

# Cisco 6400 UAC の PPPoE ベースライン アーキテクチャ

## 目次

[概要](#)

[前提条件](#)

[テクノロジーの概要](#)

[PPPoE アーキテクチャの利点と欠点](#)

[利点](#)

[欠点](#)

[PPPoE アーキテクチャの実装に関する考慮事項](#)

[PPPoE アーキテクチャの要点](#)

[結論](#)

[参考資料](#)

[関連情報](#)

## 概要

このドキュメントでは、Point-to-Point Protocol over Ethernet ( PPPoE ) を使用するエンドツーエンドの Asymmetric Digital Subscriber Line ( ADSL; 非対称デジタル加入者回線 ) アーキテクチャについて説明します。

アクセス テクノロジーの現在の環境では、リモート サイトにある複数のホストを同じ顧客宅内アクセス デバイスを通して接続するのが望ましい方法です。また、Point-to-Point Protocol ( PPP; ポイントツーポイント プロトコル ) を使用するダイヤルアップ サービスと同様の方法で、アクセス コントロールと課金機能を提供する必要があります。多くのアクセス テクノロジーでは、複数のホストを顧客宅内アクセス デバイスに接続する最も費用効果の高い方法は、イーサネットを利用するものです。さらに、この装置のコストをできるだけ低く抑え、設定要件を少なくする、または設定要件をなくすのが望ましいでしょう。

ユーザが ADSL を導入する際には、従来のブリッジング方式による Customer Premises Equipment ( CPE; 顧客宅内装置 ) の大規模な設置基盤上で、PPP 形式の認証と認可をサポートする必要があります。PPPoE を使用すると、シンプルなブリッジング アクセス デバイスを介して、ホストのネットワークをリモート アクセス コンセントレータやアグリゲーション コンセントレータ ( 加入者集約コンセントレータ ) に接続できます。このモデルでは、各ホストがそれぞれの PPP スタックを使用します。したがって、ユーザに分りやすいユーザ インターフェイスを提供します。アクセス コントロール、課金、およびタイプ オブ サービスを、サイトごとではなくユーザごとに実施できます。

## 前提条件

ベースライン アーキテクチャでは、次の要素が提供されていることを前提としています。

- PPPoE を使用する末端加入者に対する高速インターネット アクセスおよび企業アクセス
- Cisco 6400 ユニバーサル アクセス コンセントレータ ( UAC ) によって実装されている、コアバックボーン テクノロジーとしての ATM

この設計実装に関する制約によって、他のプラットフォームでのこのアーキテクチャの使用が制限される場合がありますが、PPPoE は常に発展しています。新機能およびアップデートされた機能を利用するには、関連製品の最新のリリース ノートをお読みください。

このドキュメントは、Cisco 6400 UAC を使用する現在の展開と社内テストに基づくものです。このドキュメントは、『[PPPoA ベースライン アーキテクチャ](#)』の続編で、頻繁にその内容を参照しています。「PPPoA ベースライン アーキテクチャ」White Paper を読んで PPP の基本を理解していること、および最新のソフトウェア リリースのリリース ノートを読んでいることを前提としています。

## テクノロジーの概要

RFC 2516 で指定どおりに、PPPoE に 2 つの個別の段階があります: ディスカバリステージおよび PPP セッション ステージ。ホストが PPPoE セッションを開始する際は、最初にディスカバリを実行して、クライアントの要求を満たすことができるサーバを識別する必要があります。2 番目に、それはピアのイーサネットの MAC アドレスを識別する必要があり、PPP がピア ツーピア 関係を定義する間、PPPoE セッション ID を確立するために、ディスカバリは本来クライアント サーバ 関係です。

ディスカバリ プロセスでは、ホスト (クライアント) は 1 つ以上のアクセス コンセントレータ (サーバ) を検出して、その内の 1 つを選択します。ディスカバリが正常に完了した時点で、ホストと選択されたアクセス コンセントレータの両方が、イーサネットを介してポイントツーポイント接続を確立するための情報を得ています。PPP セッションが確立された後は、ホストとアクセス コンセントレータの両方が、PPP 仮想インターフェイスにリソースを割り当てる必要があります (すべての実装に当てはまるとは限りません)。PPPoE の仕様の詳細については、RFC 2516 を参照してください。

## PPPoE アーキテクチャの利点と欠点

PPPoE アーキテクチャは、ダイヤルアップ モデルと PPPoA アーキテクチャで使用されている PPP の長所の大部分を継承しています。次のセクションでは、PPPoE の主要な長所と短所、および PPPoA との違いを挙げます。

### 利点

ここでは、PPPoE の主な長所と、PPPoA との違いを説明します。

- Password Authentication Protocol ( PAP; パスワード認証プロトコル ) または Challenge Handshake Authentication Protocol ( CHAP; チャレンジ ハンドシェイク認証プロトコル ) に基づくセッション単位の認証。認証はブリッジング アーキテクチャのセキュリティ ホールを解消するので、これは PPPoE の最大の長所です。
- セッション単位の課金が可能です。これによりサービス プロバイダーは、提供するさまざまなサービスに対するセッション時間に基づいて、加入者に課金できます。また、サービス プロバイダーは最低限のアクセス料金を要求することもできます。

- PPP にアップグレードできない、または PPPoA を実行する機能を持たない現在の CPE インスタレーションで PPPoE を使用できるので、ブリッジされたイーサネット LAN を通して、PPP セッションを PC まで延長できます。
- PPPoE では、現在のダイヤルアップ モデルで Internet Service Provider ( ISP; インターネット サービス プロバイダー ) が使用するポイントツーポイントセッションが維持される。PPPoE は、中継 IP スタックがなくてもイーサネット上でポイントツーポイントを実行できる唯一のプロトコルです。
- Network Access Provider ( NAP ) や Network Service Provider ( NSP ) は、エンドツーエンドの Permanent Virtual Circuit ( PVC; 相手先固定接続 ) を管理したり、レイヤ 3 ルーティングやレイヤ 2 トンネリング プロトコル ( L2TP ) のトンネルを使用したりしなくても、企業のゲートウェイに対するセキュアなアクセスを提供できます。これにより、大規模なサービスや Virtual Private Network ( VPN; バーチャル プライベート ネットワーク ) の販売のビジネス モデルがスケーラブルになります。
- PPPoE は、一度に複数の宛先へのホスト ( PC ) アクセスを提供できます。PVC ごとに複数の PPPoE セッションを使用できます。
- NSP では、業界標準の Remote Authentication Dial-In User Service ( RADIUS ) サーバを使用するアイドル タイムアウトとセッション タイムアウトの導入により、加入者ごとのオーバーサブスクライブが可能です。
- PPP は Service Selection Gateway ( SSG ) 機能とともに使用可能です。

## 欠点

ここでは、PPPoE の主な短所と、PPPoA との違いを説明します。

- イーサネット セグメントに接続するすべてのホスト ( PC ) に、PPPoE クライアント ソフトウェアをインストールする必要があります。つまり、アクセス プロバイダーは、PC 上の CPE とクライアント ソフトウェアを維持管理する必要があります。
- PPPoE の実装は RFC 1483 のブリッジングを使用するので、ブロードキャスト ストームの影響を受けやすく、DoS 攻撃 ( サービス拒絶攻撃 ) を受ける可能性があります。

## PPPoE アーキテクチャの実装に関する考慮事項

ここでは、このタイプのアーキテクチャを実装する前に考慮する重要なポイントについて説明します。

- サポートされる加入者数。必要な PPPoE サーバの数は、セッションの数によって決まります。
- PPP セッションを、サービス プロバイダーの集約ルータで終端するか、他の企業ゲートウェイまたは ISP に転送するか。
- IP アドレスを提供するのはサービス プロバイダーか、またはサービスの最終的な宛先か。
- ユーザが複数いる場合、すべてのユーザが同じ最終宛先またはサービスに到達する必要があるか、またはユーザごとにサービスの宛先が異なるか。末端加入者は、同時に複数の宛先にアクセスするか。
- アクセス プロバイダーが使用する PPPoE クライアント ソフトウェア、およびそのソフトウェアがテストされているか。ホストが使用するオペレーティング システム、およびそのオペレーティング システムはインテリジェントなルーティングができるか。
- サービス プロバイダーの加入者に対する課金は、定額制か、セッション使用量単位か、使用

したサービスごとか。

- CPE、DSLAM、および集約 Point of Presence ( POP; ポイント オブ プレゼンス ) の展開とプロビジョニング。
- NAP に対するビジネス モデル。 そのモデルには、セキュアな企業アクセスなどの大規模サービス、および音声や映像などの付加価値サービスの販売も含まれるか。 NAP と NSP は同じエンティティか。
- 企業のビジネス モデル。 そのモデルは独立系 Local Exchange Carrier ( LEC; 地域通信事業者 )、Competitive Local Exchange Carrier ( CLEC; 競争的地域通信事業者 )、または ISP に匹敵するか。
- NSP が末端加入者に提供するアプリケーションの種類。
- 予想されるアップストリームおよびダウンストリームのデータ フローの量。 NRP のスループット、トラフィック エンジニアリング、および QoS の問題を検討してください。

このドキュメントでは、PPPoE アーキテクチャがサービス プロバイダーごとに異なるビジネスモデルにどのように適合および拡大または縮小するのか、およびプロバイダーがこのアーキテクチャを利用してどのように利益を得られるのか、について説明します。

## ネットワーク アーキテクチャ

### PPPoE アーキテクチャの設計に関する考慮事項

このセクションでは、PPPoE アーキテクチャ固有にあてはまる問題について説明します。

アーキテクチャを展開する前に、サービス プロバイダーのビジネス モデルと、プロバイダーが提供するサービスについて理解することが不可欠です。 PC で使用されているクライアント ソフトウェアを知る必要があります。 最もよく使用されるソフトウェアは Routerware のものです。 クライアント ソフトウェアは PC にインストールされるので、サービス プロバイダーの技術者は、PC とそのオペレーティング システムについての十分な知識が必要です。

RFC 2516 で指定されているように、最大受信ユニット ( MRU ) オプションは、1492 より大きいサイズにはネゴシエーションできません。 イーサネットの最大ペイロード サイズは 1500 オクテットです。 PPPoE ヘッダーが 6 オクテット、PPP プロトコル ID が 2 オクテットであるため、PPP の Maximum Transmission Unit ( MTU; 最大伝送ユニット ) は 1492 以下である必要があります。 これは、PPPoE バーチャル テンプレート インターフェイスに対して IP MTU 1492 を設定することで実現されます。

デフォルトでは、PPPoE VPDN グループが設定されるときに、バーチャル アクセス インターフェイスはプレクローンされません。 ユーザはバーチャル テンプレート `<number> pre-clone <number>` グローバルコマンドの発行によって precloned 仮想アクセスインターフェイスの最大数を変更できます。

DoS 攻撃からルータを保護するため、PPPoE では ( デフォルトでは )、1 つの MAC アドレスを発信元とする VC 経由のセッションは 1 つだけです。 `pppoe session-limit per-mac` コマンドと `pppoe session-limit per-vc` コマンドを発行して、このデフォルトを変更できます。

アカウントिंग、許可、および認証のプロセスは、PPPoA のものと同じです。 唯一の違いは、現時点では、仮想パス識別子/仮想チャンネル識別子(VPI/VCI)ベースの認証 ( PPPoA では使用できますが、PPPoE では使用できません ) が、大規模サービス用に L2TP および SSG のアーキテクチャを使用できることです。

## [PPPoE アーキテクチャの要点](#)

## CPE

CPE は、純粋に RFC 1483 ブリッジング用に設定されています。各 CPE は 1 つの VPI/VCI ペアだけを使用し、この CPE の背後にあるホストによって開始されるすべての PPPoE セッションは、この単一の VC で伝送されます。

## IP 管理

PPPoE クライアントを実行する各ホストに対する IP アドレスの割り当ては、ダイヤルモードの PPP と IPCP 間でのネゴシエーションと同一の原理に基づいています。IP アドレスの開始位置は、加入者が購入しているタイプオブサービスと、PPP セッションが終端する場所によって決まります。PPPoE は Microsoft Windows のダイヤルアップ ネットワーキング機能を使用し、割り当てられた IP アドレスは PPP アダプタに反映されます。

IP アドレスの割り当ては、PPPoE セッションを終端するアクセス コンセントレータ、または L2TP の場合はホーム ゲートウェイが基になります。IP アドレスは、PPPoE セッションごとに割り当てられます。

CPE は、ブリッジされていて、それ自体には IP アドレスが割り当てられていないので、Network Address Translation/ Dynamic Host Configuration Protocol ( NAT/DHCP ) を行うことはできません。

## サービス先への到達方法

サービスの宛先に到達するには次の方法があります。

- サービスプロバイダーでの PPP セッションの終端
- L2TP トンネリング
- SSG の使用

これらのアーキテクチャの詳細については、別のドキュメントで説明されています。

## PPPoE の動作の説明

このリリースの PPPoE クライアント ソフトウェアは、RFC 2516 に記載されているディスカバリ ステージとセッション ステージをサポートしています。ディスカバリ ステージには 4 つのステップがあります。これが完了すると、両方のピアが PPPoE セッション ID とピアのイーサネット アドレスを認識し、PPPoE セッションが一意に定義されます。ステップは次のとおりです。

1. ホストが開始パケットをブロードキャストします。ホストは、ブロードキャスト アドレスに設定された destination\_addr とともに PPPoE Active Discovery Initiation ( PADI ) パケットを送信します。PADI は、要求しているサーバの種類を示す 1 つのタグで構成されています。
2. 1 つか複数のアクセス コンセントレータが提供パケットを送信します。アクセス コンセントレータまたはルータは、対応できる PADI を受信すると、PPPoE Active Discovery Offer ( PADO ) パケットを送信します。destination\_addr は、PADI を送信したホストのユニキャスト アドレスです。PADI に対応できないアクセス コンセントレータは、PADO に応答できません。PADI はブロードキャストであったため、ホストは複数の PADO を受信する可能性があります。

3. ホストがユニキャスト セッション要求パケットを送信します。ホストは、受信した PADO パケットを調べて、1つを選択します。選択は、各アクセス コンセントレータが提供するサービスに基づいて行います。その後ホストは、選択したアクセス コンセントレータに対して1つの PADR パケットを送信します。destination\_addr フィールドには、PADO を送信したアクセス コンセントレータまたはルータのユニキャスト イーサネット アドレスが設定されます。
4. 選択されたアクセス コンセントレータが確認のパケットを送信します。アクセス コンセントレータは、PADR パケットを受信したら、PPP セッションを開始する準備を行います。PPPoE セッションに対する一意のセッション ID を生成し、PPPoE Active Discovery Session-confirmation ( PADS ) パケットでホストに応答します。destination\_addr フィールドは、PADR を送信したホストのユニキャスト イーサネット アドレスです。

PPPoE セッションが開始されると、PPP データは、別の PPP カプセル化として送信されます。イーサネット パケットはすべてユニキャストです。

ホストまたはアクセス コンセントレータはどちらも、セッションが確立された後であればいつでも、PPPoE Active Discovery Terminate ( PADT ) パケットを送信して、PPPoE セッションが終了したことを知らせることができます。

詳細については、RFC 2516 を参照してください。

## [結論](#)

ADSL の場合、PPPoE の利用が拡大しており、PPPoA に次いで普及するようになっています。

## [参考資料](#)

- RFC 2516 – PPP over Ethernet ( PPPoE ) を送信する方式
- RFC1483 – ATM アダプテーション レイヤ 5 上のマルチポイントエンキャプシュレーション
- RFC 2364 – AAL5 上のポイントツーポイント

## [関連情報](#)

- [PPPoA ベースライン アーキテクチャ](#)
- [DSL 技術サポート](#)
- [テクニカルサポート - Cisco Systems](#)