VPDN について

内容

概要

Virtual Private Dial-up Network（VPDN）により、プライベート ネットワークのダイヤルイン サービスをリモート アクセス サーバ（L2TP Access Concentrator [LAC] として定義されている）にまで拡大することができます。

Point-to-Point Protocol（PPP）クライアントが LAC にダイヤルすると、LAC はその PPP セッションを発信元クライアント用の L2TP Network Server（LNS; L2TP ネットワーク サーバ）に転送する必要があると判断します。続いて、LNS によってユーザが認証され、PPP ネゴシエーションが開始されます。PPP 設定が完了した後は、すべてのフレームが LAC を経由してクライアントと LNS に送信されます。

前提条件

要件

このドキュメントに特有の要件はありません。

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。

このマニュアルの情報は、特定のラボ環境に置かれた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。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

表記法

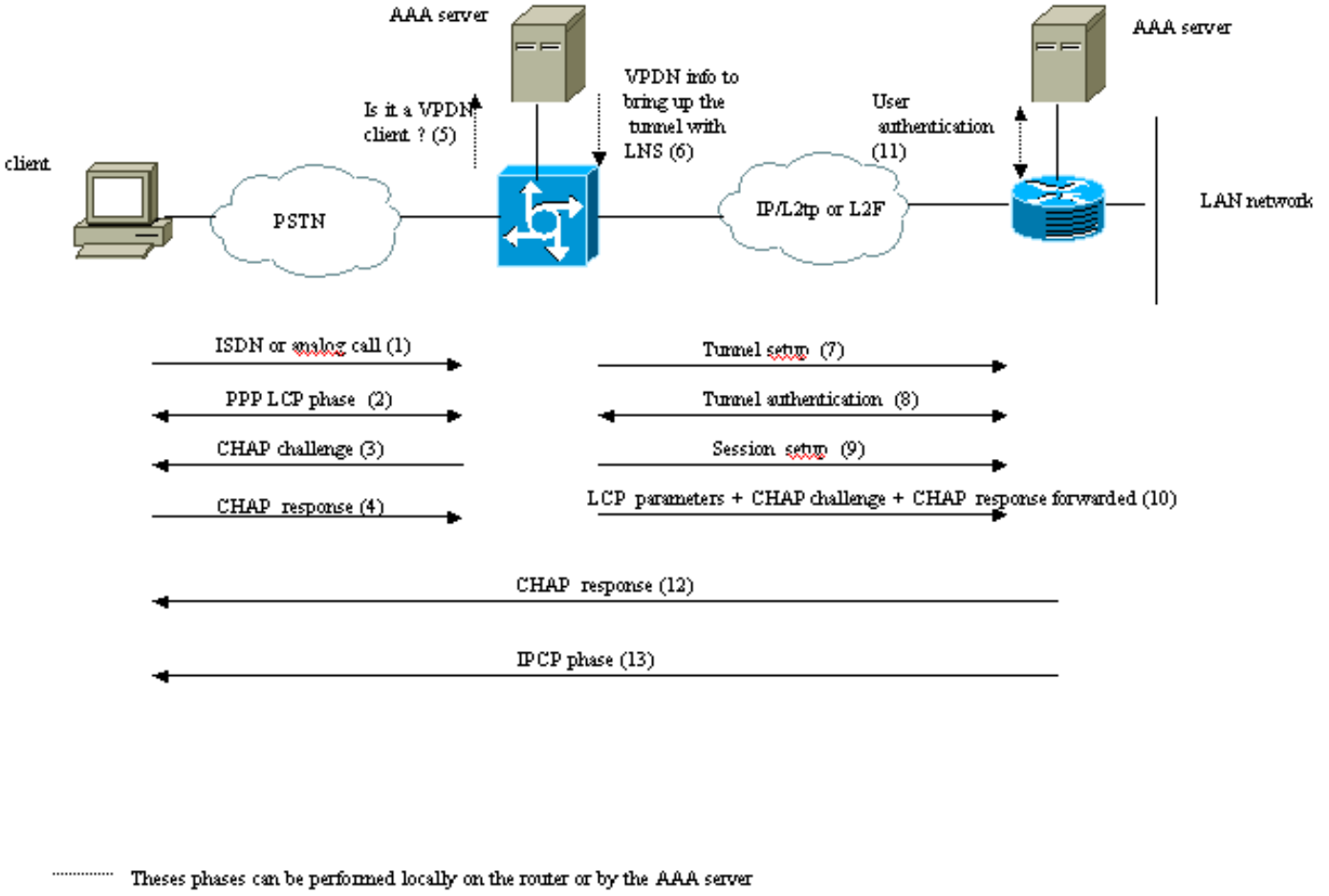
ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

用語集

- **クライアント**:リモート アクセス ネットワークに接続されている PC またはルータ。 コールの発信側となります。
- **L2TP**：レイヤ 2 トンネル プロトコル.PPP では、レイヤ 2（L2）ポイントツーポイント リンクを介してマルチプロトコル パケットを転送するための、カプセル化のメカニズムが定義されています。通常、ユーザは Plain Old Telephone Service（POTS; 一般電話サービス）へのダイヤルアップ、ISDN、Asymmetric Digital Subscriber Line（ADSL; 非対称デジタル加入者線）などの方法を使用して Network Access Server（NAS; ネットワーク アクセス サーバ）への L2 接続を確立します。 ユーザは、この接続上で PPP を実行します。このような設定では、L2 終端地点と PPP セッションのエンドポイントがどちらも同じ物理デバイス（NAS）に常駐します。L2TP ではこの PPP モデルが拡張され、L2 と PPP のそれぞれのエンドポイントが、ネットワークによって相互接続された異なるデバイスに常駐できます。L2TP では、ユーザはアクセス コンセントレータへの L2 接続を確立し、このコンセントレータによって個々の PPP フレームが NAS にトンネル伝送されます。これにより、PPP パケットの実際の処理を L2 回線の終端から分離できます。
- **L2F**：レイヤ 2 転送プロトコル。L2F は L2TP よりも古いトンネリング プロトコルです。
- **LAC**：L2TP アクセス コンセントレータ。L2TP トンネルの一方のエンドポイントとして機能するノードで、LNS に対してピアとなります。LAC は LNS とクライアントの間に配置され、両者の間でパケットを転送します。LAC から LNS に送信されるパケットには、L2TP プロトコルによるトンネリングが必要です。LAC からクライアントへの接続は一般に ISDN またはアナログ回線を通過します。
- **LNS**：L2TP ネットワーク サーバ。L2TP トンネルの一方のエンドポイントとして機能するノードで、LAC に対してピアとなります。LNS は、LAC によってクライアントからトンネリングされる PPP セッションの、論理的な終端地点です。
- **ホームゲートウェイ**:LNS と同義の L2F 用語。
- **NAS**：LAC と同義の L2F 用語。
- **トンネル**：L2TP用語では、LAC-LNSペア間にトンネルが存在します。トンネルは制御接続と 0 個以上の L2TP セッションから成ります。トンネルは、カプセル化された PPP データグラムと制御メッセージを、LAC と LNS の間で伝送します。このプロセスは L2F の場合と同じです。
- **Session**:L2TPはコネクション型です。LNS と LAC は、LAC によって開始または応答される各コールの状態を保持します。クライアントと LNS の間でエンドツーエンドの PPP 接続が確立されると、LAC と LNS の間で L2TP セッションが作成されます。PPP 接続に関連するデータグラムは LAC と LNS 間のトンネルを通じて送信されます。確立された L2TP セッションとそれに関連付けられたコールの間には、1 対 1 の関係があります。このプロセスは L2F の場合と同じです。

VPDN プロセスの概要

次の VPDN プロセスの説明では、L2TP の用語（LAC と LNS）を使用します。



1. クライアントが LAC をコールします（通常はモデムまたは ISDN カードを使用する）。
2. クライアントと LAC は LCP オプション（Password Authentication Protocol [PAP; パスワード認証プロトコル] または Challenge Handshake Authentication Protocol [CHAP] の認証方式、PPP マルチリンク、圧縮など）をネゴシエートすることで、PPP フェーズを開始します。
3. ステップ2でCHAPがネゴシエートされたと仮定します。LACがクライアントにCHAPチャレンジを送信します。
4. LAC は応答を取得します（たとえば、username@DomainName とパスワードなど）。
5. CHAP 応答で受信されたドメイン名または ISDN 設定メッセージで受信された Dialed Number Information Service（DNIS; 着信番号情報サービス）に基づいて、LAC はクライアントが VPDN ユーザであるかどうかをチェックします。そのために、ローカルの VPDN 設定を使用するか、または Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）サーバに問い合せます。
6. クライアントが VPDN ユーザであることが判明すると、LAC は LNS との間に L2TP または L2F トンネルを作成するために使用する情報を（ローカルの VPDN 設定または AAA サーバから）取得します。
7. LAC は LNS との間に L2TP または L2F トンネルを作成します。
8. LAC からの要求で受信された名前に基づいて、LNS は LAC がトンネルのオープンを許可されているかどうかをチェックします（ローカルの VPDN 設定をチェックする）。 また、LAC と LNS は相互に認証を行います（それぞれのローカル データベースを使用するか、AAA サーバに問い合せる）。 続いて、両デバイスの間でトンネルがアップします。このトンネルでは、複数の VPDN セッションを伝送できます。
9. クライアント username@DomainName の VPDN セッションが LAC から LNS へ向けてトリガされます。クライアントごとに 1 つの VPDN セッションを確立できます。

10. LAC はクライアントとネゴシエート済みの LCP オプションと、クライアントから受信された username@DomainName およびパスワードを LNS に転送します。
11. LNS は VPDN 設定で指定されている仮想テンプレートから仮想アクセスをクローニングします。LNS は LAC から受信された LCP オプションを取り出して、クライアントをローカルで認証するか、または AAA サーバに問い合せて認証します。
12. LNS は クライアントに CHAP 応答を送信します。
13. IP Control Protocol (IPCP; IP 制御プロトコル) フェーズが実行され、続いて経路が開設されます。PPP セッションがアップし、クライアントと LNS の間で実行されます。LAC は単に PPP フレームを転送するだけです。PPP フレームは LAC と LNS の間でトンネル伝送されます。

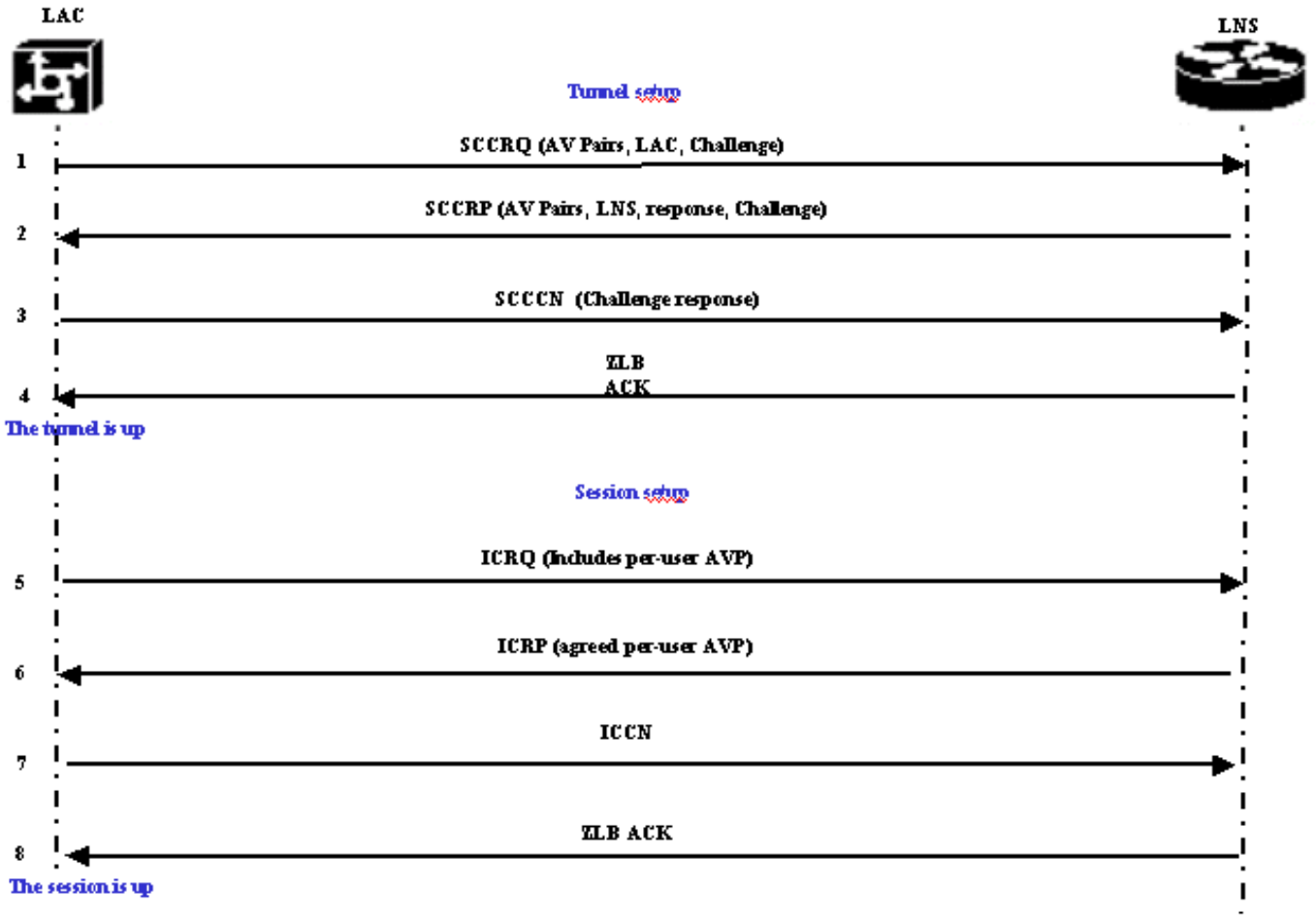
トンネリング プロトコル

VPDN トンネルは Layer-2 Forwarding (L2F; レイヤ 2 転送) または Layer-2 Tunneling Protocol (L2TP; レイヤ 2 トンネリング プロトコル) を使用して作成されます。

- L2F はシスコが Request For Comments (RFC) 2341 で導入したもので、マルチシャーシ マルチリンク PPP 用の PPP セッションの転送にも使用されます。
- RFC 2661で導入されたL2TPは、Cisco L2FプロトコルとMicrosoft Point-to-Point Tunneling Protocol(PPTP)の長所を兼ね備えています。 さらに、L2F がダイヤルイン VPDN のみをサポートするのに対し、L2TP はダイヤルイン VPDN とダイヤルアウト VPDN の両方をサポートします。

どちらのプロトコルも、UDP ポート 1701 を使用して IP ネットワークを通過するトンネルを作成し、リンク層フレームを転送します。L2TP では、PPP セッションをトンネル伝送するためのセットアップは次の 2 つのステップから成ります。

1. LAC と LNS 間のトンネルの確立。このフェーズは、両デバイス間にアクティブなトンネルがない場合のみ実行されます。
2. LAC と LNS 間のセッションの確立。



LAC は、LAC から LNS へ向けてトンネルを開始しなければならないと判断します。

1. LAC が Start-Control-Connection-Request（SCCRQ）を送信します。このメッセージには、CHAP チャレンジと AV ペアが含まれています。
2. LNS は Start-Control-Connection-Reply（SCCRP）で応答します。このメッセージには、CHAP チャレンジ、LAC のチャレンジへの応答、および AV ペアが含まれています。
3. LAC は Start-Control-Connection-Connected（SCCCN）を送信します。 このメッセージには CHAP 応答が含まれています。
4. LNS は Zero-Length Body Acknowledgement（ZLB ACK）で応答します。 この ACK は別のメッセージで伝送される場合があります。トンネルがアップします。
5. LAC は LNS に Incoming-Call-Request（ICRQ）を送信します。
6. LNS は Incoming-Call-Reply（ICRP）メッセージで応答します。
7. LAC は Incoming-Call-Connected（ICCN）を送信します。
8. LNS は ZLB ACK で応答します。この ACK も別のメッセージで伝送される場合があります。
9. セッションがアップします。

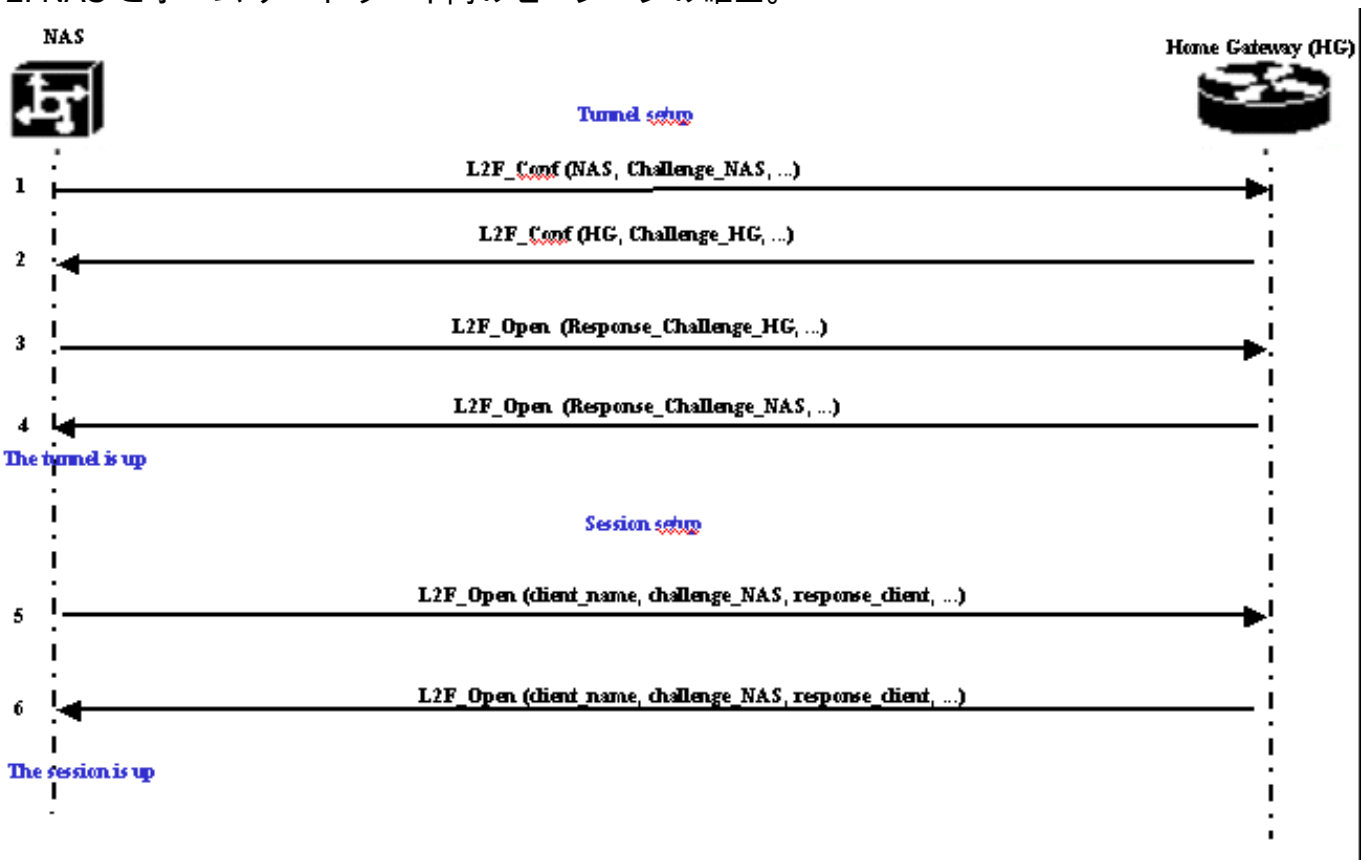
注：トンネルまたはセッションを開くために使用される上記のメッセージは、RFC 2661で定義されている属性値ペア(AVP)を伝送します。AVP にはプロパティと情報（bearercap、ホスト名、ベンダー名、ウィンドウ サイズなど）が記述されています。 AVP には必須のものとオプションのものがあります。

注：トンネルIDは、LACとLNS間のトンネルの多重化と逆多重化に使用されます。セッション ID は、トンネルを通過する特定のセッションを識別するために使用されます。

L2Fの場合、PPPセッションをトンネリングするためのセットアップは、L2TPのセットアップと

同じです。次の内容が含まれます。

1. NAS とホーム ゲートウェイ間のトンネルの確立。このフェーズは、両デバイス間にアクティブなトンネルがない場合のみ実行されます。
2. NAS とホーム ゲートウェイ間のセッションの確立。



NAS は、NAS からホーム ゲートウェイへ向けてトンネルを開始しなければならないと判断します。

1. NAS がホーム ゲートウェイに L2F_Conf を送信します。このメッセージには CHAP チャレンジが含まれています。
2. ホーム ゲートウェイは L2F_Conf で応答します。このメッセージには CHAP チャレンジが含まれています。
3. NAS は L2F_Open を送信します。このメッセージにはホーム ゲートウェイのチャレンジへの CHAP 応答が含まれています。
4. ホーム ゲートウェイは L2F_Open で応答します。このメッセージには NAS のチャレンジへの CHAP 応答が含まれています。トンネルがアップします。
5. NAS はホーム ゲートウェイに L2F_Open を送信します。このパケットには、クライアントのユーザ名（client_name）、NAS からクライアントに送信された CHAP チャレンジ（challenge_NAS）、およびその応答（response_client）が含まれています。
6. ホーム ゲートウェイは L2F_Open を送り返すことで、クライアントを受け入れます。これで、クライアントとホーム ゲートウェイの間でトラフィックがどちらの方向にも自由に流れるようになります。

注：トンネルはCLID（クライアントID）で識別されます。 トンネル内の特定の接続は Multiplex ID（MID）で識別されます。

VPDN の設定

VPDN の設定の詳細については、「バーチャル プライベート ネットワークの設定」マニュアルの「VPN の設定」の項を参照してください。

関連情報

- ダイヤルとアクセス テクノロジーのサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems