APPENDIX A

AAA プロトコル

ここでは、次の内容について説明します。

一般的な使用例

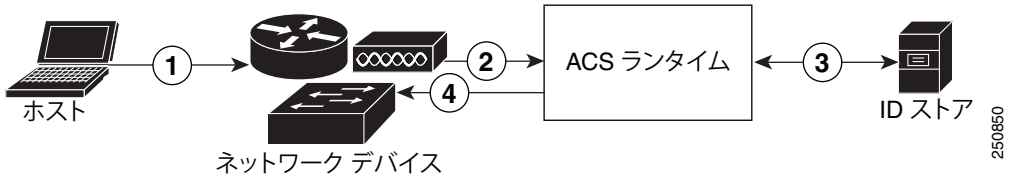
ここでは、次の内容について説明します。

デバイス管理（TACACS+）

図 A-1 に、デバイス管理に関するフローを示します。次の 2 つの主要なトリガーがあります。

- 「セッション アクセス要求（デバイス管理 [TACACS+]）」（P.A-2）。
- 「コマンド認可要求」（P.A-2）。

図 A-1　　デバイス管理フロー



セッション アクセス要求（デバイス管理 [TACACS+]）

（注）　番号は、図 A-1（P.A-1）に対応しています。

セッション要求の処理手順は、次のとおりです。

1. 管理者がネットワーク デバイスにログインします。
2. ネットワーク デバイスによって、TACACS+ アクセス要求が ACS に送信されます。
3. ACS は、ID ストアを使用してユーザのクレデンシャルを確認します。
4. ACS は、決定を適用するネットワーク デバイスに、TACACS+ 応答を送信します。応答には、セッション中の管理者アクセスのレベルを決定する特権レベルなどのパラメータが含まれています。

コマンド認可要求

（注）　番号は、図 A-1（P.A-1）に対応しています。

コマンド認可の処理手順は、次のとおりです。

1. 管理者が、ネットワーク デバイスでコマンドを発行します。
2. ネットワーク デバイスによって、TACACS+ アクセス要求が ACS に送信されます。
3. 任意の設定により、ACS では、ID ストアを使用して、ポリシー処理に含めるユーザ属性を取得します。
4. TACACS+ 応答は、管理者にコマンドの発行が認可されているかどうかを示します。

ネットワーク アクセス（EAP 使用および未使用の RADIUS）

ネットワーク アクセスでは、ホストはネットワーク デバイスに接続し、ネットワーク リソースの使用を要求します。ネットワーク デバイスは、新しく接続されたホストを識別し、転送方式として RADIUS プロトコルを使用して、ユーザの認証および認可を ACS に要求します。

ACS 5.4 では、RADIUS プロトコルを使用して転送されるプロトコルに応じて、次のカテゴリのネットワーク アクセス フローがサポートされます。

- EAP を含まない RADIUS ベースのプロトコル。
  - PAP
  - CHAP
  - MSCHAPv1
  - MSCHAPv2

  EAP を含まない RADIUS ベースのプロトコルの詳細については、「EAP 認証を使用しない RADIUS ベースのフロー」（P.A-3）を参照してください。
- RADIUS を使用して転送される EAP プロトコル ファミリ。さらに次のように分類できます。
  - 証明書を使用しない単純な EAP プロトコル。

    EAP-MD5

LEAP

- TLS ハンドシェイクを含み、クライアントが ACS サーバ証明書を使用してサーバ認証を実行する EAP プロトコル。

  PEAP。内部方式 PEAP/EAP-MSCHAPv2 および PEAP/EAP-GTC のいずれかを使用します。

  EAP-FAST。内部方式 EAP-FAST/EAP-MSCHAPv2 および EAP-FAST/EAP-GTC のいずれかを使用します。

- 完全に証明書ベースの EAP プロトコル。このプロトコルでは、TLS ハンドシェイクによってサーバ認証とクライアント認証の両方に証明書が使用されます。

  EAP-TLS

  内部方式 EAP-TLS を含む PEAP

EAP 認証を使用する RADIUS ベースのフローの詳細については、「EAP 認証を使用する RADIUS ベースのフロー」（P.A-3）を参照してください。

EAP 認証を使用しない RADIUS ベースのフロー

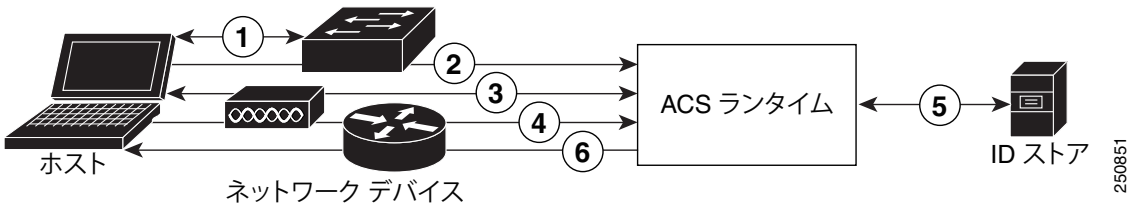
この項では、EAP 認証を使用しない RADIUS ベースのワークフローについて説明します。

PAP 認証を使用する RADIUS の処理手順は、次のとおりです。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスは、RADIUS Access-Request を ACS に送信します。使用されている特定のプロトコル（PAP、CHAP、MSCHAPv1、または MSCHAPv2）に適した RADIUS 属性が含まれています。
3. ACS は、ID ストアを使用してユーザのクレデンシャルを確認します。
4. RADIUS 応答（Access-Accept または Access-Reject）が、決定を適用するネットワーク デバイスに送信されます。

図 A-2 に、EAP を使用しない RADIUS ベースの認証を示します。

図 A-2　EAP 認証を使用しない RADIUS ベースのフロー



EAP 認証を使用する RADIUS ベースのフロー

EAP には、さまざまな認証タイプをサポートする拡張フレームワークがあります。これらのフレームワークの中で、ACS によってサポートされている具体的な EAP 方式は次のとおりです。

- 証明書を使用しない単純な EAP 方式
  - EAP-MD5
  - LEAP
- クライアントが ACS サーバ証明書を使用してサーバ認証を実行する EAP 方式
  - PEAP/EAP-MSCHAPv2

  - PEAP/EAP-GTC
  - EAP-FAST/EAP-MSCHAPv2
  - EAP-FAST/EAP-GTC
- サーバ認証とクライアント認証の両方に証明書を使用する EAP 方式
  - EAP-TLS
  - PEAP/EAP-TLS

認証プロセスで EAP が使用される場合は常に、具体的にどの EAP 方式（および該当する場合は内部方式）を使用する必要があるかを決定するネゴシエーション フェーズが先行します。

すべての EAP 認証で、次の処理が実行されます。

1. ホストがネットワーク デバイスに接続します。
2. ネットワーク デバイスが EAP 要求をホストに送信します。
3. ホストは、EAP 応答によって、ネットワーク デバイスに応答します。
4. ネットワーク デバイスは、ホストから受信した EAP 応答を RADIUS Access-Request 内に（EAP-Message RADIUS 属性を使用して）カプセル化し、RADIUS Access-Request を ACS に送信します。
5. ACS は、RADIUS パケットから EAP 応答を抽出して新しい EAP 要求を作成し、この EAP 要求を RADIUS Access-Challenge 内に（この場合も EAP-Message RADIUS 属性を使用して）カプセル化し、ネットワーク デバイスに送信します。
6. ネットワーク デバイスは、EAP 要求を抽出し、ホストへ送信します。

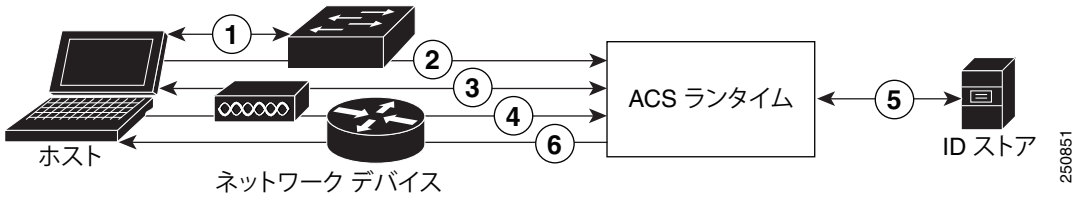
この方法で、ホストと ACS は間接的に EAP メッセージを交換します（EAP メッセージは、RADIUS を使用して転送され、ネットワーク デバイスを介して渡されます）。この方法で交換される EAP メッセージの最初のセットによって、特定の EAP 方式がネゴシエートされます。その後、認証を実行する場合に、この EAP 方式が使用されます。

その後交換される EAP メッセージは、実際の認証の実行に必要なデータを伝送するために使用されます。ネゴシエートされた特定の EAP 認証方式で必要な場合、ACS では ID ストアを使用してユーザのクレデンシャルを確認します。

ACS では、認証が成功か失敗かを決定したあと、EAP-Success または EAP-Failure メッセージを、RADIUS Access-Accept または Access-Reject メッセージ内にカプセル化された状態で、ネットワーク デバイスに（最終的にはホストにも）送信します。

図 A-3 に、EAP を使用する RADIUS ベースの認証を示します。

図 A-3　EAP を使用する RADIUS ベースの認証



ACS 5.4 の経験に影響する可能性のある既知のサプリカントの問題のリストについては、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/release/notes/acs_54_rn.html

アクセス プロトコル：TACACS+ および RADIUS

ここでは、次の内容について説明します。

ACS 5.4 は、TACACS+ アクセス プロトコルと RADIUS アクセス プロトコルを使用できます。表 A-1 に、この 2 つのプロトコルの比較を示します。

表 A-1　TACACS+ プロトコルと RADIUS プロトコルの比較

比較項目	TACACS+	RADIUS
伝送プロトコル	TCP：コネクション型トランスポート層プロトコル、信頼性の高い全二重データ伝送。	UDP：コネクションレス型トランスポート層プロトコル、確認応答も配送保証もないデータグラム交換。UDP は、IP を使用してデータ ユニット（データグラムと呼ばれる）をコンピュータ間で移動します。
使用ポート	49	認証および認可：1645 および 1812。 アカウンティング：1646 および 1813。
暗号化	完全なパケット本体の暗号化。	16 バイト以下のパスワードにかぎり、暗号化する。
AAA アーキテクチャ	認証、許可、アカウンティングの各サービスを独立制御。	認証および認可が 1 つのサービスとして統合されている。
利用目的	デバイスの管理。	ユーザ アクセスの制御。

TACACS+ の概要

ネットワーク デバイスがシスコ デバイス管理アプリケーション、アクセス サーバ、ルータ、またはファイアウォールである場合は、TACACS+ を使用する必要があります。ACS 5.4 は、TACACS+ プロトコルで IPv6 アドレスをサポートします。ACS 5.4 では、管理アプリケーションを使用して管理対象ネットワーク デバイスを設定するネットワーク ユーザに対してコマンド認可を提供することにより、シスコ デバイス管理アプリケーションをサポートします。

認可に ACS を使用するように設定されている各管理アプリケーション対して、固有のコマンド セットを使用することによって、管理アプリケーションのユーザに対するコマンド認可のサポートを実現できます。

ACS 5.4 は、管理アプリケーションとの通信に TACACS+ を使用します。管理アプリケーションが ACS と通信できるようにするには、その管理アプリケーションを、ACS 5.4 に TACACS+ を使用する AAA クライアントとして設定する必要があります。

また、デバイス管理アプリケーションに有効な管理者名とパスワードを与える必要があります。管理アプリケーションが最初に ACS と通信するとき、これらの要件が通信の正当性を保証します。

パケットのヘッダーを除き、クライアントと TACACS+ サーバが通信するすべての情報（パケット本体に含まれている）は、共有秘密情報を使用することによって暗号化されます。共有秘密情報自体は、ネットワークで直接的には送信されません。

さらに、管理アプリケーションが使用する管理者は、Command Set 特権がイネーブルになっている必要があります。

RADIUS の概要

ここでは、次の内容について説明します。

RADIUS は、クライアント/サーバ プロトコルです。リモート アクセス サーバは、このプロトコルを使用して中央サーバと通信してダイヤルイン ユーザを認証し、要求されたシステムまたはサービスへのアクセスを認可します。RADIUS を使用すると、企業は、すべてのリモート サーバが共有できる中央データベースにユーザ プロファイルを保持できます。

このプロトコルはセキュリティを向上させます。企業はこのプロトコルを使用して、単一の管理ネットワーク ポイントで適用されるポリシーを設定できます。

新旧の RFC をサポートするために、ACS 5.4 では認証の要求をポート 1645 およびポート 1812 で受け入れます。アカウンティングについては、ACS ではアカウンティング パケットをポート 1646 および 1813 で受け入れます。

RADIUS VSA

ACS 5.4 には、標準 IETF RADIUS 属性のセットがあります。現在は使用されていない RADIUS IETF 属性は、その名前で識別できます。使用されていない属性には、*attribute-nnn* という形式の名前が付けられています。*attribute* は属性の名前であり、*nnn* は属性の ID です。

また、ACS 5.4 では RADIUS VSA がサポートされています。ACS 5.4 のインストール後、次の事前定義済みの RADIUS VSA のセットを使用できます。

- Cisco
- Cisco VPN 5000
- Microsoft
- US Robotics
- Ascend
- Nortel（Bay Networks）
- RedCreek
- Juniper
- Cisco VPN 3000
- Cisco Business Service Management（BSM）
- Cisco Aironet
- Cisco Airespace

これらの事前定義済みの RADIUS VSA を変更するか、または新しい RADIUS VSA を定義できます。RADIUS VSA は、作成、編集、および複製できます。詳細については、「RADIUS ベンダー固有属性の作成、複製、および編集」（P.18-6）を参照してください。

AAA サーバとしての ACS 5.4

AAA サーバは、コンピュータ リソースへのユーザのアクセス要求を処理するサーバ プログラムであり、企業に対して AAA サービスを提供します。一般的に、AAA サーバは、ネットワーク アクセス サーバおよびゲートウェイ サーバ、ユーザ情報を格納するデータベースおよびディレクトリと連携動作します。現在、デバイスまたはアプリケーションと AAA サーバとの通信に使用されている標準は、RADIUS です。

ACS 5.4 は、1 台以上のネットワーク アクセス デバイス（NAD）の AAA サーバとして機能します。NAD は、ACS サーバのクライアントです。各クライアント NAD で ACS の IP アドレスを指定し、RADIUS プロトコルを使用してユーザ アクセス要求を ACS に送信する必要があります。

RADIUS は、エンドユーザからネットワーク リソースへのアクセスを保護するために、広く一般に使用されています。RADIUS サーバは、他の RADIUS サーバまたは他の種類の認証サーバへのプロキシとして動作できます。

NAD は、ネットワークのゲートキーパーとして機能し、ユーザの代理として Access-Request を ACS に送信します。ACS は、内部 ID ストアを使用するか、外部で設定された LDAP または Windows Active Directory ID ストアを使用して、ユーザ名、パスワード、および必要に応じてその他のデータを確認します。

ACS は、最終的に NAD に対して、Access-Reject メッセージまたは一連の認可属性を含む Access-Accept メッセージによって応答します。

ACS 5.4 では、UDP を使用したネットワーク転送を実行でき、RADIUS パケット解析および構成、必要なデータの確認、重複要求のトラッキングを含む RADIUS プロトコルが実装されています。

UDP を使用するいくつかの理由を次に示します。

- 処理時間が数秒である。
- クライアントおよびサーバの再起動またはオフライン化に特別な処理を必要としない。
- UDP はコネクションレス型プロトコルである。
- UDP は簡単にマルチスレッド サーバを実装して複数のクライアント要求を処理する。

RADIUS に対して UDP が割り当てるポート番号は、次のとおりです。

- 1812（アクセス要求）
- 1813（アカウンティング）
- 1645（アクセス要求）
- 1646（アカウンティング）

ACS 5.4 は認証システムへの入り口です。ACS は、特定の設定可能な UDP ポートで受信します。ネットワークからデータが着信した場合は、次の処理が実行されます。

1. ACS は、データを RADIUS クライアント要求またはプロキシ応答パケットとして処理しようとします。
2. ACS は、設定に登録されている NAD からパケットが着信したことを確認し、重複したパケット処理を防止します。
3. ACS は、RADIUS パケットを解析し、その内容について必要な確認を実行します。
4. 次に、ACS は処理のためにデータを適切なフローに渡します。
5. システムの応答準備が整うと、ACS では次の処理を実行します。
   a. データ処理の結果を受信します。
   b. クライアントへの対応する応答を作成します。
   c. 応答をネットワークに返します。

ACS 5.4 での RADIUS 属性サポート

ACS 5.4 では、RFC 2865 に記述されているように RADIUS プロトコルがサポートされています。

ACS 5.4 では、次のタイプの RADIUS 属性がサポートされています。

- IETF RADIUS 属性
- 一般的な VSA および Cisco VSA
- 他のベンダーの属性

ACS 5.4 では、RADIUS に対する次の拡張で定義されている属性もサポートされています。

- アカウンティング関連の属性。RFC 2866 で定義されています。
- トンネル プロトコルのサポート。RFC 2867 および 2868 で定義されています。
- EAP のサポート（EAP-Message 属性を使用）。RFC 2869 および 3579 で定義されています。

（注） RADIUS パラメータの参照には、表記法 [*attribute-number*] [*attribute name*] が使用されます。たとえば、[*1*]*User-Name* です。数字と名前は、仕様でパラメータに対して割り当てられている数字と名前に対応します。

RADIUS では、任意の RADIUS 属性の受信、送信、およびディクショナリベースの解析および構築がサポートされています。RADIUS 属性が通常の属性、VSA、または Cisco Attribute-Value（AV; 属性値）のペアのいずれであるかは関係ありません。ACS の RADIUS インターフェイスでは、RFC 2865 で定義されている次の属性データ型がサポートされています。

- *text*（UTF-8）
- *string*（バイナリ）
- *address*（IP）
- *integer*
- *time*

データ型 integer、string、および text の許可される値の列挙（ENUM）指定がサポートされています。属性値は、パケットの解析および構築が実行されるとき、これらに対してチェックされます。

ACS は、RADIUS State 属性（24）を使用して特定のカンバセーションを識別します。各カンバセーションには、固有の ID があります。すべてのカンバセーションは、特定の設定バージョン（カンバセーションが開始された時点で使用可能な最新バージョン）で処理されます。

（注） RADIUS State 属性（24）は、PAP 認証には使用されません。

クライアントと RADIUS サーバ間のすべてのトランザクションでは、各 RADIUS パケット内の Request/Response Authenticator フィールドを使用してメッセージの整合性が保護されます。このフィールドでは共有秘密情報が使用されます。共有秘密情報自体は、ネットワークで直接的には送信されません。

また、カプセル化された EAP-Message 属性が含まれるすべてのパケットを含む、一部の形式の RADIUS パケットでは、さらに、Message-Authenticator RADIUS 属性（これにも、共有秘密情報が使用されます）を使用して、すべての RADIUS 属性の整合性が保護されます。

さらに、クライアントと RADIUS サーバ間で送信される RADIUS パケット内のユーザ パスワードは常に暗号化され、セキュアでないネットワーク上の権限のないユーザがパスワードを簡単に判別できないように保護します。

認証

ACS では、RADIUS を使用して転送されるさまざまな認証プロトコルがサポートされています。EAP を使用しないサポート対象プロトコルは、次のとおりです。

- PAP
- CHAP
- MSCHAPv1
- MSCHAPv2

また、さまざまな EAP ベースのプロトコルを、RADIUS EAP-Message 属性内にカプセル化することによって、RADIUS を使用して転送できます。これらのプロトコルは、証明書を使用するかどうか、およびどの程度使用するかに応じて、より詳細に分類できます。次の作業を行います。

- 証明書を使用しない EAP 方式。
  - EAP-MD5
  - LEAP
- クライアントが ACS サーバ証明書を使用してサーバ認証を実行する EAP 方式
  - PEAP/EAP-MSCHAPv2
  - PEAP/EAP-GTC
  - EAP-FAST/EAP-MSCHAPv2
  - EAP-FAST/EAP-GTC
- サーバ認証とクライアント認証の両方に証明書を使用する EAP 方式
  - EAP-TLS
  - PEAP/EAP-TLS

認可

認可は、設定されているアクセス ポリシーに従って許可されます。

アカウンティング

RADIUS の認証機能または認可機能とは別に、RADIUS プロトコルのアカウンティング機能を使用できます。RADIUS アカウンティング機能の一部を使用して、セッションの開始時および終了時にデータを送信でき、セッション中に使用したリソースの量（時間、パケット、バイトなど）を示すことができます。

ISP では、特別なセキュリティおよび課金の必要性に対応するために、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアを使用する場合があります。

RADIUS 属性の書き換え動作

ACS 5.4 では、追加の RADIUS 属性を定義するか、または既存の属性を更新するオプションがあります。更新された属性は、RADIUS 要求で、RADIUS プロキシ サーバに送信される前に書き換えられます。これらの属性の処理はプロキシ アクセス サービス定義の一部として設定されます。RADIUS 属性の書き換え機能は、RADIUS アクセス要求にのみ有効となり、アカウンティング要求には有効になりません。

RADIUS 属性の書き換え機能により、外部サーバにリダイレクトされるアクセス要求の RADIUS アクセス属性の追加、更新、削除を行えます。属性の処理は、属性動作ステートメントを定義し、プロキシ アクセス サービスの一部として設定されます。

管理者は特定のプロキシ アクセス サービスの属性動作句を設定できます。このサービスが選択されると、ACS はアクセス要求の動作を実行し、更新されたアクセス要求を外部サーバに転送します。ACS 5.4 は既存の値の調整をサポートしません。

属性動作ステートメントの例：

```
Operator-name ADD new value: "University A"
```

次の動作が、RADIUS 属性の書き換えで使用可能です。

- 「追加属性」（P.A-10）
- 「更新属性」（P.A-10）
- 「削除属性」（P.A-11）

追加属性

追加属性は選択した RADIUS 属性の新しい属性値を追加するために使用されます。

- 複数の属性が許可されない場合、追加動作は、選択した属性が要求に存在しないときにだけ、この属性の新しい値を追加します。

  例：

  Called-Station-Id – Attribute Multiple NOT allowed:

  アクセス要求上：

  Called-Station-Id NOT on the request

  属性動作ステートメント：

  Called-Station-Id ADD 1223

  サーバに転送される要求での属性処理の結果：

  Called-Station-Id =1223

  Called-Station-ID が元の要求にある場合、ACS はこの例で追加動作を実行しません。

- 複数の属性が許可される場合、追加動作は、新しい値を持つ属性を必ず追加します。

  例：

  Login-IP-Host – attribute Multiple allowed:

  アクセス要求上：

  Login-IP-Host=10.56.21.190

  属性動作ステートメント：

  Login-IP-Host ADD 10.56.1.1

  サーバに転送される要求での属性処理の結果：

  Login-IP-Host=10.56.21.190

  Login-IP-Host=10.56.1.1

更新属性

更新属性は選択した RADIUS 属性の既存の値を更新するために使用されます。

- 複数の属性が許可されない場合、更新動作は、既存の属性が要求上に存在する場合にだけ、新しい値でその属性を更新します。
- 複数の属性が許可される場合、更新動作は、この属性のすべての発生を削除して、新しい値を持つ属性を 1 つ追加します。

例：

Login-IP-Host – attribute Multiple allowed:

アクセス要求上：

Login-IP-Host=10.56.21.190

Login-IP-Host=10.56.1.1

属性動作ステートメント：

Login-IP-Host UPDATE 10.12.12.12

サーバに転送される要求での属性処理の結果：

Login-IP-Host=10.12.12.12

- 属性が cisco-avpair（キー = 値のペア）の場合、更新はキーに基づいて行われます。

例：

アクセス要求上：

cisco-avpair = url-redirect=www.cisco.com

cisco-avpair = url-redirect=www.yahoo.com

cisco-avpair = cmd=show

属性動作ステートメント：

cisco-avpair UPDATE new value:[url-redirect=www.google.com]

サーバに転送される要求での属性処理の結果：

cisco-avpair = url-redirect=www.google.com

cisco-avpair = cmd=show

削除属性

削除属性動作は選択された RADIUS 属性の値を削除するために使用されます。

例：

Login-IP-Host – attribute Multiple allowed

アクセス要求上：

Login-IP-Host=10.56.21.190

属性動作ステートメント：

Login-IP-Host DELETE

サーバに転送される要求での属性処理の結果：

Attribute Login-IP-Host NOT on the request

RADIUS アクセス要求

ユーザ ログインでは、ネットワーク アクセス デバイスから RADIUS サーバへのクエリー（Access-Request）と、それに対応するサーバからの応答（Access-Accept または Access-Reject）が行われます。Access-Request パケットには、ユーザ名、パスワード、NAD IP アドレス、および NAD ポートと、その他の関連属性が含まれています。

RADIUS サーバでは、NAD からアクセス要求を受信すると、データベースでユーザ名を検索します。データベース クエリーの結果に応じて、受け入れまたは拒否が送信されます。アクセス拒否メッセージには、拒否の理由を示すテキスト メッセージが付加される場合があります。

RADIUS では、認証と認可は対になっています。RADIUS サーバは、ユーザ名およびパスワードが正しいことを確認すると、Access-Accept 応答を返します。この応答には、このセッションで使用するパラメータを示す属性値のペアのリストが含まれています。このパラメータのリストによって、ユーザの認可権限が設定されます。

一般的なパラメータは、次のとおりです。

- サービス タイプ
- プロトコル タイプ
- ユーザに割り当てる IP アドレス（スタティックまたはダイナミック）
- 適用するアクセス リスト
- NAD ルーティング テーブルにインストールするスタティック ルート

RADIUS サーバ内の設定情報によって、インストール時に NAD で設定するパラメータが定義されます。