(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3613453号
(P3613453)
(45)発行日　平成17年1月26日(2005.1.26)　(24)登録日　平成16年11月5日(2004.11.5)

(51)Int.Cl.[7]	F I	
H04L 12/56	H04L 11/20	102D
H04L 12/66	H04L 11/20	B
H04Q 7/22	H04Q 7/04	K
H04Q 7/28		

請求項の数 16　(全 29 頁)

(21)出願番号　特願平11-255014
(22)出願日　平成11年9月9日(1999.9.9)
(65)公開番号　特開2000-115250(P2000-115250A)
(43)公開日　平成12年4月21日(2000.4.21)
審査請求日　平成12年12月27日(2000.12.27)
(31)優先権主張番号　09/150403
(32)優先日　平成10年9月9日(1998.9.9)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．０７９７４－０６３６　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　６００
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100106703
弁理士　産形　和央
(74)代理人　100096943
弁理士　臼井　伸一

最終頁に続く

(54)【発明の名称】移動ポイント・ツー・ポイント・プロトコル

(57)【特許請求の範囲】
【請求項１】
ポイント－ツー－ポイントプロトコル（ＰＰＰ）接続を通して、トンネルプロトコルに従って確立された第１のパケットサーバおよび第２のパケットサーバとの通信セッションに関与するよう構成され、および該第１のパケットサーバと該第２のパケットサーバの間で送信されるパケットデータと関連する連続する数の状態変数を監視して、該ＰＰＰ接続の変化の存在下、該ＰＰＰ接続を再確立する必要なしに該通信セッションをパケットの順序を含め維持するようにするよう構成されたパケット装置を含む装置。
【請求項２】
請求項１に記載の装置において、
該ポイント－ツー－ポイント接続を確立するのにトンネルプロトコルが用いられる装置。
【請求項３】
請求項１に記載の装置において、
該パケット装置が、所定の数の状態変数を含み状態変数のセットを記憶し、ここでその状態変数の半分が該第１のパケットサーバと関連し、その状態変数の残りの半分が該第２のパケットサーバと関連するものである装置。
【請求項４】
請求項１に記載の装置において、
該第１のパケットサーバが、私的ネットワークである装置。
【請求項５】

請求項４に記載の装置において、
マルチポップ通信経路がソースと該私的ネットワークの間に確立されるように、第２のパケットサーバが該ソースに接合される装置。
【請求項６】
パケットサーバにて用いる方法であって、
ポイント－ツー－ポイントプロトコル（ＰＰＰ）接続を通して通信セッションをトンネルプロトコルに従って確立するステップと、
該第１のパケットサーバと該第２のパケットサーバの間で送信されるパケットデータと関連する連続する数の状態変数を監視して、該ＰＰＰ接続の変化の存在下、該ＰＰＰ接続を再確認する必要なしに該通信セッションをパケットの順序を含め維持するようにするステップとを含む方法。
【請求項７】
請求項６に記載の方法において、
トンネルプロトコルが、該ポイント－ツー－ポイント接続を確立するのに用いられる方法。
【請求項８】
請求項６に記載の方法において、さらに
所定の数の状態変数を含む状態変数のセットを記憶するステップであって、その状態変数の半分が該第１のパケットサーバと関連し、その状態変数の残りの半分が該第２のパケットサーバと関連するステップを含む方法。
【請求項９】
請求項１に記載の装置において、
該ＰＰＰ接続における変化が、該第２のパケットサーバの除去を含むものである装置。
【請求項１０】
請求項１に記載の装置において、
該ＰＰＰ接続における変化が、該第２のパケットサーバの第３のパケットサーバとの置き換えを含むものである装置。
【請求項１１】
請求項６に記載の方法において、
該ＰＰＰ接続の変化が、該第２のパケットサーバの除去を含むものである方法。
【請求項１２】
請求項６に記載の方法において、
該ＰＰＰ接続における変化が、該第２のパケットサーバの第３のパケットサーバとの置き換えを含むものである装置。
【請求項１３】
装置であって、
ポイント－ツー－ポイントプロトコル（ＰＰＰ）接続を通して、ソースおよびトンネルプロトコルに従って確立された少なくとも１つのパケットサーバとの通信セッションに関与し、それ自身と該少なくとも１つのパケットサーバの間で送信されるパケットデータと関連する連続する数の状態変数を監視して、該ＰＰＰ接続における変化の存在下、該ＰＰＰ接続を再確立する必要なしに該通信セッションをパケットの順序を含め維持する、よう構成されたパケット装置を含む装置。
【請求項１４】
請求項１３に記載の装置において、
該ＰＰＰ接続における変化が、該ソースと該パケット装置の間に第２のパケットサーバを追加することを含む装置。
【請求項１５】
パケットサーバにおいて用いる方法であって、
ポイント－ツー－ポイントプロトコル（ＰＰＰ）接続を通して、トンネルプロトコルに従ってソース及び少なくとも１つのサーバとの通信セッションを確立するステップと、

それ自身と該少なくとも１つのパケットサーバの間で送信されるパケットデータと関連する連続する数の状態変数を監視して、該ＰＰＰ接続における変化の存在下において該ＰＰＰ接続を再確立する必要なしにパケットの順序を含む該通信セッションを維持するようにするステップと、を含む方法。

【請求項１６】

請求項１５に記載の装置において、

該ＰＰＰ接続における変化が、該ソースと該パケット装置の間に第２のパケットサーバを追加することを含む装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、概して、通信に関し、特にパケット通信システムに関する。

【０００２】

【従来の技術、及び、発明が解決しようとする課題】

＜関連出願に対する相互参照＞

本発明は、１９９８年５月８日付けの同時係属米国特許出願第０９／０７４，５８２号の一部継続出願である。

【０００３】

通信手段としてのインターネットの１つの使用は、「仮想プライベート・ネットワーク」（ＶＰＮ）と呼ばれるものを提供するために、ワークグループを一緒に結合するための高度化されたデータ・バックボーンである。ＶＰＮの１つの応用は企業環境における応用であり、たとえば、家にいる従業員が、インターネットを経由して企業のデータ・ネットワークにリモートにアクセスできるような環境における応用である。ＶＰＮは公共の施設を使っているにもかかわらず、閉じられたユーザ・グループを結合するために、リモートのユーザに対してセキュリティおよび認証を提供する。実際に、ＶＰＮの使用は企業およびその従業員に対してＷＡＮに似た手段を提供する。（企業ネットワークは直接リモート・アクセスすること、たとえば、ユーザが企業ネットワークの中に直接ダイアルすることもできるが、ＶＰＮを使う方が経済的に有利である）

【０００４】

ＶＰＮを提供するために、「ポイント・ツー・ポイントのトンネリング・プロトコル」（ＰＰＴＰ）や「レイヤー２転送」（Ｌ２Ｆ）プロトコルなどのトンネリング・プロトコルが使われる。一般的に言うと、トンネリング・プロトコルによって、１つのパケットを別のパケットの内側に入れることによって、公共のネットワークを経由してプライベートなデータ・ストリームを生成することができる。ＶＰＮの場合においては、ＩＰパケットが別のＩＰパケットの内部に入れられる。業界標準を開発しようとする試みの中で、Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ（インターネット・エンジニアリング・タスク・フォース）（ＩＥＴＦ）が“Ｌａｙｅｒ ２ Ｔｕｎｎｅｌｉｎｇ Ｐｒｏｔｏｃｏｌ”（レイヤー２のトンネリング・プロトコル）（Ｌ２ＴＰ）を開発中であり、それはＰＰＴＰとＬ２Ｆプロトコルのハイブリッドである（たとえば、Ｋ．ハムゼー（Ｈａｍｚｅｈ）、Ｔ．コラール（Ｋｏｌａｒ）、Ｍ．リトルウッド（Ｌｉｔｔｌｅｗｏｏｄ）、Ｇ．サイン・ポール（Ｓｉｎｇｈ Ｐａｌｌ）、Ｊ．タールッド（Ｔａａｒｕｄ）、Ａ．Ｊ．ヴァレンシア（Ｖａｌｅｎｃｉａ）、Ｗ．ヴェルザイン（Ｖｅｒｔｈｅｉｎ）のＬａｙｅｒ ２ Ｔｕｎｎｅｌｉｎｇ Ｐｒｏｔｏｃｏｌ“Ｌ２ＴＰ”（レイヤー２のトンネリング・プロトコル）（Ｌ２ＴＰ）；Ｉｎｔｅｒｎｅｔ ｄｒａｆｔ、１９９８年３月を参照されたい）。

リモートのユーザの場合、ＶＰＮに対するアクセスの代表的な形式は、ＶＰＮサービスを提供する「インターネット・サービス・プロバイダ」（ＩＳＰ）に対して「在来型の電話サービス」（ＰＯＴＳ）の接続を経由する形式である。たとえば、ユーザはアナログのモデムをパーソナル・コンピュータまたはそれと等価な装置の中に組み込み、ここで「ホーム」ＩＳＰと呼ばれる特定のＩＳＰについて顧客の口座を有する。（また、そのユーザの

パーソナル・コンピュータは上記トンネリング・プロトコルの１つをサポートするように適切に構成されていることが仮定されている。）そのユーザはホームＩＳＰに対してデータ呼出しを単純に行うことによって、たとえば、「ホーム」ＩＳＰに関連付けられている電話番号をダイアルし、ＶＰＮに対して「ログイン」することによって、ＶＰＮにアクセスする。

【０００５】

【課題を解決するための手段】

ＩＳＰに対するアクセスは、ネットワーク・アクセス・サーバ（ＮＡＳ）経由で行われる。筆者等は、個人通信サービス（ＰＣＳ）無線環境においては、上記トンネリング・プロトコルはリモートのユーザが既存の呼出しにおいて、アクセスを提供しているＮＡＳをＶＰＮに変更することを許さないことを実感している。したがって、ユーザが物理的に移動することによって、そのユーザが既存のＶＰＮ接続から切り離されるか、あるいはドロップされる可能性がある。

【０００６】

したがって、本発明の１つの態様によれば、パケット・データを転送するための装置および方法が、既存のポイント・ツー・ポイント（ＰＰＰ）接続を１つのパケット・サーバから別のパケット・サーバへ移すことを許す「ハンドオフ」機能を提供する。

【０００７】

本発明の１つの実施形態においては、３つの新しいハンドオフ制御メッセージがパケット・サーバで使うために定義されている。すなわち、（ｉ）Ｃｏｎｔｉｎｕｅｄ Ｃａｌｌ Ｒｅｑｕｅｓｔ（継続型の呼要求）、（ｉｉ）Ｃｏｎｔｉｎｕｅｄ Ｃａｌｌ Ｒｅｐｌｙ（継続型の呼応答）、および（ｉｉｉ）Ｃｏｎｔｉｎｕｅｄ Ｃａｌｌ Ｃｏｎｎｅｃｔ（継続型の呼接続）である。これらの新しい３つの制御メッセージはＬ２ＴＰ制御メッセージ・ヘッダ、メッセージ識別子（たとえば、Ｃｏｎｔｉｎｕｅｄ Ｃａｌｌ Ｒｅｑｕｅｓｔなど）、およびいくつかのフィールドを含む。結果として、ユーザは現在のＰＰＰ接続をターミネートしてから新しいＰＰＰ接続を再確立する必要はない。

【０００８】

有利なこととして、そのようなハンドオフ制御メッセージまたは呼継続トランザクションを、ハンドオフのシナリオに関与する任意のサーバから起動することができる。たとえば、ポイント・ツー・ポイントの呼がセットアップされていて、第１のパケット・サーバ（たとえば、第１のサービス中のＬＡＣ）と第２のパケット・サーバ（たとえば、アンカーＬＡＣ）とを経由してユーザとプライベート・ネットワークとの間で進行中である初期装置を仮定する。たとえば、ユーザが第１のパケット・サーバによってサービスされている領域から移動し、第３のパケット・サーバ（たとえば、第２のサービス中のＬＡＣ）によってサービスされる領域へ入った場合、本発明によるハンドオフ制御メッセージ・トランザクションが起動される。本発明によると、第２のサービス中のＬＡＣが呼継続トランザクションを起動することができ、あるいはアンカーＬＡＣが呼継続トランザクションを起動することができる。代わりに、本発明のもう１つの態様によれば、その呼継続トランザクションを実行するために、それらのパケット・サーバにそれぞれ関連付けられている区域サーバ（Ｒａｄｉｕｓサーバ）を採用することができる。

【０００９】

本発明のもう１つの態様においては、通信径路が第２のパケット・サーバ（たとえば、アンカーＬＡＣ）と第３のパケット・サーバ（たとえば、第２のサービス中のＬＡＣ）との間にまだ設立されていないと仮定して、通信径路（たとえば、トンネル）セットアップ制御メッセージ・トランザクションを呼継続トランザクションと同時並行的に実行することができる。

【００１０】

さらに、本発明のさらに他の態様においては、少なくとも１つのパケット・サーバ（たとえば、アンカーＬＡＣ）がそこからパケット・データを受信するパケット・サーバ（たとえば、第２のサービス中のＬＡＣおよびプライベート・ネットワーク）に関連付けられて

いる状態変数を監視する。
【００１１】
【発明の実施の形態】
参照し易いように、以下の詳細説明は３つのトピック・セクション、すなわち、マルチホップ・ポイント・ツー・ポイント・プロトコル、移動ポイント・ツー・ポイント・プロトコル、およびｍＬ２ＴＰに対するペイロード・メッセージの概要および混雑制御に分割されている。
【００１２】
＜マルチホップ・ポイント・ツー・ポイント・プロトコル＞
図１は本発明の原理による例示としての通信システム１００を示している。本発明の概念は別として、その構成要素はよく知られており、詳細には説明されない。たとえば、パーソナル・コンピュータ（ＰＣ）１１０はインターネットの接続を設立するためのＩＳＰ Ｂに対して公衆電話網（ＰＳＴＮ）を経由してダイアルアップ・アクセスのためのデータ通信機器（図示せず）を含んでいる。同様に、通信システム１００の構成要素間の実線はそれぞれの終端点間のよく知られている通信機能を表しており、たとえば、ＰＣ １１０とＰＳＴＮ １１０との間の接続はローカル・ループ接続の代表であり、ＩＳＰ Ｂとインターネット１２０との間の接続は同期光ネットワーク（ＳＯＮＥＴ）上での非同期転送モード（ＡＴＭ）によってサポートされている。さらに、読者は上記Ｌ２ＴＰプロトコルについてよく知っていると仮定される。
【００１３】
図１から観察できるように、通信システム１００は２つのＩＳＰ、すなわち、ＩＳＰ Ａネットワークによって表されるＩＳＰ Ａ、およびＩＳＰ Ｂネットワークによって表されるＩＳＰ Ｂを含む。ＩＳＰ Ｂネットワークはネットワーク・アクセス・サーバ（ＮＡＳ）１１５を含み、ＮＡＳ １１５はこの分野の技術において知られているような接続点（ＰＯＰ：ｐｏｉｎｔ－ｏｆ－ｐｒｅｓｅｎｃｅ）ルータ（図示せず）、ローカル・ネットワーク１２０、およびルータ１２５を含む。同様に、ＩＳＰ ＡネットワークはＮＡＳ １５５、ローカル・ネットワーク１６０、およびルータ１６５を含む。ＩＳＰ Ａはネットワーク・サーバ（ＮＳ）１３５を経由して例示としての企業ネットワークにアクセスするために、離れた場所にいる従業員に対してＶＰＮサービスを提供し、ＮＳ １３５は他の機能以外に特にルーティングおよびファイアウォールの機能を提供する。（その企業ネットワークは、たとえば、ＮＳ １３５の背後に適切に保護されているローカル・エリア・ネットワーク（図示せず）の集合であると仮定されている。
【００１４】
リモートのユーザは、たとえ一時的であってもＩＳＰ Ａによってサービスされず、代わりにＩＳＰ Ｂによってサービスされる領域の一部分にいる可能性があることを筆者らは観察している。したがって、本発明の原理によって、リモートのユーザにはそれぞれのホーム、またはアンカーのＩＳＰの他に訪問中のあるいはサービス中のＩＳＰを経由してＶＰＮにアクセスすることが許される。（ＩＳＰ ＡとＩＳＰ Ｂとは異なるサービス・プロバイダであることが仮定されているが、これは本発明の概念に対しては不要であり、たとえば、それらは単に同じＩＳＰの内部の別のネットワークであってもよい。）したがって、ＰＣ １０５の場所にいるユーザ（図示せず）は、たとえば、その領域の中を移動しながら、企業ネットワークにアクセスすることができる。
【００１５】
ここで、以下の定義が仮定される。
ｍＬ２ＴＰ－Ｋ．ハムゼー（Ｈａｍｚｅｈ）、Ｔ．コラール（Ｋｏｌａｒ）、Ｍ．リトルウッド（Ｌｉｔｔｌｅｗｏｏｄ）、Ｇ．サイン・ポール（Ｓｉｎｇｈ Ｐａｌｌ）、Ｊ．タールッド（Ｔａａｒｕｄ）、Ａ．Ｊ．ヴァレンシア（Ｖａｌｅｎｃｉａ）、Ｗ．ヴェルザイン（Ｖｅｒｔｈｅｉｎ）のＬａｙｅｒ ２ Ｔｕｎｎｅｌｉｎｇ Ｐｒｏｔｏｃｏｌ“Ｌ２ＴＰ”（レイヤー２のトンネリング・プロトコル）（Ｌ２ＴＰ）；Ｉｎｔｅｒｎｅｔ ｄｒａｆｔ，１９９８年３月、の中で定義されているＬ２ＴＰプロトコルに、ここで

記述されているような変更を加えたもの
ＬＡＣ－ｍＬ２ＴＰのアクセス制御、すなわち、ｍＬ２ＴＰをサポートするＮＡＳ
ＬＮＳ－ｍＬ２ＴＰをサポートするＮＳ
アンカーＬＡＣ‐ＶＰＮサービスを提供するためにＬＮＳに対するトンネリングをサポートするＬＡＣ
サービス中のＬＡＣ－別のＬＡＣに対するトンネリングをサポートするＬＡＣ
これらの定義は本発明の概念の一例を単純に記述するために使われる。したがって、この技術分野の人であれば、本発明の概念はそれによって限定されるものではなく、任意のトンネリング・プロトコルおよびそれに関連付けられる処理装置に対して適用できることが分かるだろう。

【００１６】
本発明の概念によると、ＩＳＰ　Ａネットワークはアンカー ＬＡＣ　１５５を示し、ＩＳＰ　Ｂネットワークはサービス中のＬＡＣ　１５５を示している。以下にさらに説明されるように、そして本発明の概念に従って、図１のシステム１００はマルチホップ・トンネルを提供する。図１の例は、２ホップのトンネルを示している。１つのホップは、ＩＳＰ　Ｂネットワークから ＩＳＰ　Ａネットワークへのホップであり、他のホップは、ＩＳＰ　Ａネットワークから企業ネットワークへのホップである。

【００１７】
ここで図２を参照すると、本発明の概念による方法の例示としての高レベルのフローチャートを示している（サービス中のＬＡＣ　１１５および他のそれぞれのサーバは以下に説明される方法を従来のプログラミング技法（ここでは説明されない）を使って実行するように適切にプログラムされていることが仮定されている）。ステップ２０５において、リモートのユーザはＰＳＴＮ　１１０を経由してＩＳＰ　Ｂに対するＰＰＰ（ポイント・ツー・ポイント・プロトコル）の接続を起動する。ステップ２１０において、サービス中のＬＡＣ　１１５はそのユーザを部分的に認証し（たとえば、あらかじめ定義されている「ユーザ名」および「パスワード」を使って）、そしてその接続（図１の点線１によって表されている）を受け入れる。（代わりに、ＤＮＩＳ（ダイアル番号識別サービス）、ＣＬＩＤ（呼回線識別）または他の等価な形式の識別を使うことができる。）明らかに、サービス中のＬＡＣ　１１５はユーザを認証することができず、その接続は受け付けられない（このステップは図には示されていない）。

【００１８】
背景として、そしてこの分野の技術で知られているように、リモートのユーザが新しいＰＰＰセッションを確立したい時、ＰＣ　１１０はサービス中のＬＡＣに対してＰＰＰ　ＬＣＰ（リンク制御プロトコル）のＣｏｎｆｉｇ　Ｒｅｑｕｅｓｔを起動する。サービス中のＬＡＣは本発明の概念に従って、アンカーＬＡＣとの通信を開始する前に、そのユーザの機器によってこの分野の技術において知られているように、ＰＰＰ　ＬＣＰおよびＰＰＰ　ＰＡＰ／ＣＨＡＰのフェーズの両方を完了する（安全なコンジット（Ｃｏｎｄｕｉｔｓ）のために、ＩＥＴＦはＰＰＰの接続上でのセキュリティのために２つのプロトコル、すなわち、パスワード認証プロトコル（ＰＡＰ）およびチャレンジ・ハンドシェイク認証プロトコル（ＣＨＡＰ）（ＩＥＴＦのコメントに対する要求（ＲＦＣ）１３３４、「ＰＰＰ認証プロトコル」を参照されたい）を定義している。

【００１９】
ステップ２１５において、サービス中のＬＡＣ　１１５はリモートのユーザがＶＰＮサービスを使いたいかどうかを判定する。この選択は、たとえば、特定の「ユーザ名」に直接に関連付けられるか、そして／またはサービス中のＬＡＣ　１１５によって提供されるポップアップ「ハイパーテキスト・トランスポート・プロトコル」（ｈｔｔｐ）の形式によって、ユーザからの別の要求に関連付けられるようにすることができる。リモートのユーザが仮想ダイアルアップ・サービスを要求しなかった場合、サービス中のＬＡＣ　１１５は標準のインターネット・アクセスをステップ２２０において提供する。しかし、リモートのユーザがＶＰＮを使いたかった場合、サービス中のＬＡＣ　１１５はステップ２２５

において関連付けられたアンカーＬＡＣとして識別する（下記）。

【００２０】

サービス中のＬＡＣ　１１５は、たとえば、ユーザの識別を特定のアンカーＬＡＣと先験的に関連付けるＶＰＮテーブルを格納している。そのようなテーブルの一部分が下記の表１に示されている。この例においては、ＰＣ　１１０に関連付けられているリモートのユーザがアンカーＬＡＣ　ＩＳＰＡ．ｃｏｍ、すなわち、アンカーＬＡＣ　１５５に関連付けられている。

【表１】

表　１

ユーザ識別	アンカーＬＡＣ
ユーザ名	ＩＳＰＡ．ｃｏｍ

【００２１】

等価な構造または操作が使えることに注意する必要がある。たとえば、「ｕｓｅｒｎａｍｅ@ＩＳＰＡ．ｃｏｍ」のようなフォーマットのフィールドのリストを単純に維持することができる。ここで「@」の記号の後の部分はアンカーＬＡＣを示す。代わりに、ＩＳＰＢはユーザをサービスに対してマップしているデータベースを維持することができる。仮想ダイアルアップのケースにおいては、すなわち、リモートのユーザの識別がＶＰＮサービスに関連付けられている場合、そのマッピングはそのアンカーＬＡＣをさらに識別する。代わりに、サービス中のＬＡＣはこの分野の技術において知られているように、このタスクに対する自分のローカルＲａｄｉｕｓサーバによるＲａｄｉｕｓアクセス要求／応答のトランザクションを利用することができる。

【００２２】

ステップ２３０において、サービス中のＬＡＣ　１１５は自分自身とアンカーＬＡＣ　１５５との間にトンネルが存在するかどうかを知るためにチェックする。したがって、サービス中のＬＡＣ　１１５は現在のトンネルについての以下の表２に示されているようなテーブルを維持する。この表はトンネル識別子（Ｔｉｄ）の値、そのトンネルを現在使っている呼の関連付けられた呼識別子（Ｃｉｄ）、および関連付けられているアンカーＬＡＣのＩＰアドレスによって表されている。

【表２】

表　２

Ｔｉｄ	ｃｉｄ	アンカーＬＡＣのＩＰアドレス
2	5	h．j．k．l

【００２３】

サービス中のＬＡＣとアンカーＬＡＣとの間にトンネル接続が現在存在しない場合、ステップ２３５においてアンカーＬＡＣに対して１つのトンネルがサービス中のＬＡＣ　１１５によって起動される（下記）。サービス中のＬＡＣとアンカーＬＡＣとの間にトンネルが存在すると、サービス中のＬＡＣ　１１５はステップ２４０において、新しいＣｉｄを割り当て、テーブル２を更新し、ローカル・ネットワーク１２０、ルータ１２５、インターネット１３０、ルータ１６５、およびローカル・ネットワーク１６０を経由してアンカーＬＡＣ　１５５に対してＶＰＮ要求を転送することによって、アンカーＬＡＣ　１５５との１つのセッションを起動する（以下にさらに説明される）。この要求の中でサービス中のＬＡＣ　１１５はユーザの識別情報をアンカーＬＡＣ　１５５へ伝える。

【００２４】

ここで図３を参照すると、アンカーＬＡＣ　１５５はステップ３０５においてその要求を受け取る。ステップ３１０において、アンカーＬＡＣ　１５５はそのリモートのユーザの認証も実行し（たとえば、上記のように所定の「ユーザ名」および「パスワード」を使っ

て）、そしてその接続（図１の点線２によって表されている）を受け入れる。（代わりに、そのサービス中のＬＡＣと同様に、ＤＮＩＳ　ＣＬＩＤ、または他の等価な識別の形式を使うことができる。）アンカーＬＡＣ　１５５がそのユーザを認証することができない場合、その接続は受け付けられない（このステップは示されていない）。この場合、サービス中のＬＡＣ１１５はエラー・メッセージをそのリモートのユーザ（図示せず）に対して同様に送り返さなければならない。

【００２５】

アンカーＬＡＣ　１５５は、たとえば、ユーザの識別情報を特定のＬＮＳと先験的に関係付けるＶＰＮテーブルを格納している。そのようなテーブルの一部分が下記の表３に示されている。この例においては、ＰＣ　１１０に関連付けられているリモートのユーザが、ＩＰアドレスｇ．ｈ．ｉ．ｊ．によって表されているＬＮＳ　１３５と関連付けられている。

【表３】

表　３

ユーザ識別情報	ＬＮＳ
ユーザ名	ｇ．ｈ．ｉ．ｊ

【００２６】

サービス中のＬＡＣ　１１５と同様に、等価な構造または操作を使うことができることに注意する必要がある。たとえば、アンカーＬＡＣはホームＲａｄｉｕｓサーバによってＲａｄｉｕｓのアクセス要求／応答メッセージ経由で、この機能を実行することもできる。ステップ３１５において、アンカーＬＡＣ　１５５は表３を使って、これが有効なＶＰＮ要求であるかどうかをチェックする。これが有効な要求でなかった場合、アンカーＬＡＣ　１５５はステップ３２０においてその要求を拒否する。これが有効な要求であった場合、アンカーＬＡＣ　１５５はステップ３２５において、表３から関連付けられたＬＮＳを識別する。

【００２７】

アンカーＬＡＣはリモートのユーザとの確立された各ＶＰＮセッションに対して通信の各方向について以下の接続テーブルを維持すると仮定されている。

【表４】

表　４

コネクション番号	サービス中のLAC		サービス中のLAC	LNS		LNS IPアドレス	ユーザ割当てのIPアドレス
	Tid	Cid	IPアドレス	Tid	Cid		
5	2	5	d.e.f.g	1	3	g.h.i.j	a.b.c.d

【００２８】

アンカーＬＡＣは各ＶＰＮセッションと１つの接続番号とを関係付ける。さらに、この接続番号はそれぞれのユーザに対してマップされている。このテーブルは接続番号によって、サービス中のＬＡＣのＩＰアドレス（そのホップに対する関連付け付けられたトンネルＩＤおよび呼ＩＤの値を伴う）、および関連付けられたＬＮＳのＩＰアドレス（その関連付けられたホップに対する関連付けられたトンネルＩＤおよび呼ＩＤの値を伴う）をリストする。ステップ３３０において、アンカーＬＡＣ　１５５はＶＰＮセッションを確立する（認証のチェックなどを実行する）。（ふたたび、ＬＮＳ　１３５はそのＶＰＮ要求を拒否する必要があり（たとえば、リモートのユーザの不認可または容量がないことのために）、適切なエラー・メッセージがアンカーＬＡＣおよびサービス中のＬＡＣによって発生される）。本発明の概念以外に、ＬＮＳ　１３５によるＶＰＮのセッションが従来の技

術におけるように確立される。たとえば、そして本発明の原理に従って、新しいＶＰＮセッションを確立する際、アンカーＬＡＣ　１５５は新しいＣｉｄを割り当て、テーブル４を更新し、たとえば、新しい接続を追加する。この最後の接続が図１の点線３で表されている。

【００２９】

この点で、その接続性はポイント・ツー・ポイントのＰＰＰセッションであり、その端点は、一端においてはＰＣ　１０５によって表されているような、そのリモートのユーザのネットワーキング・アプリケーションであり、そして他端においては情報の他のものにおけるＬＮＳ　１３５のＰＰＰサポートへのこの接続性の終了である。必要な場合、ＬＮＳ以外に、サービス中のＬＡＣ、アンカーＬＡＣにおいてアカウンティングが実行できること、すなわち、各構成要素がパケット数、オクテット数および接続の開始および停止の時刻をカウントすることができることに留意されたい。

【００３０】

上記マルチホップ仮想ダイアルアップ・サービスのサポートにおいて、Ｌ２ＴＰ（ｍＬ２ＴＰ）プロトコルの一形式が使われ、以下にさらに説明される。Ｌ２ＴＰの場合のように、与えられたトンネル上で動作するｍＬ２ＴＰの２つの並列コンポーネント、すなわち、各ＬＡＣ－ＬＮＳペア間の制御メッセージおよび、同じＬＡＣ－ＬＮＳ間のペイロード・パケットがある。後者はＬＡＣ－ＬＮＳ間のユーザ・セッションに対してＬ２ＴＰのカプセル化されたＰＰＰパケットを転送するために使われる。Ｌ２ＴＰの場合のように、Ｎｒ（次の受信）およびＮｓ（次の送信）のフィールドは、制御メッセージの中に常に存在し、そしてペイロード・パケットの中にはオプション的に存在する。制御メッセージおよびペイロード・メッセージは異なるシーケンス番号状態を使用する。上記ＬＡＣ／ＬＮＳペアのシナリオの場合、（Ｎｒ、Ｎｓ）のメンテナンスおよび使用に関する限り、Ｌ２ＴＰのドラフト・プロトコルの定義に対する変更はない。

【００３１】

しかし、サービス中のＬＡＣとアンカーＬＡＣとの間の接続のように、サービス中のＬＡＣから送られた（Ｎｒ、Ｎｓ）の値を単に監視するだけである。すなわち、本発明の概念に従って、アンカーＬＡＣはサービス中のＬＡＣから受信された値をＬＮＳに対して単純に送信する。さらに、ここでアンカーＬＡＣはその（受信された状態、送信された状態）の値（Ｓｒ、Ｓｓ）を、サービス中のＬＡＣから送られたパケットから観察した対応している値（Ｎｒ、Ｎｓ）で更新する。サービス中のＬＡＣとアンカーＬＡＣとの間で、パケットの消失が間違いなくあるので、アンカーＬＡＣにおけるＳｓ（Ｓｒ）の値はサービス中のＬＡＣにおけるＳｓ（Ｓｒ）の値より小さい可能性がある。さらに、アンカーＬＡＣは二組の（Ｓｒ、Ｓｓ）の変数、すなわち、１つはサービス中のＬＡＣ／アンカーＬＡＣの制御接続に対するもの、そしてもう１つはアンカーＬＡＣ／ＬＮＳの制御接続に対するものを維持する。

【００３２】

ＰＰＰのトンネリングを発生させることができるより前に、本発明の概念に従って、サービス中のＬＡＣ、アンカーＬＡＣ、およびＬＮＳの間で、制御メッセージが交換されなければならない。制御メッセージはｍＬ２ＴＰの呼制御およびマネージメント情報が渡された時、ペイロード・データを転送するためにそれ以降で使われるのと同じトンネル上で交換される。

【００３３】

本発明の概念によると、追加の属性値ペア（ＡＶＰ）（下記）がＬ２ＴＰの制御メッセージの中で使うために定義される（したがって、ｍＬ２ＴＰ制御メッセージとなる）。これらの追加のＡＶＰは上記マルチホップの機能および呼転送機能をサポートするためのものである。Ｌ２ＴＰにおいて定義されているように、ＡＶＰは制御シグナリングをさらに規定するために使われる。

【００３４】

上で注記されたように、上記ＬＡＣ／ＬＮＳペアの場合、上記Ｌ２ＴＰの草案において記

述されている手順には変更がない。したがって、マルチ・ホップのケースだけが下記の追加の手順を必要とする。

【００３５】

例示としてのマルチホップ・メッセージのフローが図４に示されている。図４から分かるように、トンネル（Ｔｉｄの値によって識別される）および呼（Ｃｉｄの値によって識別される）がサービス中のＬＡＣとアンカーＬＡＣとの間に確立される。同様に、トンネルおよび呼がアンカーＬＡＣとＬＮＳとの間に確立される。図４に示されているように、本発明の概念はサービス中のＬＡＣがアンカーＬＡＣに対するトンネルを確立することを要求する。本発明の場合においては、サービス中のＬＡＣはアンカーＬＡＣを１つのＬＮＳとして扱い、Ｌ２ＴＰの手順がそのトンネルを最初にセットアップするために使われる。

【００３６】

トンネルが確立されると、本発明の原理に従ってＰＰＰセッションをセットアップするためにいくつかの制御メッセージ・トランザクションが発生する。これらは図５－図７に示されている。これらの図において、各種の制御メッセージに対する関連のフィールドだけが示されている。サービス中のＬＡＣとアンカーＬＡＣとの間のトンネルに対するトンネルのｉｄおよび呼のｉｄが、アンカーＬＡＣとＬＮＳとの間のトンネルに対するそれらの値と異なっていた場合、アンカーＬＡＣはそれらをいずれかの方向に中継するより前に、そのパケット・ヘッダの中の関連のフィールドを修正する。

【００３７】

図５に示されているように、サービス中のＬＡＣは先ず最初にＳｔａｒｔ－Ｃｏｎｔｒｏｌ－Ｃｏｎｎｅｃｔ　Ｒｅｑｕｅｓｔ　Ｍｅｓｓａａｇｅ（ＳＣＣＲＱ）メッセージ（Ｌ２ＴＰの中で定義されているような）をアンカーＬＡＣに対して送信し、それらの間のトンネルを構成する。このメッセージを受信すると、アンカーＬＡＣはＳｔａｒｔ－Ｃｏｎｔｒｏｌ－Ｃｏｎｎｅｃｔ－Ｒｅｐｌｙ　Ｍｅｓｓａｇｅ（ＳＣＣＲＰ）メッセージ（これは任意の上記認証に続いて発生する）で応答する。サービス中のＬＡＣはアンカーＬＡＣに対するＳｔａｒｔ－Ｃｏｎｔｒｏｌ－Ｃｏｎｎｅｃｔｉｏｎ‐Ｃｏｎｎｅｃｔ（ＳＣＣＣＮ）メッセージによって確認する。

【００３８】

図５に示されている制御接続開始メッセージの交換に続いて、サービス中のＬＡＣはＩｎｃｏｍｉｎｇ－Ｃａｌｌ－Ｒｅｑｕｅｓｔ（ＩＣＲＱ）メッセージを、図６に示されているようにアンカーＬＡＣに対して送信する。Ｉｎｃｏｍｉｎｇ－Ｃａｌｌ－ＲｅｑｕｅｓｔメッセージはアンカーＬＡＣがＬＮＳを識別することができるのに十分なユーザ・データおよび信用証明情報を含んでいる。

【００３９】

以前に注記されたように、アンカーＬＡＣとＬＮＳとの間にトンネルが存在しなかった場合、アンカーＬＡＣはＬ２ＴＰにおいて定義されているように、ＬＮＳとのＳＣＣＲ、ＳＣＣＲＰ、ＳＣＣＣＮメッセージの交換を先ず最初に開始する。トンネルが存在すると、そのトンネルの中の中の不使用の１つのスロット、１つのＣｉｄがアンカーＬＡＣによって割り当てられる。この点において、そして本発明の原理に従って、アンカーＬＡＣはこの新しいダイアルアップ・セッションのＬＮＳを通知するために、そのＩＣＲＱメッセージ（サービス中のＬＡＣからの）を中継する。図６に示されているように、アンカーＬＡＣはそれに従ってＩＣＲＱメッセージをＩＮＳに対して中継する前に修正する。その修正されたフィールドは「＊」、たとえば、割り当てられた呼のＩＤによって示される。また、アンカーＬＡＣは隠されたＡＶＰも追加して、どんな受信ウィンドウ・サイズをそれがサポートすることができるかをＬＮＳに知らせる（追加のホップで、アンカーＬＡＣは制御／ペイロードの接続の両方に対してネゴシエートされた最大のウィンドウ・サイズを記録することに留意されたい）。また、サービス中のＬＡＣとアンカーＬＡＣとの間の制御接続に対するウィンドウ・サイズはアンカーＬＡＣとＬＮＳとの間の制御接続のためのウィンドウ・サイズとは異なっている可能性があり、バッファリングが必要となる可能性がある。追加のバッファリングおよびシーケンス番号の監視をなくすために、アンカーＬＡ

ＣはオプションとしてＡＶＰを追加してアンカーＬＡＣ‐サービス中のＬＡＣの方向において、アンカーＬＡＣがそのペイロード・セッションに対してどんなウィンドウ・サイズをサポートできるかをＬＮＳに対して知らせる。結果として、ＬＮＳはそのＩＣＲＰ応答における適切な受信ウィンドウ・サイズの値だけを含むことになり、したがって、ＬＮＳ－アンカーＬＡＣ－サービス中のＬＡＣの方向においてペイロード・セッションに対する１つのウィンドウ・サイズだけを含むことになる。

【００４０】

以前に注記されたように、ＬＮＳはその接続を受け入れるか、あるいはそれを拒否する。リジェクションは結果の状態を含まなければならず、そしてエラー指示を含むことができる。いずれの場合においても、図６に示されているように、ＬＮＳはＩｎｃｏｍｉｎｇ－Ｃａｌｌ－Ｒｅｐｌｙ（ＩＣＲＰ）メッセージをアンカーＬＡＣに対して送信する。次に、アンカーＬＡＣはそのＩＣＲＰメッセージを適当に修正し、それを本発明に従ってサービス中のＬＡＣに対して中継する（ふたたび、修正されたフィールドは図６において「＊」によって示されている）。ＬＮＳから受信されるパケット処理遅延（ＰＰＤ）フィールドは、ＬＮＳにおける処理遅延だけしか含んでいないので、アンカーＬＡＣは、この値に自分自身のノードにおける処理遅延を加算する。次に、ＩＣＲＱメッセージがサービス中のＬＡＣに対して中継される。

【００４１】

応答において、サービス中のＬＡＣは図７に示されているように、Ｉｎｃｏｍｉｎｇ－Ｃａｌｌ－Ｃｏｎｎｅｃｔｅｄ（ＩＣＣＮ）メッセージをアンカーＬＡＣに対して送信する。このメッセージの内部で、サービス中のＬＡＣはプロキシ認証情報以外に、すべてのＬＣＰ構成要求情報を渡す。すなわち、サービス中のＬＡＣはそのユーザの装置によって実行されたＬＣＰ　Ｃｏｎｆｉｇ　Ｒｅｑｕｅｓｔ／Ａｃｋ，ＰＰＰ　ＰＡＰ／ＣＨＡＰの結果を転送している。アンカーＬＡＣはその受信されたＩＣＣＮメッセージのＰＰＰフィールドを変更した後、それをＬＮＳに対して中継する。現在、ｔｘ（送信）接続速度およびｒｘ（受信）接続速度は使われない。図には示されていはいないが、そして本発明に従って、アンカーＬＡＣはＬ２ＴＰにおいて定義されているすべてのＳｅｔ－Ｌｉｎｋ－Ｉｎｆｏ、ＨｅｌｌｏおよびＷａｎ－Ｅｒｒｏｒ－Ｎｏｔｉｆｙメッセージをも中継する。（上記はマルチホップのパケット・トンネルの概念を示していることに注意されたい。たとえば、図１は２ホップのパケット・トンネルを表している。）

【００４２】

上記マルチホップｍＬ２ＴＰトンネルはフレーム層においてのみ発生することに留意されたい。したがって、ＬＮＳによるアドレス管理の実際のポリシーは上記仮想ダイアルアップ・サービスには無関係である。というのは、ＰＰＰプロトコル処理のすべての目的に対して、リモートのユーザはそのＬＮＳに接続されているように見えるからである。

【００４３】

＜移動ポイント・ツー・ポイント・プロトコル＞

ここで図８を参照すると、本発明の概念の他の実施形態が示されている。図８は図１に似ている。本発明の概念は別として、その構成要素はよく知られており、詳細には説明されない。類似の番号は類似の機能を示し、必要な場合以外はさらには説明されない。

【００４４】

図８において、ＰＣ　８０５は個人通信サービス（ＰＣＳ）の無線ネットワーク８１０を通じてインターネットに対する無線アクセスを確立するためのデータ通信装置（図示せず）を含んでいる。ＰＣＳの無線サービスはこの分野の技術において知られており、したがって、詳細には説明されない。ＰＣＳの無線ネットワーク８１０は構成要素８１５および８２０によって表されている複数の移動交換センタを含む。各移動交換センタは１つの地理的領域（図示せず）にサービスする。構成要素８１５および８２０は１つのＮＡＳ、たとえば、図１のサービス中のＬＡＣ　１１５に似たサービス中のＬＡＣを含むと仮定されている。最初に、リモートのユーザが上記マルチホップ技法を使って企業ネットワークに対するＶＰＮセッションを確立すると仮定される。特に、リモートのユーザはこの初期接

続が接続８１４および８１６を経由して構成要素８１５を通して回送されるような地理的領域の中にいる。無線ＰＣＳアプリケーションの場合において、最初のＰＰＰ接続は構成要素８１５とＰＣ　８０５との間にある。簡単のために交換機要素の一部として示されているが、ＮＡＳの機能は別の装置において実行されるようにすることもできる。同様に、ローカル・ネットワークおよびルータなどの他の構成要素は簡単のためにここでは示されていない。

【００４５】

Ｌ２ＴＰなどの無線環境のトンネリング・プロトコルにおいて、リモートのユーザが既存のＰＰＰ接続を１つの交換機要素から別の交換機要素へ変更することはできないことを知っている。たとえば、図８はリモートのユーザが構成要素８２０（したがって、異なるＮＡＳ）に対して、たとえば、動き回る（ｒｏａｍ）時、そのユーザの通信セッションはこの分野の技術において知られているように、構成要素８２０に対してハンドオフされるとしばらくの間仮定する。しかし、既存のＰＰＰ接続（したがって、そのＶＰＮセッション）はドロップされ、そして再確立されなければならない。というのは、注記されたように、既存のＰＰＰ接続を１つのＮＡＳから別のＮＡＳへ移すための能力がないからである。この場合において、図８の通信システムはこの問題を解決する。

【００４６】

したがって、そして本発明に従って、ＮＡＳまたはＬＡＣは既存のＮＡＳが既存のＰＰＰ接続を別のＮＡＳに対してハンドオフすることができる「ハンドオフ」機能を組み込んでいる。この機能に従って、３つの新しい制御メッセージ、すなわち、（ｉ）Ｃｏｎｔｉｎｕｅｄ　Ｃａｌｌ　Ｒｅｑｕｅｓｔ、（ｉｉ）Ｃｏｎｔｉｎｕｅｄ　Ｃａｌｌ　Ｒｅｐｌｙ、および（ｉｉｉ）Ｃｏｎｔｉｎｕｅｄ　Ｃａｌｌ　Ｃｏｎｎｅｃｔが定義されている。上記の結果として、ユーザは現在のＰＰＰ接続を終了してから新しいＰＰＰ接続を再確立する必要はない。これらの新しい３つの制御メッセージはＬ２ＴＰの制御メッセージ・ヘッダ、メッセージ識別子（たとえば、ｃｏｎｔｉｎｕｅｄ　ｃａｌｌ　ｒｅｑｕｅｓｔなど）およびフィールドの番号（下記）を含む。

【００４７】

本発明の概念に従って、例示としてのハンドオフ・メッセージ・フローが図９に示されている。図９から観察できるように、トンネル（Ｔｉｄの値によって識別される）および呼（Ｃｉｄの値によって識別される）が最初に構成要素８１５（サービス中のＬＡＣを含む）とアンカーＬＡＣとの間に確立される。同様に、１つのトンネルと１つの呼がアンカーＬＡＣとＬＮＳとの間に確立される。（この初期ＶＰＮセッションを確立するための方法については上で説明された。）図９に示されているように、本発明の概念によって、既存のサービス中のＬＡＣが既存のＰＰＰ接続を、構成要素８２０によって表されているような新しいサービス中のＬＡＣに対して移すことができる。

【００４８】

ここで図１０を参照されたい。この図は「ハンドオフ機能」を提供する際に使うための方法の例示としてのフローチャートである。注記されたように、ＶＰＮセッションがＰＣ　８０５と企業ネットワークとの間に構成要素８１５を経由して存在している。それはサービス中のＬＡＣおよびアンカーＬＡＣ　１５５を含む。本発明の概念に従って、ＰＣＳ無線ネットワーク８１０は既存の呼状態変数に対して各無線呼に対するＰＰＰ接続の存在（またはその欠如）を示している追加の変数を加え、そしてＰＰＰ接続が存在していた場合、アンカーＬＡＣの識別情報、たとえば、そのアンカーＬＡＣのＩＰアドレスを含むＰＰＰ接続情報を含む。

【００４９】

図１０のステップ４０５において、ＰＣＳ無線ネットワーク８１０はハンドオフが必要であることを検出する。というのは、ＰＣ　８０５が構成要素８１５によってサービスされている地理的領域から別の地理的領域、たとえば、構成要素８２０（別のサービス中のＬＡＣを含む）によってサービスされている領域へ移動したからである。ステップ４１０において、ＰＣＳ無線システムは差し迫っているハンドオフの通知を構成要素８２０に提供

する。（ハンドオフを検出して実行するために無線システムによって使われる方法（複数の場合もある）はこの分野の技術において知られており、そして本発明の概念とは無関係である。したがって、それらはここでは説明されず、図８のシグナリング径路８１１によって表されている。）ここで呼状態情報がＰＰＰセッションの指示子およびＰＰＰ呼情報を含んでいるので、新しいサービス中のＬＡＣ（構成要素８２０の）はステップ４１５においてアンカーＬＡＣを識別する。ステップ４２０において、新しいサービス中のＬＡＣ（構成要素８２０の）は自分自身とその識別されたアンカーＬＡＣ（ここではアンカーＬＡＣ　１５５）との間に既存のトンネルがあるかどうかを知るためにチェックする。

【００５０】

トンネルが存在しなかった場合、新しいサービス中のＬＡＣは先ず最初にステップ４２５において（前に説明されたような）１つのトンネルを確立する。次に、そして本発明の概念に従って、その新しいサービス中のＬＡＣはステップ４３０においてＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｒｅｑｕｅｓｔ（ＣＣＲＱ）メッセージをアンカーＬＡＣに対して送信する。このＣＣＲＱメッセージはその既存のＰＰＰ接続に関連付けられているユーザの名前、移行された（新しい）ＰＰＰセッションのために使われるべきＴｉｄおよびＣｉｄの値を含む。

【００５１】

ステップ４３５において、アンカーＬＡＣは受信されたＣＣＲＱメッセージからユーザの名前を復元し、そしてこの情報を使って前のサービス中のＬＡＣのＬＮＳおよびＩＰアドレスを、たとえば、上記の表４によって表されている接続テーブルから決定する（また、この復元された情報はそれぞれのユーザ・データグラム・プロトコル（ＵＤＰ）のポート番号も含む場合がある）。このステップにおいて、アンカーＬＡＣはＣａｌｌ－Ｄｉｓｃｏｎｎｅｃｔ－Ｎｏｔｉｆｙメッセージ（たとえば、Ｌ２ＴＰ参照）を前のサービス中のＬＡＣに対して送信し、そしてたとえば、上記の表４において、そのリモートのユーザに対するこのＰＰＰ接続に関連付けられている既存の呼変数、たとえば、前のトンネルｉｄおよび前の呼ｉｄをも識別する。他方、アンカーＬＡＣがそのＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｒｅｑｕｅｓｔを拒否した場合、サービス中のＬＡＣは既存のＰＰＰセッションを破棄して、新しいＰＰＰセッションを起動することができるようにそのユーザに対して信号を送り返すか、あるいはそのＰＰＰセッションが単純にドロップされる（そのステップは図には示されていない）。

【００５２】

ステップ４４０において、アンカーＬＡＣは適切な受信ウィンドウ・サイズを伴うＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｒｅｐｌｙ（ＣＣＲＰ）メッセージで応答する。ＣＣＲＰメッセージは現在のＮｒおよびＮｓの値に関する情報を含む。ステップ４４５において、アンカーＬＡＣは自分の接続テーブル、たとえば、上記の表４を、Ｔｉｄ、Ｃｉｄ、およびサービス中のＬＡＣのＩＰアドレスのフィールドに対するエントリー（ステップ４３５において識別された）を、その既存のＰＰＰ接続に対する新しい呼情報で置き換えることによって更新する。ステップ４５０において、新しいサービス中のＬＡＣはそのＮｒ、Ｎｓを自分のＳｒ、Ｓｓの値の中に格納し、そして必要であれば受信されたＣＣＲＰメッセージから受信ウィンドウ・サイズをも格納し、そしてＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｃｏｎｎｅｃｔ（ＣＣＣＮ）メッセージをアンカーＬＡＣに対して送信し、これによってハンドオフが完了する。

【００５３】

ＰＰＰプロトコルに対する上記ハンドオフ機能のサポートにおいて、図１１は本発明の原理による上記の新しい制御メッセージのトランザクションを示している。図１１に示されているように、ＣＣＲＱメッセージが識別されたアンカーＬＡＣに対して送信される。

【００５４】

この実施形態においてはＣＣＲＱメッセージは以下のフィールドを含むことが好ましい。

- 割り当てられたＣｉｄ
- 呼のシリアル番号

- ベアラ（ｂｅａｒｅｒ）のタイプ
- 物理的チャネルＩＤ
- ダイアルされた番号
- ダイアル中の番号
- サブアドレス
- アンカーＬＡＣ
- チャレンジ
- ユーザＡＶＰ
- ユーザ名
- ユーザのＭＩＮ／電話機

アンカーＬＡＣのフィールドは、この情報がハンドオフの間に利用できると仮定している。代わりに、ハンドオフのプロセスが新しいサービス中のＬＡＣに対してアンカーＬＡＣに関する情報を提供しなかった場合、そのハンドオフ・プロセスは、この分野の技術において知られているように、フォーリン（Ｆｏｒｅｉｇｎ）Ｒａｄｉｕｓサーバからのヘルプを使ってアンカーＬＡＣ情報をその新しいサービス中のＬＡＣがサーチできるように、その新しいサービス中のＬＡＣに対して十分なユーザ情報を提供しなければならない。すなわち、新しいサービス中のＬＡＣはＲａｄｉｕｓのアクセス／応答メッセージ経由でホームＲａｄｉｕｓサーバからアンカーＬＡＣに関して問い合わせる。

【００５５】

ユーザのＡＶＰ情報はユーザ情報（ユーザの名前など）および他のユーザ信用証明情報、たとえば、マルチホップの仮想ダイアルアップ・サービス、ユーザのアイデンティティ（ＭＩＮ）、サービス・プロバイダの電話番号などを含む。

【００５６】

ＣＣＲＱメッセージに続いて、アンカーＬＡＣはＣａｌｌ－Ｄｉｓｃｏｎｎｅｃｔ－Ｎｏｔｉｆｙメッセージを前のサービス中のＬＡＣに対して送信する。次に、アンカーＬＡＣは自分が維持している現在のＳｒ、Ｓｓを含むＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｒｅｐｌｙ（ＣＣＲＰ）メッセージで応答する。

【００５７】

この実施形態においては、ＣＣＲＰメッセージは以下のフィールドを含むことが好ましい。

- 割り当てられたＣｉｄ
- 呼のシリアル番号
- 結果のコード
- 受信ウィンドウ・サイズ
- ＰＰＤ
- シーケンス番号ＡＶＰ；Ｎｒ、Ｎｓ
- ＡＣＣＭ　ＡＶＰ
- 最後に送信されたＬＣＰ　Ｃｏｎｆｉｇ．Ｒｅｑｕｅｓｔ
- 最後に受信されたＬＣＰ　Ｃｏｎｆｉｇ．Ｒｅｑｕｅｓｔ
- チャレンジ
- チャレンジの応答

最後に、新しいサービス中のＬＡＣはＣｏｎｔｉｎｕｅｄ‐Ｃａｌｌ　Ｃｏｎｎｅｃｔ（ＣＣＣＮ）メッセージで応答する。この実施形態においては、ＣＣＣＮメッセージは以下のフィールドを含むことが好ましい。

- 接続速度
- フレーミングのタイプ
- 変更されたウィンドウ・サイズ　ＡＶＰ
- ＰＰＤ
- チャレンジ応答

本発明による制御メッセージ・トランザクションに関しての他の実施形態が図１９に示さ

れている。そのような実施形態においては、ハンドオフ制御メッセージ（ＣＣＲＱ、ＣＣＲＰ、およびＣＣＣＮ）はトンネル・コンフィギュレーション（確立）制御メッセージ（ＳＣＣＲＱ、ＳＣＣＲＰ、およびＳＣＣＣＮ）と組み合わされていることが有利であり、そしてそれぞれ同時並行的にＬＡＣ間で送信されることが好ましい。このようにして、新しいサービス中のＬＡＣとアンカーＬＡＣとの間の移行の待ち時間が大幅に改善される。

【００５８】

この場合、既存のＰＰＰ接続またはセッションが既に、たとえば、ＰＣ　８０５、サービス中のＬＡＣ　８１５、アンカーＬＡＣ　１５５およびＮＳ　１３５（図８）の間で進行中であると仮定されている。次に、ユーザのモビリティに従って、ＰＣ８０５は別のサービス中のＬＡＣ、たとえば、サービス中のＬＡＣ　８２０のカバレージ領域の中に移動する。前に述べたように、従来の方法を使うことによってＰＰＰの接続がドロップされ、したがって、その呼を再確立する必要がある結果になる。しかし、本発明によると、その呼はユーザの見通しから中断されずに新しいサービス中のＬＡＣに対してハンドオフされる。前の実施形態においては、新しいサービス中のＬＡＣとアンカーＬＡＣとの間に既存のトンネルがないと仮定して、たとえば、図５に示されているようなトンネルを確立するためのプロセスが、たとえば、図１１に示されているようにハンドオフ・メッセージの交換に先立って実行されなければならない。しかし、図１９に示されている実施形態によると、トンネルの確立のプロセスおよびハンドオフのプロセスは同時並行的に実行される。有利なこととして、新しいサービス中のＬＡＣとアンカーＬＡＣとの間の通信に関連付けられる待ち時間が大幅に減少する。

【００５９】

したがって、トンネルの確立と呼のハンドオフを同時並行的に実行するためには、新しいサービス中のＬＡＣ（たとえば、図８の中の８２０）はＣＣＲＱメッセージにＳＣＣＲＱメッセージを付加した後、そのＣＣＲＱメッセージをアンカーＬＡＣへ送信する。次に、上記のように、アンカーＬＡＣはそのユーザの情報を使って前のＴｉｄ値、前のＣｉｄ値、および前のＩＰ／ＵＤＰポートを決定し、そしてＣａｌｌ－Ｄｉｓｃｏｎｎｅｃｔ－Ｎｏｔｉｆｙ（ＣＤＮ）メッセージを前のサービス中のＬＡＣに対して送信する。次に、アンカーＬＡＣは新しいサービス中のＬＡＣに対して、ＣＣＲＰメッセージに付加されたＳＣＣＲＰメッセージで応答する。新しいサービス中のＬＡＣはその組み合わされたＣＣＣＮとＳＣＣＣＮのメッセージをアンカーＬＡＣに対して送信する。トンネル確立制御メッセージがハンドオフ制御メッセージに対して付加されるが、その中に含まれている個々の機能および情報は上で詳細に説明されたように、不変のままに残っていることを理解されたい。

【００６０】

また、図１９はハンドオフ制御メッセージを含んでいるようなある種のフィールドを示しているが、そのようなメッセージは図１１に示されているメッセージの中にあるのと同じか、あるいは類似のフィールドを含んでいる可能性がある。さらに、図１９、図２０および図２１の場合において、ＣＣＲＱ、ＣＣＲＰ、およびＣＣＣＮに関して示されているどのフィールドも、図１１の同じメッセージの中に存在する可能性があること、およびその逆も言えることを理解されたい。また、これらの実施形態は、説明的な性質のものであるので、ここに記述されているメッセージのどれもが必ずしも示されているフィールドに限定されるものではない。

【００６１】

「ＡＶＰ」という用語はＰＰＰの動作において知られているようにＡｔｔｒｉｂｕｔｅ　Ｖａｌｕｅ　Ｐａｉｒ（属性値ペア）を指すことを理解されたい。そのようなＡＶＰは特に、受信者の装置に関連の情報を提供するメッセージの特定のフィールドの中に含まれている情報である。たとえば、ウィンドウ・サイズのＡＶＰおよび修正されたウィンドウ・サイズのＡＶＰは、それぞれ受信者に対して送信者のウィンドウの容量およびそのウィンドウ・サイズを修正するための通知を示すフィールドである。また、ＡＣＣＭのＡＶＰは非同期制御文字のマップのＡＶＰを指す。これは００（ｈｅｘ）からｉＦ（ｈｅｘ）まで

の範囲内の３２個のＡＳＣＩＩ制御文字に対する文字のエスケープをイネーブル／ディスエーブルする４オクテットのビット・マップである。さらに、シーケンス番号のＡＶＰはサーバ間で状態変数ＮｒおよびＮｓを送信するために使われるフィールドである。またさらに、「Ｌａｓｔ Ｓｅｎｔ ＬＣＰ（Ｌｉｎｋ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）Ｃｏｎｆｉｇ．Ｒｅｑｕｅｓｔ」および「Ｌａｓｔ ＲｃｖＬＣＰ（Ｌｉｎｋ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）Ｃｏｎｆｉｇ．Ｒｅｑｕｅｓｔ」はこの分野の技術において知られているように、ＰＰＰセッションのセットアップに関連付けられたＬＣＰフェーズの間にサーバ間でネゴシエートされるＬＣＰオプションである。

【００６２】

ここで図２０を参照すると、ハンドオフ制御メッセージのトランザクションを実行するためのさらに他の実施形態が示されている。そのような実施形態においては、新しいサービス中のＬＡＣではなく、アンカーＬＡＣが新しいサービス中のＬＡＣとのハンドオフ制御メッセージ・トランザクションを有利に開始することを理解されたい。すなわち、図８および図９に示されている装置に関して、ＰＣ ８０５がサービス中のＬＡＣ ８１５によってカバーされている領域からサービス中のＬＡＣ ８２０によってカバーされている領域へ移動したことの指示をＰＣＳ ８１０から（無線リンク層を経由して）受信すると、新しいサービス中のＬＡＣ ８２０がそのハンドオフ制御メッセージ・トランザクションを起動するのではなく、アンカーＬＡＣがそのトランザクションを起動する。したがって、図２０に示されているように、アンカーＬＡＣはＣＣＲＱメッセージを新しいサービス中のＬＡＣに対して送信し、新しいサービス中のＬＡＣはＣＣＲＰメッセージを返し、そしてアンカーＬＡＣはＣＣＣＮメッセージで応答する。各メッセージの中に含まれている情報、およびその機能は前に説明されたものと類似していることを理解されたい。したがって、ここでは繰り返されない。しかし、図２０においてはアンカーＬＡＣがトランザクションを起動するので、アンカーＬＡＣによって送信される図２０のＣＣＲＱメッセージの中のフィールドは、アンカーＬＡＣによって送信される図１９の中のＣＣＲＰメッセージの中のフィールドと類似している。これはアンカーＬＡＣがこの情報を持っていて、誰がそのトランザクションを起動するかには無関係に、サービス中のＬＡＣに対してそれを送信するためである。

【００６３】

また、図１９に関して示されている実施形態の場合のように、トンネル確立制御メッセージ・トランザクションはアンカーＬＡＣによっても起動され、したがって、制御メッセージＳＣＣＲＱ、ＳＣＣＲＰ、およびＳＣＣＣＮはそれぞれハンドオフの制御メッセージＣＣＲＱ、ＣＣＲＰおよびＣＣＣＮとそれぞれ組み合わされて同時並行的に送信され得ることを理解されたい。

【００６４】

ここで図１２を参照すると、前のＮＡＳがＬＮＳに対する接続を備えている場合の、１つのＮＡＳから別のＮＡＳに対して既存のＰＰＰ接続を移すことの場合において、本発明の概念のもう１つの実施形態が示されている。この例においては、サービス中のＬＡＣそれ自体が存在せず、単純に、たとえば、既存のＰＰＰ接続を直接サポートしているアンカーＬＡＣがある。図１２は図８に似ている。本発明の概念は別として、その構成要素はよく知られており、詳細には説明されない。類似の番号は類似の機能を示し、必要な場合以外はさらには説明されない。

【００６５】

図１２において、ＰＣ ８０５は、個人通信サービス（ＰＣＳ）無線ネットワーク９１０を通じてインターネットに対する無線のアクセスを確立するためのデータ通信装置（図示せず）を含む。ＰＣＳの無線サービスはこの分野の技術において知られており、詳細には説明されない。ＰＣＳ無線ネットワーク９１０は構成要素８７５および８８８によって表されているような複数の移動交換センタを含む。各移動交換センタは１つの地理的領域（図示せず）にサービスする。構成要素８７５および８８０はＮＡＳ（たとえば、図１のアンカーＬＡＣ １１５と同様なＬＡＣ）を含むことが仮定されている。最初に、リモート

のユーザがこの分野の技術において知られているように、たとえば、Ｌ２ＴＰのその部分を使って企業ネットワークに対するＶＰＮセッションを確立すると仮定されている。特に、リモートのユーザはこの初期接続が接続８７４および８７６を経由して構成要素８７５を通じてＬＮＳ　９３５へ回送されるような地理的領域の中にいる。無線ＰＣＳのアプリケーションの場合において、初期ＰＰＰ接続は構成要素８７５とＰＣ　８０５との間にある。簡単のために交換機要素の一部として示されているが、ＮＡＳの機能は別の装置の中で実行することもできる。同様に、簡単のためにローカル・ネットワークやルータなどの他の構成要素も示されていない。

【００６６】

この実施形態においては、上記ＣＣＲＱ、ＣＣＲＰ、ＣＣＣＮのメッセージが新しいＬＡＣとＬＮＳとの間で交換されること以外は、同じハンドオフの手順がＬＡＣ／ＬＮＳペアに対して実行される。本発明の概念に従って、例示としてのハンドオフのメッセージ・フローが図１３に示されている。図１３から観察されるように、トンネル（Ｔｉｄの値によって識別される）および呼（Ｃｉｄの値によって識別される）が、最初に構成要素８７５（１つのＬＡＣを含む）とＬＮＳ９３５との間に確立される。図１３に示されているように、本発明の概念によって既存のＬＡＣが既存のＰＰＰ接続を、構成要素８８０によって表されているような新しいＬＡＣに対して移すことができる。

【００６７】

ここで図１４を参照されたい。図１４は「ハンドオフ機能」の提供において使うための方法の例示としてのフローチャートである。注記されたように、ＶＰＮセッションがＰＣ　８０５と企業ネットワークとの間に構成要素８７５（１つのＬＡＣを含む）を経由して存在していると仮定される。本発明の概念に従って、ＰＣＳ無線ネットワーク９１０は既存の呼状態変数に対して、各無線呼に対するＰＰＰ接続の存在（あるいはその欠如）を示している追加の変数を加え、そしてＰＰＰ接続が存在する場合、ＬＮＳの識別情報、たとえば、そのＬＮＳのＩＰアドレスを含むＰＰＰ接続の情報を加える。

【００６８】

図１４のステップ５０５において、ＰＣＳ無線ネットワーク９１０はハンドオフのための必要性を検出する。というのは、ＰＣ　８０５が構成要素８７５によってサービスされている地理的領域から別の地理的領域、たとえば、構成要素８８０（別のＬＡＣを含む）によってサービスされている領域へ移動したからである。ステップ５１０において、ＰＣＳ無線システムは構成要素８８０に対して差し迫っているハンドオフの通知を提供する。（ハンドオフを検出して実行するために無線システムによって使われる方法はこの技術分野において知られており、本発明の概念とは無関係である。したがって、それらはここでは説明されず、図１２のシグナリング径路９１１によって表されている。）呼状態の情報は、ここではＰＰＰセッションの指示子およびＰＰＰ呼情報を含むので、新しいＬＡＣ（構成要素８８０の）はステップ５１５においてそのＬＮＳを識別する。ステップ５２０において、新しいＬＡＣ（構成要素８８０の）は自分自身とその識別されたＬＮＳ（ここではＬＮＳ　９３５）との間に既存のトンネルが存在するかどうかをチェックして調べる。

【００６９】

トンネルが存在していなかった場合、新しいＬＡＣは先ず最初にステップ５２５において、１つのトンネルを確立する（前に説明されたように）。次に、本発明の概念に従って、新しいＬＡＣはＣｏｎｔｉｎｕｅｄ‐Ｃａｌｌ‐Ｒｅｑｕｅｓｔ（ＣＣＲＱ）メッセージをステップ５３０においてＬＮＳに対して送信する。このＣＣＲＯメッセージはその既存のＰＰＰ接続に関連付けられているユーザの名前、移行された（新しい）ＰＰＰセッションに対して使われるべきＴｉｄおよびＣｉｄの値を含む。

【００７０】

ステップ５３５において、ＬＮＳは受信されたＣＣＲＱメッセージからそのユーザの名前を復元し、そしてこの情報を使って前のＬＡＣのＩＰアドレスを決定する（この復元された情報はそれぞれのユーザ・データグラム・プロトコル（ＵＤＰ）のポート番号も含むことができる）。このステップにおいて、ＬＮＳはＣａｌｌ－Ｄｉｓｃｏｎｎｅｃｔ－Ｎｏ

ｔｉｆｙメッセージ（たとえば、Ｌ２ＴＰ参照）を前のＬＡＣに対して送信し、そしてまた、上記の表４の中に示されているものと似ている接続テーブルの中で、しかし、サービス中のＬＡＣ情報などなしで、そのリモートのユーザに対するこのＰＰＰ接続に関連付けられている既存の呼変数、たとえば、前のトンネルＩＤ、および前の呼ＩＤを識別する。他方、ＬＮＳがＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｒｅｑｕｅｓｔを拒否すべきである場合、新しいＬＡＣは既存のＰＰＰセッションを破棄することができ、そして新しいＰＰＰセッションを起動することができるようにユーザに対して信号を送り返すか、あるいはそのＰＰＰセッションは単純にドロップされる（そのステップは図には示されていない）。

【００７１】

ステップ５４０において、ＬＮＳは適切な受信ウィンドウ・サイズを伴うＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｒｅｐｌｙ（ＣＣＲＰ）メッセージで応答する。そのＣＣＲＰメッセージは現在のＮｒおよびＮｓの値についての情報を含む。ステップ５４５において、ＬＮＳはＴｉｄ、Ｃｉｄ、およびＬＡＣ　ＩＰアドレス・フィールド（ステップ５３５において識別された）を、その既存のＰＰＰ接続に対する新しい呼情報で置き換えることによって、その接続テーブルを更新する。ステップ５５０において、新しいＬＡＣは必要に応じて受信されたＣＣＲＰメッセージからＮｒ、Ｎｓ、および受信ウィンドウ・サイズを更新し、そしてＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｃｏｎｎｅｃｔ（ＣＣＣＮ）メッセージをＬＮＳに対して送信し、それによってハンドオフが完了する。

【００７２】

ＰＰＰプロトコルに対する上記ハンドオフ機能のサポートにおいて、図１５は本発明の原理による上記の新しい制御メッセージ・トランザクションを示している。図１５に示されているように、ＣＣＲＱメッセージが識別されたＬＮＳに対して送信される。代わりに、ハンドオフのプロセスがＬＮＳに関する情報を新しいＬＡＣに対して提供しなかった場合、そのハンドオフ・プロセスは、この分野の技術において知られているように、フォーリンＲａｄｉｕｓサーバからの支援を使ってＬＮＳ情報を新しいＬＡＣがサーチできるように、新しいＬＡＣに対して十分なユーザ情報を提供しなければならない。すなわち、新しいＬＡＣはＲａｄｉｕｓのアクセス／応答メッセージを経由してホームＲａｄｉｕｓサーバからＬＮＳに関する情報を尋ね出す。ＣＣＲＱメッセージに続いて、ＬＮＳはＣｏｎｔｉｎｕｅｄ‐Ｄｉｓｃｏｎｎｅｃｔ－Ｎｏｔｉｆｙメッセージを前のＬＡＣに対して送信する。次に、ＬＮＳはＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｒｅｐｌｙ（ＣＣＲＰ）メッセージで応答する。このメッセージはＬＮＳが維持している現在のＳｒ、Ｓｓの値を含む。最後に、新しいＬＡＣはＣｏｎｔｉｎｕｅｄ‐Ｃａｌｌ　Ｃｏｎｎｅｃｔ（ＣＣＣＮ）メッセージで応答する。

【００７３】

上記のように、ＰＰＰ接続が１つのＮＡＳから別のＮＡＳへ移される。新しく定義されたメッセージのサポートにおいて、追加の呼状態が以下の表５および６に示されているように、それぞれのＮＡＳに対して定義されている。

【表５】

表５－新しいＬＡＣ（またはＮＡＳ）

呼の状態	イベント	アクション	新しい状態
アイドル	ハンドオフの通知	CCRQの送信	CCRP応答の待機
CCRP応答の待機	CCRPを受信する	クリーンアップ	アイドル
CCRP応答の待機	受信CCRPが受け付けられた	CCCNを送信する	確立された

【００７４】
観察できるように、追加の、あるいは新しい、継続される呼に対する新しいＬＡＣ（またはＮＡＳ）に関連付けられたｍＬ２ＴＰに対する呼の状態は、ＣＣＲＰ応答の待機状態である。
【００７５】
ここで図２１を参照すると、ハンドオフの制御メッセージのトランザクションを実行するための、さらにもう１つの他の実施形態が示されている。そのような実施形態においては、新しいサービス中のＬＡＣではなく、ＬＮＳが新しいサービス中のＬＡＣとのハンドオフ制御メッセージ・トランザクションを起動することを理解されたい。すなわち、図１２および図１３へ示されている装置に関して、新しいサービス中のＬＡＣ　８８０がハンドオフ制御メッセージ・トランザクションを起動するのではなく、ＰＣ　８０５がサービス中のＬＡＣ　８７５によってカバーされている領域からサービス中のＬＡＣ　８８０によってカバーされている領域へ移動したことの指示を、ＬＮＳがＰＣＳ　９１０から（無線リンク層を経由して）受信した時、そのトランザクションを起動する。したがって、図２１に示されているように、ＬＮＳがＣＣＲＱメッセージを新しいサービス中のＬＡＣに対して送信し、新しいサービス中のＬＡＣはＣＣＲＰメッセージを返し、そしてＬＮＳがＣＣＣＮメッセージで応答する。各メッセージの中に含まれている情報およびその機能は前に説明されたものと同様であることが分かるはずであり、したがって、ここでは繰り返されない。また、図１９に関して示されている実施形態の場合ように、トンネル確立制御メッセージ・トランザクションはＬＮＳによって起動される可能性もあり、したがって、制御メッセージＳＳＣＲＱ、ＳＣＣＲＰ、およびＳＣＣＣＮはそれぞれハンドオフの制御メッセージＣＣＲＱ、ＣＣＲＰ、およびＣＣＣＮと組み合わされて、同時並行的に送信される可能性がある。
【００７６】
ここで図２２および図２３を参照すると、Ｒａｄｉｕｓサーバを採用することによって、本発明に従って、ハンドオフの制御メッセージ・トランザクションを実行するためのそれぞれの他の実施形態が示されている。特に、図２２は図８および図９に示されている装置に類似した装置を示し、一方、図２３は図１２および図１３に示されている装置に類似した装置を示している。前に述べられたように、Ｒａｄｉｕｓサーバは、この分野の技術において知られているように、通信機能を実行するために必要な特定の情報を識別および／または確認することを支援するために、通信径路の中で採用されている他のサーバ（たとえば、サービス中のＬＡＣアンカーＬＡＣ、ＬＮＳ）によって使われる可能性がある。たとえば、説明されたように、Ｒａｄｉｕｓサーバはサービス中のＬＡＣに対して動作できるように結合されており、特定のユーザを特定のアンカーＬＡＣと関連付けるデータベースを含むことができる。このようにして、サービス中のＬＡＣは自分のＲａｄｉｕｓサーバと相談してそのような情報を求める。同様に、アンカーＬＡＣはそれに対して動作可能なように結合されているＲａｄｉｕｓサーバ（ホーム）と相談して、ユーザおよびユーザが関連付けられているＮＡＳに関する同様な情報を知ることができる。
【００７７】
しかし、本発明によると、Ｒａｄｉｕｓサーバはそれらの間でのハンドオフの制御メッセージ・トランザクションを実行するためにも利用されるのが有利である可能性がある。すなわち、サービス中のＬＡＣとアンカーＬＡＣまたはサービス中のＬＡＣとＬＮＳがそのトランザクションを実行するのではなく、それに対して動作可能なように結合され、互いに結合されているそれぞれのＲａｄｉｕｓサーバがこれらの制御メッセージを転送するために使われる。そのような場合、サービス中のＬＡＣ、アンカーＬＡＣ、およびＬＮＳは単にこれらのメッセージによって生じた追加の処理を実行するだけである。
【００７８】
図２２はアンカーＬＡＣに関連して、前のサービス中のＬＡＣ　８１５から新しいサービス中のＬＡＣ　８２０への、ＰＰＰ接続のハンドオフの場合におけるそのような装置を示している。新しいサービス中のＬＡＣ８２０に関連付けられているＲａｄｉｕｓサーバ８

２２は、アンカーＬＡＣに関連付けられているＲａｄｉｕｓサーバ８２４と通信する。したがって、本発明によると、ハンドオフの通知がＰＣＳ　８１０（図８）から受信されると、Ｒａｄｉｕｓサーバ８２２および８２４は制御メッセージ、ＣＣＲＱ、ＣＣＲＰ、およびＣＣＣＮをそれらの間で直接転送する。本発明によると、いずれのＲａｄｉｕｓサーバもその転送を起動することができる。

【００７９】

同様に、図２３はＬＮＳ　９３５に関して、前のサービス中のＬＡＣ　８７５から新しいサービス中のＬＡＣ　８８０への、ＰＰＰ接続のアプリケーションの場合におけるそのような装置を示している。新しいサービス中のＬＡＣ　８８０に関連付けられているＲａｄｉｕｓサーバ９２２が、ＬＮＳに関係付けられているＲａｄｉｕｓサーバ９２４と通信している。したがって、本発明によると、ハンドオフの通知がＰＣＳ　９１０（図１２）から受信されると、Ｒａｄｉｕｓサーバ９２２および９２４は制御メッセージ、ＣＣＲＱ、ＣＣＲＰ、およびＣＣＣＮをそれらの間で直接転送する。本発明によると、いずれのＲａｄｉｕｓサーバもその転送を起動することができる。

【００８０】

＜Ｌ２ＴＰに対するペイロード・メッセージの概要および混雑制御＞

ｍＬ２ＴＰに対するペイロード・メッセージに関して、サービス中のＬＡＣおよびＬＮＳはＬ２ＴＰの手順に従う。アンカーＬＡＣはそのペイロード・パケットに対するＴｉｄおよびＣｉｄをスワップする。また、アンカーＬＡＣはサービス中のＬＡＣから送られた（Ｎｒ、Ｎｓ）の値を監視する。（サービス中のＬＡＣとアンカーＬＡＣとの間でパケットの消失があり得るので、アンカーＬＡＣにおけるＳｒおよびＳｓの値は両方とも、サービス中のＬＡＣにおいて維持されているそれらの値の後に遅れる可能性があることが予期されることに注意されたい。）アンカーＬＡＣはいずれの方向においてもペイロード・パケットの（Ｎｒ、Ｎｓ）を変更しない。アンカーＬＡＣがそれ自身のＳｒ、Ｓｓの値を使うのは、アンカーＬＡＣが新しいサービス中のＬＡＣからＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｒｅｑｕｅｓｔメッセージを受信した時だけである。

【００８１】

混雑制御に関して、ウィンドウ・サイズをいつ受信するか、Ｎｒ／Ｎｓをいつ受信するか、そしてＡＣＫをいつ送信するかについてのＬ２ＴＰの条件がｍＬ２ＴＰに適用される。さらに、ｍＬ２ＴＰはサービス中のＬＡＣおよびアンカーＬＡＣに対する以下の追加の条件も有する。

【００８２】

アンカーＬＡＣはサービス中のＬＡＣから送信された（Ｎｒ、Ｎｓ）の値を監視する必要がある。アンカーＬＡＣはサービス中のＬＡＣから受信したＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｃｏｎｎｅｃｔメッセージに応答する時、自分が維持する（Ｓｒ、Ｓｓ）の値をＣｏｎｔｉｎｕｅｄ－Ｃａｌｌ－Ｒｅｐｌｙメッセージの中に含める必要がある。サービス中のＬＡＣとアンカーＬＡＣとの間のネットワークは消失の可能性が大きいので、アンカーＬＡＣによって維持されているＳｒの値がサービス中のＬＡＣの背後に遅れている可能性がある。

【００８３】

本発明のマルチホップ・ポイント・ツー・ポイント・プロトコルによって影響される、ｍＬ２ＴＰに関連付けられたペイロード処理規則について以下に詳細に説明される。前に説明されたように、マルチホップのシナリオの場合、アンカーＬＡＣがペイロード・パケットに対するＴｉｄおよびＣｉｄの値のスワッピングを実行する。さらに、アンカーＬＡＣはｎＬ２ＴＰのペイロード・パケットに対して四組の状態変数（$Ｓｒ^{S}$　、$Ｓｓ^{S}$　、$Ｓｒ^{L}$　、$Ｓｓ^{L}$　）を維持する。アンカーＬＡＣはサービス中のＬＡＣから送られた（Ｎｒ、Ｎｓ）の値を（$Ｓｒ^{S}$　、$Ｓｓ^{S}$　）の中に格納し、そしてＬＮＳからの（Ｎｒ、Ｎｓ）の値を（$Ｓｒ^{L}$　、$Ｓｓ^{L}$　）の中に格納する。

【００８４】

サービス中のＬＡＣとアンカーＬＡＣとの間でパケットの消失および／または遅延があり

得るので、Sr^S ＜ＳｒおよびSs^S ＜Ｓｓであることが予期される。ここでＳｒおよびＳｓはサービス中のＬＡＣにおいて維持されている状態変数である。同様に、パケットの消失および／または遅延がアンカーＬＡＣとＬＮＳとの間にもあるので、Sr^L ＜ＳｒそしてＳｓ^L ＜Ｓｓであることが予期される。ここで、ＳｒおよびＳｓはＬＮＳにおいて維持されている状態変数である。アンカーＬＡＣはいずれの方向においてもペイロード・パケットの（Ｎｒ、Ｎｓ）の値を変更しないことを理解されたい。本発明による状態変数の監視がどのように行われるかについての３つの例が以下に示される。

【００８５】

第１の監視の例は１ホップの装置から２ホップの装置へ通信のシナリオが変わる場合に関するものである。１ホップの装置は、たとえば、ＰＣ、アンカーＬＡＣおよびＬＮＳの間の通信リンクを含むことを理解されたい。２ホップの装置は、たとえば、ＰＣ、サービス中のＬＡＣ、アンカーＬＡＣ、およびＬＮＳの間の通信リンクを含む。アンカーＬＡＣが以前に１つのＰＰＰセッションに対して二組の状態変数を維持し、そしてＣＣＲＱメッセージを受け取った場合、アンカーＬＡＣは自分が１ホップのセッションから２ホップのセッションへ変わる必要があることを知る。アンカーＬＡＣは先ず最初に自分の現在の二組の状態変数（Ｓｒ、Ｓｓ）を使ってＣＣＲＰメッセージの中でＮｒ＝Ｓｒ、そしてＭｓ＝Ｓｓに設定する。次に、アンカーＬＡＣはその状態変数を四組に変更し、Sr^S ＝Ｓｒ、Ss^S ＝Ｓｓ、Sr^L ＝ｘ、そしてSr^L ＝ｘに設定する。アンカーＬＡＣがハンドオーバの後で第１のパケットをＬＮＳから受信した時、それはそのSs^L およびSr^L の変数を観察された（Ｎｒ、Ｎｓ）の値で更新する。たとえば、前のＬＡＣがＳｓ＝１３およびＳｒ＝６を有し、そしてＬＮＳがＳｓ＝７そしてＳｒ＝１０を有していると仮定する。現在はアンカーＬＡＣである前のＬＡＣがＣＣＲＰメッセージの中でＮｒ＝ＳｒそしてＮｓ＝Ｓｓに設定する。ハンドオーバの後、新しいサービス中のＬＡＣはＳｓ＝１３そしてＳｒ＝６を有し、ＬＮＳはＳｓ＝７＋そしてＳｒ＝１０＋を有し、そしてアンカーＬＡＣ（前のＬＡＣ）はSs^S ＝１３、Sr^S ＝６、Ss^L ＝７＋、そしてSr^L ＝１０＋を有する。ある種の値におけるプラスの記号（＋）はハンドオフのプロセスの間にシーケンス番号が更新されているかどうかに依存して、その値が大きくなり得ることを意味する。

【００８６】

第２の監視の例は通信のシナリオが２ホップの装置から１ホップの装置へ変わる場合に関する例である。ふたたび、１ホップの装置は、たとえば、ＰＣ、アンカーＬＡＣ、およびＬＮＳの間の通信リンクを含み、一方、２ホップの装置は、たとえば、ＰＣ、サービス中のＬＡＣ、アンカーＬＡＣ、およびＬＮＳの間の通信リンクを含むことを理解されたい。２ホップのＰＰＰセッションが１ホップのセッションに変えられること（たとえば、ｍＬ２ＴＰのＣＣＲＱメッセージではなく、リンク層のハンドオーバ・メッセージを受信して）の指示を受信した場合、アンカーＬＡＣは四組の状態変数を二組の状態変数に変換し、Ｓｓ＝Ss^S 、そして$Sr=Ss^L$ に設定する。たとえば、新しいサービス中のＬＡＣがＳｓ＝１３、そしてＳｒ＝５を有し、ＬＮＳがＳｓ＝７、そしてＳｒ＝１０を有し、そしてアンカーＬＡＣがSs^S ＝１２、Sr^S ＝４、Ss^L ＝６、そしてSr^L ＝９を有していると仮定する。その時、２ホップの装置から１ホップの装置への変換後、アンカーＬＡＣはＳｓ＝１２、そしてＳｒ＝６を有し、そしてＬＮＳはＳｓ＝７＋、そしてＳｒ＝１０＋を有する。

【００８７】

第３の監視例は通信のシナリオが、たとえば、図９に示されているように、２ホップの装置から別の２ホップの装置へ変わる場合に関する例である。アンカーＬＡＣがＣＣＲＱメッセージを受信し、そしてＰＰＰセッションが既に２ホップであった場合、アンカーＬＡＣはサービス中のＬＡＣの変化があることを知る。その時、アンカーＬＡＣはＣＣＲＰメッセージの中で$Nr=Ss^L$ および$Ns=Ss^S$ に設定する。また、アンカーＬＡＣはSr^S をSr^S ＝Ss^L に更新する。たとえば、前のサービス中のＬＡＣがＳｓ＝１８、そしてＳｒ＝５を有し、ＬＮＳがＳｓ＝７、そしてＳｒ＝１０を有し、そしてア

ンカーＬＡＣＬＡＣがＳｓ＝１２、$Ｓｒ^{S}$ ＝４、$Ｓｓ^{L}$ ＝６、そして$Ｓｒ^{L}$ ＝９を有していると仮定する。その時、アンカーＬＡＣは新しいサービス中のＬＡＣに対して送られるＣＣＲＰメッセージの中で、Ｎｓ＝$Ｓｓ^{S}$ 、そしてＮｒ＝$Ｓｓ^{L}$ に設定する。そのハンドオーバの後、新しいサービス中のＬＡＣはＳｓ＝１２、そしてＳｒ＝６を有し、ＬＮＳはＳｓ＝７＋、そしてＳｒ＝１０＋を有し、そしてアンカーＬＡＣは$Ｓｓ^{S}$ ＝１２、$Ｓｒ^{S}$ ＝４、$Ｓｓ^{L}$ ＝６＋、そして$Ｓｒ^{L}$ ＝９＋を有する。

【００８８】

さらに、サービス中のＬＡＣはこの分野の技術において呼ばれているように、単純な受信機ではなく、完全な受信機を実装している。この条件は新しいサービス中のＬＡＣがＰＰＰセッションの寿命期間の間にサービス中のＬＡＣの変化があった時に上部層に対してシーケンスから外れた、あるいは複製のパケットを渡すことを禁止する。

【００８９】

図１６を簡単に参照すると、代表的なＮＡＳの高レベルのブロック図が示されている。ＮＡＳはストアード・プログラムの制御ベースのプロセッサ・アーキテクチャであり、プロセッサ６５０、プログラム命令およびデータを格納するためのメモリ６６０（たとえば、上記接続テーブルなど）および径路６６６によって表されているような１つまたはそれ以上の通信施設に対して結合するための通信インターフェース６６５を含む。

【００９０】

上記は本発明の原理を単に示しているだけであり、そしてこの分野の技術に熟達した人であれば、ここには明示的には記述されていないが、本発明の原理を具体化し、そしてその精神および範囲内にある数多くの代替装置を工夫することができることを理解されたい。たとえば、本発明の概念は入接続呼に対するマルチホップ・トンネルの確立を、サービス中のＮＡＳが起動する場合において記述されたが、本発明の概念は、たとえば、出接続呼に対してマルチホップ・シーケンスの確立を、ＬＮＳが起動するように等しく適用できる。そのような変更は直接的であり、図１７－図１８によってここで例示されているように、説明されない。

【図面の簡単な説明】

【図１】本発明の原理による通信システムを示す図である。

【図２】図１の通信システムにおいて使うための例示としての方法のフローチャートを示す図である。

【図３】図１の通信システムにおいて使うための例示としての方法のフローチャートを示す図である。

【図４】例示としてのマルチホップ・メッセージ・フローを示す図である。

【図５】例示としての制御メッセージ・トランザクションを示す図である。

【図６】例示としての制御メッセージ・トランザクションを示す図である。

【図７】例示としての制御メッセージ・トランザクションを示す図である。

【図８】本発明の原理による通信システムのもう１つの実施形態を示す図である。

【図９】例示としてのハンドオフ・メッセージ・フローを示す図である。

【図１０】図８の通信システムにおいて使うための例示としての方法のフローチャートを示す図である。

【図１１】例示としての制御メッセージ・トランザクションを示す図である。

【図１２】本発明の原理による通信システムの他の実施形態を示す図である。

【図１３】例示としてのハンドオフ・メッセージ・フローを示す図である。

【図１４】図１２の通信システムにおいて使うための例示としての方法のフローチャートを示す図である。

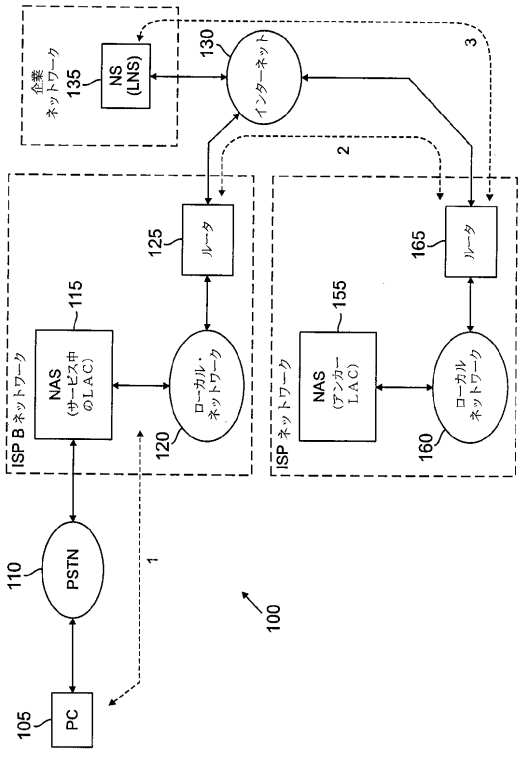
【図１５】例示としての制御メッセージ・トランザクションを示す図である。

【図１６】例示としてのネットワーク・アクセス・サーバの高レベルのブロック図を示す図である。

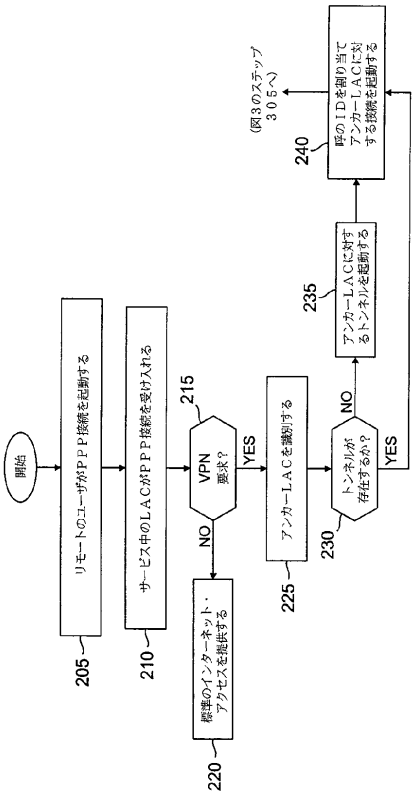
【図１７】出接続呼に対する例示としての制御メッセージ・トランザクションを示す図である。

【図１８】出接続呼に対する例示としての制御メッセージ・トランザクションを示す図である。
【図１９】他の例示としての制御メッセージ・トランザクションを示す図である。
【図２０】さらに他の例示としての制御メッセージ・トランザクションを示す図である。
【図２１】さらに他の例示としての制御メッセージ・トランザクションを示す図である。
【図２２】制御メッセージ・トランザクションを実行するためのＲａｄｉｕｓサーバを採用している実施形態を示す図である。
【図２３】制御メッセージ・トランザクションを実行するためにＲａｄｉｕｓサーバを採用している他の実施形態を示す図である。

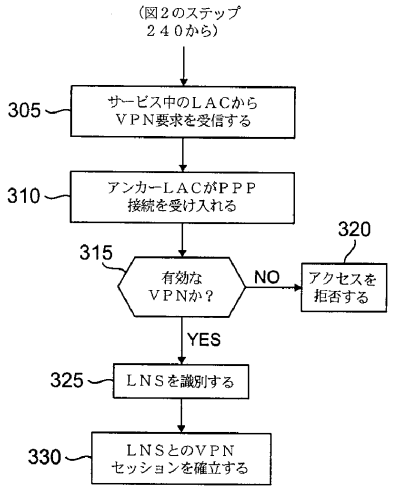
【図１】



【図２】



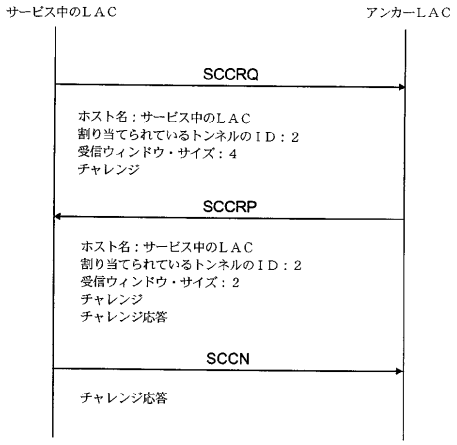
【図３】


（図２のステップ
２４０から）
305
サービス中のＬＡＣから
ＶＰＮ要求を受信する
310
アンカーＬＡＣがＰＰＰ
接続を受け入れる
315
有効な
ＶＰＮか？
NO
320
アクセスを
拒否する
YES
325
ＬＮＳを識別する
330
ＬＮＳとのＶＰＮ
セッションを確立する

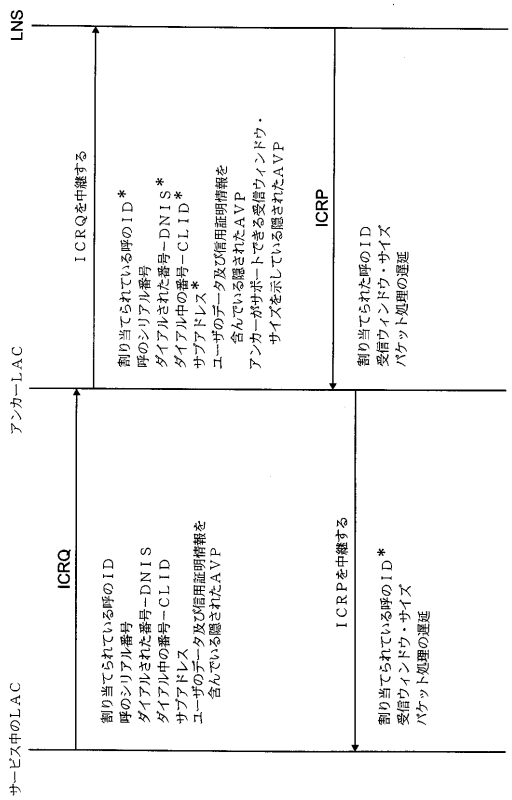
【図４】


サービス中
のＬＡＣ
TID = 2
CID = 5
アンカー
LAC
TID = 1
CID = 3
LNS

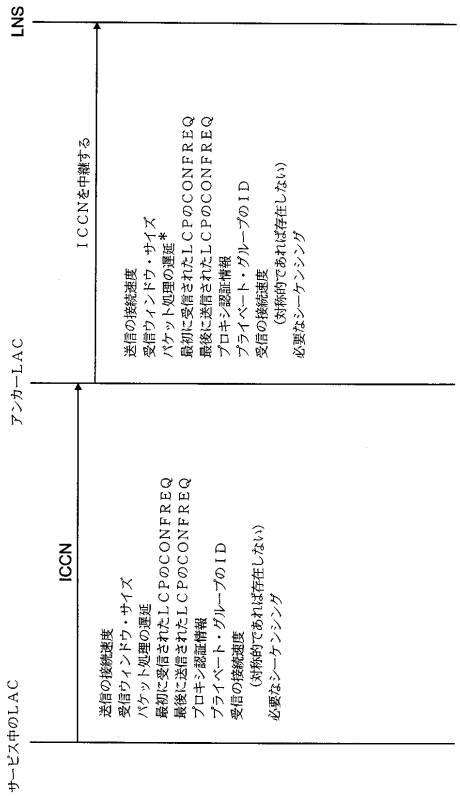
【図５】


サービス中のＬＡＣ
アンカーＬＡＣ
SCCRQ
ホスト名：サービス中のＬＡＣ
割り当てられているトンネルのＩＤ：２
受信ウィンドウ・サイズ：４
チャレンジ
SCCRP
ホスト名：サービス中のＬＡＣ
割り当てられているトンネルのＩＤ：２
受信ウィンドウ・サイズ：２
チャレンジ
チャレンジ応答
SCCN
チャレンジ応答

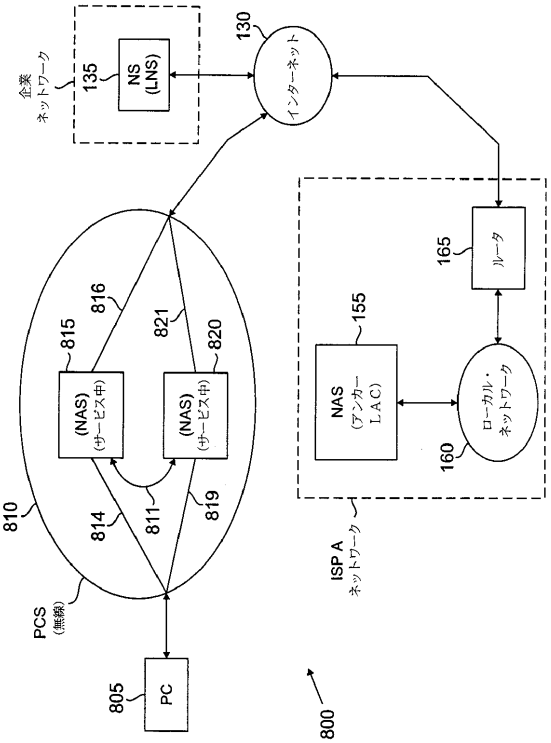
【図６】


LNS
アンカーＬＡＣ
サービス中のＬＡＣ
ＩＣＲＱを中継する
割り当てられている呼のＩＤ*
呼のシリアル番号
ダイアルされた番号－ＤＮＩＳ*
ダイアル中の番号－ＣＬＩＤ*
サブアドレス*
ユーザのデータ及び信用証明情報を
含んでいる隠されたＡＶＰ
アンカーがサポートできる受信ウィンドウ・
サイズを示している隠されたＡＶＰ
ICRP
割り当てられた呼のＩＤ
受信ウィンドウ・サイズ
パケット処理の遅延
ICRQ
割り当てられている呼のＩＤ
呼のシリアル番号
ダイアルされた番号－ＤＮＩＳ
ダイアル中の番号－ＣＬＩＤ
サブアドレス
ユーザのデータ及び信用証明情報を
含んでいる隠されたＡＶＰ
ＩＣＲＰを中継する
割り当てられている呼のＩＤ*
受信ウィンドウ・サイズ
パケット処理の遅延

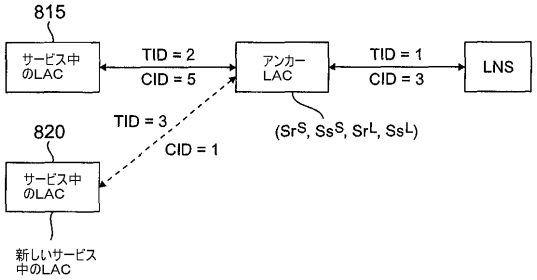
【図７】


LNS
アンカーＬＡＣ
サービス中のＬＡＣ
ＩＣＣＮを中継する
送信の接続速度
受信ウィンドウ・サイズ
パケット処理の遅延*
最初に受信されたＬＣＰのＣＯＮＦＲＥＱ
最後に送信されたＬＣＰのＣＯＮＦＲＥＱ
プロキシ認証情報
プライベート・グループのＩＤ
受信の接続速度
（対称的であれば存在しない）
必要なシーケンシング
ICCN
送信の接続速度
受信ウィンドウ・サイズ
パケット処理の遅延
最初に受信されたＬＣＰのＣＯＮＦＲＥＱ
最後に送信されたＬＣＰのＣＯＮＦＲＥＱ
プロキシ認証情報
プライベート・グループのＩＤ
受信の接続速度
（対称的であれば存在しない）
必要なシーケンシング

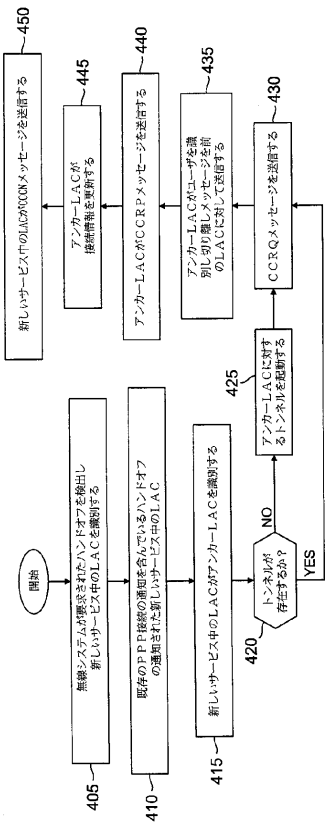
【図８】


企業ネットワーク
135
NS (LNS)
130
インターネット
165
ルータ
155
NAS (アンカーLAC)
160
ローカル・ネットワーク
ISP A ネットワーク
815
816
821
820
(NAS) (サービス中)
(NAS) (サービス中)
810
814
811
819
PCS (無線)
805
PC
800

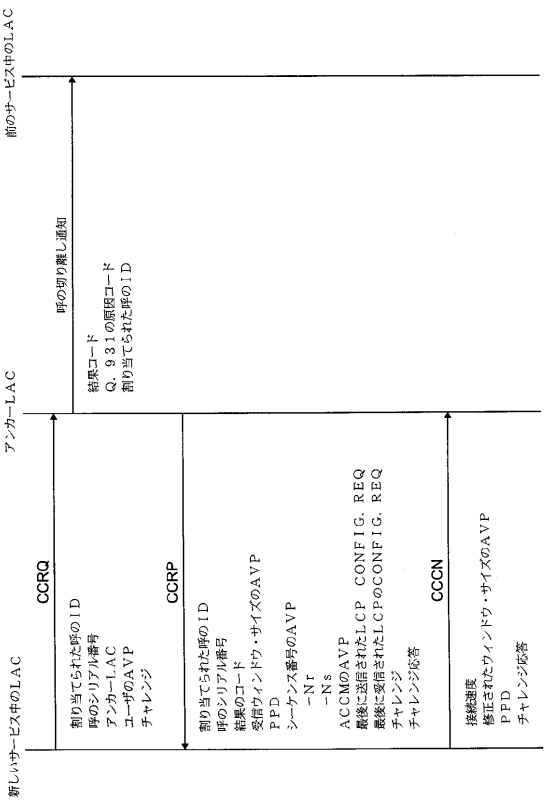
【図９】


815
サービス中のLAC
TID = 2
CID = 5
アンカーLAC
TID = 1
CID = 3
LNS
TID = 3
CID = 1
(SrS, SsS, SrL, SsL)
820
サービス中のLAC
新しいサービス中のLAC

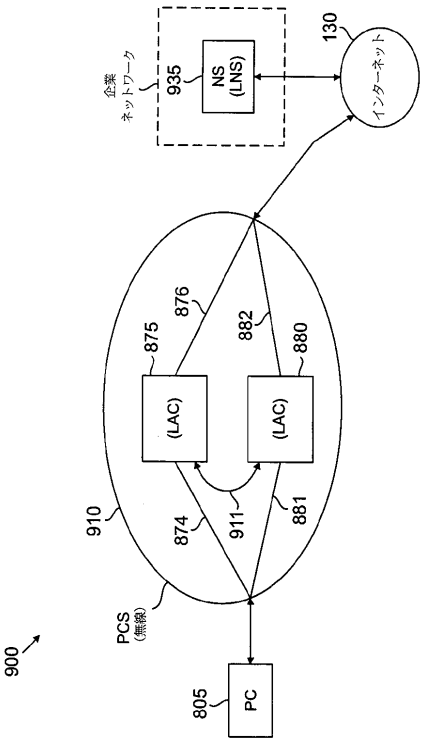
【図１０】


開始
無線システムが要求されたハンドオフを検出し新しいサービス中のLACを識別する
405
既存のPPP接続の通知を含んでいるハンドオフの通知された新しいサービス中のLAC
410
新しいサービス中のLACがアンカーLACを識別する
415
トンネルが存在するか？
420
NO
YES
アンカーLACに対するトンネルを起動する
425
CCRQメッセージを送信する
430
アンカーLACがユーザを識別し切り離しメッセージを前のLACに対して送信する
435
アンカーLACがCCRPメッセージを送信する
440
アンカーLACが接続情報を更新する
445
新しいサービス中のLACがCCOMメッセージを送信する
450

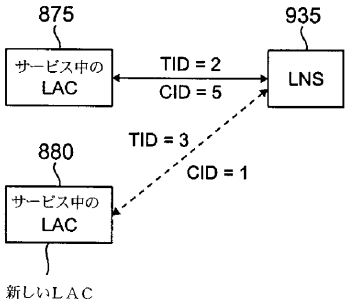
【図１１】


新しいサービス中のLAC
アンカーLAC
前のサービス中のLAC
CCRQ
割り当てられた呼のID
呼のシリアル番号
アンカーLAC
ユーザのAVP
チャレンジ
呼の切り離し通知
結果コード
Q.931の原因コード
割り当てられた呼のID
CCRP
割り当てられた呼のID
呼のシリアル番号
結果のコード
受信ウィンドウ・サイズのAVP
PPD
シーケンス番号のAVP
-Nr
-Ns
ACCMのAVP
最後に送信されたLCP CONFIG. REQ
最後に受信されたLCPのCONFIG. REQ
チャレンジ
チャレンジ応答
CCCN
接続速度
修正されたウィンドウ・サイズのAVP
PPD
チャレンジ応答

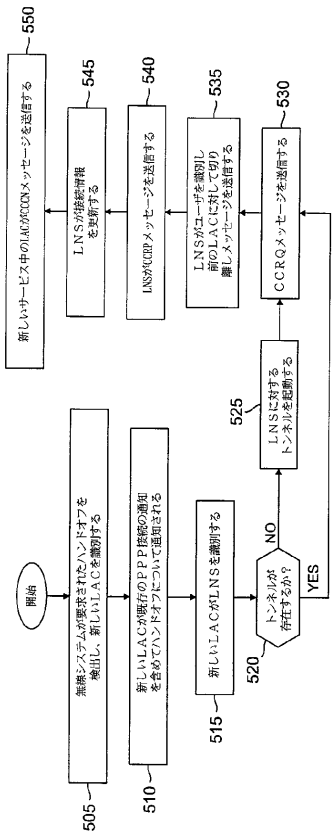
【図１２】



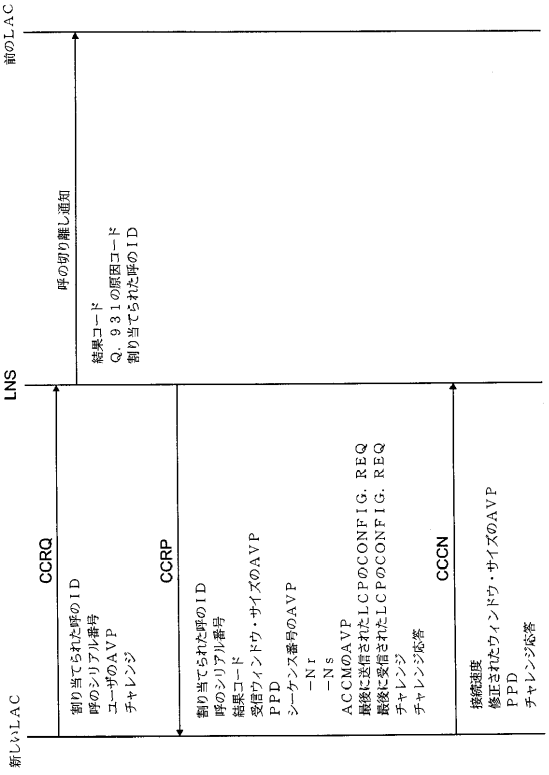
【図１３】



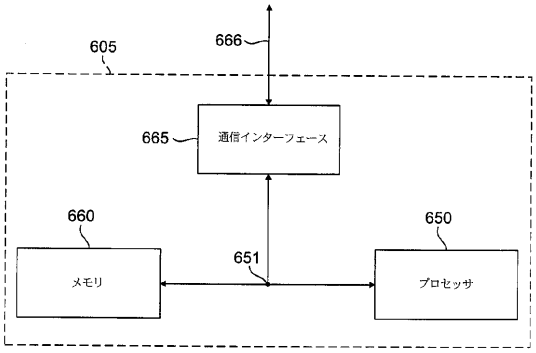
【図１４】



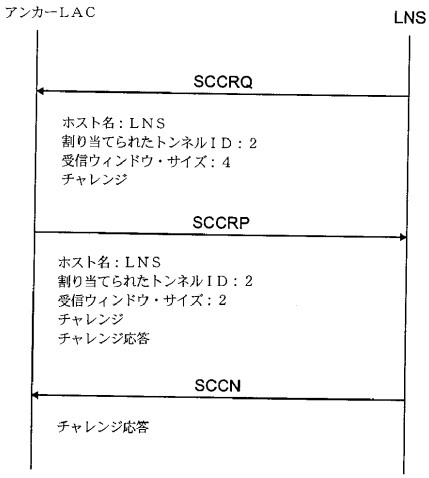
【図１５】



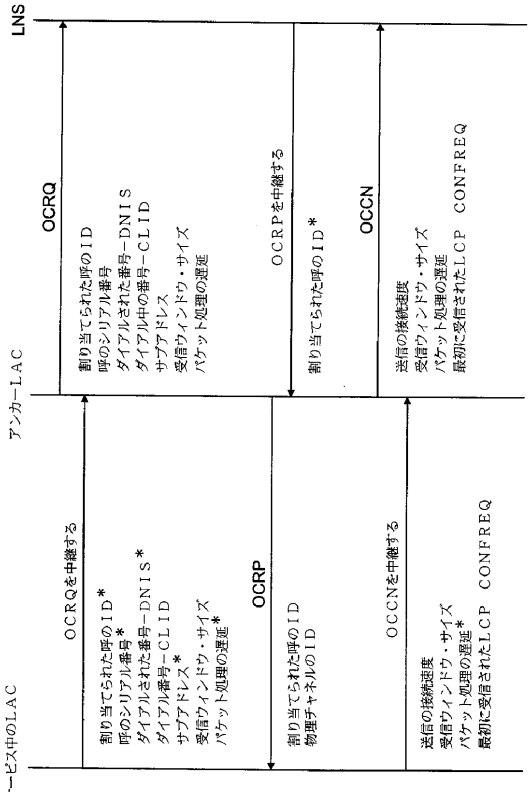
【図１６】



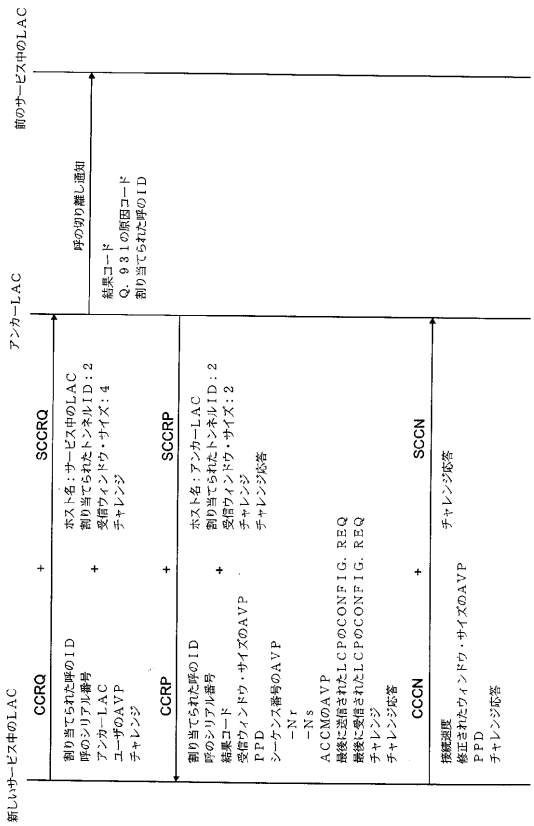
【図１７】



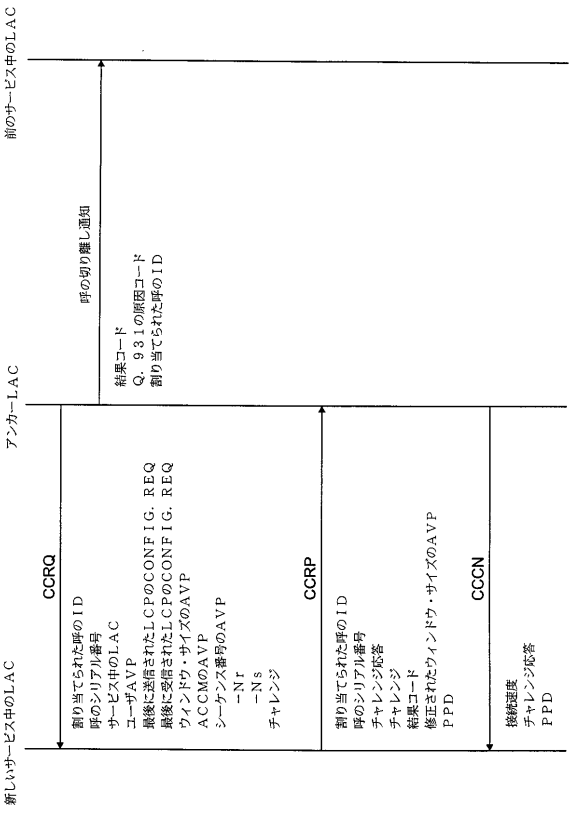
【図１８】



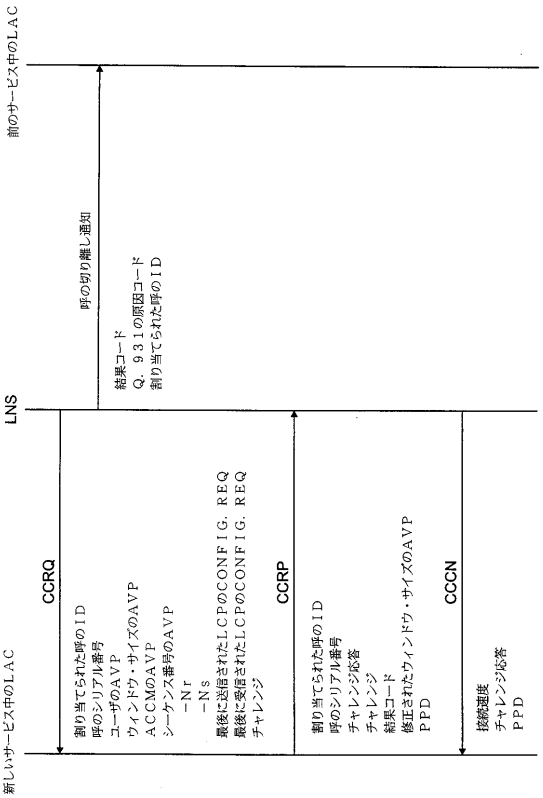
【図１９】



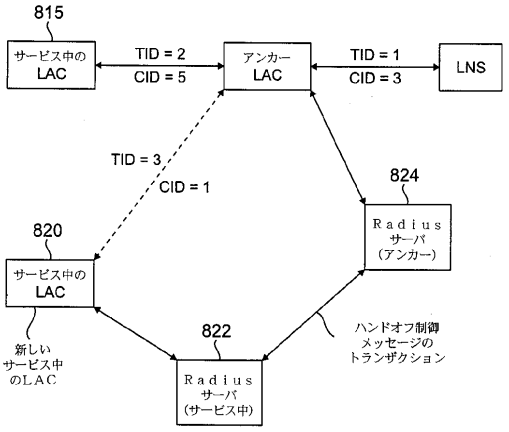
【図２０】



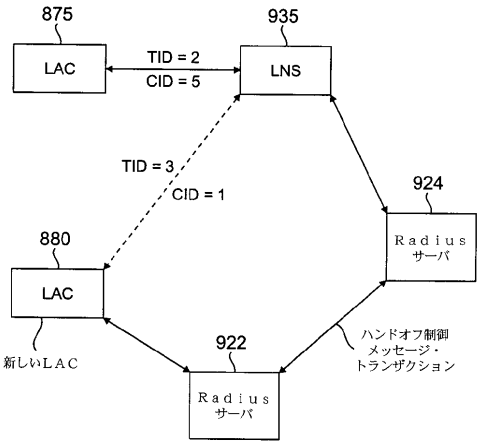
【図２１】


前のサービス中のLAC
呼の切り離し通知
結果コード
Q.931の原因コード
割り当てられた呼のID
LNS
CCRQ
割り当てられた呼のID
呼のシリアル番号
ユーザのAVP
ウィンドウ・サイズのAVP
ACCMのAVP
シーケンス番号のAVP
－Nr
－Ns
最後に送信されたLCPのCONFIG. REQ
最後に受信されたLCPのCONFIG. REQ
チャレンジ
CCRP
割り当てられた呼のID
呼のシリアル番号
チャレンジ応答
チャレンジ
結果コード
修正されたウィンドウ・サイズのAVP
PPD
CCCN
接続速度
チャレンジ応答
PPD
新しいサービス中のLAC

【図２２】


815
サービス中の LAC
TID = 2
CID = 5
アンカー LAC
TID = 1
CID = 3
LNS
TID = 3
CID = 1
824
Radius サーバ (アンカー)
820
サービス中の LAC
新しい サービス中 のLAC
822
Radius サーバ (サービス中)
ハンドオフ制御 メッセージの トランザクション

【図２３】


875
LAC
TID = 2
CID = 5
935
LNS
TID = 3
CID = 1
924
Radius サーバ
880
LAC
新しいLAC
922
Radius サーバ
ハンドオフ制御 メッセージ・ トランザクション

フロントページの続き

(74)代理人 100101498
弁理士 越智 隆夫
(74)代理人 100096688
弁理士 本宮 照久
(74)代理人 100104352
弁理士 朝日 伸光
(72)発明者 モーイ チョー チュー
アメリカ合衆国 ０７７２４ ニュージャーシィ，イートンタウン，イートンクレスト ドライヴ １８４ビー
(72)発明者 ギリシュ ライ
アメリカ合衆国 ６０１０３ イリノイズ，バートレット，レディ スミス ロード ５２３

審査官 石井 研一

(56)参考文献 特開平０８－０４６６４３（ＪＰ，Ａ）
特開平０７－１７０２８６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04L 12/56
H04L 12/66
H04Q 7/22
H04Q 7/28