H3C MSR
L2TP コンフィギュレーションガイド

New h3c Technologies Co., Ltd.

http://www.h3c.com

ドキュメントバージョン:6W103-20200507製品バージョン:R5426P02

L2TPの設定

L2TPについて

Layer 2 Tunneling Protocol(L2TP)は、Virtual Private Dialup Network(VPDN)トンネリングプロトコルです。L2TPは、パブリックネットワーク(インターネットなど)を介してポイントツーポイントトンネルを設定し、カプセル化されたPPPフレーム(L2TPパケット)をトンネル経由で送信します。L2TPでは、リモートユーザーは、PPPを使用してパブリックネットワークに接続した後、L2TPトンネルを介してプライベートネットワークにアクセスできます。

L2TPは、レイヤ2 VPNテクノロジーとして、リモートユーザーがプライベートネットワークにアクセスするための安全でコスト効率の高いソリューションを提供します。

一般的なL2TPネットワーキング

図1 L2TPネットワーク図

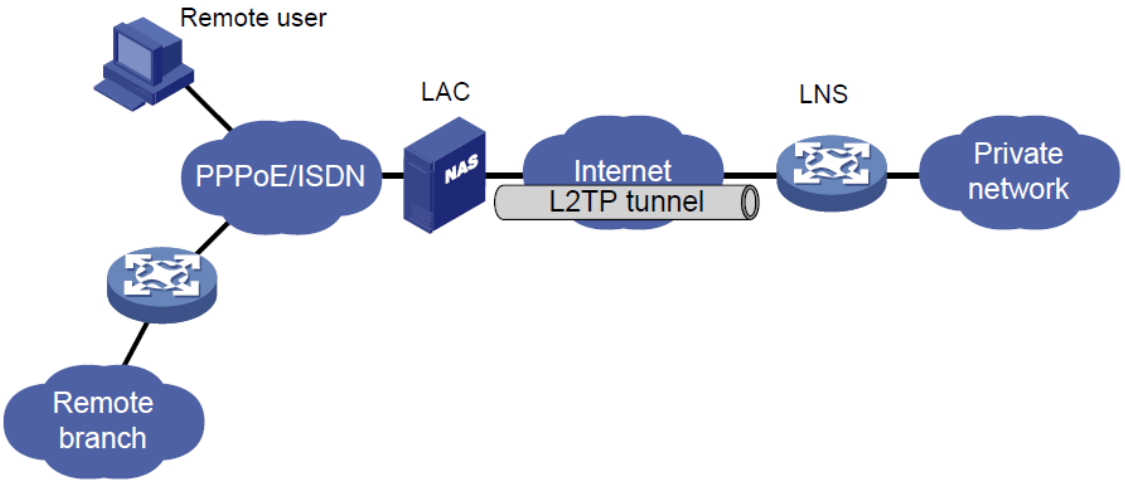


図1に示すように、一般的なL2TPネットワークには次のコンポーネントがあります。

- **リモートシステム**: 通常、リモートシステムは、プライベートネットワークにアクセスする必要があるリモートユーザーのホストまたはリモートブランチのデバイスです。
- **LAC**: L2TP Access Concentrator(LAC)は、PPPとL2TPの両方に対応しています。通常は、ローカルISPに配置されたNetwork Access Server(NAS)で、主にPPPユーザーにアクセスサービスを提供します。

  LACは、L2TPトンネルのエンドポイントであり、LNSとリモートシステムの間にあります。L2TPを使用してリモートシステムから受信したパケットをカプセル化し、カプセル化されたパケットをLNSに送信します。LNSから受信したパケットをカプセル化解除し、カプセル化解除されたパケットを目的のリモートシステムに送信します。
- **LNS**: L2TP Network Server(LNS)は、PPPおよびL2TPの両方に対応しています。通常、エンタープライズネットワーク上のエッジデバイスです。

  LNSは、L2TPトンネルのもう一方のエンドポイントです。これは、LACによってトンネリングされるPPPセッションの論理終端ポイントです。L2TPは、トンネルを確立することによって、PPPセッションの終端ポイントをNASからLNSに拡張します。

L2TPメッセージタイプとカプセル化構造

L2TPでは、次のタイプのメッセージを使用します。

- 制御メッセージL2TPトンネルおよびセッションを確立、維持、および削除するために使用されます。制御メッセージは、フロー制御および輻輳制御をサポートする信頼性の高い制御チャネルを介して送信されます。
- データメッセージ:図2に示すように、PPPフレームをカプセル化するために使用されます。データメッセージは、信頼性の低いデータチャネルを介して送信され、パケット損失が発生した場合には再送信されません。データメッセージは、シーケンス番号を使用して、転送中に無秩序になったパケットの順序を変更できます。

図2 データメッセージフォーマット

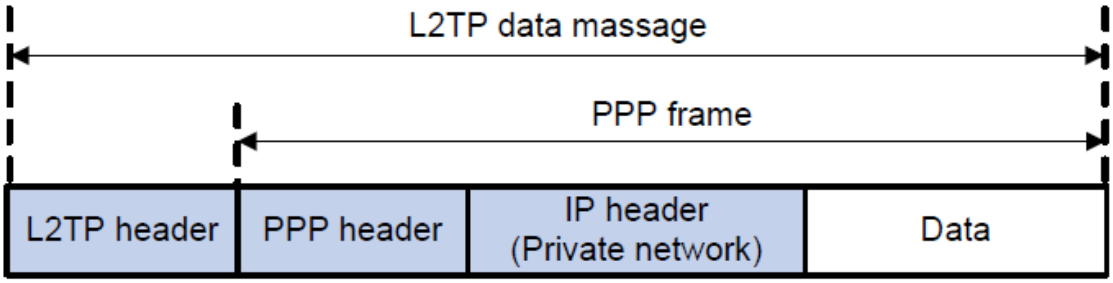


図3に示すように、制御メッセージとデータメッセージの両方がUDPデータグラムにカプセル化されます。

図3 L2TPカプセル化の構造

L2TP トンネルとセッション

L2TPトンネルは、LACとLNS間の仮想的なポイントツーポイント接続です。LNSとLACの間に複数のL2TPトンネルを確立できます。L2TPトンネルは、1つ以上のL2TPセッションを伝送できます。各L2TPセッションはPPPセッションに対応し、L2TPトンネル上で多重化されます。L2TPセッションは、リモートシステムとLNSの間でエンドツーエンドPPPセッションが確立されるときに、LACとLNSの間で確立されます。PPPセッションのデータフレームは、LACとLNSの間のトンネルを介して送信されます。

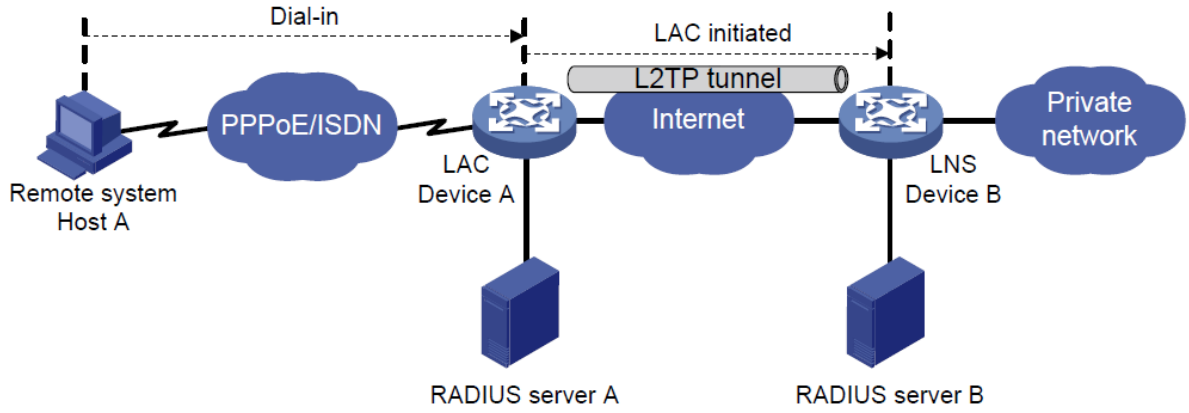
L2TPトンネリングモードおよびトンネル確立プロセス

L2TPトンネリングモードには、NAS開始、クライアント開始、およびLAC自動開始があります。

NAS起動トンネリングモード

図4に示すように、リモートシステムはPPPoE/ISDNネットワークを介してLACにダイヤルインします。LACはインターネットを介してLNSにトンネリング要求を開始します。

図4 NAS開始トンネリングモード



NAS開始トンネルには、次の特性があります。

- リモートシステムはPPPをサポートするだけでよく、L2TPをサポートする必要はありません。
- リモートシステムの認証およびアカウンティングは、LACまたはLNSに実装できます。

図5 NASが開始したトンネル確立プロセス

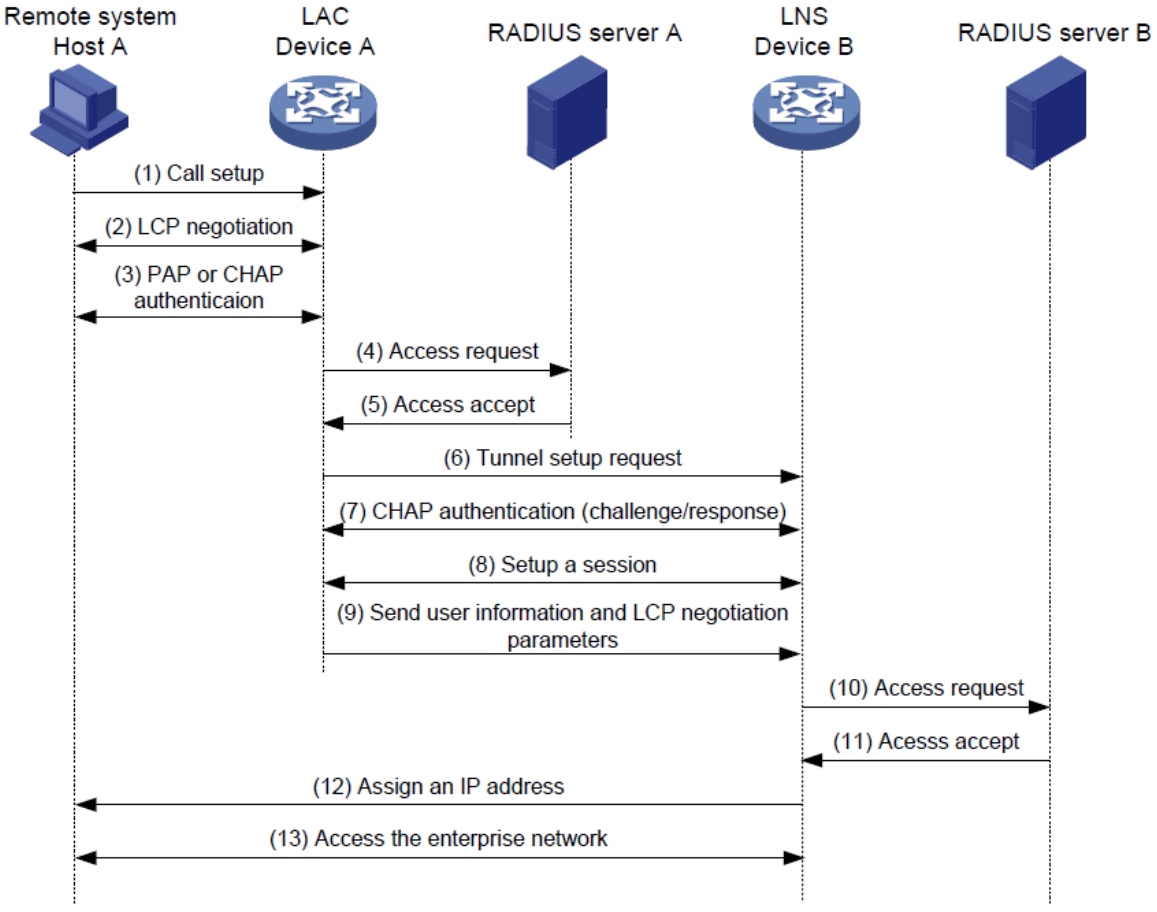


図5に示すように、次のワークフローを使用して、NAS開始トンネルを確立します。

1. リモートシステム(ホストA)がLAC(デバイスA)へのPPP接続を開始します。
2. リモートシステムとLACは、PPP LCPネゴシエーションを実行します。
3. LACは、PAPまたはCHAPを使用してホストAのPPPユーザー情報を認証します。
4. LACは認証情報(ユーザー名とパスワード)を認証のためにRADIUSサーバー(RADIUSサーバーA)

に送信します。

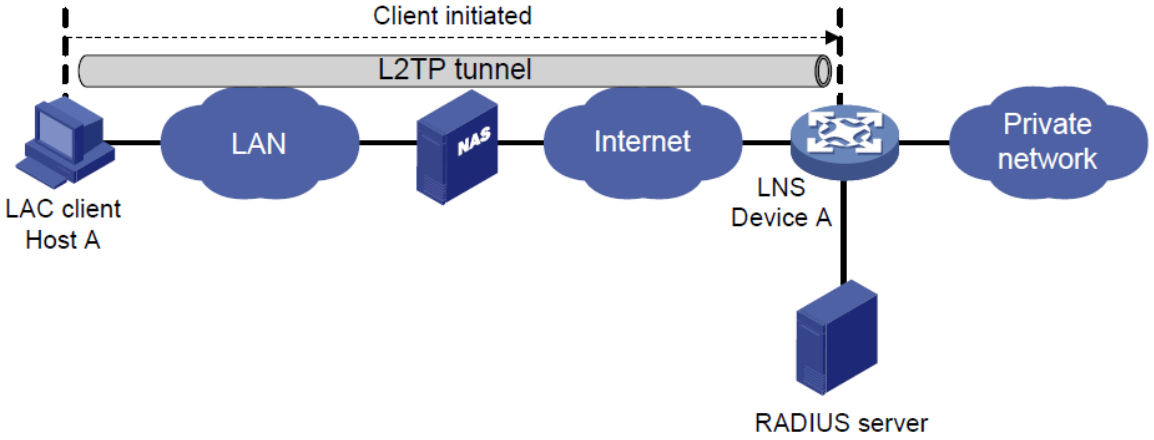
5. RADIUSサーバーAはユーザーを認証し、結果を返します。
6. 次の条件が存在する場合、LACはLNS(デバイスB)にL2TPトンネリング要求を開始します。
   - ユーザーは認証に合格します。
   - ユーザーは、ユーザー名またはユーザーが属するISPドメインに従って、L2TPユーザーであると判断されます。
7. トンネル認証が必要な場合、L2TPトンネルを正常に確立する前に、LACとLNSはCHAPチャレンジメッセージを送信して互いを認証します。
8. LACとLNSは、L2TPセッションを確立するためにネゴシエートします。
9. LACは、PPPユーザー情報とPPPネゴシエーションパラメータをLNSに送信します。
10. LNSは認証情報を認証のためにRADIUSサーバー(RADIUSサーバーB)に送信します。
11. RADIUSサーバーBはユーザーを認証し、結果を返します。
12. ユーザーが認証に合格すると、LNSはプライベートIPアドレスをリモートシステム(ホストA)に割り当てます。
13. PPPユーザーは、企業の内部リソースにアクセスできます。

ステップ12および13では、LACがリモートシステムとLNSにパケットを転送します。ホストAとLACはPPPフレームを交換し、LACとLNSはL2TPパケットを交換します。

クライアント起動トンネリングモード

図6に示すように、L2TPを実行するリモートシステム(LACクライアント)には、インターネットを介してLNSと通信するためのパブリックIPアドレスがあります。LACクライアントは、専用のLACデバイスを使用せずに、LNSへのトンネリング要求を直接開始できます。

図6 クライアント起動トンネリングモード

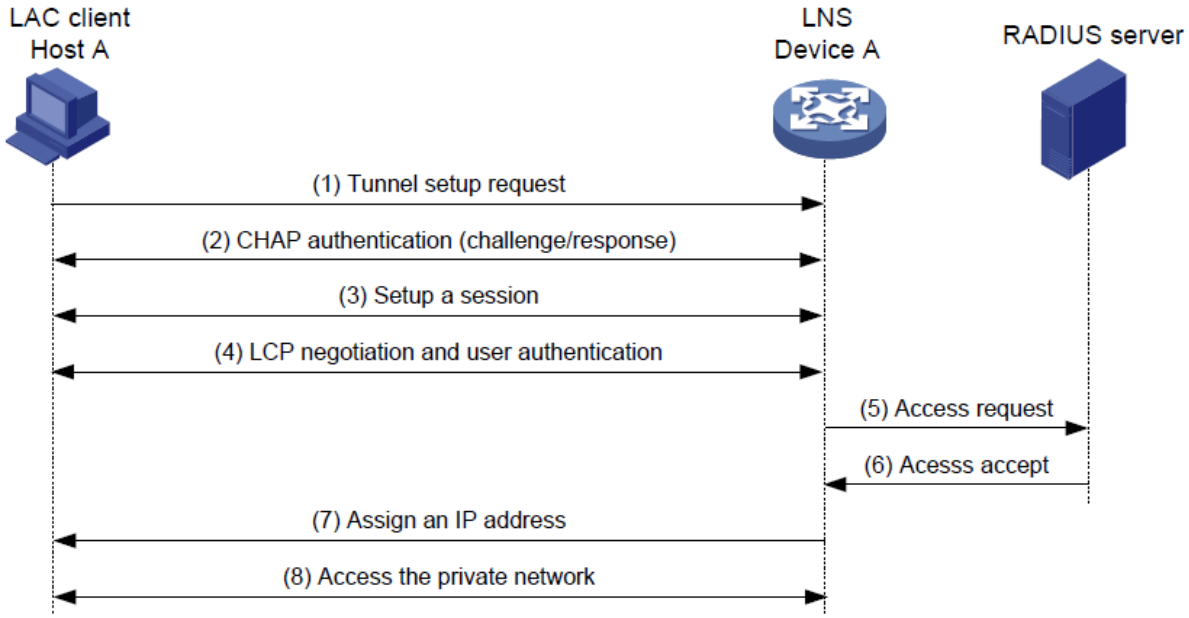


クライアントが開始するトンネルには、次の特性があります。

- クライアントが開始するトンネルは、リモートシステムとLNSの間で確立されるため、セキュリティが高くなります。
- リモートシステムはL2TPをサポートし、LNSと通信できる必要があります。このため、拡張性が低くなります。

図7に示すように、クライアントが開始するトンネルを確立するためのワークフローは、NASが開始するトンネルを確立するためのワークフローと同様です(詳細は示されていません)。

図7 クライアントが開始するトンネル確立プロセス

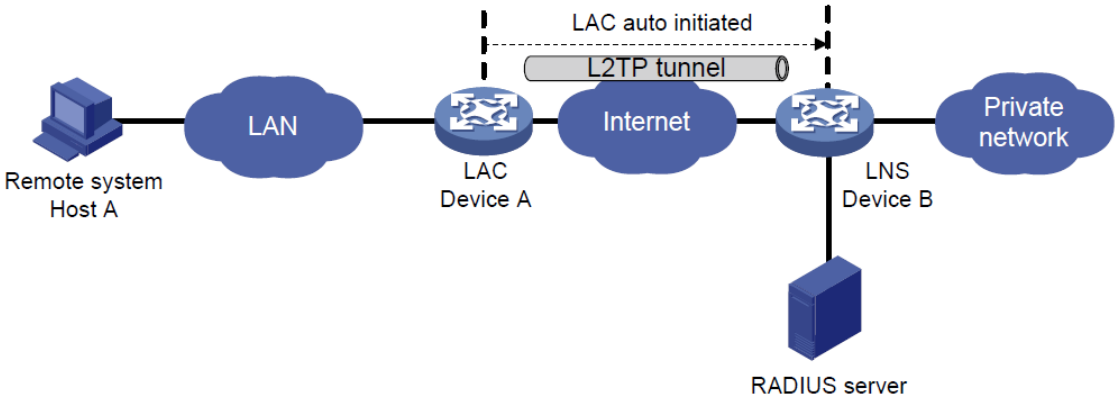


LAC自動開始トンネリングモード

NAS起動モードでは、リモートシステムがPPPoEまたはISDNを介してLACに正常にダイヤルインする必要があります。

LAC自動開始モードでは、LAC上でl2tp-auto-clientコマンドを使用してLACをトリガーし、LNSへのトンネリング要求を開始できます。リモートシステムがプライベートネットワークにアクセスすると、LACはL2TPトンネルを介してデータを転送します。

図8 LAC自動開始トンネリングモード

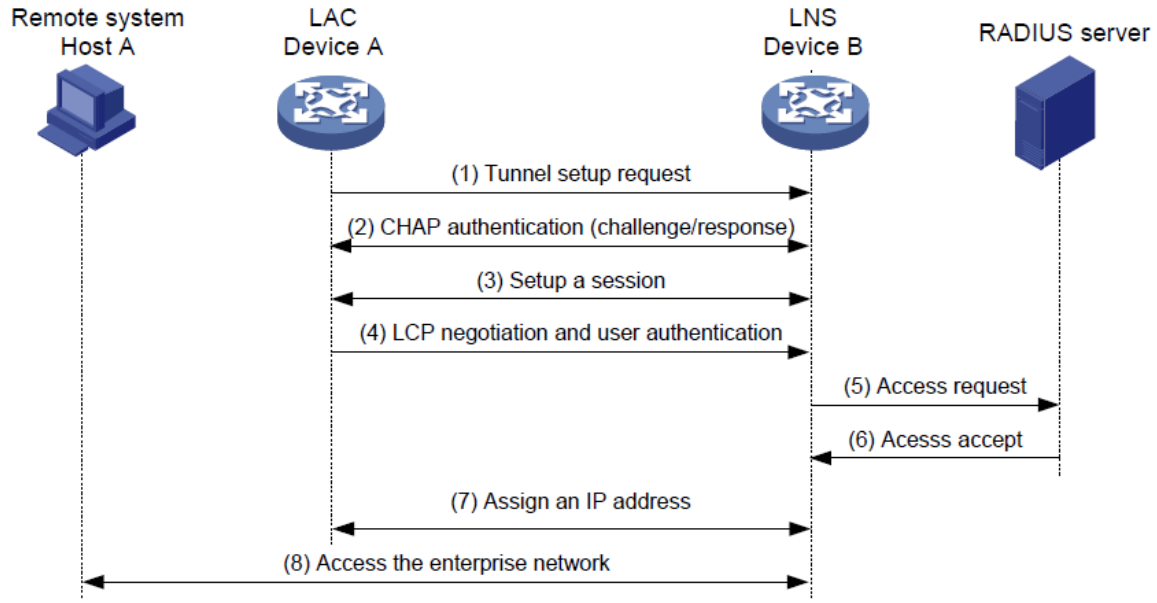


LA C自動開始トンネルには、次の特性があります。

- リモートシステムとLAC間の接続はダイヤルアップ接続に限定されず、任意のIPベースの接続にすることができます。
- L2TPセッションは、L2TPトンネルが確立された直後に確立されます。次に、LACとLNSがそれぞれPPPoEクライアントとPPPoEサーバーとして動作し、PPPネゴシエーションを実行します。
- LNSは、リモートシステムではなくLACにプライベートIPアドレスを割り当てます。

図9に示すように、LAC自動開始トンネルを確立するためのワークフローは、NAS開始トンネルを確立するためのワークフローと同様です(詳細は示されていません)。

図9 LAC自動開始トンネルの確立プロセス



L2TP 機能

- **柔軟なアイデンティティ認証メカニズムと高いセキュリティ:** L2TPだけでは、接続のセキュリティは提供されません。ただし、PPPのすべてのセキュリティ機能があり、PPP認証(CHAPまたはPAP)が可能です。また、L2TPはIPSecと連携して、トンネリングされたデータのセキュリティを向上させることもできます。
- **マルチプロトコル送信**: L2TPはPPPフレームをトンネリングします。これは、複数のネットワーク層プロトコルのパケットをカプセル化するために使用できます。
- **RADIUS認証** :LACまたはLNSは、認証のためにリモートユーザーのユーザー名とパスワードをRADIUSサーバーに送信できます。
- **プライベートアドレスの割り当て**: LNSはリモートユーザーにプライベートアドレスをダイナミックに割り当てることができます。これにより、プライベートインターネット(RFC 1918)のアドレス割り当てが容易になり、セキュリティが向上します。
- **フレキシブルアカウンティング**: アカウンティングはLACとLNSで同時に実行できます。これにより、ISP側で課金が生成され、エンタープライズゲートウェイで課金および監査が処理されます。L2TPは、着信および発信トラフィック統計情報(パケットおよびバイト単位)、接続の開始時間および終了時間などのアカウンティングデータを提供できます。AAAサーバーは、これらのデータをフレキシブルアカウンティングに使用します。
- **信頼性** :L2TPはLNSバックアップをサポートします。プライマリLNSへの接続が切断されると、LACはセカンダリLNSへの新しい接続を確立できます。この冗長性により、L2TPサービスの信頼性が向上します。
- **RADIUSサーバーからLACへのトンネルアトリビュートの発行**: NAS開始モードでは、RADIUSサーバーからLACにトンネルアトリビュートを発行できます。LACがこれらのアトリビュートを受信するには、L2TPをイネーブルにし、LAC上のPPPユーザーに対してリモートAAA認証を設定します。

  L2TPユーザーがLACにダイヤルインすると、RADIUSクライアントとしてのLACがユーザー情報をRADIUSサーバーに送信します。RADIUSサーバーはPPPユーザーを認証し、その結果をLACに返し、PPPユーザーのL2TPトンネルアトリビュートをLACに発行します。次に、LACは発行されたL2TPトンネルアトリビュートに基づいてL2TPトンネルとセッションを設定します。

表1 RADIUSサーバーが発行できるトンネルアトリビュート

属性番号	属性名	説明
64	トンネルタイプ	トンネルタイプ(L2TPだけ)。
65	トンネル-中型-タイプ	トンネルの伝送メディアタイプ(IPv4だけ)。
67	トンネルサーバーエンドポイント	LNSのIPアドレス。
69	トンネルパスワード	トンネルのピアを認証するために使用されるキー。
81	トンネル-プライベート-グループ-I D	トンネルのグループID。 LACはこの値をLNSに送信して、LNSがそれに応じた動作を実行できるようにします。
82	トンネル割り当てID	トンネルの割り当てID。 これは、セッションが割り当てられているトンネルを示すために使用されます。L2TPユーザーとTunnel-Assignment-ID、Tunnel-Server-Endpoint、およびTunnel-Passwordアトリビュートは、L2TPトンネルを共有します。
90	トンネルクライアント認証ID	トンネル名。 ローカルトンネルを示すために使用されます。

RADIUSサーバーは、RADIUSパケット内のL2TPトンネルアトリビュートのセットを1つだけ発行できます。

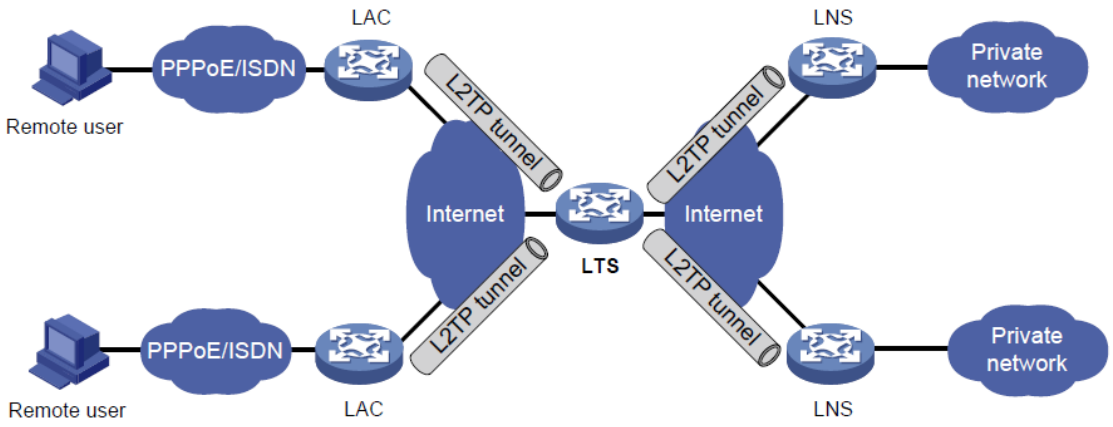
RADIUSが発行したトンネルアトリビュートは、LAC上で手動で設定されたトンネルアトリビュートを上書きしますが、その逆は行われません。

- **L2TPトンネルスイッチング**: マルチホップL2TPトンネリングとも呼ばれます。図10に示すように、Layer 2 Tunnel Switch(LTS)は、各LACからのL2TPパケットをLNSとして終端し、次にこれらのパケットをLACとして宛先LNSに送信します。

  L2TPトンネルスイッチングには次の機能があります。

  - シンプルな構成と導入LACとLNSが異なる管理ドメインにある場合:
    - すべてのLA CはLTSをLNSと見なし、ネットワーク上でLNSを区別する必要はありません。
    - すべてのLNSはLTSをLACと考え、LACの付加や欠失によって影響されることはない
  - **L2TPトンネル共有**: 異なるユーザーは、LACとLTSの間で同じL2TPトンネルを共有できます。LTSは、異なるユーザーのデータを異なるLNSに配信します。

図10 L2TPトンネルスイッチングのネットワーク図



L 2 TPベースのEAD

EADは、アクセス認証を通過するPPPユーザーを認証します。EAD認証を通過するPPPユーザーは、ネットワークリソースにアクセスできます。EAD認証に失敗したPPPユーザーは、隔離領域内のリソースだけにアクセスできます。

EADでは次の手順を使用します。

1. INodeクライアントはL2TPを使用してLNSにアクセスします。クライアントがPPP認証に合格すると、CAMS/IMCサーバーはLNSに隔離ACLを割り当てます。LNSは隔離ACLを使用して着信パケットをフィルタリングします。
2. IPCPネゴシエーションの後、LNSはCAMS/IMCサーバーのIPアドレスをINodeクライアントに送信します。サーバーのIPアドレスは、隔離ACLによって許可されます。
3. CAMS/IMCサーバーはINodeクライアントを認証し、INodeクライアントのセキュリティチェックを実行します。INodeクライアントがセキュリティチェックに合格すると、CAMS/IMCサーバーはINodeクライアントのセキュリティACLをLNSに割り当てます。INodeクライアントはネットワークリソースにアクセスできます。

プロトコルと標準

- RFC 1661『The Point-to-Point Protocol(PPP)』
- RFC 1918『Address Allocation for Private Internets』
- RFC 2661、レイヤ2トンネリングプロトコル「L2TP」
- RFC 2868『RADIUS Attributes for Tunnel Protocol Support』

L2TPの前提条件

L2TPを設定する場合は、次の作業を実行します。

1. ネットワーキング環境に応じて、必要なネットワークデバイスを決定します。
   - NAS開始モードおよびLAC自動開始モードの場合は、LACとLNSの両方を設定します。
   - クライアント起動モードの場合は、LNSだけを設定する必要があります。
2. ネットワーク上の目的のロール(LACまたはLNS)に基づいてデバイスを設定します。

L2TPタスクの概要

LACタスクの概要

NAS起動モードまたはLAC自動起動モードでデバイスをLACとして設定するには、次の作業を実行します。

1. 基本的なL2TP機能の設定
2. LACの設定
   - ユーザーのトンネリング要求を開始するためのLACの設定
     このタスクは、NAS開始モードでは必須であり、LAC自動開始モードでは不要です。
   - LNSのIPアドレスの指定
   - L2TPトンネルパケットの送信元IPアドレスの設定
   - (任意)非表示モードでのAVPデータの転送をイネーブルにします。
   - LACでのAAA認証の設定
     このタスクは、NAS開始モードでは必須であり、LAC自動開始モードでは不要です。
   - L2TPトンネルを自動的に確立するようにLACを設定する
     このタスクは、NAS開始モードでは必須であり、LAC自動開始モードでは不要です。
   - (任意)ポーリング機能の設定
   - (任意)仮想PPPインターフェイスのトラフィック処理スロットの指定
   - (任意)仮想PPPインターフェイスのデフォルト設定の復元
3. (任意)オプションのL2TPパラメータの設定
   - L2TPトンネル認証の設定
   - Hello間隔の設定
   - セッションフロー制御のイネーブル化
   - L2TPパケットのDSCP値の設定
   - トンネルピアのVPNへの割り当て
   - LTSのTSA IDの設定

LNSタスクの概要

1. 基本的なL2TP機能の設定
2. LNSの設定
   - VTインターフェイスの作成
   - (任意)VAプールの設定
   - LACからのL2TPトンネリング要求を受け入れるようにLNSを設定する方法
   - (任意)LNSでのユーザー認証の設定
   - (任意)LNSでのAAA認証の設定
   - (任意)LNSが1秒間に処理できるICRQパケットの最大数の設定
3. (任意)オプションのL2TPパラメータの設定
   - L2TPトンネル認証の設定
   - Hello間隔の設定

- セッションフロー制御のイネーブル化
- L2TPパケットのDSCP値の設定
- トンネルピアのVPNへの割り当て
- LTSのTSA IDの設定
- L2TPトンネルの受信ウィンドウサイズの設定
- L2TPトンネルの送信ウィンドウサイズの設定

4. L 2 TPベースのEADのイネーブル化

   セキュリティポリシーサーバーを使用して、L2TP認証に合格したユーザーのセキュリティチェックをさらに実行するには、次の作業を実行します。

5. IMSI/SNバインディング認証の設定

   この作業は、次のいずれかの状況で実行します。

   - 3Gまたは4GルータはLACクライアントとして動作し、クライアント開始モードでLNSにアクセスします。
   - 4GルータはLACとして動作し、LAC自動開始モードでLNSにアクセスするように自動的にトリガーされます。

基本的なL2TP機能の設定

このタスクについて

基本的なL2TP機能設定には、次の作業が含まれます。

- **L2TP設定を有効**: L2TP設定を有効にするには、L2TP-L2TPをイネーブルにする必要があります。
- **L2TPグループの作成**: L2TPグループは、パラメータのグループを表すことを目的としています。これにより、デバイス上での柔軟なL2TP設定だけでなく、1対1およびLACおよびLNS用の1対多ネットワーキングアプリケーションです。L2TPグループはローカルにだけ意味を持ちます。ただし、LACおよびLNS上のL2TPグループの関連する設定は一致する必要があります。たとえば、LAC上に設定されたローカルトンネル名は、LNS上に設定されたトンネルピア名と一致する必要があります。
- **ローカルトンネル名の設定**: ローカルトンネル名は、LACとLNSの間のトンネルネゴシエーション中にローカルエンドでトンネルを識別します。

手順

1. システムビューに入ります。

   system-view

2. L2TPをイネーブルにします。

   l2tp enable

   デフォルトでは、L2TPはディセーブルです。

3. L2TPグループを作成し、そのモードを指定して、ビューを入力します。

   l2tp-group *group-number* **mode { lac | lns }**

   モードは、LAC側でlac、LNS側でlnsと指定します。

4. ローカルトンネル名を指定します。

   tunnel name *name*

   デフォルトでは、デバイス名が使用されます。

   LACに設定されたローカルトンネル名は、LNSに設定されたトンネルピア名と一致する必要があります。

LACの設定

ユーザーのトンネリング要求を開始するためのLACの設定

このタスクについて

この作業では、ユーザーのLNSへのトンネリング要求を開始するようにLACを設定します。PPPユーザー情報が指定されたユーザーと一致すると、LACはPPPユーザーがL2TPユーザーであると判断し、LNSへのトンネリング要求を開始します。

ユーザーを指定するには、次のいずれかの項目を設定します。

- **完全修飾名** :LACは、PPPユーザーのユーザー名が設定された完全修飾名と一致する場合にだけ、LNSへのトンネリング要求を開始します。
- **ドメイン名**: LACは、PPPユーザーのISPドメイン名が設定されたドメイン名と一致する場合にだけ、LNSへのトンネリング要求を開始します。

手順

1. システムビューに入ります。

   system-view
2. LACモードでL2TPグループビューを入力します。

   l2tp-group *group-number* **[mode lac]**
3. ユーザーのトンネリング要求を開始するようにLACを設定します。

   user { domain *domain-name* | **fullusername** *user-name* }

   デフォルトでは、LACはどのユーザーに対してもトンネリング要求を開始しません。

LNSのIPアドレスの指定

このタスクについて

最大5つのLNSのIPアドレスを指定できます。LACは、LNSから確認応答を受信するまで、指定されたLNSに対して設定順に連続してL2TPトンネリング要求を開始します。その後、LNSがトンネルピアになります。

手順

1. システムビューに入ります。

   system-view
2. LACモードでL2TPグループビューを入力します。

   l2tp-group *group-number* **[mode lac]**
3. LNSのIPアドレスを指定します。

   lns-ip { *ip-address* } **&<1-5>**

   デフォルトでは、LNSのIPアドレスは指定されません。

L2TPトンネルパケットの送信元IPアドレスの設定

制限事項とガイドライン

ハイアベイラビリティを実現するには、ベストプラクティスとして、ループバックインターフェイスのIPアドレスをLAC上のL2TPトンネルパケットの送信元IPアドレスとして使用します。LACとLNSの間に等コストルーティングパスが存在する場合は、ループバックインターフェイスのIPアドレスをL2TPトンネルパケットの送信元IPアドレスとして使用する必要があります。これを行うには、source-ipコマンドを使用するか、RADIUSサーバーを使用してループバックインターフェイスアドレスを割り当てます。

手順

1. システムビューに入ります。

   system-view
2. LACモードでL2TPグループビューを入力します。

   l2tp-group *group-number* **[mode lac]**
3. L2TPトンネルパケットの送信元IPアドレスを設定します。

   source-ip *ip-address*

   デフォルトでは、L2TPトンネルパケットの送信元IPアドレスは、出力インターフェイスのIPアドレスです。

非表示モードでのAVPデータの転送のイネーブル化

このタスクについて

L2TPはAttribute Value Pairs(AVP)を使用して、トンネルネゴシエーションパラメータ、セッションネゴシエーションパラメータ、およびユーザー認証情報を送信します。非表示モードでAVPデータを転送すると、ユーザーパスワードなどの機密性の高いAVPデータを非表示にできます。この機能は、送信前にtunnel passwordコマンドを使用して設定されたキーでAVPデータを暗号化します。

制限事項とガイドライン

この設定は、トンネル認証機能がイネーブルになっている場合にだけ有効になります。トンネル認証の設定の詳細については、『L2TPトンネル認証の設定』を参照してください。

手順

1. システムビューに入ります。

   system-view
2. LACモードでL2TPグループビューを入力します。

   l2tp-group *group-number* **[mode lac]**
3. 非表示モードでAVPデータの転送をイネーブルにします。

   tunnel avp-hidden

   デフォルトでは、AVPデータはプレーンテキストで転送されます。

LACでのAAA認証の設定

LACでAAA認証を設定して、リモートダイヤルアップユーザーを認証し、資格のあるユーザーだけにトンネリング要求を開始できます。資格のないユーザーに対してはトンネルは確立されません。

デバイスは、ローカルAAA認証とリモートAAA認証の両方をサポートします。

- ローカルAAA認証では、ローカルユーザーを作成し、LAC上の各リモートユーザーにパスワードを設定します。次に、LACは、指定されたユーザー名とパスワードをローカルに設定されたユーザー名とパスワードと照合することによって、リモートユーザーを認証します。
- リモートAAA認証の場合は、RADIUS/HWTACACSサーバー上で各ユーザーのユーザー名とパスワードを設定します。LACは次に、認証のためにリモートユーザーのユーザー名とパスワードをサーバーに送信します。

AAAの詳細については、『Security Configuration Guide』を参照してください。

LACでAAA認証をイネーブルにするには、ユーザークセスインターフェイスでPPPユーザーのPAP認証またはCHAP認証も設定する必要があります。PAPまたはCHAPの設定については、『Layer 2 WAN Access Configuration Guide』の「Configuring PPP」を参照してください。

L2TPトンネルを自動的に確立するようにLACを設定する

1. システムビューに入ります。

   system-view

2. 仮想PPPインターフェイスを作成し、そのビューを入力します。

   interface virtual-ppp interface-number

3. 仮想PPPインターフェイスのIPアドレスを設定します。

   ○ 仮想PPPインターフェイスにIPアドレスを割り当てます。

   ip address *address mask*

   デフォルトでは、IPアドレスは設定されていません。

   ○ 仮想PPPインターフェイス上でIPアドレスネゴシエーションをイネーブルにします。

   ip address ppp-negotiate

   デフォルトでは、仮想PPPインターフェイスのIPアドレスネゴシエーションはディセーブルになっています。

4. 認証されるようにピアを設定します。

   ppp papまたはppp chapコマンドを使用して、PPP認証方式を指定し、PPPユーザーのユーザー名とパスワードを設定します。次に、LNSはPPPユーザーを認証します。詳細については、『Layer 2 WAN Access Command Reference』の「PPPコマンド」を参照してください。

5. (任意)インターフェイスの説明を設定します。

   description *text*

   デフォルトでは、インターフェイスの説明はinterface-name Interfaceの形式になっています(Virtual-PPP254 Interfaceなど)。

6. (任意)インターフェイスのMTUサイズを設定します。

   mtu *size*

   デフォルト設定は1500バイトです。

7. (任意)インターフェイスの予想帯域幅を設定します。

   bandwidth *bandwidth-value*

   デフォルトでは、予想される帯域幅(kbps)は、インターフェイスボーレートを1000で割った値です。

8. (任意)インターフェイスを起動します。

   undo shutdown

   デフォルトでは、インターフェイスはアップ状態です。

9. LNSとのL2TPトンネルを自動的に確立するようにLACを設定します。

   l2tp-auto-client l2tp-group *group-number*

デフォルトでは、LACはL2TPトンネルを確立しません。

LA C自動開始モードで自動的に確立されたL2TPトンネルは、undo l2tp-auto-clientコマンドまたはundo L2TP-group group-numberコマンドを使用してトンネルを削除するまで存在します。

ポーリング機能の設定

このタスクについて

ポーリング機能は、L2TP-LINK状態をチェックします。

L2TPカプセル化を使用するインターフェイスでは、リンク層はキープアライブインターバルでキープアライブを送信して、ピアのアベイラビリティを検出します。キープアライブリトライ制限に達したときにインターフェイスがキープアライブの受信に失敗した場合、インターフェイスはリンクを切断し、リンク層ダウンイベントを報告します。

キープアライブリトライ制限を設定するには、timer-hold retryコマンドを使用し

ます。キープアライブインターバルを0に設定すると、キープアライブの送信が

ディセーブルになります。

制限事項とガイドライン

低速リンクでは、インターフェイスの誤ったシャットダウンを防ぐために、キープアライブインターバルを増やします。この状況は、リンク上で大きなパケットが送信されているためにキープアライブが遅延する場合に発生する可能性があります。

キープアライブインターバルは、ネゴシエーションタイムアウト時間よりも短くする必要があります。

手順

1. システムビューに入ります。

   system-view
2. 仮想PPPインターフェイスビューを入力します。

   interface virtual-ppp *interface-number*
3. キープアライブインターバルを設定します。

   timer-hold *seconds*

   デフォルト設定は10秒です。
4. キープアライブ再試行制限を設定します。

   timer-hold retry *retries*

   デフォルト設定は5です。

仮想PPPインターフェイスのトラフィック処理スロットの指定

このタスクについて

仮想PPPインターフェイス上のすべてのトラフィックを同じスロットで処理する必要がある機能の場合は、トラフィック処理スロットを指定します。

高可用性のために、プライマリトラフィック処理スロットとバックアップトラフィック処理スロットを1つずつ指定できます。
serviceコマンドとservice standbyコマンドです。

インターフェイスにプライマリスロットとバックアップスロットの両方を指定した場合、そのインターフェイス上

のトラフィックは次のように処理されます。

- バックアップスロットは、プライマリスロットが使用できなくなったときに引き継ぎます。バックアップスロットは、プライマリスロットが再び使用可能になった後も、インターフェイスのトラフィックを処理し続けます。バックアップスロットが使用できなくなるまで、スイッチオーバーは発生しません。
- 使用可能なトラフィック処理スロットが指定されていない場合、トラフィックは到着したスロットで処理されます。その後、最初に使用可能になった処理スロットが再び使用可能になります。

インターフェイスにプライマリまたはバックアップトラフィック処理スロットを指定しない場合、そのインターフェイス上のトラフィックは、トラフィックが到着するスロットで処理されます。

このコマンドは、L2TPデータメッセージだけに影響します。制御メッセージは常にアクティブMPUで処理されます。

ハードウェアと機能の互換性

ハードウェア	機能の互換性
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK	しない
MSR810-CNDE-SJK	
MSR810-LMS、MSR810-LUS	しない
MSR810-LMS-EA、MSR810-LME	• スタンドアロンモード:No • IRFモードの場合:はい
MSR2600-6-X1、MSR2600-10-X1	しない
MSR 2630	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3600-28、MSR3600-51	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3600-28-SI、MSR3600-51-SI	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES、MSR3610-IE-EAD	しない
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	• スタンドアロンモード:No • IRFモードの場合:はい
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3610-G、MSR3620-G	• スタンドアロンモード:No • IRFモードの場合:はい

ハードウェア	機能の互換性
MSR 810-W-WInt、MSR 810-LM-WInt	• スタンドアロンモード:No • IRFモードの場合:はい
MSR830-4LM-WiNet	• スタンドアロンモード:No • IRFモードの場合:はい
MSR 830-5 BEI-WInt、MSR 830-6 EI-WInt、MSR 830-10 BEI-WInt	• スタンドアロンモード:No • IRFモードの場合:はい

MSR 830-6 BHI-WInt、MSR 830-10 BHI-WInt	• スタンドアロンモード:No • IRFモードの場合:はい
MSR 2600-6-WInt、MSR 2600-10-X 1-WInt	• スタンドアロンモード:No • IRFモードの場合:はい
MSR 2630-WInt	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3600-28-WiNet	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3610-X1-WiNet	• スタンドアロンモード:No • IRFモードの場合:はい
MSR 3610-WInt、MSR 3620-10-WInt、MSR 3620-DP-WInt、 MSR 3620-WInt、MSR 3660-WInt	• スタンドアロンモード:No • IRFモードの場合:はい

ハードウェア	機能の互換性
MSR2630-XS	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3600-28-XS	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3610-XS	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3620-XS	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3610-I-XS	• スタンドアロンモード:No • IRFモードの場合:はい
MSR3610-IE-XS	• スタンドアロンモード:No • IRFモードの場合:はい

ハードウェア	機能の互換性
MSR810-LM-GL	しない
MSR810-W-LM-GL	しない
MSR830-6EI-GL	• スタンドアロンモード:No • IRFモードの場合:はい
MSR830-10EI-GL	• スタンドアロンモード:No • IRFモードの場合:はい
MSR830-6HI-GL	• スタンドアロンモード:No • IRFモードの場合:はい
MSR830-10HI-GL	• スタンドアロンモード:No • IRFモードの場合:はい
MSR2600-6-X1-GL	しない
MSR3600-28-SI-GL	• スタンドアロンモード:No • IRFモードの場合:はい

制限事項とガイドライン

スロットスイッチオーバーの処理を回避するには、バックアップスロットを指定する前にプライマリスロットを指定します。プライマリスロットを指定する前にバックアップスロットを指定すると、プライマリスロットを指定した直後にトラフィックがプライマリスロットにスイッチオーバーされます。

手順

1. システムビューに入ります。

   system-view
2. 仮想PPPインターフェイスビューを入力します。

   interface virtual-ppp *interface-number*
3. インターフェイスのプライマリトラフィック処理スロットを指定します。

   IRFモードの場合:

   service slot *slot-number*

   デフォルトでは、インターフェイスにプライマリトラフィック処理スロットは指定されていません。
4. インターフェイスのバックアップトラフィック処理スロットを指定します

   IRFモードの場合:

   service standby slot *slot-number*

   デフォルトでは、インターフェイスにバックアップトラフィック処理スロットは指定されていません。

仮想PPPインターフェイスのデフォルト設定の復元

制限事項とガイドライン

defaultコマンドは、進行中のネットワークサービスを中断する可能性があります。このコマンドをライブネットワークで実行する場合は、このコマンドの影響を十分に認識していることを確認してください。

defaultコマンドは、コマンドの依存関係やシステム制限などの理由で、一部のコマンドのデフォルト設定の復元に失敗する場合があります。これらのコマンドを識別するには、インターフェイスビューでこのコマンドを表示します。これらのコマンドのundo形式を使用するか、コマンドリファレンスに従って個々にデフォルト設定を復元します。復元が失敗する場合は、エラーメッセージの指示に従って問題を解決します。

手順

1. システムビューに入ります。

   system-view
2. 仮想PPPインターフェイスビューを入力します。

   interface virtual-ppp *interface-number*
3. インターフェイスのデフォルト設定を復元します。

   default

LNSの設定

VTインターフェイスの作成

L2TPセッションが確立されると、ピアとのデータ交換にVirtual Access(VA)インターフェイスが必要になります。システムは、Virtual Template(VT)インターフェイスのパラメータに基づいて、VAインターフェイスを動的に作成します。LNSを設定するには、まずVTインターフェイスを作成し、次のパラメータを設定します。

- インターフェイスのIPアドレス。
- PPPユーザーの認証モード。
- LNSによってPPPユーザーに割り当てられたIPアドレス。

VTインターフェイスの設定については、『Layer 2 WAN Access Configuration Guide』の「PPP configuration」および『Layer 3 IP Services Configuration Guide』の「IP addressing configuration」を参照してください。

VAプールの設定

このタスクについて

VAプールには、VAインターフェイスのグループが含まれています。VAプールを設定して、L2TP接続の確立または終端のパフォーマンスを向上させることができます。LNSは、要求元ユーザーのプールからVAインターフェイスを選択し、ユーザーがオフラインになったときにVAインターフェイスを解放します。VAプールが枯渇すると、システムはL2TP接続のVAインターフェイスを作成し、ユーザーがオフラインになったときに削除します。

制限事項とガイドライン

VTインターフェイスは、1つのVAプールだけに関連付けることができます。VAプールの容量を変更するには、以前の設定を削除し、VAプールを再設定します。

VAプールを作成または削除するには時間がかかります。VAプールを作成または削除するプロセスでは、ユーザーはオンラインまたはオフラインにできますが、VAプールは有効になりません。

リソース不足のため、指定された数よりも少ないVAインターフェイスを含むVAプールが作成される場合があります。使用可能なVAインターフェイスの数およびVAプールの現在の状態を表示するには、display l2tp va-poolコマンドを使用します。

VAプールは多くのシステムメモリを占有するため、適切な容量のVAプールを作成します。VAプールを削除しても、VAプール内でVAインターフェイスを使用しているユーザーはログオフされません。

手順

1. システムビューに入ります。

   system-view
2. VAプールを作成します。

l2tp virtual-template *template-number* **va-pool** *va-volume*

デフォルトでは、VAプールは存在しません。

LACからのL2TPトンネリング要求を受け入れるようにLNSを設定する方法

このタスクについて

トンネリング要求を受信すると、LNSは次の動作を実行します。

- トンネルピア(LAC)の名前が設定されている名前と一致するかどうかをチェックして、トンネリング要求を受け入れるかどうかを決定します。
- VAインターフェイスの作成に使用するVTインターフェイスを決定します。

手順

1. システムビューに入ります。

   system-view
2. LNSモードでL2TPグループビューを入力します。

   l**2tp-group** *group-number* **[mode lns]**
3. LACからのトンネリング要求を受け入れるようにLNSを設定し、トンネル設定に使用するVTインターフェイスを指定します。
   - L2TPグループ番号が1の場合:

     allow l2tp virtual-template *virtual-template-number* [**remote** *remote-name*]
   - L2TPグループ番号が1でない場合:

     allow l2tp virtual-template *virtual-template-number* **remote** *remote-name*

   デフォルトでは、LNSはすべてのLACからのトンネリング要求を拒否します。

   L2TPグループ番号が1の場合、remote remote-nameオプションはオプションです。このオプションを指定しない場合、LNSは任意のLACからのトンネリング要求を受け入れます。

LNSでのユーザー認証の設定

このタスクについて

LNSは、セキュリティを強化するために、LAC上で認証に合格したユーザーを認証するように設定できます。この場合、ユーザーはLAC上で1回、LNS上で1回認証されます。L2TPトンネルは、両方の認証が成功した場合にだけ確立できます。

LNSには、次の認証方式がプライオリティの昇順で提供されます。

- **プロキシ認証**: LNSはLACを認証プロキシとして使用します。LACは、ユーザーからのすべてのユーザー認証情報と、LAC自体に設定されている認証方式をLNSに送信します。次に、LNSは、受信した情報とローカルに設定された認証方式に従って、ユーザーの有効性をチェックします。
- **必須CHAP認証**: LNSはCHAP認証を使用して、LAC上で認証に合格したユーザーを再認証します。
- **LCP再ネゴシエーション**: LNSはLACプロキシ認証情報を無視し、ユーザーとのLCPネゴシエーションの新しいラウンドを実行します。

LNSは、設定に応じて認証方式を選択します。

- LCP再ネゴシエーションと必須CHAP認証の両方を設定した場合、LNSはLCP再ネゴシエーションを使用します。

- 必須CHAP認証だけを設定した場合、LNSはプロキシ認証が成功した後にユーザーのCHAP認証を実行します。
- LCP再ネゴシエーションも必須CHAP認証も設定しない場合、LNSはプロキシ認証にLACを使用します。

LNSでのユーザー認証に関する制約事項および注意事項

この必須のCHAP認証方式およびLCP再ネゴシエーション方式は、NASが開始するL2TPトンネルに対してだけ有効です。

必須CHAP認証を有効にするには、LNSのVTインターフェイス上でPPPユーザーのCHAP認証も設定する必要があります。

LNSがLCPネゴシエーションパラメータを受け入れないようにするには、LNSとユーザーの間で新しいラウンドのLCPネゴシエーションを実行するようにこの機能を設定します。この場合、LNSは、対応するVTインターフェイスに設定された認証方式を使用してユーザーを認証します。

必須CHAP認証の設定

1. システムビューに入ります。

   system-view
2. LNSモードでL2TPグループビューを入力します。

   l2tp-group *group-number* **[mode lns]**
3. 必須CHAP認証を設定します。

   mandatory-chap

   デフォルトでは、CHAP認証はLNSでは実行されません。

   一部のユーザーはLNSでの認証をサポートしていない可能性があります。この場合、LNSでのCHAP認証は失敗するため、この機能をイネーブルにしないでください。
4. システムビューに戻ります。

   quit
5. VT interface viewと入力し、PPPユーザーの認証タイプをCHAPに設定します。

   VTインターフェイスの詳細については、『Layer 2 WAN Access Configuration Guide』の「PPP configuration」を参照してください。

LCP再ネゴシエーションの設定

1. システムビューに入ります。

   system-view
2. LNSモードでL2TPグループビューを入力します。

   l2tp-group *group-number* **[mode lns]**
3. ユーザーとのLCP再ネゴシエーションを実行するようにLNSを設定します。

   mandatory-lcp

   デフォルトでは、LNSはユーザーとのLCP再ネゴシエーションを実行しません。

   このコマンドは、NASが開始するL2TPトンネルに対してだけ有効です。

   LCP再ネゴシエーションをイネーブルにしても、対応するVTインターフェイスに認証を設定しない場合、LNSはユーザーに対して追加認証を実行しません。

LNSでのAAA認証の設定

LNSでAAA認証を設定すると、LNSはリモートアクセスユーザーのユーザー名とパスワードを認証できます。ユーザーがAAA認証に合格した場合、そのユーザーはLNSと通信してプライベートネットワークにアク

セスできます。

次のいずれかの場合に、LNSでAAA認証を設定します。

- LCP再ネゴシエーションは、NAS開始モードでは設定されません。
- VTインターフェイスはPPPユーザー認証で設定され、LCP再ネゴシエーションはNAS開始モードで設定されます。
- VTインターフェイスは、クライアント起動モードまたはLAC自動起動モードでPPPユーザー認証を使用して設定されます。

LNS側のAAA設定は、LAC上の設定と類似しています(『Configuring AAA authentication on an LAC』を参照)。

LNSが1秒間に処理できるICRQパケットの最大数の設定

制限事項とガイドライン

デバイスのパフォーマンス低下を回避し、LNSがICRQ要求を正しく処理できることを確認するには、この機能を使用してICRQパケット処理レート制限を調整します。

手順

1. システムビューに入ります。

   system-view
2. LNSが1秒間に処理できるICRQパケットの最大数を設定します。

   l2tp icrq-limit *number*

   デフォルトでは、LNSが1秒間に処理できるICRQパケットの最大数は制限されていません。

オプションのL2TPパラメータの設定

L2TPトンネル認証の設定

このタスクについて

トンネル認証を使用すると、LACとLNSは互いに認証できます。LACまたはLNSのいずれかがトンネル認証要求を開始できます。

トンネル認証は、両側または両側でイネーブルにできます。

トンネル認証が両側または両側でイネーブルになっている場合に、トンネルの確立を成功させるには、LACとLNSに同じ非ヌルキーを設定します。トンネル認証キーを設定するには、tunnel passwordコマンドを使用します。

どちらの側もトンネル認証をイネーブルにしていない場合、LACとLNSのキー設定はトンネルの確立に影響しません。

制限事項とガイドライン

トンネルセキュリティを確保するには、トンネル認証をイネーブルにします。

トンネル認証キーを変更しても、現在のトンネルの通常の通信には影響しません。トンネル認証キーの変更は、次のトンネル確立時に有効になります。

手順

1. システムビューに入ります。

system-view

2. L2TPグループビューを入力します。

   l2tp-group *group-number* **[mode { lac | lns }]**

3. L2TPトンネル認証をイネーブルにします。

   tunnel authentication

   デフォルトでは、L2TPトンネル認証はイネーブルです。

4. トンネル認証キーを設定します。

   tunnel password { cipher | simple } *string*

   デフォルトでは、キーは設定されていません。

Hello間隔の設定

このタスクについて

トンネルの接続性をチェックするために、LACとLNSは定期的に互いにHelloパケットを送信します。Helloパケットを受信すると、LACまたはLNSは応答パケットを返します。LACまたはLNSは、Hello間隔内にピアから応答パケットを受信しない場合、Helloパケットを再送信します。Helloパケットを5回送信した後にピアから応答パケットを受信しない場合、L2TPトンネルがダウンしていると見なされます。

手順

1. システムビューに入ります。

   system-view

2. L2TPグループビューを入力します。

   l2tp-group *group-number* **[mode { lac | lns }]**

3. ハローインターバルを設定します。

   tunnel timer hello *hello-interval*

   デフォルト設定は60秒です。

セッションフロー制御のイネーブル化

このタスクについて

この機能は、送信されたパケットにシーケンス番号を追加し、それらの番号を使用して、順番どおりに到着しないパケットを並べ替え、失われたパケットを検出します。

この機能は、送受信されたL2TPデータメッセージの両方で有効になります。L2TPセッションは、LACまたはLNSのいずれかがこの機能でイネーブルになっている場合に、この機能をサポートします。

手順

1. システムビューに入ります。

   system-view

2. L2TPグループビューを入力します。

   l2tp-group *group-number* **[mode { lac lns }]**

3. セッションフロー制御機能をイネーブルにします。

   tunnel flow-control

   デフォルトでは、この機能はディセーブルになっています。

L2TPパケットのDSCP値の設定

このタスクについて

DSCPフィールドは、IP ToSバイトの最初の6ビットです。このフィールドは、転送するIPパケットのプライオリティを示します。この機能は、L2TPがPPPフレームをIPパケットにカプセル化するときに、IPパケットのDSCP値を設定します。

手順

1. システムビューに入ります。
   system-view
2. L2TPグループビューを入力します。
   l2tp-group *group-number* **[mode { lac | lns }]**
3. L2TPパケットのDSCP値を設定します。
   ip dscp *dscp-value*
   デフォルト設定は0です。

トンネルピアのVPNへの割り当て

このタスクについて

デフォルトでは、デバイスはL2TP制御メッセージおよびデータメッセージをパブリックネットワーク経由で送信します。この機能を使用すると、デバイスは、VPN内のルーティングテーブルを検索することによって、これらをVPN内で送信します。

制限事項とガイドライン

1つのL2TPエンドポイントがVPN内にある場合は、2つのエンドポイント間の正しいパケット転送のために、ピアエンドポイントをVPNに割り当てます。

トンネルピアおよびトンネルピアに接続する物理ポートは、同じVPNに属している必要があります。この物理ポートが属するVPNは、ip binding vpn-instanceコマンドを使用して設定されます。

手順

1. システムビューに入ります。
   system-view
2. L2TPグループビューを入力します。
   l2tp-group *group-number* **[mode { lac | lns }]**
3. トンネルピアをVPNに割り当てます。
   vpn-instance *vpn-instance-name*
   デフォルトでは、トンネルピアはパブリックネットワークに属します。

LTSのTSA IDの設定

このタスクについて

ループを検出するために、LTSは設定されたTSA IDを受信したICRQパケット内の各TSA ID AVPと比較します。

- 一致するものが見つかると、ループが存在します。LTSはただちにセッションを切断します。
- 一致するものが見つからない場合、LTSは次の操作を実行します。

- 設定されたTSA IDを新しいTSA ID AVPにカプセル化します。
- パケットに追加します。
- パケットをネクストホップLTSに送信します。

制限事項とガイドライン

ループ検出エラーを回避するには、各LTSのTSA IDが一意であることを確認します。

手順

1. システムビューに入ります。

   system-view
2. LTSのTSA IDを設定し、LTSでL2TPループ検出をイネーブルにします。

   l2tp tsa-id *tsa-id*

   デフォルトでは、LTSのTSA IDは設定されておらず、L2TPループ検出はLTSでディセーブルになっています。

L2TPトンネルの受信ウィンドウサイズの設定

このタスクについて

デバイスが多数の不規則なパケットを処理できるようにするには、このコマンドを使用して、L2TPトンネルの受信ウィンドウサイズを拡大します。

デバイスは、受信ウィンドウを使用して、パケットシーケンス番号に基づいて不規則なパケットを並べ替えます。

パケットのシーケンス番号が受信ウィンドウ内にあるが、ウィンドウの最小値と等しくない場合、デバイスは次の動作を実行します。

1. デバイスはパケットをバッファします。
2. 受信側ウィンドウの最小値と最大値が1ずつ増加します。
3. デバイスは次に到着するパケットのチェックを継続します。

パケットのシーケンス番号が受信ウィンドウの最小値に等しい場合、デバイスは次の動作を実行します。

1. デバイスはパケットを処理します。
2. 受信側ウィンドウの最小値と最大値が1ずつ増加します。
3. デバイスは、受信ウィンドウの新しい最小値に等しいシーケンス番号を持つパケットがないか、バッファされたパケットをチェックします。
4. 必要なパケットが見つからない場合、デバイスは次に到着するパケットをチェックします。

パケットのシーケンス番号が受信ウィンドウ内にない場合、デバイスはパケットをドロップします。

制限事項とガイドライン

L2TPトンネル確立プロセスでは、デバイスはL2TPグループビューで指定された値を受信ウィンドウサイズとして使用します。

L2TPトンネルの確立後に受信ウィンドウサイズを変更しても、確立されたL2TPトンネルには影響しません。

手順

1. システムビューに入ります。

   system-view
2. L2TPグループビューを入力します。

   l2tp-group *group-number* **[mode { lac | lns }]**

3. L2TPグループの受信ウィンドウサイズを設定します。

   tunnel window receive *size*

   デフォルトでは、L2TPトンネルの受信ウィンドウサイズは1024です。

L2TPトンネルの送信ウィンドウサイズの設定

このタスクについて

一部のネットワークでは、ピアエンドのパケット処理能力がピアエンドの受信ウィンドウサイズと一致しない場合があります。たとえば、ピアエンドの実際のパケット処理能力は10ですが、ピアエンドの受信ウィンドウサイズは20です。安定したL2TPサービスを確保するために、デバイスの送信ウィンドウサイズを調整して、ピアエンドの実際のパケット処理能力に一致させることができます。

制限事項とガイドライン

L2TPグループビューで設定された送信ウィンドウサイズは、L2TPトンネル確立プロセスで取得されます。

- 送信ウィンドウサイズが0の場合、デバイスはデフォルトの送信ウィンドウサイズを使用します。
- 送信ウィンドウサイズが0でない場合、デバイスは指定された値を送信ウィンドウサイズとして使用します。

L2TPトンネルの確立後に送信ウィンドウサイズを変更しても、確立されたL2TPトンネルには影響しません。

手順

1. システムビューに入ります。

   system-view

2. L2TPグループビューを入力します。

   l2tp-group *group-number* **[mode { lac | lns }]**

3. L2TPグループの送信ウィンドウサイズを設定します。

   tunnel window send *size*

   デフォルトでは、L2TPトンネルの送信ウィンドウサイズは0です。これは、トンネル確立プロセスでピアエンドから送信されたメッセージで伝送される受信ウィンドウサイズの値を使用することを意味します。ピアエンドからのメッセージがトンネル確立プロセスで受信ウィンドウサイズを伝送しない場合、デバイスの送信ウィンドウサイズは4になります。

L2TPベースのEADのイネーブル化

このタスクについて

高度なセキュリティを必要とする一部のネットワーク環境では、この機能を構成し、セキュリティポリシーサーバーを使用して、L2TP認証に合格したユーザーに対してさらにセキュリティチェックを実行します。EAD認証に合格したユーザーは、ネットワークリソースにアクセスできます。EAD認証に失敗したユーザーは、隔離領域内のリソースにのみアクセスできます。

制限事項とガイドライン

LNSでEADがイネーブルになっていても、CAMS/IMCサーバーでACLまたはルールが設定されていない場合、または間違っている場合、EAD認証は失敗します。

LNSは異なるACLを使用して、異なるINodeクライアントからのパケットをフィルタリングできます。

ベストプラクティスとして、インターネット上のINodeクライアントにはEAD認証を使用し、LAN上のINodeクライアントにはポータル認証を使用します。

前提条件

L2TPベースのEADをイネーブルにする前に、AAA、RADIUS、L2TP、Portal、およびセキュリティポリシーサーバーが必要に応じて設定されていることを確認します。

AAA、RADIUS、およびポータルの詳細については、『Security Configuration Guide』を参照してください。

セキュリティポリシーサーバーの設定の詳細については、『CAMS EAD Security Policy Manager Help』および『CAMS EAD Security Policy Manager Help』を参照してください。

手順

1. システムビューに入ります。

   system-view
2. VTインターフェイスを作成し、そのビューを入力します。

   interface virtual-template *interface-number*
3. L 2 TPベースのEADをイネーブルにします。

   ppp access-control enable

   デフォルトでは、L 2 TPベースEADはディセーブルになっています。

IMSI/SNバインディング認証の設定

LNSでのIMSI/SNバインディング認証の設定

このタスクについて

この機能により、3Gおよび4Gネットワークのセキュリティが向上します。この機能を設定すると、AAAサーバーは、LNSから受信したユーザー名/パスワードおよびIMSI/SN情報がAAAサーバーの設定と一致するかどうかをチェックします。ユーザーがオンラインになるのは、LNSがユーザー名/パスワード認証とIMSI/SN情報チェックの両方に合格した場合だけです。3Gおよび4Gの詳細については、「3G/4Gモデムの管理」を参照してください。

制限事項とガイドライン

次のいずれかの条件でIMSI/SNバインディング認証を開始するようにLNSにこの機能を設定します。

- 3Gまたは4GルータはLACクライアントとして動作し、クライアント開始モードでLNSにアクセスします。
- 4GルータはLACとして動作し、LAC自動開始モードでLNSにアクセスするように自動的にトリガーされます。

LNSがLACクライアントまたはLACのIMSI/SN情報を正常にネゴシエートするには、LNSとのL2TPトンネルを確立するLACクライアントまたはLAC上で、この機能を設定します。

手順

1. システムビューに入ります。

   system-view
2. VT interface viewと入力します。

   interface virtual-template *interface-number*
3. 次のいずれかの方法を使用して、IMSI/SNバインディング認証情報を設定します。
   - 次のコマンドを順番に実行して、LNSがIMSI/SNバインディング認証要求を開始できるようにします。

     ppp lcp imsi request

     ppp lcp sn request

     デフォルトでは、LNSはIMSI/SNバインディング認証要求を開始しません。

- 受信した認証情報の区切り文字を設定します。

  ppp user accept-format imsi-sn split *splitchart*

  デフォルトでは、受信した認証情報にはセパレータは設定されていません。

ネゴシエーションされたIMSI/SN情報は、受信した認証情報から分割されたIMSIまたはSN情報よりも優先されます。認証プロセス中にピアからIMSIまたはSN情報を受信しなかった場合、受信した認証情報から分割されたIMSIまたはSN情報が使用されます。

4. (任意)クライアントのユーザー名を認証用のIMSIまたはSN情報に置き換えます。

   ppp user replace { imsi | sn }

   デフォルトでは、クライアントのユーザー名が認証に使用されます。

LACクライアントでのIMSI/SNバインディング認証の設定

このタスクについて

この機能を設定した後、LACクライアントは認証プロセス中に次のいずれかの操作を実行します。

- LACクライアントがLNSからバインディング認証要求を受信すると、LACクライアントは応答メッセージを通じてローカルIMSI/SN情報をLNSに送信します。
- クライアントがLNSからバインディング認証要求を受信しない場合、LACクライアントは、ppp user attach-format imsi-sn splitコマンドで設定された規則を使用して、ローカルIMSI/SN情報をユーザー名に含めます。

制限事項とガイドライン

この機能は、デバイスが3Gまたは4Gルータとして動作する場合にだけサポートされます。3Gおよび4Gルータの詳細については、「3G/4Gモデムの管理」を参照してください。

手順

1. システムビューに入ります。

   system-view

2. シリアルインターフェイスビューを入力します。

   interface serial *cellular-number:set-number*

   シリアルインターフェイスは、serial-setコマンドを使用して、セルラーインターフェイスからチャネル化されます。

3. LACクライアントがLNSからのIMSIバインディング認証要求を受け入れるようにします。

   ppp lcp imsi accept

   デフォルトでは、LACクライアントはIMSIバインディング認証要求を受け入れません。

4. LACクライアントがLNSからのSNバインディング認証要求を受け入れるようにします。

   ppp lcp sn accept

   デフォルトでは、LACクライアントはSNバインディング認証要求を受け入れません。

5. (任意)LACクライアント上でIMSI情報を設定します。

   ppp lcp imsi string *imsi-info*

   デフォルトでは、LACクライアントは自動的にデバイスからIMSI情報を取得します。

6. (任意)LACクライアント上でSN情報を設定します。

   ppp lcp sn string *sn-info*

   デフォルトでは、LACクライアントは自動的にデバイスからSN情報を取得します。

7. (任意)送信される認証情報の区切り文字を設定します。

   ppp user attach-format imsi-sn split *splitchart*

デフォルトでは、送信される認証情報にはセパレータは設定されていません。

L2TPの表示コマンドおよびメンテナンスコマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
L2TPトンネル情報を表示します。	**display l2tp tunnel [statistics]**
L2TPセッション情報を表示します。	**display l2tp session [statistics]**
一時的なL2TPセッションに関する情報を表示します。	**display l2tp session temporary**
仮想PPPインターフェイスに関する情報を表示します。	**display interface [virtual-ppp** [interface-number]] [**brief** [**description** | **down**]]
L2TPのVAプール情報を表示します。	**display l2tp va-pool**
VTインターフェイス上のPPPセッションのアクセスコントロール情報を表示します。	**display ppp access-control interface virtual-template** *interface-number*
L2TPトンネルを切断します。	**reset l2tp tunnel { id** *tunnel-id* | **name** *remote-name* }
仮想PPPインターフェイスの統計情報を消去します。	**reset counters interface** [**virtual-ppp** [*interface-number*]]

L2TPの設定例

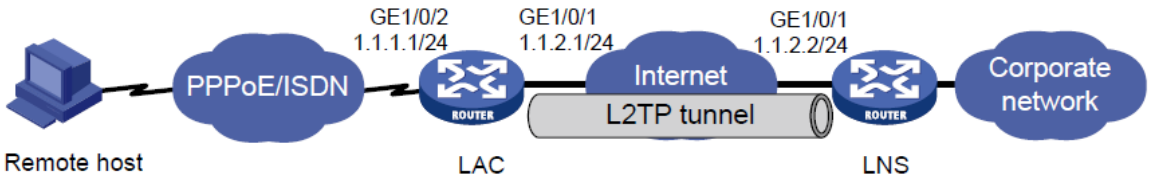
例:NAS開始L2TPトンネルの設定

ネットワーク構成

図11に示すように、PPPユーザーはLACを介してLNSに接続されています。

PPPユーザーが企業ネットワークにアクセスできるように、LACとLNSの間にL2TPトンネルを設定します。

図11 ネットワーク図



手順

1. LACを設定します。

   #インターフェイスのIPアドレスを設定します(詳細は省略します)。

   #vpdnuserという名前のローカルユーザーを作成し、パスワードを設定して、PPPサービスを有効にします。

   <LAC> system-view

   [LAC] local-user vpdnuser class network

   [LAC-luser-network-vpdnuser] password simple Hello

[LAC-luser-network-vpdnuser] service-type ppp

[LAC-luser-network-vpdnuser] quit

#ISPドメインシステムでPPPユーザーのローカル認証を設定します。

[LAC] domain system

[LAC-isp-system] authentication ppp local

[LAC-isp-system] quit

#インターフェイスVirtual-Template 1でCHAP認証を設定します。

[LAC] interface virtual-template 1

[LAC-Virtual-Template1] ppp authentication-mode chap domain system

[LAC-Virtual-Template1] quit

#GigabitEthernet1/0/2上でPPPoEサーバーをイネーブルにし、インターフェイスを仮想:テンプレート1にバインドします

[LAC] interface gigabitethernet 1/0/2

[LAC-GigabitEthernet1/0/2] pppoe-server bind virtual-template 1

[LAC-GigabitEthernet1/0/2] quit

#L2TPを有効にします。

[LAC] l2tp enable

#L2TPグループ1をLACモードで作成します。

[LAC] l2tp-group 1 mode lac

#ローカルトンネル名をLACとして設定します。

[LAC-l2tp1] tunnel name LAC

#LACがトンネリング要求を開始する条件として、PPPユーザーvpdnuserを指定します。

[LAC-l2tp1] user fullusername vpdnuser

LNS IPアドレスを 1.1.2.2に指定します。

[LAC-l2tp1] lns-ip 1.1.2.2

#トンネル認証をイネーブルにし、トンネル認証キーをaabbccに指定します。

[LAC-l2tp1] tunnel authentication

[LAC-l2tp1] tunnel password simple aabbcc

[LAC-l2tp1] quit

2. LNSを設定します。

#インターフェイスのIPアドレスを設定します(詳細は表示されません)。

#vpdnuserという名前のローカルユーザーを作成し、パスワードを設定して、PPPサービスを有効にします。

<LNS> system-view

[LNS] local-user vpdnuser class network

[LNS-luser-network-vpdnuser] password simple Hello

[LNS-luser-network-vpdnuser] service-type ppp

[LNS-luser-network-vpdnuser] quit

#ISPドメインシステムでPPPユーザーのローカル認証を設定します。

[LNS] domain system

[LNS-isp-system] authentication ppp local

[LNS-isp-system] quit

#L2TPを有効にします。

[LNS] l2tp enable

#PPPアドレスプールを作成します。

[LNS] ip pool aaa 192.168.0.10 192.168.0.20

[LNS] ip pool aaa gateway 192.168.0.1

#Create Virtual-Template 1で、そのPPP認証モードをCHAPに指定し、アドレスプールaaaを使用してIPアドレスをPPPユーザーに割り当てます。

[LNS] interface virtual-template 1

[LNS-virtual-template1] ppp authentication-mode chap domain system

[LNS-virtual-template1] remote address pool aaa

[LNS-virtual-template1] quit

#LNSモードでL2TPグループ1を作成します。

[LNS] l2tp-group 1 mode lns

#ローカルトンネル名をLNSとして設定します。

[LNS-l2tp1] tunnel name LNS

#LACからコールを受信するVirtual-Template 1を指定します。

[LNS-l2tp1] allow l2tp virtual-template 1 remote LAC

#トンネル認証をイネーブルにし、トンネル認証キーをaabbccに指定します。

[LNS-l2tp1] tunnel authentication

[LNS-l2tp1] tunnel password simple aabbcc

[LNS-l2tp1] quit

3. リモートシステムで、ユーザー名としてvpdnuserを入力し、パスワードとしてHelloを入力します。

   ダイヤルアップネットワークウィンドウでPPPoE接続にダイヤルします。

設定の確認

#ダイヤルアップ接続が確立されたら、display ppp access-userコマンドを使用してオンラインユーザー情報を表示します。

[LNS] display ppp access-user user-type lns

Interface	Username	MAC address	IP address	IPv6 address	IPv6 PDPrefix
VA0	vpdnuser	-	192.168.0.10	-	-

#ダイヤルアップ接続が確立されると、リモートシステムはIPアドレスを取得し、LNSのプライベートIPアドレスにpingできます。

#LNSで、display L2TP tunnelコマンドを使用して、確立されたL2TPトンネルをチェックします。

[LNS] display l2tp tunnel

LocalTID RemoteTID StateSessions RemoteAddressRemotePort RemoteName
1963542Established11.1.2.11701LAC

#LNSで、display L2TP sessionコマンドを使用して、確立されたL2TPセッションをチェックします。

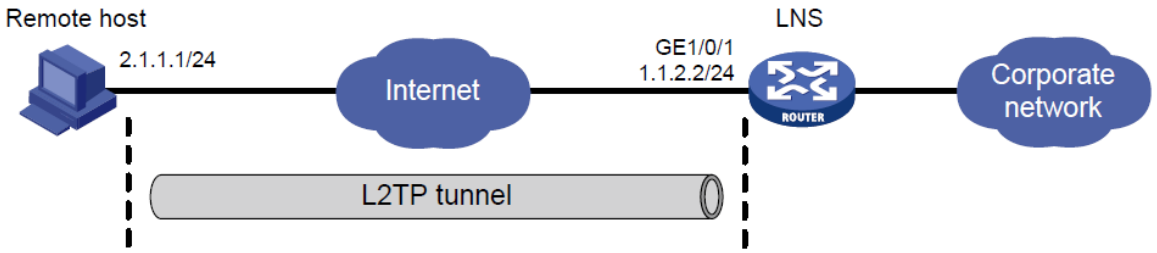
[LNS] display	l2tp session		
LocalSID	RemoteSID	LocalTID	State
2041	64	196	Established

例:クライアントが開始するL2TPトンネルの設定

ネットワーク構成

図12に示すように、PPPユーザーは直接LNSにトンネリング要求を開始して、企業ネットワークにアクセスします。

図12:ネットワーク図



手順

1. LNSを設定します。

   #インターフェイスのIPアドレスを設定します(詳細は表示されません)。

   #LNSとリモートホスト間のルートを設定します(詳細は表示されません)。

   #vpdnuserという名前のローカルユーザーを作成し、パスワードを設定して、PPPサービスを有効にします。

   [LNS] local-user vpdnuser class network

   [LNS-luser-network-vpdnuser] password simple Hello

   [LNS-luser-network-vpdnuser] service-type ppp

   [LNS-luser-network-vpdnuser] quit

   #ISPドメインシステムでPPPユーザーのローカル認証を設定します。

   [LNS] domain system

   [LNS-isp-system] authentication ppp local

   [LNS-isp-system] quit

#L2TPを有効にします。

[LNS] l2tp enable

#PPPアドレスプールを作成します。

[LNS] ip pool aaa 192.168.0.10 192.168.0.20

[LNS] ip pool aaa gateway 192.168.0.1

#Create Virtual-Template 1で、そのPPP認証モードをCHAPに指定し、アドレスプールaaaを使用してIPアドレスをPPPユーザーに割り当てます。

[LNS] interface virtual-template 1

[LNS-virtual-template1] ppp authentication-mode chap domain system

[LNS-virtual-template1] remote address pool aaa

[LNS-virtual-template1] quit

#LNSモードでL2TPグループ1を作成します。

[LNS] l2tp-group 1 mode lns

#ローカルトンネル名をLNSとして設定します。

[LNS-l2tp1] tunnel name LNS

#コールを受信するVirtual-Template 1を指定します。

[LNS-l2tp1]allow l2tp virtual-template 1

#トンネル認証をディセーブルにします。

[LNS-l2tp1] undo tunnel authentication

2. リモートホストを設定します。

#リモートホストのIPアドレスを2.1.1.1に設定し、LNSへのルート(1.1.2.2)を設定します。

#Windowsシステムを使用して仮想プライベートL2TPネットワーク接続を作成するか、L2TP LACクライアントソフトウェア(WinVPNクライアントなど)をインストールします。

#次の設定手順を実行します(手順はクライアントソフトウェアによって異なります)。

- PPPユーザー名をvpdnuserに、パスワードをHelloに指定します。
- セキュリティゲートウェイのインターネットインターフェイスアドレスをLNSのIPアドレスとして指定します。この例では、LNS上のトンネルのイーサネットインターフェイスのIPアドレスは1.1.2.2です。
- 接続属性を変更します。プロトコルをL2TPに設定し、暗号化属性をに設定します。

  カスタマイズされ、認証モードがCHAPになります。

設定の確認

#リモートホストで、L2TP接続を開始します。ダイヤルアップ接続が確立されたら、display ppp access-userコマンドを使用してオンラインユーザー情報を表示します。

[LNS] display ppp access-user user-type lns

Interface Username MAC address IP address IPv6 addressIPv6 PDPrefix

VA0vpdnuser - 192.168.0.1 --
0

#接続が確立されると、リモートホストはIPアドレス192.168.0.10を取得し、LNSのプライベートIPアドレスにpingを実行できます(192.168.0.1)。

#LNSで、display L2TP sessionコマンドを使用して、確立されたL2TPセッションをチェックします。

[LNS-l2tp1] display l2tp session

LocalSIDRemoteSIDLocalTIDState

893624510878Established

#LNSで、display L2TP tunnelコマンドを使用して、確立されたL2TPトンネルをチェックします。

[LNS-l2tp1] display l2tp tunnel

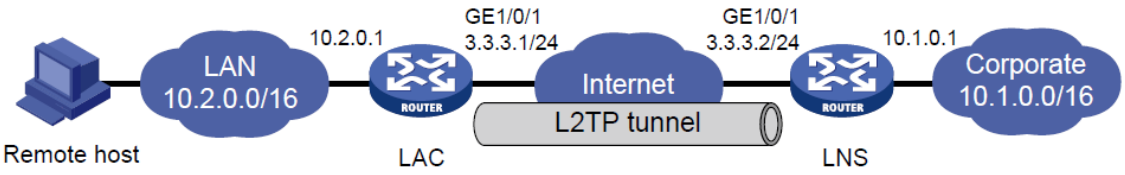
LocalTID RemoteTID StateSessions RemoteAddressRemotePort RemoteName
1087821、12.1.1.11701 PCを確立

例:LAC自動開始L2TPトンネルの設定

ネットワーク構成

図13に示すように、LNSとのL2TPトンネルをLAC自動開始モードで確立するようにLACを設定します。PPPユーザーが接続を開始すると、確立されたトンネルを使用して企業ネットワークにアクセスします。

図13:ネットワーク図



手順

1. LNSを設定します。

   #インターフェイスのIPアドレスを設定します(詳細は省略します)。

   #vpdnuserという名前のローカルユーザーを作成し、パスワードを設定して、PPPサービスを有効にします。

   <LNS> system-view

   [LNS] local-user vpdnuser class network

   [LNS-luser-network-vpdnuser] password simple Hello

   [LNS-luser-network-vpdnuser] service-type ppp

   [LNS-luser-network-vpdnuser] quit

   #Create Virtual-Template 1にIPアドレスを割り当て、PPP認証モードを次のように指定する。

   PAPを使用し、IPアドレス192.168.0.10をPPPユーザーに割り当てます。

   [LNS] interface virtual-template 1

   [LNS-virtual-template1] ip address 192.168.0.1 24

   [LNS-virtual-template1] ppp authentication-mode pap

[LNS-virtual-template1] remote address 192.168.0.10

[LNS-virtual-template1] quit

#ISPドメインシステムでPPPユーザーのローカル認証を設定します。

[LNS] domain system

[LNS-isp-system] authentication ppp local

[LNS-isp-system] quit

#L2TPをイネーブルにし、LNSモードでL2TPグループ1を作成します。

[LNS] l2tp enable

[LNS] l2tp-group 1 mode lns

#ローカルトンネル名をLNSとして設定し、LACからのトンネリング要求を受信する Virtual-Template 1を指定します。

[LNS-l2tp1] tunnel name LNS

[LNS-l2tp1] allow l2tp virtual-template 1 remote LAC

#トンネル認証をイネーブルにし、認証キーをaabbccとして設定します。

[LNS-l2tp1] tunnel authentication

[LNS-l2tp1] tunnel password simple aabbcc

[LNS-l2tp1] quit

#ネクストホップアドレスが192.168.0.10(LNSがLACのVirtual-PPP 1に割り当てるIPアドレス)のスタティックルートを設定して、PPPユーザー宛てのパケットがL2TPトンネル経由で転送されるようにします。

[LNS] ip route-static 10.2.0.0 16 192.168.0.10

2. LACを設定します。

#インターフェイスのIPアドレスを設定します(詳細は表示されません)。

#L2TPをイネーブルにします。

<LAC> system-view

[LAC] l2tp enable

#L2TPグループ1をLACモードで作成します。

[LAC] l2tp-group 1 mode lac

#ローカルトンネル名をLACとして設定し、トンネルピア(LNS)のIPアドレスを指定します。

[LAC-l2tp1] tunnel name LAC

[LAC-l2tp1] lns-ip 3.3.3.2

#トンネル認証をイネーブルにし、認証キーをaabbccとして設定します。

[LAC-l2tp1] tunnel authentication

[LAC-l2tp1] tunnel password simple aabbcc

[LAC-l2tp1] quit

#Create Virtual-PPP 1。ユーザー名とパスワードをvpdnuserとHellotに設定し、PPP認証はPAPを使用します。

[LAC] interface virtual-ppp 1

[LAC-Virtual-PPP1] ip address ppp-negotiate

[LAC-Virtual-PPP1] ppp pap local-user vpdnuser password simple Hello

[LAC-Virtual-PPP1] quit

#企業ネットワーク宛てのパケットがL2TPトンネルを介して転送されるように、スタティックルートを設定します。

[LAC] ip route-static 10.1.0.0 16 virtual-ppp 1

#LACをトリガーして、LNSとのL2TPトンネルを確立します。

[LAC] interface virtual-ppp 1

[LAC-Virtual-PPP1] l2tp-auto-client l2tp-group 1

3. リモートホストで、LACをゲートウェイとして設定します。

設定の確認

#LNSで、display L2TP sessionコマンドを使用して、確立されたL2TPセッションを表示します。

[LNS] display l2tp session

LocalSID	RemoteSID	LocalTID	State
21409	3395	4501	Established

#LNSで、確立されたL2TPトンネルを表示するには、display L2TP tunnelコマンドを使用します。

[LNS] display l2tp tunnel

LocalTID	State	Sessions	RemotePort
RemoteTID		RemoteAddress	RemoteName

4501524Established13.3.3.11701LAC

#LNSで、LAC側のプライベートネットワークアドレスである10.2.0.1にpingできることを確認します。これは、10.2.0.0/16上のホストと10.1.0.0/16上のホストがL2TPトンネルを介して相互に通信できることを示します。

[LNS] ping -a 10.1.0.1 10.2.0.1

Ping 10.2.0.1 (10.2.0.1): 56 data bytes, press CTRL_C to break

56 bytes from 10.2.0.1: icmp_seq=0 ttl=128 time=1.000 ms

56 bytes from 10.2.0.1: icmp_seq=1 ttl=128 time=1.000 ms

56 bytes from 10.2.0.1: icmp_seq=2 ttl=128 time=1.000 ms

56 bytes from 10.2.0.1: icmp_seq=3 ttl=128 time=1.000 ms

56 bytes from 10.2.0.1: icmp_seq=4 ttl=128 time=1.000 ms

--- Ping statistics for 10.2.0.1 ---

5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss

round-trip min/avg/max/std-dev = 1.000/1.000/1.000/0.000 ms

L2TPのトラブルシューティング

プライベートネットワークへのアクセスの失敗

症状

リモートシステムはプライベートネットワークにアクセスできません。

解決方法

問題を解決するには、次の手順に従います。

1. トンネル設定の失敗を回避するために、次の項目を確認します。
   - LNSのアドレスは、LAC上で正しく設定されています。詳細については、を参照してください。
     lns-ipコマンド。
   - LNSは、LACからのL2TPトンネリング要求を受け入れることができます。詳細については、を参照してください。
     allowコマンド。
   - トンネル認証はLACとLNSの両方でイネーブルにされ、2つの側で設定されたトンネル認証キーが一致します。
2. PPPネゴシエーションの失敗を回避するために、次の項目を確認します。
   - ユーザー名とパスワードは、LACおよびLNSで正しく設定されています。
   - リモートシステムおよびLNSのIPアドレスネゴシエーション設定は正しい。
   - 認証タイプは一貫しています。たとえば、Windows 2000で作成されたVPN接続のデフォルトの認証タイプはMS-CHAPです。ピアがMS-CHAPをサポートしていない場合は、Windows 2000で認証タイプをCHAPに変更します。

データ伝送障害

症状

データ送信に失敗しました。接続は確立されていますが、データを送信できません。たとえば、LACとLNSは互いにpingできません。

解決方法

問題を解決するには、次の手順に従います。

1. LACおよびLNSでdisplay ip routing-tableコマンドを使用して、LACがLNSの背後にあるプライベートネットワークへのルートを持ち、その逆も同様であることを確認します。使用可能なルートがない場合は、スタティックルートまたはダイナミックルーティングプロトコルを設定します。
2. リンク帯域幅を増やしてリンクの可用性を向上させます。

   インターネットバックボーンの輻輳および高いパケット損失率は、データ伝送障害を引き起こす可能性があります。L2TPデータ伝送は、パケットエラー制御機能を提供しないUDPに基づいています。回線が不安定な場合、LACとLNSは相互にpingできない可能性があります。