RADIUSの動作を確認する

内容

概要

このドキュメントでは、RADIUSサーバの概要とその動作について説明します。

前提条件

要件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

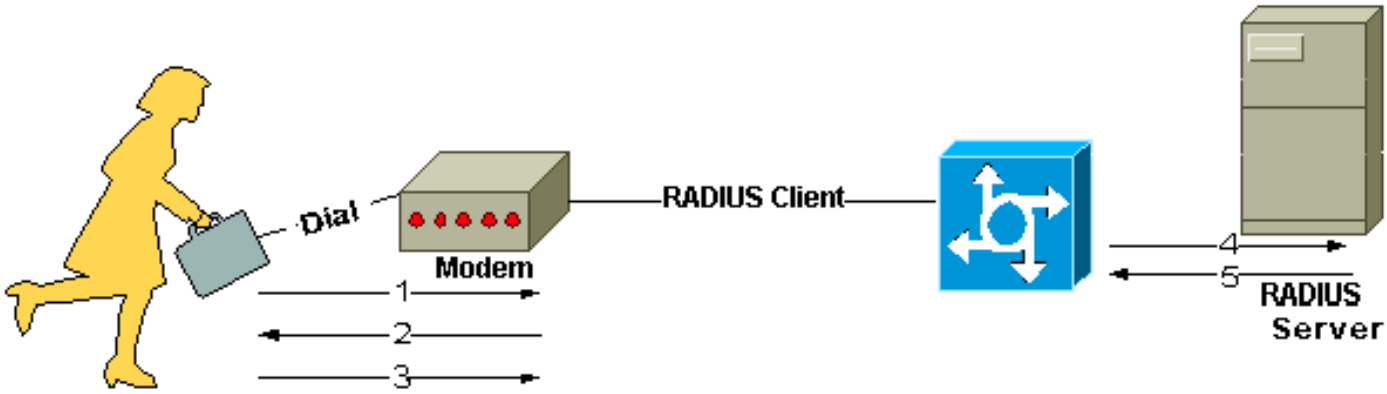
Remote Authentication Dial-In User Service（RADIUS）プロトコルは、アクセス サーバ認証およびアカウンティング プロトコルとして Livingston Enterprises, Inc. で開発されました。RADIUS 仕様 RFC 2865 は RFC 2138 に取って代わりました。RADIUS アカウンティング標準規格 RFC 2866 は RFC 2139 に取って代わりました。

ネットワーク アクセス サーバ (NAS) と RADIUS サーバとの間の通信はユーザ データグラム プロトコル (UDP) に基づいています。一般に、RADIUS プロトコルはコネクションレス型サービスと見なされます。サーバの可用性、再送信、タイムアウトに関する問題は、伝送プロトコルではなく、RADIUS 対応デバイスにより処理されます。

RADIUSはクライアント/サーバプロトコルである

RADIUSクライアントは通常NASであり、RADIUSサーバは通常、UNIXまたはWindows NTマシン上で動作するデーモンプロセスです。クライアントは、指定されたRADIUSサーバにユーザ情報を渡し、返された応答に従って動作します。RADIUS サーバはユーザ接続要求を受信し、ユーザを認証してから、このユーザへのサービス提供にクライアントが必要とする設定情報を返します。RADIUS サーバは、他の RADIUS サーバや、他の種類の認証サーバに対するプロキシ クライアントとして動作します。

次の図は、ダイヤルイン ユーザと RADIUS クライアントおよびサーバ間の交流を示します。



ダイヤルインユーザとRADIUSクライアントおよびサーバ間のインタラクション

1. ユーザは NAS に対する PPP 認証を開始します。
2. NAS がユーザ名とパスワード (Password Authentication Protocol [PAP] の場合) またはチャレンジ (Challenge Handshake Authentication Protocol [CHAP] の場合) の入力を求めます。
3. ユーザが応答します。
4. RADIUS クライアントは、RADIUS サーバにユーザ名と暗号化されたパスワードを送信します。
5. RADIUS サーバは、承認、拒否、またはチャレンジを返します。
6. RADIUS クライアントは、承認または拒否とバンドルされたサービスおよびサービス パラメータに応じて動作します。

認証および認可

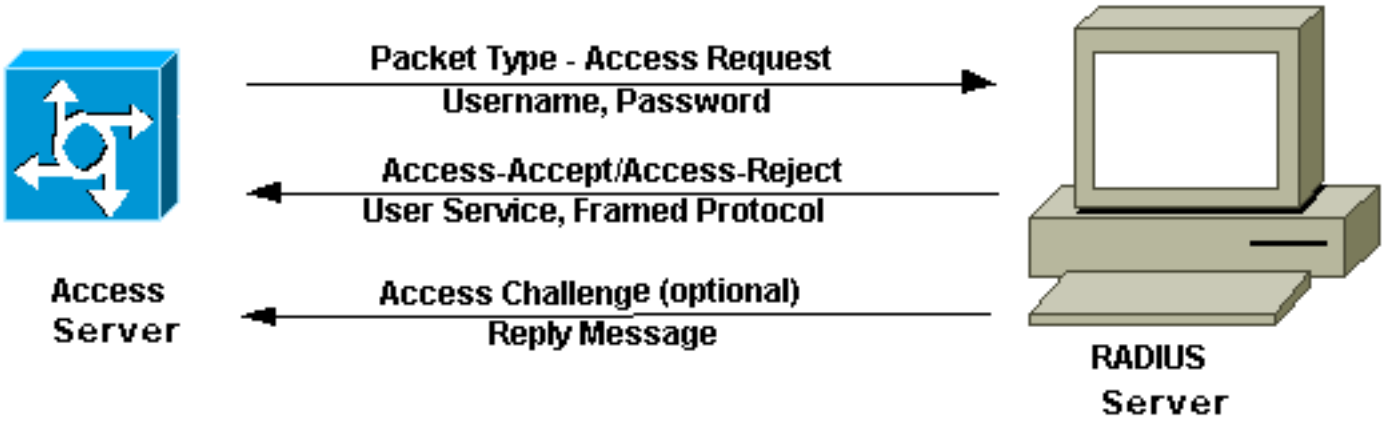
RADIUS サーバは、ユーザを認証するさまざまな方法をサポートできます。ユーザが指定したユーザ名と元のパスワードを入力すれば、PPP、PAP または CHAP、Unix ログイン、およびその他の認証メカニズムをサポートできます。

通常、ユーザ ログインでは、NAS から RADIUS サーバへのクエリ (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 のパケットには、ユーザ名、暗号化されたパスワード、NAS IP アドレス、ポートが含まれます。RADIUSの初期の導入ではUDPポート番号1645が使用されていましたが、これは「データメトリック」サービスと競合します。この競合が原因となり、RFC 2865 は正式に RADIUS に

対してポート番号 1812 を割り当てました。シスコ デバイスとアプリケーションのほとんどは、どちらのセットのポート番号もサポートします。要求の形式も、ユーザが開始するセッションのタイプに関する情報を提供します。たとえば、クエリが文字モードで表示される場合、"Service-Type = Exec-User" と推測されますが、要求が PPP パケット モードで表される場合、"Service Type = Framed User" および "Framed Type = PPP" と推測されます。

RADIUS サーバでは、NAS から Access-Request を受信すると、データベースにリストされているユーザ名を検索します。ユーザ名がデータベースに存在しない場合は、デフォルトプロファイルがロードされるか、RADIUSサーバが即座にAccess-Rejectメッセージを送信します。この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を添付できます。

RADIUS では、認証と認可は対になっています。ユーザ名が見つかり、パスワードが正しい場合、RADIUSサーバは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されるパラメータを記述した属性と値のペアのリストが含まれています。一般的なパラメータには、サービス タイプ (シェルまたはフレーム) 、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、または NAS 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 ルートなどがあります。RADIUSサーバの設定情報は、NASにインストールできる内容を定義します。次の図は、RADIUS認証および許可シーケンスを示しています。



RADIUS認証および許可シーケンス

アカウンティング

RADIUS プロトコルのアカウンティング機能は、RADIUS 認証または認可とは独立して使用できます。RADIUSアカウンティング機能を使用すると、セッションの開始時と終了時にデータを送信できます。このデータは、セッション中に使用されたリソースの量 (時間、パケット、バイトなど) を示します。インターネットサービスプロバイダー(ISP)は、RADIUSアクセス制御およびアカウンティングソフトウェアを使用して、特別なセキュリティおよび課金のニーズを満たすことができます。ほとんどのCiscoデバイスのRADIUSのアカウンティングポートは1646ですが、1813にすることもできます(RFC 2139で指定されているポートの変更のため)。

クライアントと RADIUS サーバとの間のトランザクションは、共有秘密を使用して認証されます。共有秘密はネットワーク上に送信されることはありません。さらに、ユーザパスワードはクライアントとRADIUSサーバの間で暗号化されて送信されるため、安全でないネットワークをスヌーピングしている何者かがユーザパスワードを特定する可能性がなくなります。

関連情報

- **認証プロトコル**

- Requests for Comments (RFCs)
- テクニカルサポート - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。