Point-to-Point Tunneling Protocol

情報工学専攻 修士 1 年 荒木研究室 渡辺 義和

平成 14 年 3 月 31 日

1 概要

PPTP(Point-to-Point Tunneling Protocl) は、IP ネットワーク上で PPP(Point to Point Protocol) をトンネリングさせるためのプロトコルである。PPP ユーザは通常、PSTN や ISDN などの公衆回線網を用いて NAS(Network Access Server) に接続し、PPP を実行することにより NAS が接続しているネットワークに参加する。そのため、PPP により遠隔のネットワークに参加するためには、そのネットワーク上に公衆回線網を通じて直接接続できる NAS が存在しなければならない。

PPTP では、PPP ユーザが接続する NAS の機能をサーバ・クライアント機構により分断することで、インターネットを介して遠隔のネットワークに PPP を用いて参加する VPN(Virtual Private Network) の機能を実現している。サーバは PNS(PPTP Network Server)、クライアントは PAC(PPTP Access Concentrator) と呼ばれ、PPTP は PNS と PAC の間での PPP データの転送 (トンネリング) 方法を規定している。

図 1 に PPP を用いた NAS によるインターネットへのアクセスの様子を、図 2 に PPTP を用いたプライベートネットワークへのアクセスの様子を示す。

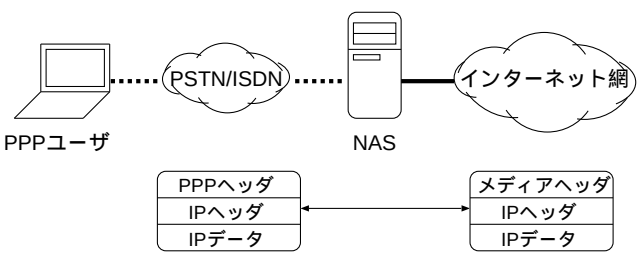

図 1: PPP を用いた NAS によるインターネットへのアクセス

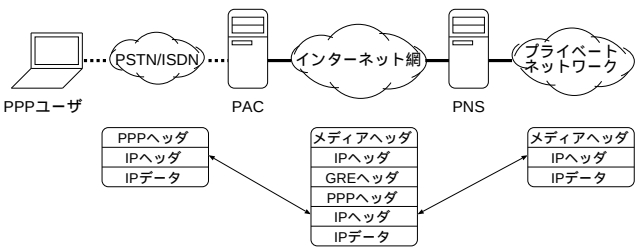

図 2: PPTP を用いたプライベートネットワークへのアクセス (VPN)

2 PPTP の概要

2.1 NAS の機能の分割

NAS は PPP クライアントに対してネットワーク接続のサービスを提供しており、以下のような機能を実装している。

1. PSTN または ISDN への物理的な接続と、外部モデムまたは TA の管理
2. PPP の LCP セッションの論理的終端
3. PPP 認証プロトコルへの参加
4. PPP マルチリンクプロトコルに対するチャネルの集約および管理
5. PPP の様々な NCP の論理的終端
6. マルチプロトコルルーティングおよび NAS インターフェース間のブリッジング

PPTP では、NAS の上記の機能のうち 1、2 を PAC に、4、5、6 を PNS に割り当てている。3 の機能は、場合によって PAC および PNS のどちらかが受け持つとしている。

2.2 PPTP の動作

PPTP は、インターネットにそれぞれ接続している PNS と PAC の間で PPP データのトンネリングを行なう。トンネリングを開始する際にはまず PNS と PAC の間に TCP コネクションが確立され、このコネクション上で PPTP 制御コネクションが確立される。PPTP 制御コネクションでさまざまメッセージを交換することにより、PNS から PAC への発呼の指示や、PAC から PNS への着呼の通知が行なわれる。

PPP ユーザと PAC の間で呼が確立されると、それに対応する 1 つのトンネリングセッションが作成される。PAC は PPP ユーザから受け取った PPP データを IP を用いて PNS へと転送し、それを受信した PNS はそのデータの処理を行なう。また、PNS から PPP ユーザへのデータはまず IP により PAC へと転送され、PAC はそれを PPP ユーザへと送信する。このようにして、PPP のトンネリングが行なわれる。

3 節では PPTP 制御コネクション上で使用されるメッセージの説明を行ない、4 節では PPP データのトンネリングの際に用いられるプロトコルの説明を行なう。

3 PPTP 制御コネクション

この節では、PPTP の制御コネクション上で使用される制御メッセージについて説明する。制御メッセージは、制御コネクション管理、呼管理、エラー報告、PPP セッション制御の 4 種類に分類できる。

3.1 制御コネクション管理

3.1.1 制御コネクションの確立

PPTP の制御コネクションの確立は、Start-Control-Connection-Request メッセージおよび Start-Control-Connection-Reply メッセージを用いて行われる。

PAC と PNS の間で TCP コネクションが確立されると、TCP コネクションを生成した側が Start-Control-Connection-Request メッセージを送信する。このメッセージを受信した PAC または PNS は、応答として制御コネクション確立の可否を含む Start-Control-Connection-Reply メッセージを送信する。制御コネクションが確立できない場合としては、プロトコルバージョンの不一致などがある。

上記のメッセージ交換によって制御コネクションは確立されるが、この時発生する問題としてコリジョンがある。ある PAC と PNS の間の制御コネクションは 1 つでなければならないが、PAC と PNS が同時に TCP コネクションを確立し、それぞれ制御コネクションの確立を試みる場合がある。これをコリジョンと呼ぶ。コリジョンが発生した場合、PAC と PNS のうちより大きい IP アドレスを持つ方が勝者となり、敗者は自分が確立した TCP コネクションをすぐに閉じる。制御コネクションの確立は、勝者が確立した TCP コネクション上で行う。

3.1.2 制御コネクションの切断

PPTP の制御コネクションの切断は、Stop-Control-Connection-Request メッセージおよび Stop-Control-Connection-Reply メッセージを用いて行われる。

制御コネクションを切断したい PAC または PNS は Stop-Control-Connection-Request メッセージを送信する。このメッセージを受信した側は、Stop-Control-Connection-Reply メッセージを送信し、これらのメッセージ交換終了後 TCP コネクションを切断する。

3.1.3 制御コネクションの維持

PPTP では、制御コネクション上で 60 秒間メッセージを受信しなかった場合、制御コネクションが確立されていることの確認をするよう規定している。この制御コネクションの確認のために、Echo-Request メッセージおよび Echo-Reply メッセージが用いられる。Echo-Request メッセージを受信すると、その応答として Echo-Reply を送信する。Echo-Request メッセージを送信して 60 秒以内に対応する Echo-Reply の受信が出来なかった場合、すぐに制御コネクションを切断する。

3.2 呼管理

3.2.1 外部への発呼

PAC から新たに外部へ発呼を行う場合には、Outgoing-Call-Request メッセージおよび Outgoing-Call-Reply メッセージが用いられる。

新たに回線を接続する際、PNS は PAC に対して Outgoing-Call-Request メッセージを送信する。このメッセージは、接続先の電話番号や、接続に成功した後その接続上で行われる PPP セッションに対する PNS 側のコール ID などの情報を含んでいる。このメッセージを受信した PAC は、指定されてた番号への発信を試み、その結果を Outgoing-Call-Reply メッセージにより通知する。そのメッセージには、呼の確立が成功した場合、その接続上で行われる PPP セッションに対する PAC 側のコール ID が含まれる。

3.2.2 外部からの着呼

外部から PAC に対して着呼があった場合、その着呼への対応に 3 つのメッセージ、Incoming-Call-Request メッセージ、Incoming-Call-Reply メッセージおよび Incoming-Call-Connected メッセージが用いられる。

PAC に外部から着呼があると、PAC は着呼に応じる前に PNS に対して Incoming-Call-Request メッセージを送信する。このメッセージには呼び出された電話番号や発信元の電話番号、および接続に成功した後その接続上で行われる PPP セッションに対する PAC 側のコール ID などの情報を含んでいる。このメッセージを受信した PNS は、その着呼に応じるべきかを Incoming-Call-Request メッセージにより PAC に通知する。また、着呼に応じる場合にはその接続上で行われる PPP セッションに対する PNS 側のコール ID もそのメッセージにより通知する。PAC は、PNS から指示された場合着呼に応じ、PNS に対して Incoming-Call-Connected メッセージを送信しその結果を通知する。

以上のように、PAC に対して外部から着呼があった場合、スリーウェイハンドシェイク方式により PPTP セッションを確立させる。着呼に応じるかどうかの判断は PNS が行い、PAC は PNS の判断に従う。

3.2.3 呼の切断

呼の切断は、Call-Clear-Rquest メッセージおよび Call-Disconnect-Notify メッセージにより行われる。

PNS が呼を切断したい場合には、PAC に対して Call-Clear-Request メッセージを送信する。その際、どの呼を切断するかの指定はコール ID により行う。このメッセージを受信した PAC は呼の切断を行う。PNS からの指示による場合を含め、呼が何らかの原因により切断された場合、PAC は Call-Disconnect-Notify メッセージによりそのことを PNS に通知する。このメッセージは切断された呼に対応するコール ID を含んでいる。

3.3 エラー報告

PAC において WAN でエラーが発生した場合、WAN-Error-Notify メッセージにより PNS に通知される。通知されるエラーとしては CRC エラー数やバッファオーバーラン数などがある。エラー状態は新しい呼が確立されるたびにクリアされ、またこのメッセージの送信は 60 秒間に最大 1 回に制限されている。

3.4 PPP セッション制御

PPP の実行により決定された接続に関するオプションを PNS から PAC に通知するために、Set-Link-Info メッセージが使用される。指定されるオプションには、Send ACCM および Receive ACCM がある。これらのオプションは PPP セッション中においていつでも変更可能となっており、変更された場合 PNS はこのメッセージにより新しい値を通知する。

4 トンネリングプロトコル

この節では、PAC と PNS の間で PPP データをトンネリングする際に用いられるプロトコルについて説明を行なう。

4.1 概要

PPTP では PPP データをトンネリングする際、まず PPP データを GRE パケットによりカプセル化し、カプセル化したパケットを IP により PAC・PNS 間で転送する。PAC が PPP ユーザから受信した PPP データには、HDLC フラグや制御文字などのメディア固有のフレーミング要素が含まれる場合があるが、カプセル化する際には除去する。また、CRC の送信も行なわない。PAC・PNS 間で転送される IP パケットの構造を図 3 に示す。

図 3: PAC・PNS 間で転送される IP パケットの構造

PPTP では、GRE を若干拡張したものを利用している。具体的には、GRE ヘッダに Acknowledgment 番号フィールドを追加しており、このフィールドによりあるパケットが相手に届いたかどうかの確認を行う。これは、そのセッションへのデータ送出速度を決定するためであり、データパケットの再送のためではない。PPTP ではデータパケットの再送は一切おこなわない。

4.2 流量制御アルゴリズム

PPTP はデータを送受信する際に使用する流量制御アルゴリズムを規定していないが、RFC2637 では 1 つの流量制御アルゴリズムを提案している。このアルゴリズムはスライディングウィンドウプロトコルにより輻輳・流量の制御を行なうもので、PAC および PNS はそれぞれ送信ウィンドウを持ち、その大きさは最初受信側の受信バッファサイズの半分に設定される。PAC および PNS の受信バッファサイズは、PPTP 制御コネクション上でセッションが確立される際に通知される。送信側は送信ウィンドウサイズ内でパケットを送出し、肯定応答を受信するたびに送信ウィンドウサイズを受信側の受信バッファサイズに到達するまで 1 ずつ大きくしていく。パケットを送出した際にはタイマが設定され、タイマがタイムアウトするまでに肯定応答が得られなかった場合、送信ウィンドウサイズを半分にする。この時、データの再送信は行なわない。また、タイマがタイムアウトする時間は肯定応答が届くたびに再計算を行なう。

5 PPTP の実装

PPTP の実装として、pptp-linux を紹介する。

pptp-linux は PAC の機能を実装する PPTP クライアントソフトで、遠隔から接続したいネットワーク上に PNS を用意しておき、その PNS に対して ppp-linux を使用することで、VPN の実現が可能となる。この場合、PPP クライアントソフトと pptp-linux を同一ホスト上で実行し、PAC と PPP ユーザの間は公衆回線網等ではなく直接接続される。

pptp-linux は pptp と pptp_callmgr の 2 つのプログラムから成っている。pptp は PPTP セッションの管理およびトンネリングの処理を行うプログラムで、PPTP セッション毎に 1 つの pptp プログラムを起動する。pptp_callmgr は PPTP 制御コネクションの管理を行うプログラムで、接続する PNS 毎に 1 つの pptp_callmgr を起動する。これらのプログラムの関係を図 4 に示す。

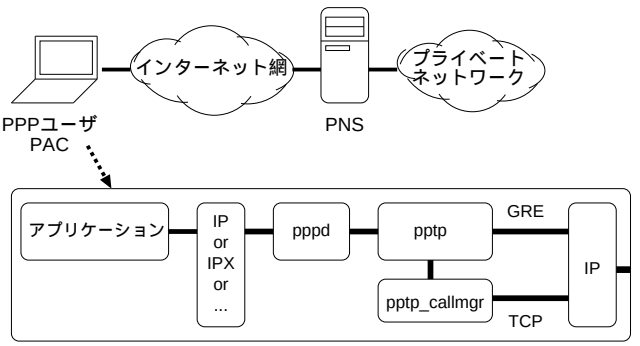

図 4: pptp-linux の各プログラムの関係

6 まとめ

PPTP は NAS の機能を PAC と PNS に分割し、PAC と PNS の間でのデータ転送の方法を規定することにより、PPP データのトンネリングを可能としている。

PPTP を用いると、PPTP でトンネリングする PPP セッションにおいて認証やデータの暗号化を行うことで、容易に安全な VPN の構築を行うことが出来る。