送信するまでの時間を指定します。この範囲は 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 コマンド設定を上書きします。**radius-server host** コマンドでタイムアウトが設定されていない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しないか、応答が遅い場合に、RADIUS 要求をそのサーバに再送信する回数を指定します。この範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信値が設定されていない場合は、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、スイッチと RADIUS サーバ上で稼働する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。 **（注）** 鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要のある文字列です。鍵は、必ず **radius-server host** コマンドの最後の項目として設定します。先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。 1 つの IP アドレスに関連付けられた複数のホスト エントリをスイッチが認識するように設定するには、必要な回数だけこのコマンドを入力し、それぞれの UDP ポート番号が必ず異なるようにしてください。スイッチ ソフトウェアは、指定された順序でホストを検索します。特定の RADIUS ホストで使用するタイムアウト、再送信回数、および暗号化鍵の値を設定します。
ステップ 4	`Router (config)# aaa group server radius group-name`	グループ名で AAA サーバ グループを定義します。 このコマンドによって、ML シリーズ カードはサーバ グループ コンフィギュレーション モードになります。
ステップ 5	`Router (config-sg-radius)# server ip-address`	特定の RADIUS サーバを定義済みサーバ グループに対応付けます。AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。

	コマンドの説明	目的
ステップ 6	`Router (config-sg-radius)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Router # show running-config`	エントリを確認します。
ステップ 8	`Router # copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「AAA ログイン認証の設定」（p.19-13）を参照してください。

特定の RADIUS サーバを削除するには、**no radius-server host** *hostname* | *ip-address* 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。コンフィギュレーション リストからサーバ グループを削除するには、**no aaa group server radius** *group-name* 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 サーバ の IP アドレスを削除するには、**no server** *ip-address* サーバ グループ コンフィギュレーション コマンドを使用します。

この例では、ML シリーズ カードが、2 つの異なる RADIUS グループ サーバ（*group1* と *group2*）を認識するように設定されます。group1 では、同一の RADIUS サーバ上の 2 つの異なるホスト エントリに同じサービスを設定しています。2 番めのホスト エントリは、最初のエントリのフェールオーバー バックアップとして機能します。

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

ユーザ イネーブル アクセスおよびネットワーク サービス用の RADIUS 許可の設定

AAA 許可は、ユーザが利用できるサービスを制限します。AAA 許可がイネーブルに設定されていると、ML シリーズ カードはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、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許可されます。

ML シリーズ カードでのイネーブル レベルの設定または **priv-lvl** コマンドの使用は、サポートされていません。RADIUS サーバで認証されたユーザは、デフォルトのログイン権限レベルであるイネーブル モード 1 でのみ ML シリーズ カードにアクセスできます。このため、RADIUS サーバに設定されている priv-lvl は、priv-lvl 0 または 1 になります。ユーザが認証されて ML シリーズ カードへのアクセスが許可されると、イネーブル パスワードを使用してイネーブル EXEC 認証を得ることができ、権限レベル 15 のスーパーユーザになることができます。これは、イネーブル モードのデフォルトの権限レベルです。

この ML シリーズ カード ユーザ レコードの例は、RADIUS サーバからの出力で、権限レベルを示しています。

```
CISCO15 Auth-Type := Local, User-Password == "otbu+1"
Service-Type = Login,
Session-Timeout = 100000,
Cisco-AVPair = "shell:priv-lvl=1"
```

aaa authorization グローバル コンフィギュレーション コマンドに **radius** キーワードを付けて使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを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、以下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、イネーブル EXEC アクセス許可に RADIUS を使用します。
- 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。

（注）　許可が設定されていても、CLI 経由でログインして認証されたユーザに対して、許可が省略されます。

イネーブル EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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 2	`Router (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するユーザ RADIUS 許可を ML シリーズ カードに設定します。
ステップ 3	`Router (config)# aaa authorization exec radius`	イネーブル EXEC アクセスの有無を、ユーザ RADIUS 許可によって判別するように ML シリーズ カードを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）を返すことができます。
ステップ 4	`Router (config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Router# show running-config`	エントリを確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* 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 アカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスしているサービスと、ユーザが消費しているネットワーク リソースを追跡します。AAA アカウンティングがイネーブルに設定されていると、ML シリーズ カードは、アカウンティング レコードの形式でユーザの活動状況を RADIUS セキュリティ サーバにレポートします。各アカウンティング レコードには、アカウンティングの Attribute-Value（AV）のペアが含まれ、セキュリティ サーバ上に保存されます。このデータを分析し、ネットワーク管理、クライアントへの課金、または監査に利用できます。

各 Cisco IOS 権限レベルおよびネットワーク サービスに関する RADIUS アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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 2	`Router (config)# aaa accounting network start-stop radius`	ネットワーク関連のすべてのサービス要求に関する RADIUS アカウンティングをイネーブルにします。
ステップ 3	`Router (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、イネーブル EXEC プロセスの開始時に記録開始アカウンティング通知を送信し、終了時に記録停止通知を送信します。
ステップ 4	`Router (config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Router# show running-config`	エントリを確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} **start-stop** *method1...* 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 パケット内の nas-ip-address の設定

RADIUS リレー モードの ML シリーズ カードを使用すると、ユーザは各 ML シリーズ カードに対して個別の nas-ip-address を設定できます。RADIUS スタンドアロン モードでは、このコマンドは Cisco IOS CLI に隠されています。これにより、RADIUS サーバが同一 ONS ノード内の ML シリーズ カードを個別に識別できます。サーバに要求を送信した特定の ML シリーズ カードを識別できると、サーバのデバッグ時に便利です。nas-ip-address は、主に RADIUS 認証およびアカウンティング要求の検証に使用されます。

この値が設定されていない場合、nas-ip-address は、**ip radius-source** コマンドで設定された値を使用して通常の Cisco IOS メカニズムによって設定されます。値が設定されていない場合は、サーバへルーティング可能な最良の IP アドレスが使用されます。ルーティング可能なアドレスを使用できない場合は、サーバの IP アドレスが使用されます。

nas-ip-address を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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 2	`Router (config)# [no] ip radius nas-ip-address` {*hostname* | *ip-address*}	RADIUS パケット内にある属性 4（nas-ip-address）の IP アドレスまたはホスト名を指定します。 ONS ノードに ML シリーズ カードが 1 つしかない場合は、このコマンドを使用するメリットはありません。ONS ノードのパブリック IP アドレスは、サーバに送信される RADIUS パケット内の nas-ip-address として機能します。
ステップ 3	`Router (config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show running-config`	エントリを確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

すべての RADIUS サーバに対する設定

ML シリーズ カードとすべての RADIUS サーバ間のグローバル通信設定を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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 2	`Router (config)# radius-server key` *string*	ML シリーズ カードとすべての RADIUS サーバとの間で使用する、共有シークレット文字列を指定します。 （注）　鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要のある文字列です。先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。
ステップ 3	`Router (config)# radius-server retransmit` *retries*	ML シリーズ カードが、サーバに各 RADIUS 要求を送信する回数を指定します。デフォルトは 3 で、指定できる範囲は 1 ～ 1000 です。
ステップ 4	`Router (config)# radius-server timeout` *seconds*	ML シリーズ カードが、RADIUS 要求に対する応答を待って要求を再送信するまでの秒数を指定します。デフォルトは 5 秒で、指定できる範囲は 1 ～ 1000 です。
ステップ 5	`Router (config)# radius-server deadtime` *minutes*	認証要求への応答に失敗した RADIUS サーバに [dead] とマーキングするまでの分数を指定します。[dead] としてマーキングされている RADIUS サーバは、指定した *分数*の間追加の認証要求をスキップされます。これにより、要求がタイムアウトするまで待たずに、次の設定サーバを試行できます。すべての RADIUS サーバが [dead] としてマーキングされている場合、スキップは行われません。 デフォルト は 0 で、指定できる範囲は 0 ～ 1440 分です。
ステップ 6	`Router (config)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Router# show running-config`	エントリを確認します。
ステップ 8	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

再送信、タイムアウト、デッドタイムの設定をデフォルトに戻すには、これらのコマンドの **no** 形式を使用します。

ベンダー固有の RADIUS 属性用の ML シリーズ カードの設定

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト規格では、VSA（Vendor-Specific Attribute; ベンダー固有属性）（属性 26）を使用して、ML シリーズカードと RADIUS サーバとの間のベンダー固有情報の通信方式を定めています。VSA を使用すると、ベンダーは、汎用に適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装では、仕様で推奨された形式を使用して 1 つのベンダー固有オプションをサポートします。シスコのベンダー ID は 9 で、サポート対象のオプションにはベンダータイプ 1 が設定されており、*cisco-avpair* と名前が付けられています。この値は次の形式の文字列です。

```
protocol : attribute sep value *
```

protocol は、特定のタイプの許可に対応する シスコ プロトコル属性です。*attribute* と *value* は、シスコ Terminal Access Controller Access Control System Plus（TACACS+）仕様で定義されている適切な AV のペアです。*sep* は、必須属性の場合は =、任意属性の場合は * です。TACACS+ 許可で利用できるすべての機能は、RADIUS にも使用できます。

たとえば、次の AV ペアは、IP 許可時（PPP［ポイントツーポイント プロトコル］の Internet Protocol Control Protocol [IPCP] アドレス割り当て時）に、シスコの *複数の名前付き IP アドレス プール*機能をアクティブにします。

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

次の例では、RADIUS サーバ データベース内の許可 VLAN を指定する方法を示します。

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-ID(#81)=vlanid"
```

次の例では、この接続中に ASCII 形式の入力 Access Control List（ACL; アクセス コントロール リスト）をインターフェイスに適用する方法を示します。

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

次の例では、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する方法を示します。

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

その他のベンダーにも、独自に一意のベンダー ID、オプション、および対応する VSA が割り当てられます。ベンダー ID と 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。

VSA を認識して使用するように ML シリーズ カードを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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 2	`Router (config)# radius-server vsa send [accounting | authentication]`	ML シリーズ カードが、RADIUS IETF 属性 26 に定義されている VSA を認識して使用できるようにします。 • （任意）**accounting** キーワードを使用して、認識される VSA の集合をアカウンティング属性のみに限定します。 • （任意）**authentication** キーワードを使用して、認識されるベンダー固有の属性の集合を認証属性に限定します。 キーワードなしでこのコマンドを入力すると、アカウンティングおよび認証の 両方の VSA が使用されます。 AAA サーバは、ML シリーズ カードの VSA 応答メッセージに認証レベルを含めます。
ステップ 3	`Router (config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Router# show running-config`	エントリを確認します。
ステップ 5	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

RADIUS 属性の完全リスト、またはベンダー固有の属性 26 の詳細については、『*Cisco IOS Security Configuration Guide*』Release 12.2 の付録「RADIUS Attributes」を参照してください。

ベンダー固有の RADIUS サーバ通信用の ML シリーズ カードの設定

RADIUS に関する IETF ドラフト規格では、ML シリーズ カードと RADIUS サーバとの間のベンダー固有情報の通信方式を規定していますが、一部のベンダーは、固有の方法で RADIUS 属性の集合を機能拡張しています。Cisco IOS ソフトウェアは、ベンダー固有仕様の RADIUS 属性のサブセットをサポートします。

前述したように、RADIUS（ベンダー固有または IETF のドラフト準拠）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、および ML シリーズ カードと共有するシークレット文字列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文字列を指定するには、**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。

ベンダー固有の RADIUS サーバ ホスト、および共有シークレット文字列を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	`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 2	**Router (config)# radius-server host** {*hostname* | *ip-address*} **non-standard**	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、ベンダー固有の RADIUS 実装を使用していることを明確にします。
ステップ 3	**Router (config)# radius-server key** *string*	ML シリーズ カードとベンダー固有の RADIUS サーバとの間で使用する、共有シークレット文字列を指定します。ML シリーズ カードおよび RADIUS サーバは、この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。 **（注）** 鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要のある文字列です。先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。
ステップ 4	`Router (config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Router# show running-config`	エントリを確認します。
ステップ 6	`Router# copy running-config startup-config`	（任意）コンフィギュレーション ファイルにエントリを保存します。

ベンダー固有の RADIUS ホストを削除するには、**no radius-server host** {*hostname* | *ip-address*} **non-standard** 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。鍵をディセーブルにするには、**no radius-server key** 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。

次の例では、ベンダー固有の RADIUS ホストを指定して、ML シリーズ カードとサーバの間で *rad124* という秘密鍵を使用する方法を示します。

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

RADIUS 設定の表示

RADIUS 設定を表示するには、**show running-config** イネーブル EXEC コマンドを使用します。