(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第3973038号

(P3973038)

(45)発行日　平成19年9月5日(2007.9.5)　(24)登録日　平成19年6月22日(2007.6.22)

(51)Int.Cl.		F I		
H04L 12/56	(2006.01)	H04L	12/56	A
H04Q 7/38	(2006.01)	H04L	12/56	100D
H04L 29/08	(2006.01)	H04B	7/26	109R
		H04B	7/26	109M
		H04L	13/00	307A

請求項の数 9　(全 14 頁)

(21)出願番号　特願2003-392103(P2003-392103)
(22)出願日　平成15年11月21日(2003.11.21)
(65)公開番号　特開2005-159519(P2005-159519A)
(43)公開日　平成17年6月16日(2005.6.16)
審査請求日　平成17年8月31日(2005.8.31)

(73)特許権者　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(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　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　小林　修
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

最終頁に続く

(54)【発明の名称】パケット交換網の呼確立方法

(57)【特許請求の範囲】

【請求項１】

情報端末(TE)および無線アクセス端末(AT)を含むユーザ側システムと、前記情報端末との間に前記無線アクセス端末を介して無線リンクを確立する無線基地局を含む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側システムとから構成されネットワークにおいて、前記情報端末(TE)とPDSNとの間にPPPコネクションを確立するための呼確立方法において、

情報端末(TE)からPDSNへ認証要求メッセージを送信する手順と、

前記認証要求メッセージに対して、前記無線アクセス端末(AT)が代理で認証応答メッセージを返信する手順とを含むことを特徴とするパケット交換網の呼確立方法。

【請求項２】

前記情報端末(TE)がPDSNに対して、IPアドレスの要求メッセージを送信する手順と、

前記アドレス要求メッセージに前記無線アクセス端末(AT)が代理で応答し、前記情報端末(TE)に対してIPアドレスを割り当て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確立方法。

【請求項３】

前記PDSNが無線アクセス端末(AT)に対して、CHAPを採用したユーザ認証要求を送信する手順と、

前記無線アクセス端末(AT)が前記ユーザ認証要求に応答して、前記情報端末(TE)に対し

てCHAPを採用したユーザ認証要求を送信する手順とを含み、
前記PDSNから無線アクセス端末(AT)へ送信されるユーザ認証要求のパケットフォーマットが、IDフィールド、LengthフィールドおよびNameフィールドを含まない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確立方法。
【請求項４】
前記情報端末(TE)が、前記ユーザ認証要求に応答して、CHAPを採用したユーザ認証応答をPDSNに対して送信する手順と、
前記ユーザ認証応答を無線アクセス端末(AT)が代理で受信する手順と、
前記無線アクセス端末(AT)が、前記代理受信したユーザ認証応答をパケット交換データ網(PDSN)に対して送信する手順とを含み、
前記無線アクセス端末(AT)からPDSNに対して送信されるユーザ認証応答のパケットフォーマットが、IDフィールド、LengthフィールドおよびValue-sizeフィールドを含まないことを特徴とする請求項３に記載のパケット交換網の呼確立方法。
【請求項５】
前記情報端末(TE)が、前記ユーザ認証要求に応答して、PAPを採用したユーザ認証応答をPDSNに対して送信する手順と、
前記ユーザ認証応答を無線アクセス端末(AT)が代理で受信する手順と、
前記無線アクセス端末(AT)が、前記代理受信したユーザ認証応答をPDSNに対して送信する手順とを含み、
前記無線アクセス端末(AT)からPDSNに対して送信されるユーザ認証応答のパケットフォーマットが、IDフィールドおよびLengthフィールドを含まないことを特徴とする請求項３に記載のパケット交換網の呼確立方法。
【請求項６】
全アルファベットの各大文字および各小文字、ならびに「０」～「９」の整数の計６２文字を、６ビットで表記できる６４種類のコードのうちの６２種類と一義的に対応付ける第１のコード表と、
所定の英数字および記号を０ｘ００～０ｘ７Ｆ（１６進表記で００～７Ｆ：以下同様）のアスキーコードと一義的に対応付ける第２のコード表と、
所定の文字列を０ｘ８０～０ｘＦＦの８ビットコードと一義的に対応付ける第３のコード表と、
少なくとも一つの特殊文字を、前記６４種類のコードのうちの前記６２種類のコード以外の２つのコードの一方である第１特殊コードと対応付ける第４のコード表とを予め用意し、
送信パケットに登録する識別情報をコード化する際に、
前記６２文字に属する英数字を、前記第１のコード表に基づいてコード化する手順と、
前記特殊文字を、前記第４のコード表に基づいてコード化する手順と、
前記６２文字以外の記号を、前記第２のコード表に基づいてコード化する手順と、
前記アスキーコードの前に、前記６４種類のコードのうちの前記６２種類のコード以外の２つのコードの他方である第２特殊コードを付する手順と、
前記所定の文字列を、前記第３のコード表に基づいてコード化する手順と、
前記８ビットコードの前に前記第２特殊コードを付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確立方法。
【請求項７】
前記特殊文字が「@」および「．」であることを特徴とする請求項６に記載のパケット交換網の呼確立方法。
【請求項８】
全アルファベットの各大文字および各小文字、ならびに「０」～「９」の整数の計６２文字を、６ビットで表記できる６４種類のコードのうちの６２種類と一義的に対応付ける第１のコード表と、
所定の英数字および記号を０ｘ００～０ｘ７Ｆのアスキーコードと一義的に対応付ける

第２のコード表と、
所定の文字列を０ｘ８０～０ｘＦＦの８ビットコードと一義的に対応付ける第３のコード表と、
少なくとも一つの特殊文字を、前記６４種類のコードのうちの前記６２種類のコード以外の２つのコードの一方である第１特殊コードと対応付ける第４のコード表とを予め用意し、
受信パケットに登録されている識別情報をデコードする際に、
前記６２種類に属する６ビットコードを、前記第１のコード表に基づいてデコードする手順と、
前記第１特殊コードを、前記第４のコード表に基づいてデコードする手順と、
前記第２特殊コードに続くアスキーコードを、前記第２のコード表に基づいてデコードする手順と、
前記第２特殊コードに続く前記８ビットコードを、前記第３のコード表に基づいてデコード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確立方法。
【請求項９】
前記特殊文字が「@」および「．」であり、最初の第１特殊コードは「@」に変換し、二番目以降の第１特殊コードは全て「．」にデコードする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確立方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、PPP（Point to Point Protocol）に準拠した手順でパケット交換網の呼を高速に確立する呼確立方法に関する。
【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、データ通信の呼確立にPPPが採用されている。
【０００３】
図１１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：パケットデータ交換ノード)およびAAA (Authentication, Authorization and Accounting)サーバが接続される。移動機側あるいはユーザ側には、AT (Access Terminal)およびTE (Terminal Equipment)から構成される通信装置が設置される。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。
【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。
【０００５】
図１８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。

【０００６】

手順(a)：AT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(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)：TEがPDSNに対してCHAPによる認証を要求する。

手順(d)：PDSNがTEに対してCHAPによる認証を要求し、かつPDSNが受信可能な最大パケットサイズMRUを伝達する。これにより、AT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TE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TEへ送信される。

手順(h)：TE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。

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TE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TE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TEに対して要求する。

手順(m)：アドレスを割り当てられていないTE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TEに対して、IPアドレス「y」の使用を要求する。

手順(o)：TE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)：TE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、TEがIPアドレス「y」を使うことが了承される。この後、TE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応答する。

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。

【０００７】

図１９は、前記Simple IP(SIP)コールでの認証時にPAP（Password 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、PAPはPPP 接続で用いられる認証プロトコルであるが、前記CHAP と異なり、パスワードなどの情報は平文（暗号化されていないプレーンテキスト）で送られる。

【０００８】

手順(a)：AT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(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)：TEがPDSNに対してPAPによる認証を要求する。

手順(d)：PDSNがTEに対してPAPによる認証を要求し、かつPDSNが受信可能な最大パケットサイズMRUを伝達する。これにより、AT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)：PAPによる認証がPDSNにおいて了承される。

手順(f)：TEがPDSNに対してPAPによる認証を要求する。

手順(g)：PDSNがTEに対してPAPによる認証を要求する。

手順(h)：TEがPAPによる認証を了承する。

手順(i)：TEがユーザ名(username)とパスワード(password)をPDSNへ送信する。

手順(j)：PDSNからAAAサーバへ、前記ユーザ名(username)とパスワード(password)とが認証用プロトコルを用いて送信される。

手順(k)：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TE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(l)：PDSNからTEへ認証結果が送信される。
手順(m)：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TEに対して要求する。
手順(n)：アドレスを割り当てられていないTE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(o)：PDSNがTEに対して、IPアドレス「y」の使用を要求する。
手順(p)：TE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(q)：TEが自身のIPアドレスとして「y」を使うことをPDSNに対して要求する。
手順(r)：PDSNにおいて、TEがIPアドレス「y」を使うことが了承される。この後、TE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応答する。
手順(s)：PDSNが認証サーバに対して課金の開始を要求する。
手順(t)：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.
【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】
【０００９】
PPPはもともと、モデムを用いたダイア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確立に利用すると効率が悪い。
【００１０】
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１８）では、手順(c)、(e)においてTEがPDSNを認証する要求／応答メッセージが交換されるが、実際には行われないため冗長である。また、手順(m)においてTE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TE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。
【００１１】
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。
【００１２】
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順を省略し、さらには上り方向のデータ量を削減することにより、呼確立に要する時間を短縮できるパケット交換網の呼確立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、情報端末(TE)および無線アクセス端末(AT)を含むユーザ側システムと、前記情報端末との間に前記無線アクセス端末を介して無線リンクを確立する無線基地局を含む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（パケット交換データ網)を含むネットワーク側システムとから構成されネットワークにおいて、前記情報端末(TE)とPDSNとの間にPP

Pコネクションを確立するための呼確立方法において、以下のような手段を講じた点に特徴がある。

【００１４】

(1)情報端末(TE)からPDSNへ認証要求メッセージを送信する手順と、前記認証要求メッセージに対して、前記無線アクセス端末(AT)が代理で認証応答メッセージを返信する手順とを含むことを特徴とする。

【００１５】

(2)情報端末(TE)がPDSNに対して、IPアドレスの要求メッセージを送信する手順と、前記アドレス要求メッセージに前記無線アクセス端末(AT)が代理で応答し、前記情報端末(TE)に対してIPアドレスを割り当てる手順とを含むことを特徴とする。

【発明の効果】

【００１６】

本発明によれば、以下のような効果が達成される。

(1)ユーザ側の情報端末(TE)から要求されたネットワークの認証要求に対して、PDSNではなくATが代理で応答するので、この認証に要する時間が短縮されるのみならず、認証要求メッセージおよび認証応答メッセージが無線区間を跨がないので、通信資源の節約が可能になる。

【００１７】

(2)TEからPDSNへ送信されるアドレス要求メッセージに対して、PDSNではなくATが代理で応答するので、アドレス割当に要する時間が短縮されるのみならず、アドレス要求メッセージおよびアドレス応答メッセージが無線区間を跨がないので、通信資源の節約が可能になる。

【発明を実施するための最良の形態】

【００１８】

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１１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、本発明に係る通信方法の第１実施形態を適用した場合のシーケンスを示した図である。本実施形態では、従来のCHAPから冗長な手順を省略することで呼確立までの時間を短縮している。

【００１９】

手順(a)：TEからPDSNに対してCHAPによる認証が要求される。このメッセージは、PDSNに代わってATにより受信される。

手順(b)：PDSNに代わってATからTEへCHAPによる認証が要求され、かつPDSNが受信可能な最大パケットサイズMRU（予めATに設定されている）がTEに伝達される。

手順(c)：ATがPDSNに代わってCHAPによる認証を了承する。

手順(d)：TEがCHAPによる認証およびPDSNのMRUを了承する。このメッセージも、PDSNに代わってATにより受信される。

手順(e)：PDSNからATへ、CHAP認証のためのchallengeメッセージが送信される。

手順(f)：ATからTEへ、CHAP認証のためのchallengeメッセージが送信される。

手順(g)：TEによりCHAP responseが生成され、ユーザ名(username)と共にPDSNへ送信される。このメッセージもPDSNに代わってATにより受信される。

手順(h)：ATからPDSNへ、受信したユーザ名(username)およびCHAP Responseが送信される。

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

手順(j)：AAAからPDSNへ、認証結果（成功または失敗）および必要に応じてTE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)：認証が成功するとPDSNからATへ、PDSNが使用するIPアドレス「x」およびTEが使用するIPアドレス「y」が送信される（Success）。認証失敗時には、図８に関して後述するフォーマットのパケットが送信される（Failure）。

手順(l)：認証が成功した場合には、ATからTEに対して、PDSNにおいてIPアドレス「x」を使うことが要求される。
手順(m)：アドレスを割り当てられていないTEが、IPアドレス「0.0.0.0」を使いたいことをPDSNへ要求する。このメッセージも、PDSNに代わってATにより受信される。
手順(n)：ATがTEに対して、IPアドレスとして「y」を使うことを、PDSNに代わって要求する。
手順(0)：TEはPDSNがIPアドレス「x」を使うことを了承する。このメッセージもPDSNに代わってATにより受信される。
手順(p)：TEは自身のIPアドレスとして「y」を使うことをPDSNに要求する。このメッセージもPDSNに代わってATにより受信される。
手順(q)：ATはTEがIPアドレス「y」を使うことを了承する。この後、TE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応答する。

【００２０】

なお、TEとATとの間でのPPPシーケンスが失敗した場合には、その時点でATからPDSNに対して、後に図８に関して説明するフォーマットでメッセージが送信される（Failure）。また、TEとATとの間で全てのシーケンスが成功した場合には、ATがPDSNに対して、後に図７に関して詳述するフォーマットのメッセージを送信してもよい。

【００２１】

このように、本実施形態によれば手順(a)～(d)で実行されるユーザ側の情報端末(TE)によるネットワークの認証に対して、PDSNではなくATが代理で応答する。したがって、この認証に要する時間が短縮されるのみならず、認証要求および認証応答用のメッセージが無線区間を跨がないので、通信資源の節約が可能になる。

【００２２】

さらに、SIPコールでは、手順(m)で実行されるユーザ側からのIPアドレスの要求に対しても、PDSNではなくATが代理で応答するので、この応答に要する時間が短縮されるのみならず、アドレス要求メッセージおよびアドレス応答メッセージが無線区間を跨がないので、通信資源の節約が可能になる。

【００２３】

図２は、cdma2000で規定されているSimple IP(SIP)コールでの認証時に、本発明に係る通信方法の第２実施形態を適用した場合のシーケンスを示した図である。本実施形態では、従来のPAPから冗長な手順を省略することで呼確立までの時間を短縮している。

【００２４】

手順(a)：TEからにPDSNに対してPAPによる認証が要求される。このメッセージはPDSNに代わってATにより受信される。
手順(b)：ATからTEに対してCHAPによる認証が要求され、かつPDSNが受信可能な最大パケットサイズMRU（予めATに設定されている）がTEに伝達される。
手順(c)：ATがPDSNに代わってPAPによる認証を了承する。
手順(d)：TEからにPDSNに対してPAPによる認証が要求される。このメッセージも、PDSNに代わってATにより受信される。
手順(e)：ATがPDSNに代わってPAPによる認証を要求する。
手順(f)：TEがPDSNに対してPAPによる認証を了承する。このメッセージも、PDSNに代わってATにより受信される。
手順(g)：PDSNがCHAP認証のためのchallengeメッセージをATへ送信する。送信タイミングは手順(g)以前であればいつでもよい。
手順(h)：TEはユーザ名(username)とパスワード(password)をPDSNに送信する。このメッセージも、PDSNに代わってATにより受信される。
手順(i)：ATがTEのユーザ名(username)とパスワード(password)をPDSNに送信する。
手順(j)：PDSNはPAPによる認証と認識し、認証用プロトコルを用いてAAAサーバにユーザ名(username)とパスワード(password)を送信する。
手順(k)：AAAサーバは認証用プロトコルを用いて認証結果（成功または失敗）および必

要に応じてTEが利用するIPアドレス「y」をPDSNに送信する。
手順(l)：PDSNは認証成功時に、PDSNのIPアドレス「x」およびTEが使用するIPアドレス「y」をATに送信する（Success）。認証失敗時には、図８に関して後述するフォーマットのパケットを送信する（Failure）。
手順(m)：ATがPDSNに代わって、認証結果をTEへ送信する。
手順(n)：認証が成功した場合には、ATがPDSNに代わって、IPアドレスとして「x」を使うことをTEに要求する。
手順(o)：アドレスを割り当てられていないTEは、IPアドレスとして「0.0.0.0」を使うことをPDSNに要求する。このメッセージも、PDSNに代わってATにより受信される。
手順(p)：ATはTEに対して、IPアドレスとして「y」を使うことを要求する。
手順(q)：TEはPDSNがIPアドレス「x」を使うことを了承する。このメッセージも、PDSNに代わってATにより受信される。
手順(r)：TEはIPアドレスとして「y」を使うことをPDSNに要求する。このメッセージも、PDSNに代わってATにより受信される。
手順(s)：ATはTEがIPアドレス「y」を使うことを了承する。この後、TE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応答する。

【００２５】

TEとAT間でのPPPのシーケンスが失敗した場合には、その時点でATからPDSNに対してメッセージを送信する（Failure）。また、TEとAT間で全てのシーケンスが成功した場合には、ATがPDSNにメッセージを送信してもよい。

図３は、前記図１の手順(e)および図２の手順(g)において、PDSNからATへ送信されるCHAP Challengeメッセージのパケットフォーマットを示した図であり、図４は、従来の標準PPPにおけるCHAP Challengeメッセージのパケットフォーマットを示している。

【００２６】

本発明では、無線区間を跨ぐパケットのフォーマットとしてCHAP、PAP、Success、Failureの4種類（タイプ）が定義されれば十分なので、先頭の２ビットをタイプの識別に利用する。このため、標準のPPPフォーマットでは必要であったCodeフィールが不要となり、その代わりに当該１バイト分の領域に、タイプ(Type）と圧縮情報（NAI compression）とが登録される。

【００２７】

前記タイプ領域には、当該パケットが前記CHAP、PAP、SuccessおよびFailureのいずれに関するものであるかを示す情報が登録される。圧縮情報領域には、Nameに格納されているデータが、後に詳述する圧縮データであるか否かが登録される。

【００２８】

また、本実施形態ではIDとして要求／応答メッセージで同じ値を使えばよいのでPDSNで管理する必要がない。さらに、全てのPPPパケットはPCF－PDSN間においてR－Pコネクション上を流れ、かつR－Pコネクションは接続AT毎にユニークに識別されるため、PDSNにおいてIDがなくても曖昧さはなく、省略可能である。Lengthはパケット全体（Code～Nameの最後まで）の長さを格納するが、Nameを除いて可変なのはChallenge Valueであり、これはValue-sizeに格納されているのでLengthフィールドが省略されても曖昧さはない。さらに、本発明ではTEがPDSNを認証しないので、最後のNameが利用されることはない。

【００２９】

以上の観点から、CHAP Challengeメッセージのパケットフォーマットが、本発明（図３）では従来の標準PPP（図４）との比較において、IDフィールドの１byte、Lengthフィールドの２byteおよびNameフィールドの３byteだけ短くできるので、合計で６byte分だけ短くなる。

【００３０】

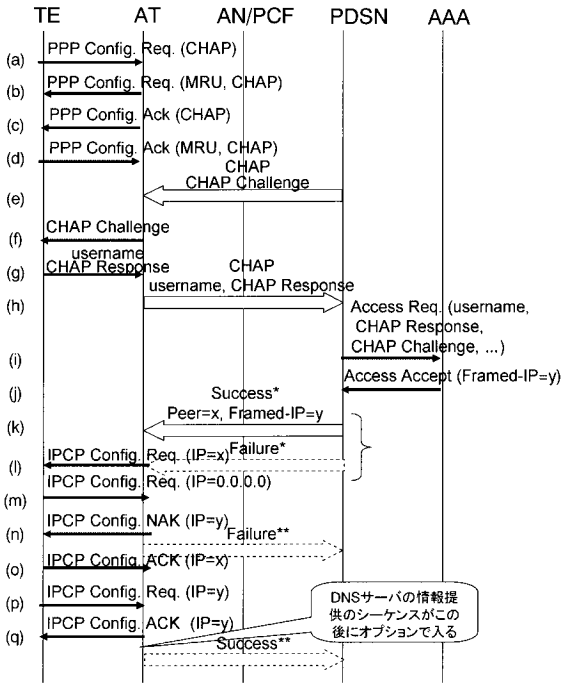
図５は、前記図１の手順(h)において、ATからPDSNへ送信されるCHAP Responseメッセージのパケットフォーマットを示した図であり、図６は、従来の標準PPPにおけるCHAP Responseメッセージのパケットフォーマットを示した図である。

【００３１】
ここでも、前記CHAP Challengeメッセージの場合と同様にCodeフィールドがタイプ領域や圧縮情報領域として利用される。また、CHAP Response値は16バイトと固定なのでValue-sizeは不要である。ただし、NameにはTEのユーザ名が入り、これは可変なのでName-sizeは必須である。
【００３２】
以上の観点から、CHAP Responseメッセージのパケットフォーマットが、本発明（図５）では従来の標準PPP（図６）との比較において、IDフィールドの１byte、Lengthフィールドの２byteおよびValue-sizeフィールドの１byteだけ短くでき、Name-sizeの１byteが増えるので、合計で３byte分だけ短くなる。
【００３３】
図７は、前記図１の手順(k)および図２の手順(l)において、PDSNからATへ送信されるメッセージ（Success）のパケットフォーマットを示した図である。PPPのシーケンスでTEが必要とする値はPDSNのIPアドレス(TEにとってはゲートウェイアドレス)、TEが利用するIPアドレス(Framed-IP)ならびに第１(primary)および第２(secondary) DNSサーバIPアドレスであり、これらを一括してPDSNからATへ送信する。本実施形態ではIPv4を仮定し、アドレスの長さを全て４オクテットとしているので、パケット長が定義されていなくても曖昧さはない。
【００３４】
図８は、前記メッセージ（Success）と選択的に送信されるメッセージ(Failure)のパケットフォーマットを示した図であり、任意に定める失敗の原因を示す識別子がReason Codeフィールドに格納される。
【００３５】
図９は、前記図２の手順(i)において、ATからPDSNへ送信されるPAP Requestメッセージのパケットフォーマットを示した図であり、図１０は、従来の標準PPPにおけるPAP Requestメッセージのパケットフォーマットを示した図である。
【００３６】
ここでも、前記CHAP Challengeメッセージの場合と同様に、IDフィールドおよびLengthフィールドが省略されているので、パケット長を合計で３byte分だけ短くできる。
【００３７】
次いで、上り方向（ATからPDSN方向）の情報量を削減するために、図５に関して説明したCHAP ResponseのNameフィールド、および図９に関して説明したPAP RequestのUsernameフィールドに挿入されるNAI (Network Access Identifier)のデータ量を圧縮するアルゴリズムに関して説明する。
【００３８】
本実施形態では、図１２に示したように、全アルファベット２６文字の各大文字[A～Z]および各小文字[a～z]、ならびに「０」～「９」の１０個の整数を合わせた計６２文字を、６ビットで表記できる６４種類のコード0x00（0xは１６進表記の略）～0x3fのうちの６２種類0x00～0x3dと一義的に対応付ける第１のコード表と、図１３に示したように、英数字および記号等を８ビットで表記される0x00～0x7fのアスキーコードと一義的に対応付ける第２のコード表と、図１４に示したように、使用頻度の高い「ezweb.ne.jp」、「yahoo.com」あるいは「dion.ne.jp」等の所定の文字列を８ビットで表記される0x80～0xffの各コードと一義的に対応付ける第３のコード表とが予め用意されている。
【００３９】
また、本実施形態では、前記６４種類のコードのうちの前記６２種類のコード以外の２つのコード「0x3f」，「0x3e」を、それぞれ第１および第２の特殊コードと定義した。そして、前記第２のコード表および第３のコード表に基づいて変換されたコード0x00～0x7f，0x80～0xffには、これを他のコードと識別するために第２の特殊コード「0x3e」を直前に付加するものとし、「@」および「．（ピリオド）」はいずれも第１の特殊コード「0x3f」と対応付けるものとした。

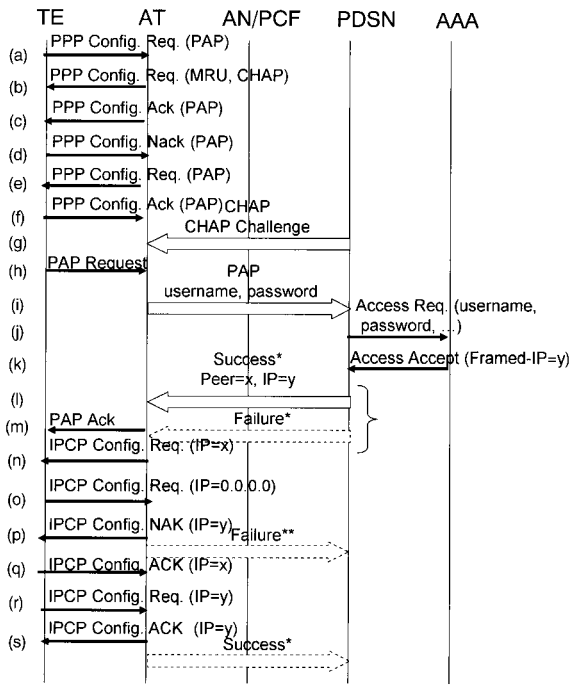
【００４０】
図１５は、本実施形態による圧縮方法の一例を模式的に表現した図であり、ここでは、識別情報「yokota@yahoo.com」のコード化を考える。
【００４１】
「yokota」の各アルファベットは、前記図１２に示した第１のコード表に基づいて、それぞれ６ビットコード[0x18(＝y)], [ox0e(＝o)], [0x0a(＝k)], [0x0e(＝o)], [0x13(＝t)], [0x00(＝a)]にコード化される。「@」は第１の特殊コード[3f]にコード化される。「yahoo.com」は、図１４に示した第３のコード表に基づいて８ビットコード(0x81)にコード化され、その直前には、当該コード(0x81)が前記第３のコード表に基づいてコード化されていることを示す前記第２の特殊コード[0x3e]が付与される。この結果、全データ量は６bitsコードが８個と８bitsコードが１個の計５６bits（＝７octet）となる。これに対して、全文字列を従来通りに全てアスキーコードで表現すると、１６文字分の１６octetとなる。したがって、本実施形態によれば４３．７５％（７／１６）の圧縮率が得られる。
【００４２】
図１６は、本実施形態による圧縮方法の他の一例を模式的に表現した図であり、ここでは、「@」および「．（カンマ）」を同時に含む文字列「××@××．××．××」（×は任意の文字・数字・記号）のコード化を考える。
【００４３】
本実施形態では、上記したように「@」に対して６ビットの第１特殊コード[0x3f」を割り当てると共に、「．（ピリオド）」に対しても同一コード[0x3f」を割り当てる。そして、デコード時には、最初に表れた第１特殊コード[0x3f」、すなわち表記順で最も左側の第１特殊コード[0x3f」のみを「@」に変換し、それ以降の第１特殊コード[0x3f」は、全て「．」に変換するようにしている。このようにすれば、「@」および「．」に同一の特殊コード[0x3f」を割り当てても、両者を確実に識別することができる。
【００４４】
図１７は、本実施形態による圧縮方法のさらに他の一例を模式的に表現した図であり、ここでは、複数個の「@」を含む文字列「××@××@××．××．××」の圧縮を考える。
【００４５】
図１６に関して説明した変換方法では、「@」が複数含まれる場合にそれぞれを区別できない。そこで本実施形態では、最後に表れる「@」以外にはアスキーコードを割り当て、最後に表れる「@」に対してのみ、前記と同様に第１特殊コード[0x3f」を割り当てるようにしている。このようにすれば、複数個の「@」を含む文字列も同様にコード化できるようになる。
【００４６】
なお、上記のようにしてコード化された識別情報を含むパケットを受信し、これをデコードする場合には、上記とは逆に、前記６２種類に属する６ビットコードは前記第１のコード表に基づいてデコードし、前記第１特殊コード[0x3f」は、その出現位置に基づいて、最初の第１特殊コードは「@」にデコードし、二番目以降の第１特殊コードは全て「．」にデコードする。前記第２特殊コード[0x3e」に続くアスキーコード（0x00～0x7f）は、前記第２のコード表に基づいてデコードし、前記第２特殊コード[0x3e」に続く８ビットコード（0x80～0xff）は、前記第３のコード表に基づいてデコードする。
【図面の簡単な説明】
【００４７】
【図１】本発明に係る呼確立手順（CHAPによる認証）の第１実施形態のシーケンスを示した図である。
【図２】本発明に係る呼確立手順の（PAPによる認証）第２実施形態のシーケンスを示した図である。
【図３】本発明におけるCHAP Challengeメッセージのパケットフォーマットを示した図で

ある。
【図４】従来の標準PPPにおけるCHAP Challengeメッセージのパケットフォーマットを示した図である。
【図５】本発明におけるCHAP Responseメッセージのパケットフォーマットを示した図である。
【図６】従来の標準PPPにおけるCHAP Responseメッセージのパケットフォーマットを示した図である。
【図７】PDSNからATへ送信されるメッセージ（Success）のパケットフォーマットを示した図である。
【図８】PDSNからATへ送信されるメッセージ（Failure）のパケットフォーマットを示した図である。
【図９】ATからPDSNへ送信されるPAP Requestメッセージのパケットフォーマットを示した図である。
【図１０】従来の標準PPPにおけるPAP Requestメッセージのパケットフォーマットを示した図である。
【図１１】本発明に係る呼確立手順が適用されるパケット網のネットワーク構成を示した図である。
【図１２】NAI の符号化／復号化用いられる第１のコード表の一例を示した図である。
【図１３】NAI の符号化／復号化用いられる第２のコード表の一例を示した図である。
【図１４】NAI の符号化／復号化用いられる第３のコード表の一例を示した図である。
【図１５】本実施形態によるNAI の圧縮方法の一例を説明する図である。
【図１６】本実施形態によるNAI の圧縮方法の他の一例を説明する図である。
【図１７】本実施形態によるNAI の圧縮方法の更に他の一例を説明する図である。
【図１８】SIPコールでの認証時にCHAPを採用した場合のシーケンスを示した図である。
【図１９】SIPコールでの認証時にPAPを採用した場合のシーケンスを示した図である。

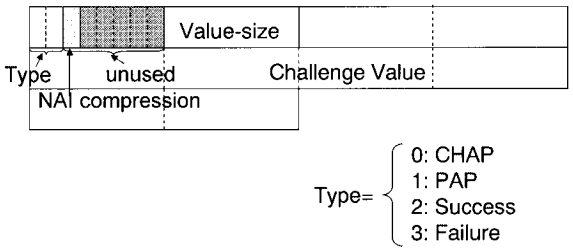
【図１】



【図２】



【図３】

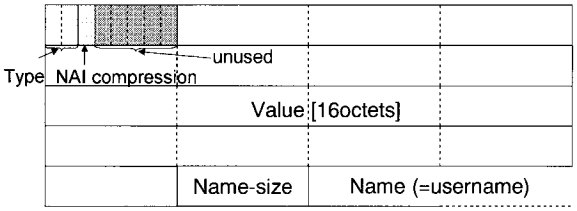


【図４】

標準PPP CHAP Challenge

Code	ID	Length
Value-size	Challenge Value	
	Name	

【図５】

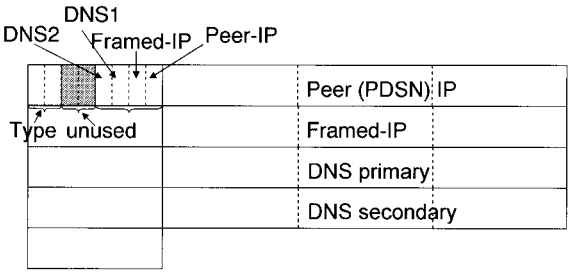


【図６】

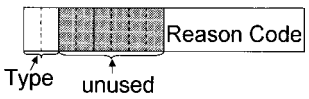
標準PPP CHAP Response

Code	ID	Length
Value-size	Value (CHAP Response)	
	Name(=username)	

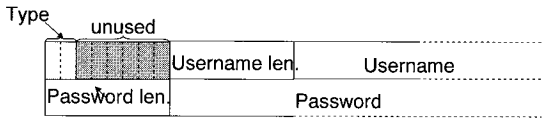
【図７】



【図８】



【図９】

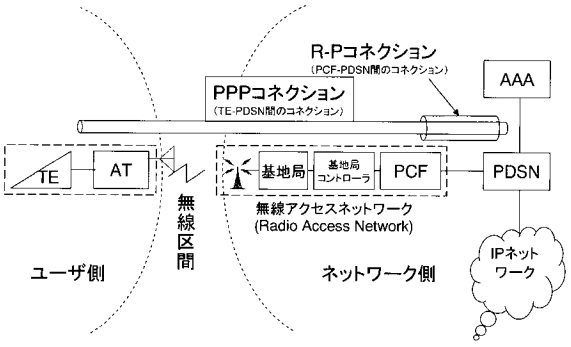


【図１０】

標準PPP PAP Request

Code	ID	Length
Username len.	Username	
Password len.	Password	

【図１１】



【図１２】

00:a	08:i	10:q	18:y	20:G	28:O	30:W	38:4
01:b	09:j	11:r	19:z	21:H	29:P	31:X	39:5
02:c	0a:k	12:s	1a:A	22:I	2a:Q	32:Y	3a:6
03:d	0b:l	13:t	1b:B	23:J	2b:R	33:Z	3b:7
04:e	0c:m	14:u	1c:C	24:K	2c:S	34:0	3c:8
05:f	0d:n	15:v	1d:D	25:L	2d:T	35:1	3d:9
06:g	0e:o	16:w	1e:E	26:M	2e:U	36:2	3e:
07:h	0f:p	17:x	1f:F	27:N	2f:V	37:3	3f:

第１のコード表

【図１３】

00:		30:0	41:A	61:a	
01:		31:1	42:B	62:b	
02:		32:2	43:C	63:c	
		33:3	44:D	64:d	
		34:4	45:E	65:e	
・ ・ ・	・ ・	・ ・ ・	・ ・ ・	・ ・ ・	7f:・

第２のコード表

【図１４】

80: .ezweb.ne.jp
81: .yahoo.com
82: .dion.ne.jp
83: .co.jp
84: .jp

第３のコード表

【図１５】

yokota@yahoo.com

⇩

[0x18] [0x0e] [0x0a] [0x0e] [0x13] [0x00] [0x3f] [0x3e] (81).

「y」 「o」 「k」 「o」 「t」 「a」 「@」 「yahoo.com」

=6bits × 8 + 1octet = 7octets

[ ] : 6bits
( ) : 8bits

圧縮率 7/16 = 43.75%

【図１６】

XX@XX.XXX.XX

⇩

・・・ [0x3f] ・・・ [0x3f] ・・・ [0x3f] ・・・

・・・ 「@」 ・・・ 「.」 ・・・ 「.」 ・・・

【図１７】

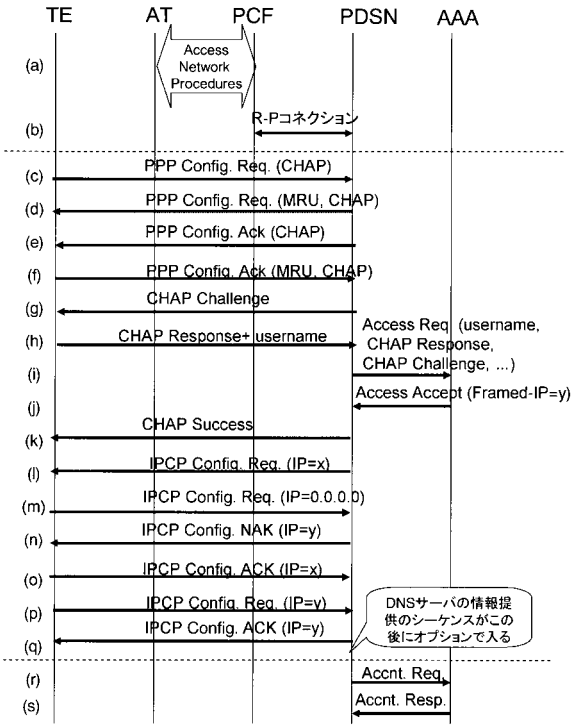
XX@XX@XX.XXX.XX

⇩

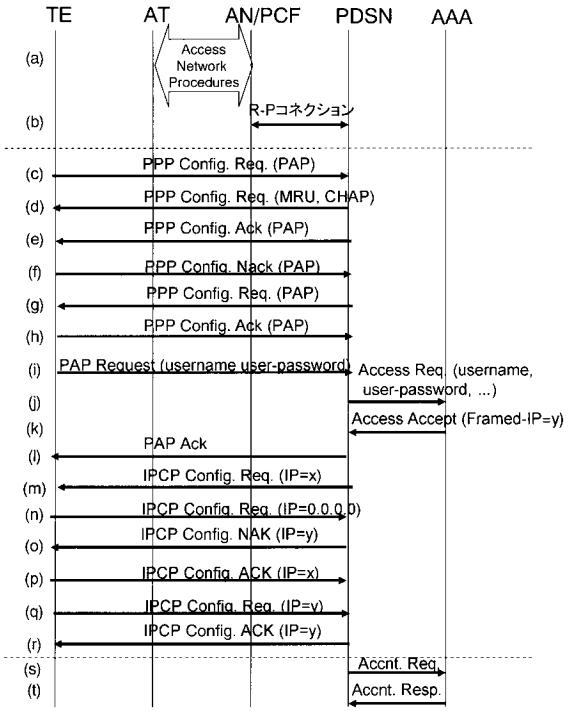
・・・ [0x3e] [0x40] ・・・ [0x3f] ・・・ [0x3f] ・・・ [0x3f] ・・・

・・・ 「@」 ・・・ 「@」 ・・・ 「.」 ・・・ 「.」 ・・・

【図１８】



【図１９】



フロントページの続き

(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

審査官　衣鳩　文彦

(56)参考文献　特開２００２－２１７９９８（ＪＰ，Ａ）
特開２００３－２３４７８６（ＪＰ，Ａ）
特表２００３－５１６０５８（ＪＰ，Ａ）
濱田　樹欣，ＣＤＭＡ２０００　１ｘＥＶ－ＤＯ　音声とデータを分け最大２．４Ｍビット／秒を実現，日経バイト，２００３年　５月２２日，第241号，p.86～91

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／５６
Ｈ０４Ｌ　２９／０８
Ｈ０４Ｑ　７／３８