

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2006-19934
(P2006-19934A)

(43) 公開日 平成18年1月19日(2006.1.19)

(51) Int. Cl. F I テーマコード (参考)
H O 4 L 12/56 (2006.01) H O 4 L 12/56 A 5 K O 3 O

審査請求 未請求 請求項の数 7 O L (全 17 頁)

(21) 出願番号	特願2004-194376 (P2004-194376)	(71) 出願人	000208891 K D D I 株式会社 東京都新宿区西新宿二丁目 3 番 2 号
(22) 出願日	平成16年6月30日 (2004. 6. 30)	(74) 代理人	100084870 弁理士 田中 香樹
		(74) 代理人	100079289 弁理士 平木 道人
		(74) 代理人	100119688 弁理士 田邊 壽二
		(72) 発明者	千葉 恒彦 埼玉県上福岡市大原二丁目 1 番 1 5 号 株 式会社K D D I 研究所内
		(72) 発明者	新保 宏之 埼玉県上福岡市大原二丁目 1 番 1 5 号 株 式会社K D D I 研究所内

最終頁に続く

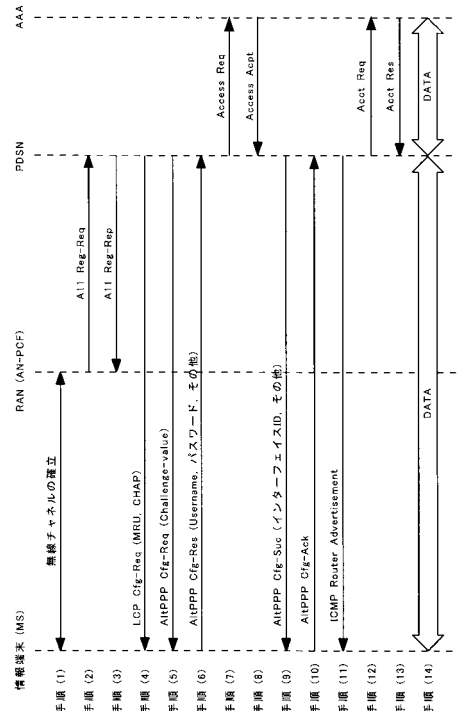
(54) 【発明の名称】 パケット交換網の呼設定方法

(57) 【要約】

【課題】 PPP非標準のメッセージを用いて手順やデータ量を削減することにより呼設定に要する時間を短縮し、さらには端末あるいはPDSNが非標準メッセージに未対応であってもPPP標準の手順で呼設定手順を継続可能とする。

【解決手段】 情報端末とPDSNとの間に無線リンクを確立する手順と、PDSNから情報端末へPPP標準のLCP Cfg-Requestメッセージを送信する手順と、PDSNから情報端末へPPP非標準のAltPPP Cfg-Requestメッセージを送信する手順と、情報端末が、非標準メッセージに対応していればAltPPP Cfg-Requestメッセージに応答して非標準のAltPPP Cfg-Responseを返信し、非標準メッセージに未対応であればLCP Cfg-Requestメッセージに応答して標準のLCP Cfg--Responseを返信する手順と、PDSNが、前記標準または非標準のCfg--Responseメッセージに基づいて情報端末の認証を行う手順とを含む。

【選択図】 図 1



【特許請求の範囲】

【請求項 1】

無線情報端末と、当該無線情報端末との間に無線リンクを確立する無線アクセスネットワークおよび当該無線アクセスネットワークを広域ネットワークに接続するPDSN(パケットデータ交換ノード)を含むネットワークシステムとから構成されるネットワークにおいて、前記情報端末とPDSNとの間にPPPコネクションを確立するための呼設定方法において

前記情報端末とPDSNとの間に無線リンクを確立する手順と、
 前記PDSNから情報端末へ標準の設定要求メッセージを送信する手順と、
 前記PDSNから情報端末へ非標準の設定要求メッセージを送信する手順と、
 前記情報端末が、前記標準および非標準の設定要求メッセージのいずれか一方に応答して、それぞれ標準または非標準の設定応答メッセージを送信する手順と、
 前記PDSNが、前記標準または非標準の設定応答メッセージの内容に基づいて情報端末の認証を行う手順とを含み、
 前記情報端末は、前記非標準メッセージに対応しているか否かに応じて、前記非標準の設定要求メッセージに対して優先的に応答することを特徴とするパケット交換網の呼設定方法。

10

【請求項 2】

前記非標準メッセージに対応した情報端末が、
 前記標準の設定要求メッセージを受信した後、当該メッセージへ応答せずに所定時間だけ待機する手順と、
 前記待機時間内に非標準の設定要求メッセージを受信すると、当該非標準の設定要求メッセージに
 応答して非標準の設定応答メッセージを送信する手順と、
 前記待機時間内に非標準の設定要求メッセージを受信できないと、前記標準の設定要求
 メッセージに
 応答して標準の設定応答メッセージを送信する手順とを含むことを特徴とする請求項 1 に記載の
 パケット交換網の呼設定方法。

20

【請求項 3】

前記非標準のメッセージは、複数の標準メッセージに分散登録される複数の設定要求が一括登録されるオプションフィールドを含み、前記複数の設定要求が前記非標準のメッセージで一括送信されることを特徴とする請求項 1 または 2 に記載の
 パケット交換網の呼設定方法。

30

【請求項 4】

前記非標準のメッセージは、そのメッセージ種別およびオプションデータの代表値が登録されるオプションフィールドを含むことを特徴とする請求項 1 または 2 に記載の
 パケット交換網の呼設定方法。

【請求項 5】

前記オプションフィールドが複数ビットの領域を有し、各メッセージ種別およびそのオプションデータの代表値が所定の 1 ビットに登録されることを特徴とする請求項 4 に記載の
 パケット交換網の呼設定方法。

【請求項 6】

前記非標準の設定応答メッセージが、ドメイン代表値フィールド、サブドメイン代表値フィールド、ユーザ名構築ルールフィールドおよびPAP/CHAP拡張フィールドを含み、
 前記PDSNが、前記ドメイン代表値フィールド、サブドメイン代表値フィールド、ユーザ名構築ルールフィールドおよびPAP/CHAP拡張フィールドに登録された情報に基づいてユーザ名を構築する手順をさらに含み、
 前記ユーザ名を構築する手順が、
 前記ユーザ名構築ルールが第 1 タイプのときに、受信メッセージのPAP/CHAP拡張フィールドに登録されているユーザ名を認証用ユーザ名とする手順と、
 前記ユーザ名構築ルールが第 2 タイプのときに、情報端末のIMSI、前記ドメイン代表値と関連付けられたドメイン名、および前記サブドメイン代表値と関連付けられたサブドメ

40

50

イン名とに基づいて認証用ユーザ名を構築する手順とを含むことを特徴とする請求項 1 ないし 5 のいずれかに記載の packets 交換網の呼設定方法。

【請求項 7】

前記ユーザ名を構築する手順がさらに、

前記ユーザ名構築ルールが第 3 タイプのときに、情報端末の IMSI を認証用ユーザ名とする手順を含むことを特徴とする請求項 6 に記載の packets 交換網の呼設定方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、PPP (Point to Point Protocol) に準拠した手順で packets 交換網の呼設定を短時間で行う呼設定方法に関する。 10

【背景技術】

【0002】

インターネットに接続する際のトランスポートレイヤプロトコルとして TCP (Transmission Control Protocol) が普及している。また、端末が公衆網を経由してインターネットへ接続する場合には、TCP/IP (TCP/Internet Protocol) の下位レイヤであるデータリンクレイヤプロトコルとして、PPP (Point to Point Protocol) が一般的に使用されている。また、第 3 世代携帯電話の標準方式 cdma2000 においても、データ通信の呼設定に PPP が採用されている。

【0003】

図 18 に示したように、3GPP2 (3rd Generation Partnership Project 2) で標準化が進められている次世代移動体通信システムの cdma2000 では、IP データ通信を実現するために、ネットワーク側には基地局、基地局コントローラ、PCF (Packet Control Function)、PDSN (Packet Data Serving Node: packets データ交換ノード) および AAA (Authentication, Authorization and Accounting) サーバが接続される。ユーザ側の無線情報端末 (MS) には、AT (Access Terminal) および TE (Terminal Equipment) が設置される。TE はパーソナルコンピュータなどの情報端末であり、AT は無線アクセス端末である。 20

【0004】

前記基地局は、AT との間に無線チャネルを確立する。基地局コントローラは基地局を制御する。PCF は基地局コントローラと PDSN との間でデータ通信を制御する。PDSN は、無線アクセスネットワークと IP ネットワークとを接続して論理リンクを終端する。PPP コネクションは、TE と PDSN との間に確立されるデータ通信路である。R-P コネクションは、PPP コネクションを確立するときに PCF と PDSN との間に確立されるデータ通信路であり、PPP コネクションごとに確立され、ユニークな識別子が割り当てられている。 30

【0005】

図 19 は、cdma2000 で規定されている Simple IP (SIP) コールでの認証時に、CHAP (Challenge Handshake Authentication Protocol) を採用した場合のシーケンスを示した図である。ここで、CHAP は回線上でサポートされるセキュリティ機能であり、無認可のアクセスを防御するために PPP カプセル化を用いる。 40

【0006】

手順 (a) : 情報端末 (MS) と RAN (無線アクセスネットワーク) との間に無線チャネルが確立される。

手順 (b) : PCF と PDSN との間に個別の R-P コネクションが確立される。

手順 (c) : 無線端末が PDSN に対して CHAP による認証を要求する。

手順 (d) : PDSN が情報端末に対して CHAP による認証を要求し、かつ PDSN が受信可能な最大 packets サイズ MRU を伝達する。これにより、情報端末と無線アクセスネットワークとの間に無線チャネルが確立される。

手順 (e) : CHAP による認証が PDSN において了承される。

手順 (f) : CHAP による認証および PDSN の MRU が情報端末において了承される。

手順 (g) : CHAP 認証のための challenge メッセージが PDSN から情報端末へ送信される。 50

手順(h)：情報端末によりchallenge responseが生成され、ユーザ名 (Username) と共にPDSNへ送信される。

【 0 0 0 7 】

手順(i)：PDSNからAAAサーバへ、前記Username、CHAP challenge、CHAP responseが認証用プロトコルを用いて送信される。

手順(j)：AAAサーバからPDSNへ、認証結果 (成功または失敗) および必要に応じて情報端末が利用するIPアドレス「y」が、認証用プロトコルを用いて送信される。

手順(k)：PDSNから情報端末へ認証結果が送信される。

手順(l)：認証が成功した場合には、PDSNが自身のIPアドレスとして「x」を使うことを情報端末に対して要求する。

10

手順(m)：アドレスを割り当てられていない情報端末は、自身のIPアドレスとして「0.0.0.0」の使用をPDSNに要求する。

手順(n)：PDSNが情報端末に対して、IPアドレス「y」の使用を要求する。

【 0 0 0 8 】

手順(o)：情報端末において、PDSNが自身のIPアドレスとして「x」を使うことが了承される。

手順(p)：情報端末が自身のIPアドレスとして「y」を使うことをPDSNへ要求する。

手順(q)：PDSNにおいて、情報端末がIPアドレス「y」を使うことが了承される。この後、情報端末がDNSサーバのアドレスなどを要求した場合には、それらに対して適切に回答する。

20

手順(r)：PDSNが認証サーバに対して課金の開始を要求する。

手順(s)：認証サーバがPDSNに対して課金の開始を了承する。

【非特許文献1】Simpson, "The Point to Point Protocol (PPP)", RFC 1661, July 1994.

【非特許文献2】P.R0001, "Wireless IP Network Architecture based on IETF Protocols", 3GPP2, July 2000.

【非特許文献3】P.S0001-A Version 3.0.0, "Wireless IP Network Standard", 3GPP2, July 2001.

【非特許文献4】Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

30

【非特許文献5】A.S0007-0 version 1.0, "1xEV-DO Inter-Operability Specification (IOS) for CDMA 2000 Access Network Interfaces", 3GPP2, July 2001.

【発明の開示】

【発明が解決しようとする課題】

【 0 0 0 9 】

PPPはもともと、モデムを用いたダイヤルアップ接続用に策定されたプロトコルであり、cdma2000では必ずしも利用しないパラメータおよびシーケンスが存在する。したがって、これをそのままパケット交換網のデータ通信における呼設定に利用すると効率が悪い。

【 0 0 1 0 】

例えば、SIPコールでの認証時にCHAPを用いる場合のシーケンス (図19) では、手順(c)、(e)において情報端末がPDSNを認証する要求/応答メッセージが交換されるが、実際には行われなため冗長である。また、手順(m)において情報端末がIPアドレス(0.0.0.0)を送信したのち、PDSNから手順(n)において情報端末が使用すべきアドレスが送信されるが、IPアドレスは常にPDSNから付与されるために手順(m)のシーケンスは冗長である。

40

【 0 0 1 1 】

また、cdma2000 1X EV-DOでは上り回線の速度が低いため、できるだけ情報量を削減する必要がある。しかしながら、PPPでは上り下りで対象のシーケンスが実行されるので効率が悪い。

【 0 0 1 2 】

本発明の目的は、上記した従来技術の課題を解決し、SIPコールでの認証時に冗長な手

50

順を省略すると共に、PPP非標準のメッセージを用いて手順やデータ量を削減することにより呼設定に要する時間を短縮し、さらには端末あるいはPDSNが前記非標準メッセージに未対応であってもPPP標準の手順で呼設定手順を継続できるパケット交換網の呼設定方法を提供することにある。

【課題を解決するための手段】

【0013】

上記した目的を達成するために、本発明は、無線情報端末と、当該無線情報端末との間に無線リンクを確立する無線アクセスネットワークおよび当該無線アクセスネットワークを広域ネットワークに接続するPDSN(パケットデータ交換ノード)を含むネットワークシステムとから構成されるネットワークにおいて、前記情報端末とPDSNとの間にPPPコネクションを確立するための呼設定方法において、以下のような手段を含むことを特徴とする。

10

【0014】

(1)情報端末とPDSNとの間に無線リンクを確立する手順と、PDSNから情報端末へ標準の設定要求メッセージを送信する手順と、PDSNから情報端末へ非標準の設定要求メッセージを送信する手順と、情報端末が、前記標準および非標準の設定要求メッセージのいずれか一方に応答して、それぞれ標準または非標準の設定応答メッセージを送信する手順と、前記PDSNが、前記標準または非標準の設定応答メッセージの内容に基づいて情報端末の認証を行う手順とを含み、情報端末は、非標準メッセージに対応しているか否かに応じて、非標準の設定要求メッセージに対して優先的に応答することを特徴とする。

20

(2)前記非標準メッセージに対応した情報端末が、標準の設定要求メッセージを受信した後、当該メッセージへ応答せずに所定時間だけ待機する手順と、前記待機時間内に非標準の設定要求メッセージを受信すると、当該メッセージに応答して非標準の設定応答メッセージを送信する手順と、前記待機時間内に非標準の設定要求メッセージを受信できないと、前記標準の設定要求メッセージに応答して標準の設定応答メッセージを送信する手順とを含むことを特徴とする。

【0015】

(3)非標準のメッセージは、複数の標準メッセージに分散登録される複数の設定要求が一括登録されるオプションフィールドを含み、前記複数の設定要求が前記非標準のメッセージで一括送信されることを特徴とする。

30

(4)非標準のメッセージは、そのメッセージ種別およびオプションデータの代表値が登録されるオプションフィールドを含むことを特徴とする。

(5)オプションフィールドが複数ビットの領域を有し、各メッセージ種別およびそのオプションデータの代表値が所定の1ビットに登録されることを特徴とする。

【0016】

(6)非標準の設定応答メッセージが、ドメイン代表値フィールド、サブドメイン代表値フィールド、ユーザ名構築ルールフィールドおよびPAP/CHAP拡張フィールドを含み、前記PDSNが、前記ドメイン代表値フィールド、サブドメイン代表値フィールド、ユーザ名構築ルールフィールドおよびPAP/CHAP拡張フィールドに登録された情報に基づいてユーザ名を構築する手順をさらに含み、前記ユーザ名を構築する手順が、ユーザ名構築ルールが第1タイプのときに、受信メッセージのPAP/CHAP拡張フィールドに登録されているユーザ名を認証用ユーザ名とする手順と、ユーザ名構築ルールが第2タイプのときに、情報端末のIMSI、前記ドメイン代表値と関連付けられたドメイン名、および前記サブドメイン代表値と関連付けられたサブドメイン名とに基づいて認証用ユーザ名を構築する手順とを含むことを特徴とする。

40

(7)前記ユーザ名を構築する手順がさらに、ユーザ名構築ルールが第3タイプのときに、情報端末のIMSIを認証用ユーザ名とする手順を含むことを特徴とする。

【発明の効果】

【0017】

(1)請求項1の発明によれば、非標準メッセージに対応したPDSNからは、非標準の設定

50

要求メッセージに加えて標準の設定要求メッセージも送信される。したがって、無線情報端末が非標準メッセージに対応していれば非標準の設定要求メッセージに返信して非標準の設定応答メッセージを返信できる一方、無線情報端末が非標準メッセージに非対応であっても標準の設定要求メッセージに返信して標準の設定応答メッセージを返信できる。

【0018】

(2)請求項2の発明によれば、非標準メッセージに対応した情報端末は、PDSNから標準の設定要求メッセージを受信しても直ぐには応答せずに所定時間だけ待機し、この所定時間内に非標準の設定要求メッセージを受信できない場合だけ、前記標準の設定要求メッセージに返信して標準の設定応答メッセージを送信する。したがって、PDSNが非標準メッセージに対応していれば、当該メッセージに対して非標準のメッセージで優先的に応答できる一方、PDSNが非標準メッセージに未対応であっても標準のメッセージで応答できる。

【0019】

(3)請求項3の発明によれば、非標準のメッセージには、複数の標準メッセージに分散登録されていた複数の設定要求が登録されて一括送信されるので、呼設定に要するメッセージ数を減じることができる。

(4)請求項4の発明によれば、標準メッセージの拡張フィールドにおいて数十ビットを占有していたオプションデータが、そのメッセージ種別と共に代表値としてオプションフィールドに登録されるので、拡張フィールドの短縮によるデータ量の削減が可能になる。

【0020】

(5)請求項5の発明によれば、標準メッセージの拡張フィールドにおいて数十ビットを占有していたオプションデータを、非標準メッセージ上では1ビットで表現できるようになる。

(6)請求項6,7の発明によれば、情報端末からPDSNへ認証用のユーザ名そのものを送信することなく、当該ユーザ名をPDSN側において構築するのに必要な情報のみを送信すれば良いので、情報端末からPDSNへ送信する情報量を減じることができる。

【発明を実施するための最良の形態】

【0021】

以下、図面を参照して本発明の好ましい実施の形態について詳細に説明する。図1は、前記図18に関して説明したネットワークシステムにおいて、cdma2000で規定されているSIPコールでの認証時に本発明を適用した場合のシーケンスを示した図であり、図17は、その状態遷移図である。

【0022】

手順(1):リンク停止(Dead)フェーズにおいて、情報端末(MS)と無線アクセスネットワーク(RAN)との間に無線チャネルが確立される。

手順(2):端末認証が成功した後、RANのPCFからPDSNへA11 Registration Request(登録要求)が送出される。

手順(3):PDSNからPCFへ、手順(2)のA11 Registration Requestに返信してA11 Registration Reply(登録応答)が送出される。この結果、PCFとPDSNとの間にR-Pコネクション(A10/11)が確立されてリンク確立(Establish)フェーズへ移行する。

【0023】

手順(4):PDSNが情報端末との間にデータリンク層で無線チャネルを確立するために、初期(Initial)フェーズにおいてPPP標準のLCP(Link Control Protocol) Cfg-Request(設定要求)メッセージが送信される。このメッセージには、CHAPによる認証要求およびPDSNにおいて受信可能な最大パケットサイズMRUが登録されている。

【0024】

手順(5):PDSNから情報端末へ、前記LCP Cfg-Requestと同時に、本発明に固有であってPPP非標準のCfg-Requestメッセージが送出される。なお、本実施形態では非標準メッセージと標準メッセージとを区別するために、非標準メッセージには添字「AltPPP」を付している。このAltPPP Cfg-Requestには、CHAP認証で使用する暗号鍵(challenge value)が含まれる。なお、実装に際しては、手順(4)のLCP Cfg-Requestと手順(5)のAltPPP Cfg-Re

questとを同一のA10パケットに含めることが望ましい。その後、PDSNは待機(Waiting)フェーズへ移行する。

なお、本実施形態では情報端末におけるメッセージの受信漏れを防ぐために、当該メッセージは所定の複数回数だけ再送される。このとき、IDおよびChallenge value等は同一とする。

【0025】

手順(6)：本実施形態では、情報端末が前記非標準メッセージに対応しているので、情報端末からPDSNへ、前記AltPPP Cfg-Requestメッセージに回答してPPP非標準のAltPPP Cfg-Response(設定応答)メッセージが送出される。このメッセージは、後に詳述する「ドメイン代表値フィールド」、「サブドメイン代表値フィールド」、「ユーザ名構築ルールフィールド」および「拡張(Extention)フィールド」を含み、拡張フィールドにはCHAP/PAP認証用のデータが登録される。その後、情報端末は手続(Proceeding)フェーズへ移行する。

10

【0026】

手順(7)：PDSNは、AltPPP Cfg-Responseを情報端末から受信すると前記AltPPP Cfg-Requestの再送を停止し、AAA(Accounting, Authentication, and Authorization: 課金、認証、認定)サーバへRADIUS Access-Requestメッセージを送信して手続(Proceeding)フェーズへ移行する。

このとき、PDSNで受信されたAltPPP Cfg-ResponseメッセージにCHAP/ResponseあるいはPAP/Requestが登録されておらず、かつPDSNにパスワードが事前登録されていないなど、RADIUS Access-Requestを送出できる条件が揃っていない場合には、PDSNから情報端末へAltPPP Cfg-Nackメッセージが送信される。

20

【0027】

手順(8)：AAAサーバからPDSNへRADIUS Access-Acceptが送信される。このメッセージには、認証結果(成功または失敗)および必要に応じて情報端末で利用されるIPアドレスが含まれる。

手順(9)：PDSNから情報端末へAltPPP Cfg-Successが送出される。このメッセージには、IPv4アドレスやIPv6 Interface-ID、IPv4 DNSアドレス情報等が含まれる。その後、PDSNは開放(Opening)フェーズへ移行する。

【0028】

手順(10)：情報端末は、前記AltPPP Cfg-Successの受信に回答してPDSNへAltPPP Cfg-Ackを返信し、その後、開放(Opening)フェーズへ移行する。この時点で情報端末はサービス開始できる。あるいは、手続(Proceeding)フェーズのままAltPPP Cfg-Nackを送信する。

30

PDSNは、AltPPP Cfg-Successを受信してPPPネットワークフェーズへ移行し、その後、標準のPPPにしたがってサービスを開始できる。なお、情報端末からAltPPP Cfg-Nackメッセージを受信した場合、開放(Opening)フェーズのままAltPPP Cfg-Successメッセージを送出する。このとき、IPCP/IPv6CP等のConfigure-Requestの該当するオプションをNackの内容にあわせて設定し、その他のパラメータについては過去に送出したAltPPP Cfg-Successメッセージと同一の内容とする。

40

【0029】

手順(11)：PDSNから情報端末へRouter Advertisementが送出される。このメッセージには、IPv6 Prefix情報やIPv6 DNSアドレス情報が含まれる。

手順(12)：PDSNからAAAサーバに対してRADIUS Accounting Request(課金要求)が送信され、課金の開始が要求される。

手順(13)：AAAからPDSNに対してRADIUS Accounting Response(課金応答)が返信され、課金開始が了承される。

手順(14)：情報端末とPDSNとの間でデータ通信が開始される。

【0030】

図2は、前記AltPPP(非標準)メッセージのフォーマットを示した図であり、RFC2153

50

の規定通りに、メッセージの種別が登録されるCodeフィールドと、送信者の識別子が登録されるIDフィールドと、パケット全体 (Code ~ Extensionの最後まで) の長さが登録されるLengthフィールドと、エラー検出用のMagic-Numberフィールドとを含む。

【 0 0 3 1 】

前記AltPPPメッセージはさらに、ベンダあるいは通信事業者の識別子が登録されるOUIフィールドと、拡張ヘッダ(Extension)の有無およびメッセージの種別が登録されるKindフィールドと、ドメイン名を特定するための代表値が登録されるDomainフィールドと、サブドメイン名を特定するための代表値が登録されるSub-domainフィールドと、ユーザ名を利用したドメイン名の構築ルールが登録されるユーザ名構築ルールフィールドと、これまでは複数の標準メッセージに分散されて送信されていた各種の設定要求や、標準メッセージの拡張フィールドにおいて数十ビットを占有していたオプションデータを、そのメッセージ種別と共に代表するデータが登録されるReq-Optionsフィールドとを含む。本実施形態では、各データの論理和がReq-Optionsフィールドに登録される。

10

【 0 0 3 2 】

前記Kindフィールドには、本実施形態では拡張ヘッダが存在する場合に、その最上位ビットに「1」がセットされる。さらに具体的に説明すれば、図3に一例を示したように、Kindフィールドが「1」または「129」であれば、PDSNからMSへ送信されるConfigure-Requestメッセージであり、MSへCHAP challenge valueを通知したり、あるいは情報端末へA10コネクションが確立したことを通知するために利用される。

【 0 0 3 3 】

同様に、Kindフィールドが「2」または「130」であれば、情報端末からPDSNへ送信されるConfigure-Responseメッセージであり、PDSNへユーザ名あるいはパスワードに関する情報を通知したり、あるいはPDSNから通知してほしい情報(IPv4アドレス、etc)をオプションリクエストとして通知するために利用される。

20

【 0 0 3 4 】

同様に、Kindフィールドが「3」または「131」であれば、PDSNから情報端末へ送信されるConfigure-Successメッセージであり、サービスが許可された場合、必要な情報(IPv4アドレス、etc)を情報端末へ通知したり、あるいはPDSNが使用する情報(IPv4アドレス、etc)をオプションリクエストとして通知するために利用される。

【 0 0 3 5 】

同様に、Kindフィールドが「4」または「132」であれば、情報端末からPDSNへ送信されるConfigure-Ackメッセージであり、前記Configure-Successを受信したことをPDSNに通知するために利用される。

30

【 0 0 3 6 】

同様に、Kindフィールドが「5」または「133」であれば、PDSNから情報端末へ送信されるConfigure-Nakメッセージであり、サービスが許可されなかった場合に、これを情報端末へ通知したり、あるいはPDSNからのオプションリクエストに対して受け入れられない場合にreject/nakの内容をPDSNに通知するために利用される。

【 0 0 3 7 】

前記Domainフィールドには、図4に一例を示したように、ユーザ名を設定しない場合には「0」が設定され、ドメイン名として「ezweb.ne.jp」を指定する場合には「1」が設定される。同様に、使用頻度の高いドメイン名に関しては、それぞれ「2」、「3」...がドメイン名を代表するドメイン名代表値として登録される。

40

【 0 0 3 8 】

前記Sub-domainフィールドには、図5に一例を示したように、ユーザ名あるいはSub-domainを設定しない場合には「0」が設定され、サブドメイン名として「ev01」を指定する場合には「1」が設定される。同様に、使用頻度の高いサブドメイン名に関しては、それぞれ「2」、「3」...がサブドメイン名を代表するサブドメイン名代表値として登録される。

【 0 0 3 9 】

50

前記ユーザ名構築ルールフィールドには、後に図 1 4 を参照して詳述するように、拡張フィールドのCHAP/ResponseまたはPAP/Requestに含まれるUsernameをユーザ名とする場合には「0」が登録され、A11メッセージに含まれるIMSIをユーザ名とする場合には「1」が登録され、IMSI@Sub-domain.Domainをユーザ名とする場合には「2」が登録される。ユーザ名構築ルールが「1」または「2」の場合は、拡張フィールドにUsernameが登録されている場合であっても無視される。

【0040】

前記Req-Optionsフィールドには、これまで複数の標準メッセージに分散されて送信されていた各種の設定要求が一括して登録されると共に、標準メッセージの拡張フィールドにおいて数十ビットを占有していたオプションデータおよびそのメッセージ種別を代表する値が、いずれも1ビットで登録される。

10

【0041】

図 6 は、Req-Optionsフィールドの各ビットの状態と設定内容との関係を示した図であり、従来はIPCP Cfg-Req メッセージおよびIPv6CP Cfg-Req メッセージの2つに分散されて送信されたIPv4およびIPv6の設定要求が、Req-Optionsフィールドの上位2ビットがセットされた唯一のAltPPP Cfg-Req メッセージを送信するだけで可能になる。これにより、本実施形態では呼設定手順の削減が可能になる。

【0042】

さらに、例えば図 1 9 の手順(m)では、情報端末がIPアドレスの割り当てをPDSNに対して要求する際に、IPCP Cfg-Req メッセージの拡張フィールドに32ビットのオプションデータフィールドを確保し、当該フィールドにダミーアドレス[0.0.0.0]を登録して送信する必要があった。

20

【0043】

しかしながら、本実施形態ではReq-Optionsフィールドの上位第3ビット目がセットされたAltPPP Cfg-Req メッセージを送信すれば、その拡張フィールドにダミーアドレスを登録することなく、PDSNに対してIPアドレスの割り当てを要求できる。同様に、情報端末がDNSのアドレスをPDSNに対して要求する際も、本実施形態ではReq-Optionsフィールドの上位第5ビット目あるいは第6ビット目がセットされたAltPPP Cfg-Req メッセージを送信すれば、その拡張フィールドにDNSのダミーアドレス[0.0.0.0]を登録することなく、PDSNに対してDNSのアドレスを要求できる。これにより、本実施形態では拡張フィールドの短縮によるデータ量の削減が達成される。

30

【0044】

図 7 は、LCP/IPCP/IPv6CPにおける前記拡張フィールドのフォーマットを示した図であり、Protocol IDフィールドには、図 8 に一例を示したように、IANAにてアサインされたDLL Protocol Numbersが設定される。Codeフィールドには、図 9 にLCPおよびIPCPの場合を例にして示したように、LCP、IPCP等で規定されているCodeが設定される。Lengthフィールドには、オプションパラメータのバイト数がLCP、IPCP等で規定されている通りに設定される。

【0045】

Type-X (X=A, B...) フィールドには、図 1 0 にLCPの場合を例にして示したように、オプションパラメータのTypeについてLCP、IPCP等で規定されている値が設定される。Length-Xフィールドには、オプションパラメータのバイト数がLCP、IPCP等で規定されている通りに設定される。Value-Xフィールドには、オプションパラメータについてLCP、IPCP等で規定されているValueが設定される。

40

【0046】

図 1 1 は、PAP/CHAP拡張フィールドのフォーマットを示した図であり、Protocol IDフィールドには、図 1 2 に一例を示したように、IANAにてアサインされたDLL Protocol Numbersが設定される。Codeフィールドには、図 1 3 にCHAPの場合を例にして示したようにCHAPで規定されているCodeが設定される。IDフィールドには、PAP、CHAP等で規定されている値が設定される。Lengthフィールドには、PAP、CHAP等で規定されている値が設定され

50

る。Dataフィールドには、PAP、CHAP等で規定されている値(Usernameを含む)が設定される。

【0047】

次いで、PDSNが前記図1の手順(6)で受信したAltPPP Cfg-Responseメッセージの登録データに基づいてユーザ名を構築し、その認証を行う方法について、図14のフローチャートに沿って説明する。

【0048】

本実施形態では、前記AltPPP Cfg-Responseメッセージが、ドメイン代表値フィールド、サブドメイン代表値フィールド、ユーザ名構築ルールフィールドおよびPAP/CHAP拡張フィールドを含み、このAltPPP Cfg-Responseメッセージを受信したPDSNが、前記ドメイン代表値フィールド、サブドメイン代表値フィールド、ユーザ名構築ルールフィールドおよびPAP/CHAP拡張フィールドに登録されているデータに基づいて、以下の手順でユーザ名を構築し、その認証をAAAサーバへ要求する。

10

【0049】

ステップS1では、AltPPP Cfg-Responseメッセージのユーザ名構築ルールフィールドが参照される。ステップS2では、参照結果に基づいてユーザ名構築ルールが判別される。このユーザ名構築ルールは、PDSNが前記各フィールドに登録されているデータに基づいて認証用のユーザ名を構築する際のルールを規定するものであり、ユーザ名構築ルールが「0」であればステップS3へ進む。ステップS3、S4では、PAP/CHAP拡張フィールドにCHAP/responseおよびPAP/requestのいずれが登録されているかが判定される。

20

【0050】

PAP/CHAP拡張フィールドにCHAP/responseが登録されていればステップS5へ進み、CHAP/response拡張フィールドのDataフィールドに登録されているUsernameが認証用ユーザ名として登録される。ステップS6では、前記ステップS5で構築された認証用ユーザ名と、前記手順(5)で情報端末へ送信したAltPPP Cfg-Requestに登録したCHAP challenge valueと、前記CHAP/response拡張フィールドのDataフィールドに登録されているCHAPパスワードとが、前記手順(7)においてAAAサーバへ送信される。

【0051】

これに対して、前記PAP/CHAP拡張フィールドにPAP/requestが登録されていればステップS7へ進み、PAP/request拡張フィールドのDataフィールドに登録されているUsernameが認証用ユーザ名として登録される。ステップS8では、前記ステップS7で構築された認証用ユーザ名と、前記PAP/request拡張フィールドのDataフィールドに登録されているユーザパスワードとが、前記手順(7)においてAAAサーバへ送信される。なお、前記PAP/CHAP拡張フィールドにCHAP/responseおよびPAP/requestのいずれもが登録されていなければ、ステップS9へ進んで「パスワードなし」接続となる。

30

【0052】

一方、前記ステップS2において、ユーザ名構築ルールが「0」以外と判定されればステップS10へ進む。ステップS10では、ユーザ名構築ルールが「1」および「2」のいずれであるかが判定される。ユーザ名構築ルールが「2」であればステップS11へ進み、前記AltPPP Cfg-ResponseメッセージのDomainフィールドに登録されているドメイン代表値、およびSub-domainフィールドに登録されているサブドメイン代表値が抽出される。ステップS12では、前記各代表値と予め対応付けられているドメイン名およびサブドメイン名が検索される。

40

【0053】

ステップS13では、前記A11メッセージに含まれるIMSIと、前記検索されたドメイン名およびサブドメイン名とを組み合わせる「IMSI@サブドメイン名.ドメイン名」がユーザ名として登録される。すなわち、図4に一例を示したように、ドメイン代表値が「1」であればドメイン名は「ezweb.ne.jp」となり、サブドメイン代表値が「1」であればサブドメイン名は「ev01」となる。したがって、この場合のユーザ名は「IMSI@ev01.ezweb.ne.jp」となる。なお、前記ステップS10において、ユーザ名構築ルールが

50

「1」と判定されていればステップS18へ進み、前記IMSIそのものが認証用ユーザ名として登録される。

【0054】

ステップS14, S15では、PAP/CHAP拡張フィールドにCHAP/responseおよびPAP/requestのいずれが登録されているかが判定される。CHAP/responseが登録されていればステップS16へ進み、前記ステップS13またはS18で構築された認証用ユーザ名と、前記手順(5)で情報端末へ送信したAltPPP Cfg-Requestに登録したCHAP challenge valueと、前記CHAP/response拡張フィールドのDataフィールドに登録されているCHAPパスワードとが、前記手順(7)においてAAAサーバへ送信される。

【0055】

これに対して、前記PAP/CHAP拡張フィールドにPAP/requestが登録されていればステップS17へ進み、前記ステップS13またはS18で構築された認証用ユーザ名と、前記PAP/request拡張フィールドのDataフィールドに登録されているユーザパスワードとが、前記手順(7)においてAAAサーバへ送信される。

【0056】

なお、PAP/CHAP拡張フィールドにCHAP/responseおよびPAP/requestのいずれもが登録されていなければステップS19へ進み、ドメインまたはサブドメイン毎に予め設定されたパスワード(ドメインで共通)に基づいてCHAP計算が行われ、CHAPパスワードおよびCHAP-Challenge valueが、前記手順(7)においてAAAサーバへ送信される。

【0057】

このように、本実施形態では情報端末からPDSNへ認証用のユーザ名そのものを送信することなく、当該ユーザ名をPDSN側において構築するのに必要な情報のみが送信されるので、情報端末からPDSNへ送信する情報量を減じることができる。

【0058】

図15は、前記非標準のAltPPPメッセージにPDSNのみが対応しており、情報端末(MS)が非対応の場合のシーケンスを示した図である。

【0059】

情報端末(MS)では、手順(4)でPPP標準のLCP Cfg-Reqメッセージを受信し、これと同時に手順(5)でPPP非標準のAltPPP Cfg-Reqメッセージを受信するが、非対応の情報端末では非標準のAltPPP Cfg-Reqが無視され、標準のLCP Cfg-Reqに回答して、手順(6)でLCP Cfg-Ackメッセージが送信される。これ以後は従来のPPP標準のシーケンスが実行される。

【0060】

このように、本実施形態ではPDSNから情報端末へ、PPP非標準のAltPPP Cfg-Reqメッセージのみならず、これと同時にPPP標準のLCP Cfg-Reqメッセージも送信されるので、非標準メッセージに未対応の情報端末であってもPDSNからの要求に回答できる。そして、これ以後はPPP標準のシーケンスが従来と同様に実行されるので、非標準メッセージに対応したPDSNと未対応の情報端末との間でも通信が可能になる。

【0061】

図16は、上記とは逆に非標準のAltPPPメッセージに情報端末のみが対応しており、PDSNが非対応の場合のシーケンスを示した図である。

【0062】

情報端末(MS)は、手順(4)でPPP標準のLCP Cfg-ReqメッセージをPDSNから受信しても、これに対して直ぐには応答せずに、PPP非標準のAltPPP Cfg-Reqメッセージの受信に備えて所定時間だけ待機する。この待機時間内にAltPPP Cfg-Reqメッセージが受信されれば、図1に関して説明した実施形態と同様に、PPP非標準のAltPPP Cfg-Resメッセージを返信する。

【0063】

これに対して、AltPPP Cfg-Reqメッセージを受信できずに待機時間がタイムアウトすると、前記手順(4)で受信したPPP標準のLCP Cfg-Reqに回答して、手順(5)でLCP Cfg-Ackメッセージが送信される。これ以後は従来のPPP標準のシーケンスが実行される。

10

20

30

40

50

【 0 0 6 4 】

このように、本実施形態では情報端末がPPP標準のLCP Cfg-Reqメッセージを受信しても、これに対して直ぐには応答せずに、PPP非標準のAltPPP Cfg-Reqメッセージの受信に備えて所定時間だけ待機し、待機時間が経過してもAltPPP Cfg-Reqを受信できない場合はPPP標準のシーケンスへ移行するので、非標準メッセージに対応した情報端末と未対応のPDSNとの間でも通信が可能になる。

【 図面の簡単な説明 】

【 0 0 6 5 】

【 図 1 】 SIPコールでの認証時に本発明を適用した場合のシーケンスを示した図である。

【 図 2 】 AltPPP (非標準) メッセージのフォーマットを示した図である。 10

【 図 3 】 Kindフィールドの登録内容の一例を示した図である。

【 図 4 】 Domainフィールドの登録内容の一例を示した図である。

【 図 5 】 Sub-domainフィールドの登録内容の一例を示した図である。

【 図 6 】 Req-Optionsフィールドの登録内容の一例を示した図である。

【 図 7 】 拡張フィールドのフォーマットを示した図である。

【 図 8 】 Protocol IDフィールドの登録内容の一例を示した図である。

【 図 9 】 Codeフィールドの登録内容の一例を示した図である。

【 図 1 0 】 Type-Xフィールドの登録内容の一例を示した図である。

【 図 1 1 】 PAP/CHAP拡張フィールドのフォーマットを示した図である。

【 図 1 2 】 PAP/CHAP拡張フィールドのProtocol IDフィールドの登録内容の一例を示した図である。 20

【 図 1 3 】 PAP/CHAP拡張フィールドのCodeフィールドの登録内容の一例を示した図である。

【 図 1 4 】 PDSNにおけるユーザ名の構築および認証方法を示したフローチャートである。

【 図 1 5 】 非標準のAltPPPメッセージにPDSNのみが対応し、情報端末が非対応の場合におけるシーケンスを示した図である。

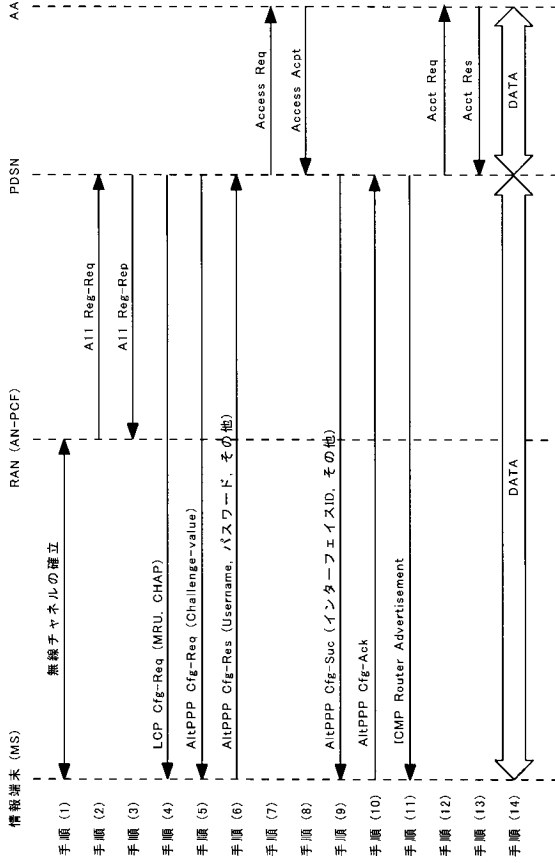
【 図 1 6 】 非標準のAltPPPメッセージに情報端末のみが対応し、PDSNが非対応の場合におけるシーケンスを示した図である。

【 図 1 7 】 情報端末およびPDSNの状態遷移図である。

【 図 1 8 】 本発明が根起用されるパケット交換網のネットワーク構成を示した図である。 30

【 図 1 9 】 SIPコールでの認証時にCHAPを採用した場合のシーケンス図である。

【 図 1 】



【 図 2 】

0	7	15	23	31
Code	ID	Length		
Magic-Number				
OUI			Kind	
Domain	Sub-domain	ユーザ名 タイプ	rsv	Req-Options
reserved	Extension(s)			

【 図 3 】

Kindフィールド		メッセージ種別	宛先	内容	拡張ヘッダ
1	129	Configure-Request	PDSN→MS	MSに対して、challenge値を通知する。 MSに対して、A10コネクションが確立したことを通知する。	無 有
2	130	Configure-Response	MS→PDSN	PDSNに対して、Username/passwordにかかわる情報を通知する。 PDSNから通知してほしい情報(IPv4アドレス、etc)をPDSNに対してオプショナルリンクエントリとして通知する。	無 有
3	131	Configure-Success	PDSN→MS	サービスが許可された場合、必要な情報(IPv4アドレス、etc)をMSに列して通知する。また、PDSNが使用する情報(IPv4アドレス、etc)をオプショナルリンクエントリとして通知する。	無 有
4	132	Configure-Ack	MS→PDSN	Configure-Successを受信したことをPDSNに通知する。	無 有
5	133	Configure-Nak	PDSN→MS	サービスが許可されなかった場合、PDSNがMSに通知する。 PDSNからのオプショナルリンクエントリに対して受け入れられない場合、reject/nakの内容をMSがPDSNに通知する。	無 有

【 図 4 】

Domainフィールド	
データ	ドメイン名
0	NULL (設定なし)
1	ezweb.ne.jp
2	
...	

【 図 5 】

Sub-domainフィールド	
データ	サブドメイン名
0	NULL (設定なし)
1	ev01
2	
...	

【 図 6 】

Req-Option フィールド	
データ	内容
1000 0000	IPv4 (IPCP Configure-Requestの送出と同等)
0100 0000	IPv6 (IPv6CP Configure-Requestの送出と同等)
0010 0000	IPv4 address (IPCPのIPv4アドレスオプション=0の送出と同等)
0001 0000	IPv6 Interface-ID (IPv6CPのInterface-IDオプション=0の送出と同等)
0000 1000	IPv4 Primary DNS address (IPCPのオプション=0の送出と同等)
0000 0100	IPv4 Secondary DNS address (IPCPのオプション=0の送出と同等)
0000 0010	VJ Compression with IPCP (IPCPのVJ Compressionオプションと同等)
0000 0001	Reserved
0000 0000	Reserved (Req-Optionsが0の場合)

【 図 7 】

Protocol ID	Code	Length
Type-A	Length-A	Value-A
Type-B	Length-B	Value-B
.	.	.
.	.	.
.	.	.

【 図 8 】

Protocol ID フィールド	
データ	内容
0x8021	Internet Protocol Control Protocol
0x8057	IPv6 Control Protocol
0xc021	Link Control Protocol

【 図 9 】

Code (LCP and IPCP) フィールド	
データ	内容
0	Vendor Specific
1	Configure-Request
2	Configure-Ack
3	Configure-Nak
4	Configure-Reject
5	Terminate-Request
6	Terminate-Ack

【 図 10 】

Type-X (LCP) フィールド	
データ	内容
0	RESERVED
1	Maximum-Receive-Unit
3	Authentication-Protocol
4	Quality-Protocol
5	Magic-Number
7	Protocol-Field-Compression
8	Address-and-Control-Field-Compression

【 図 13 】

Code (CHAP) フィールド	
データ	内容
1	Challenge
2	Response
3	Success
4	Failure

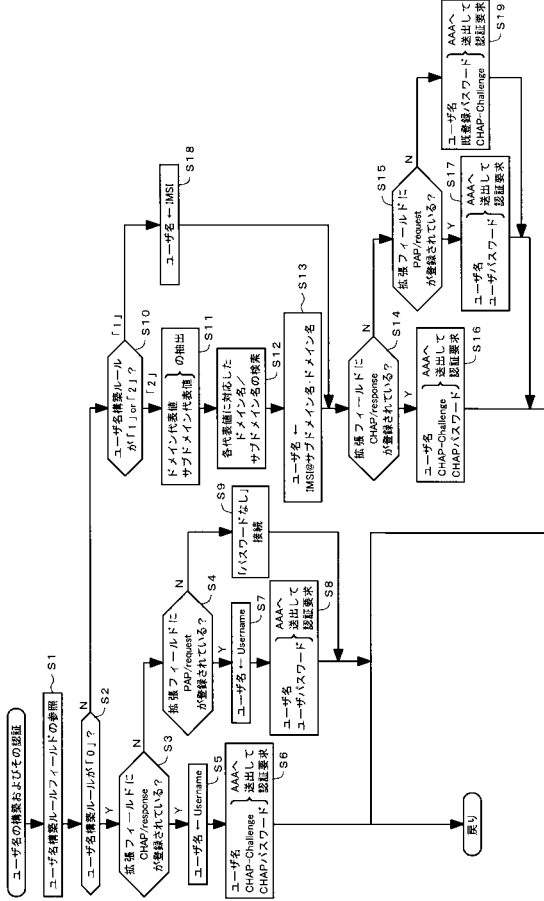
【 図 11 】

Protocol ID	Code	ID
Length	Data	

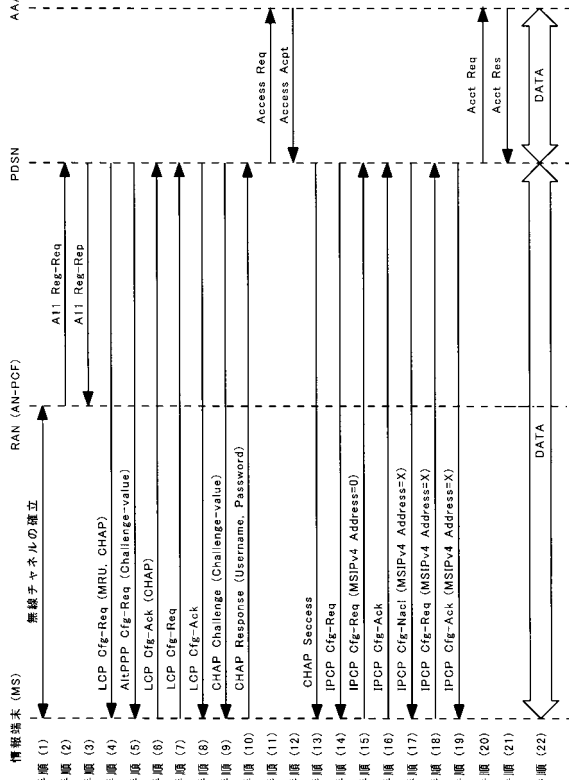
【 図 12 】

Protocol ID フィールド	
データ	内容
0xc023	Password Authentication Protocol
0xc223	Challenge Handshake Authentication Protocol

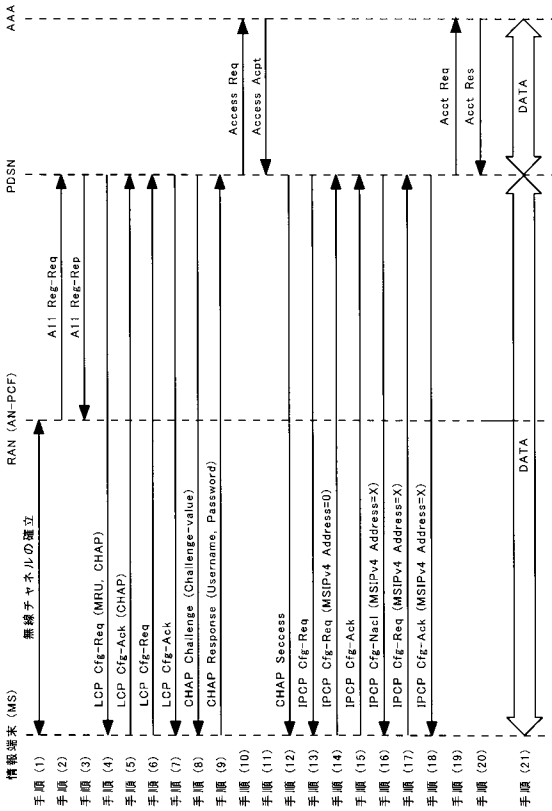
【 図 1 4 】



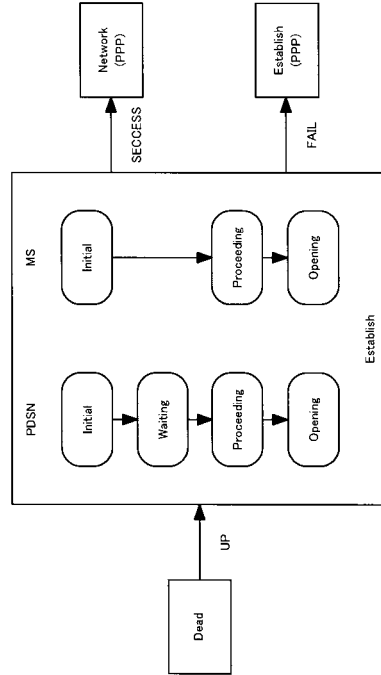
【 図 1 5 】



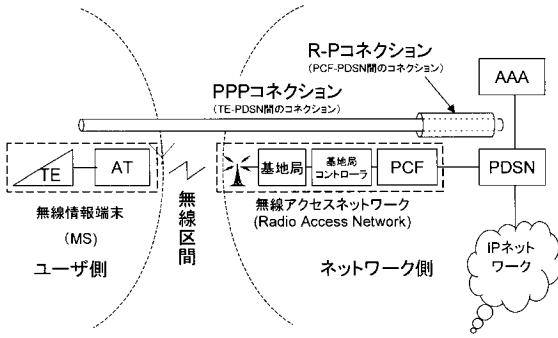
【 図 1 6 】



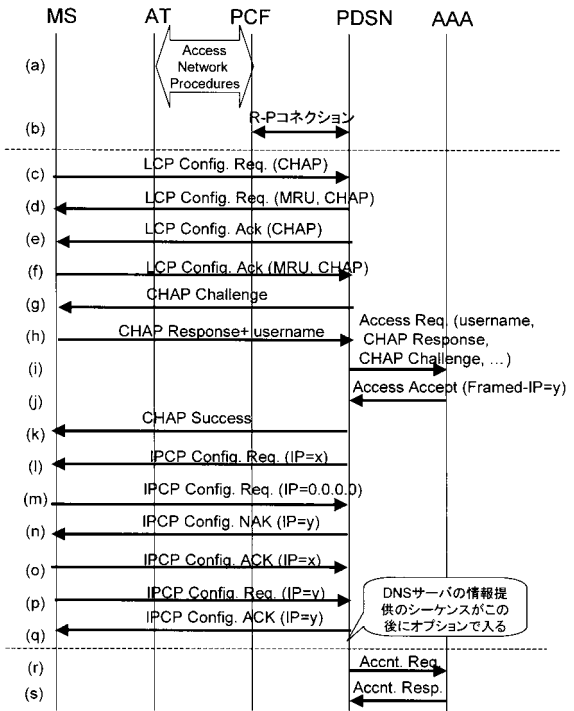
【 図 1 7 】



【 図 18 】



【 図 19 】



フロントページの続き

(72)発明者 横田 英俊

埼玉県上福岡市大原二丁目1番15号 株式会社KDDI研究所内

(72)発明者 井戸上 彰

埼玉県上福岡市大原二丁目1番15号 株式会社KDDI研究所内

Fターム(参考) 5K030 GA15 HA08 HC01 JL01 LB02