(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年12 月9 日 (09.12.2004)

PCT

(10) 国際公開番号
WO 2004/107671 A1

(51) 国際特許分類[7]: H04L 12/46, G06F 13/00

(21) 国際出願番号: PCT/JP2003/006609

(22) 国際出願日: 2003 年5 月27 日 (27.05.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県 川崎市 中原区上小田中4丁目1番1号 Kanagawa (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 織田 壮太郎 (ODA,Sotaro) [JP/JP]; 〒812-0011 福岡県 福岡市 博多区博多駅前三丁目22番8号 富士通九州ディジタル・テクノロジ株式会社内 Fukuoka (JP). 北田 敦史 (KITADA,Atsushi) [JP/JP]; 〒211-8588 神奈川県 川崎市 中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 大菅 義之 (OSUGA,Yoshiyuki); 〒102-0084 東京都 千代田区 二番町８番地２０ 二番町ビル３F Tokyo (JP).

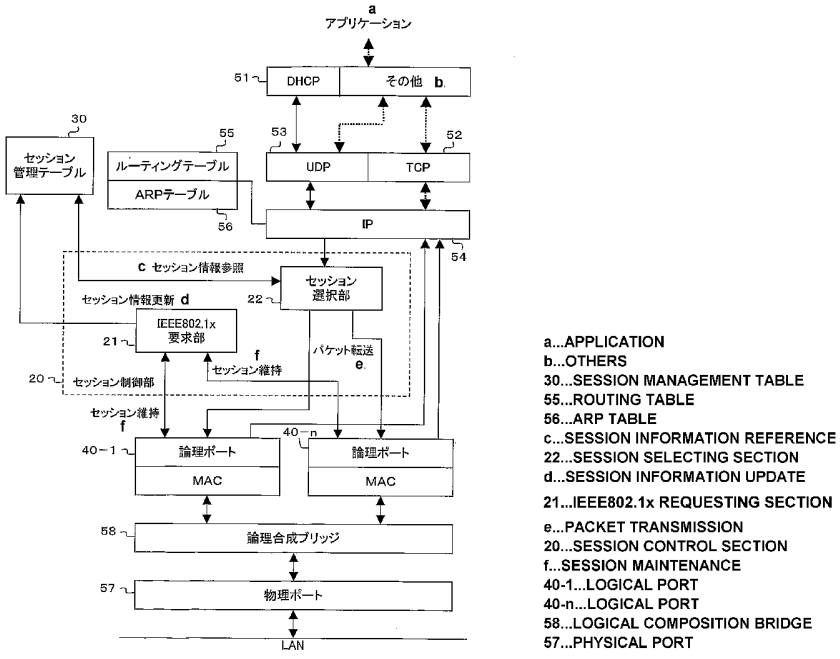
(81) 指定国 (国内): JP, US.

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: COMMUNICATION DEVICE

(54) 発明の名称: 通信装置



a...APPLICATION
b...OTHERS
30...SESSION MANAGEMENT TABLE
55...ROUTING TABLE
56...ARP TABLE
c...SESSION INFORMATION REFERENCE
22...SESSION SELECTING SECTION
d...SESSION INFORMATION UPDATE
21...IEEE802.1x REQUESTING SECTION
e...PACKET TRANSMISSION
20...SESSION CONTROL SECTION
f...SESSION MAINTENANCE
40-1...LOGICAL PORT
40-n...LOGICAL PORT
58...LOGICAL COMPOSITION BRIDGE
57...PHYSICAL PORT

(57) Abstract: An IEEE802.1x requesting section (21), via an unused logical port (40-1 to 40-n), transmits a message for user authentication to an authentication system in order to establish a new session. A session establishment table (30) manages the relationship between the logical port used to transmit the message and a session for which user authentication is successful. When an IP processing section (54) generates a transmission frame, a session selecting section (22) searches the session establishment table (30) according to the content of the frame and finds the corresponding logical port. The MAC address which is allocated to the found logical port is given to the transmission frame as the sender address, and the frame is sent out.

[続葉有]

WO 2004/107671 A1

(57) 要約：ＩＥＥＥ８０２．１ｘ要求部２１は、新たなセッションを確立する際には、未使用の論理ポート４０−１～４０−ｎを介してユーザ認証のためのメッセージを認証システムに送る。セッション確立テーブル３０は、上記メッセージを送出した論理ポートとユーザ認証に成功したセッションとの対応関係を管理する。ＩＰ処理部５４により送信フレームが生成されると、セッション選択部２２は、そのフレームの内容に基づいてセッション確立テーブル３０を検索して対応する論理ポートを検出する。送信フレームは、その送信元アドレスとして上記検出された論理ポートに割り当てられているＭＡＣアドレスが付与されて送出される。

明細書

通信装置

技術分野

本発明は、ネットワークを介して通信を行う通信装置、およびそのためのセッションを確立する方法に係わる。

背景技術

ネットワークのブロードバンド化が進むにつれて、インターネット等の公衆ネットワーク介して提供される通信サービスの種類は増加しつつある。そして、提供される通信サービス毎に、様々なサービスプロバイダ（ｘＳＰ）が誕生している。

一方、各サービスプロバイダは、通常、予め契約をしているユーザに対してのみ特定のサービスを提供する。このため、各サービスプロバイダは、接続を要求してくるユーザの認証を行う必要がある。そして、代表的なユーザ認証システムとして、ＰＰＰｏＥ（Point to Point over Ethernet）システムおよびＩＥＥＥ８０２．１ｘ認証システムが知られている。なお、イーサネット（Ｅｔｈｅｒｎｅｔ）は、登録商標である。

ＰＰＰｏＥは、ＰＰＰのリンク確立手順をイーサネットフレーム上で実行するための仕様（ＲＦＣ２５１６）であり、イーサネット網上でユーザ名やパスワードをチェックする認証機能を含んでいる。そして、ＰＰＰｏＥは、現在、多くのインターネット接続プロバイダ（ＩＳＰ）が提供するＡＤＳＬ（Asymmetric Digital Subscriber Line）接続サービス、或いはＦＴＴＨ（Fiber to the Home）接続サービスにおいて、ユーザ認証およびセッション管理等のための方式として広く普及している。

図１は、ＰＰＰｏＥを導入した通信システムの構成図である。図１において、ユーザ端末１００は、中継局１１０を介してサービスプロバイダ（ＩＳＰ）１２０に接続されている。ここで、サービスプロバイダ１２０は、ルータ装置１２１、ＲＡＤＩＵＳ（Remote Authentication Dial-In User Service）サーバ１２２、および各種サーバ１２３を備えている。また、中継局１１０は、ＤＳＬＡＭ（Digital Subscriber Line Access Multiplexer）１１１、ＢＲＡＳ（Broadband Remote Access Server）１１２などを備えている。そして、ユーザ端末は、ＰＰＰｏＥクライアントとして動作する。また、ＢＲＡＳ１１２は、加入者管理サーバであって、ＰＰＰｏＥサーバとして動作する。なお、ＢＲＡＳ１１２の一形態として、数千～数万ユーザを収容して、ユーザ名およびパスワードをチェック、契約ユーザを指定ＩＳＰに接続する処理、帯域の調整などを行うことができる装置が知られている。

ＰＰＰｏＥにおいては、各フレームに設定される送信元ＭＡＣアドレスおよびセッションＩＤを用いてセッションが識別される。ここで、ＰＰＰｏＥフレームのフォーマットは、図２に示す通りであり、ＰＰＰｏＥ領域の中にセッションＩＤが格納されている。このため、ＰＰＰｏＥによる通信では、ＭＡＣアドレスを１つだけ有するユーザ端末であっても、複数のセッションＩＤを保持することにより、同時に複数のセッションを確立することができる。従って、ユーザ端末１００は、例えば、図３に示すように、複数のサービスプロバイダから並列に複数のサービスを受けることができる。なお、図３に示す例では、サービスプロバイダＡからＨＴＴＰ（Hypertext Transfer Protocol ）サービスを受けながら、サービスプロバイダＢからＶｏＩＰ（Voice over IP ）サービスを受けている。

しかし、ＰＰＰｏＥでは、通信時にデータがＰＰＰでカプセル化されるとともに、各データフレームにある意味で余計なヘッダが付加されるので、処理が

遅くなってしまう。また、中継局のＢＲＡＳにトラヒックが集中するので、同時に多数のセッションが存在する場合には、ＢＲＡＳの負荷が指数関数的に増大してしまう。さらに、ＢＲＡＳ自体が高価であるという問題もある。

このため、近年、ＰＰＰｏＥにかわるユーザ認証システムとして、ＩＥＥＥ８０２．１ｘが注目を集めている。ＩＥＥＥ８０２．１ｘは、ポート単位でアクセスの可否を判断するユーザ認証方式の規格であり、特に、ＩＥＥＥ８０２．１１ｂ等の無線ＬＡＮにおけるユーザ認証のために普及しつつある。なお、ＩＥＥＥ８０２．１ｘは、ＰＰＰｏＥと異なり、通信データの暗号化を行わないので、高速処理が可能である。また、ＩＥＥＥ８０２．１ｘでは、ＰＰＰｏＥで使用される高価なＢＲＡＳのかわりに、比較的安価なレイヤ２スイッチおよびプロキシＲＡＤＩＵＳサーバにより認証を行うことができるので、システム全体として低コスト化が図れる。

図４は、ＩＥＥＥ８０２．１ｘの動作ブロック図を示す。ここでは、ＰＰＰの拡張プロトコルであるＥＡＰ（Extensible Authentication Protocol）をＬＡＮ上で使用できるようにしたシステムが示されている。なお、このようなシステムは、ＥＡＰｏＬ（EAP over LAN）と呼ばれ、様々な認証プロトコルをサポートできる。

上記構成において、アクセス要求ポート（Supplicant Port Access Entity ）から接続要求が発行されると、認証システム（Authentication System ）は、認証サーバ（Authentication Server ）と連携して、その要求についての許可／拒絶を判断する。そして、認証に失敗したポートからの通信を遮断し、認証に成功したポートの通信のみを許可する。なお、現在、多くの認証システムにおいて、アクセス要求ポートのＭＡＣアドレスを用いてユーザ認証を行う機能が実装されている。そして、その認証されたＭＡＣアドレスにより各通信が識別されるようになっている。

ＰＰＰｏＥについては、例えば、下記の特許文献１、２に記載されている。また、ＰＰＰｏＥをＩＥＥＥ８０２．１ｘに置き換えたシステムについては、特許文献２に記載されている。

上述のように、ＩＥＥＥ８０２．１ｘは、ＰＰＰｏＥと比較して様々な有利な効果を有している。しかし、ＩＥＥＥ８０２．１ｘでは、複数のセッションを同時に確立することができない。すなわち、ＩＥＥＥ８０２．１ｘで使用されるフレーム（ここでは、ＥＡＰｏＬフレーム）は、図５に示すように、「セッションＩＤ」が存在しない。そして、ネットワーク側では、各フレームに設定されている送信元ＭＡＣアドレスのみに基づいてセッションを識別する。

このように、ＩＥＥＥ８０２．１ｘでは、各フレームの送信元ＭＡＣアドレスのみに基づいてセッションが識別されるので、１個のネットワークインタフェース（物理ポート）に対して複数のセッションを同時に確立することができない。ここで、一般的な端末装置は、ネットワークインタフェース（物理ポート）を１つしか備えていない。したがって、ＩＥＥＥ８０２．１ｘを使用するシステムでは、各ユーザは、図３に示すようなマルチセッション環境を享受することができない。ＩＥＥＥ８０２．１ｘを利用してユーザ認証が行われるシステムにおける従来の通信形態の一例を図６に示す。

特許文献１

特開２００２－２１７９９８号公報（図１、図３　段落０００３～００２５）

特許文献２

特開２００３－６０６７５号公報（段落０００８～００４６、００７１～００７３）

発明の開示

本発明の目的は、認証システム側の負荷が軽い通信プロトコルを使用しなが

らマルチセッションを実現することである。具体的には、各フレームの送信元アドレスでセッションを識別するプロトコル（例えば、ＩＥＥＥ８０２．１ｘ）において、マルチセッションを実現することである。

本発明の通信装置は、フレームに設定されている送信元アドレスに基づいてセッションが識別されるネットワークを介して通信を行う通信装置であって、上記ネットワークに接続するインタフェース手段と、複数のアドレスを管理する管理手段と、セッション確立要求を含むフレームを上記インタフェース手段を介して上記ネットワーク上に設けられている認証システムに送信する確立要求手段と、上記セッション確立要求を含むフレームの送信元アドレスとして上記管理手段により管理されている複数のアドレスの中の１つを設定するアドレス設定手段、を有する。

この発明において、認証システムは、管理手段により管理されている複数のアドレスの中の１つが設定されたフレームを受信し、そのフレームに格納されているセッション確立要求について許可するか否かを判断する。そして、認証システムにより許可されたセッションは、以降、上記セッション確立要求を含むフレームに設定されていたアドレスにより識別される。他方、本発明の通信装置は、複数のアドレスを有しており、必要に応じてそれらのアドレスを使い分けることができる。したがって、上記インタフェース手段が当該通信装置の唯一のネットワークインタフェースであっても、同時に複数のセッションを確立できる。

本発明の他の態様の通信装置は、フレームに設定されている送信元アドレスに基づいてセッションが識別されるネットワークを介して通信を行う通信装置であって、上記ネットワークに接続する物理ポートと、それぞれ互いに異なるアドレスが付与されている複数の論理ポートと、送信フレームの内容を解析する解析手段と、上記解析手段の解析結果に基づいて上記複数の論理ポートの中

から１つの論理ポートを選択する選択手段、を有する。そして、上記選択手段により選択された論理ポートは、上記送信フレームの送信元アドレスとしてその論理ポートに付与されているアドレスを設定し、上記物理ポートを介して上記ネットワークへ送出する。

この発明においては、送信フレーム毎にそのフレームの内容（例えば、送信元ＩＰアドレス、ポート番号等）に応じて論理ポートが選択される。そして、選択された論理ポートは、送信フレームの送信元アドレスとしてその論理ポートに付与されているアドレスを設定し、物理ポートを介してネットワークへ送出する。ここで、ネットワークは、フレームに設定されている送信元アドレスに基づいてセッションを識別する。したがって、本発明の通信装置は、ネットワークインタフェースとしての物理ポートを１つしか有していなくても、複数の論理ポートを用意することにより、同時に複数のセッションを利用して通信を行うことができる。

図面の簡単な説明

図１は、ＰＰＰｏＥを導入した通信システムの構成図である。

図２は、ＰＰＰｏＥフレームのフォーマットを示す図である。

図３は、ＰＰＰｏＥによるマルチセッションの利用例を示す図である。

図４は、ＩＥＥＥ８０２．１ｘの動作ブロック図である。

図５は、ＩＥＥＥ８０２．１ｘで使用されるフレームのフォーマットを示す図である。

図６は、ＩＥＥＥ８０２．１ｘを利用してユーザ認証が行われるシステムにおける従来の通信形態の一例である。

図７は、本発明の通信装置が接続されるネットワークの一例の構成図である。

図８は、本発明の概念を説明する図である。

図９は、フレーム送出の概略動作を示すフローチャートである。

図１０は、ユーザ端末のブロック図である。

図１１は、セッション管理テーブルの実施例である。

図１２は、セッション管理テーブルを作成する処理を示すフローチャートである。

図１３Ａ～図１３Ｃは、セッション管理テーブルを更新する処理の実施例である。

図１４は、ユーザ認証手順におけるメッセージ交換を示す図である。

図１５は、フレームを送信する処理を示すフローチャートである。

図１６は、送信フレームの一例のフォーマットを示す図である。

図１７は、送信フレームに送信元ＭＡＣアドレスを設定する方法を説明する図（その１）である。

図１８は、送信フレームに送信元ＭＡＣアドレスを設定する方法を説明する図（その２）である。

図１９は、論理ポートの実現方法を説明する図（その１）である。

図２０は、論理ポートの実現方法を説明する図（その２）である。

図２１は、本発明の通信装置を利用した通信の実施例である。

図２２は、本発明の他の適用例を示す図である。

発明を実施するための最良の形態

以下、本発明の実施形態について説明する。

図７は、本発明の通信装置（ここでは、端末装置）が接続されるネットワークの一例の構成図である。なお、図７および上述した図１において共通して使用されている符号は、同じものを指し示している。

ユーザ端末１は、中継局１３０を介してサービスプロバイダ（ＩＳＰ）１２

０に接続されている。ここで、サービスプロバイダ１２０には、ルータ装置１２１、ＲＡＤＩＵＳ（Remote Authentication Dial-In User Service）サーバ１２２、ＤＨＣＰ（Dynamic Host Configuration Protocol ）サーバ１２４、及びコンテンツサーバ等の各種サーバ１２３が設けられている。なお、ルータ装置１２１は、パケットのルーティング処理を行う。また、ＲＡＤＩＵＳサーバ１２２は、ユーザ情報を管理しており、ユーザ名やパスワード等を利用してユーザ認証を行う。さらに、ＤＨＣＰサーバ１２４は、ユーザ端末１からの要求に応じてＩＰアドレスを割り当てるサーバ装置である。

中継局１３０は、ＤＳＬＡＭ（Digital Subscriber Line Access Multiplexer）１１１、レイヤ２スイッチ（Ｌ２ＳＷ）１３１、プロキシＲＡＤＩＵＳサーバ１３２を備えている。ここで、ＤＳＬＡＭ１１１は、多数のｘＤＳＬモデムを収容しており、ｘＤＳＬ回線を多重化する。また、レイヤ２スイッチ１３１は、ＭＡＣアドレスに基づいてフレームを転送する。なお、レイヤ２スイッチ１３１は、ＩＥＥＥ８０２．１ｘをサポートするものとする。さらに、プロキシＲＡＤＩＵＳサーバ１３２は、ＲＡＤＩＵＳサーバ１２２の代わりにユーザ認証手順の少なくとも一部を実行する。

上記システムにおいて、ユーザ認証は、基本的には、中継局１３０に設けられているプロキシＲＡＤＩＵＳサーバ１３２により、またはプロキシＲＡＤＩＵＳサーバ１３２がＲＡＤＩＵＳサーバ１２２と連携することにより行われる。ここで、認証プロトコルは、ＩＥＥＥ８０２．１ｘが採用されているものとする。

図８は、本発明の概念を説明する図である。ここで、アクセス要求物理ポート１１は、ユーザ端末１が備えるネットワークインタフェースとしての通信ポートである。なお、ユーザ端末１は、アクセス要求物理ポート１１を１つだけ備えるものとする。また、認証システムおよび認証サーバは、例えば、図７に

示したプロキシＲＡＤＩＵＳサーバ１３２またはＲＡＤＩＵＳサーバ１２２により実現される。

一般に、端末装置が同時に複数のサービスプロバイダに接続するためには、必要数のセッションを生成して保持しなければならない。ところが、ユーザ認証プロトコルとしてＩＥＥＥ８０２．１ｘが採用されている場合、セッション（ＩＥＥＥ８０２．１ｘセッション）は、端末装置から送出されるフレームの送信元ＭＡＣアドレスのみにより識別される。また、１つの通信ポートには、通常、ＭＡＣアドレスが１つだけ割り当てられている。したがって、端末装置が備える通信ポートが１つのみの場合は、その端末装置装置は、１つのセッションしか保持できず、同時に複数のサービスプロバイダに接続できないこととなる。

そこで、本発明では、１つの物理ポートに対して複数の論理ポートを用意して、各論理ポートに対して互いに異なるＭＡＣアドレスを割り当てている。図８に示す例では、１つのアクセス要求物理ポート１１に対して複数のアクセス要求論理ポート１２－０～１２－３が用意されている。そして、各アクセス要求論理ポート１２－０～１２－３に対して、それぞれＭＡＣアドレス０～ＭＡＣアドレス３が割り当てられている。なお、これらのＭＡＣアドレスは、グローバルにユニークなアドレスとするためには、通信ポートの製造者から取得する必要があるが、ＬＡＮ等において使用するプライベートアドレスである場合には、任意の値を選ぶことができる。

また、ユーザ端末１は、論理ポートごとにセッションを保持する機能を持っている。そして、異なるサービスプロバイダに接続する際には、異なる論理ポートを介してフレームが送出される。このとき、各論理ポートには、互いに異なるＭＡＣアドレスが割り当てられており、各論理ポートは、送信すべきフレームの送信元アドレスとして、その論理ポートに割り当てられているＭＡＣア

ドレスを挿入する。たとえば、アクセス要求論理ポート１２－０を介してフレームを送出する際には、そのフレームの送信元アドレスとして「ＭＡＣアドレス０」が設定され、アクセス要求論理ポート１２－１を介してフレームを送出する際には、そのフレームの送信元アドレスとして「ＭＡＣアドレス１」が設定される。

従って、認証システムにとっては、実際には１台のユーザ端末のみが接続されている場合であっても、複数のクライアント装置が接続されているように見えることになる。すなわち、認証プロトコルとしてＩＥＥＥ８０２．１ｘが採用されている場合であっても、１台のユーザ端末でマルチセッションを実現することができる。

図９は、ユーザ端末１がフレームを送出する動作の概略を示すフローチャートである。ここでは、上位レイヤのソフトウェアにより、フレーム送信要求が生成された後の動作を示す。

ステップＳ１では、接続先のセッションを判別する。ここで、接続先のセッションは、例えば、送信しようとするフレームのペイロードを解析することにより判断される。ステップＳ２では、判別されたセッションに対応する論理ポートを検出し、送信しようとするフレームをその論理ポートへ送る。また、ステップＳ３では、判別されたセッションに対応するＭＡＣアドレスを検出する。なお、各論理ポートに対して対応するＭＡＣアドレスが固定的に割り当てられている場合には、ステップＳ２およびＳ３の処理は、実質的に、１つの処理として実行される。

ステップＳ４では、送信しようとするフレームの送信元ＭＡＣアドレスとしてステップＳ３で検出したＭＡＣアドレスを挿入する。なお、この処理は、たとえば、ステップＳ２で検出された論理ポートにより行われる。ステップＳ５では、物理ポートに接続する。そして、ステップＳ６において、そのフレーム

をネットワークに送出する。

このように、ユーザ端末１は、接続先のセッションを判別すると、そのセッションに対応するＭＡＣアドレスを送信元ＭＡＣアドレスとして設定したフレームをネットワークに送出する。そして、ネットワーク上に設けられている通信装置は、このフレームの送信元ＭＡＣアドレスに基づいてセッションを識別し、そのフレームをそのセッションに対応する装置へ転送する。このとき、ユーザ端末１は、複数の論理ポートを備え、複数のＭＡＣアドレスを使用できる。また、ネットワーク上の通信装置は、ＭＡＣアドレス毎にセッションを識別する。よって、マルチセッションを実現することができる。すなわち、ユーザ端末１は、通信ポートを１つだけ備える構成であっても、同時に複数のサービスプロバイダに接続できる。

図１０は、ユーザ端末１のブロック図である。なお、ここでは、主に、通信処理を行う部分（特に、ＩＥＥＥ８０２．１ｘクライアントとして動作する部分）のブロック図が描かれている。

ユーザ端末１の特徴的構成は、セッション制御部２０、セッション管理テーブル３０、複数の論理ポート４０－１～４０－ｎを備えることであり、他の部分は既存の技術により実現可能である。すなわち、ＤＨＣＰクライアント部５１は、ＤＨＣＰサーバからＩＰアドレスを取得する。ＴＣＰ処理部５２およびＵＤＰ処理部５３は、それぞれＴＣＰおよびＵＤＰに従ってパケットの分解／組立などを行う。ＩＰ処理部５４は、ルーティングテーブル５５およびＡＲＰ（Address Resolution Protocol ）テーブル５６を備え、ルーティング処理等を行う。

物理ポート５７は、ネットワークとのインタフェースであり、通信回線が接続される。なお、論理合成ブリッジ５８は、フレームを送信する際には、バッファとして動作する。また、物理ポート５７を介してネットワークから受信し

たフレームのＭＡＣアドレスを解析し、そのフレームを対応する論理ポートに転送する処理を行う。

セッション制御部２０は、ＩＰ処理部５４において作成されたフレームを、接続すべきセッションに対応する論理ポートに転送する。ここで、ＩＥＥＥ８０２．１ｘ要求部２１は、ＩＥＥＥ８０２．１ｘによるセッション確立手順を実行する機能に加え、セッション管理テーブル３０により管理されているセッション情報を更新する機能を備えている。一方、セッション選択部２２は、ＩＰ処理部５４において作成されたフレームの内容を解析し、その解析結果を検索キーとしてセッション管理テーブル３０を参照する。そして、その参照結果に基づいて、ＩＰ処理部５４において作成されたフレームを対応する論理ポート４０－１～４０－ｎに転送する。

セッション管理テーブル３０は、後で詳しく説明するが、１または複数のセッションを管理するためのセッション情報を格納する。論理ポート４０－１～４０－ｎは、それぞれ論理的な通信ポートであり、それぞれＭＡＣアドレスが割り当てられている。

このように、ユーザ端末１において、論理ポート４０－１～４０－ｎは、ＯＳＩ階層モデルの第３層のプロトコル（ここでは、ＩＥＥＥ８０２．１ｘ、ＩＰ）と、物理ポートとの間に設けられている。そして、各論理ポート４０－１～４０－ｎには、互いに異なるＭＡＣアドレスが割り当てられている。このため、論理ポート４０－１～４０－ｎは、上位プロトコル（アプリケーションを含む）から見ると、互いに独立したネットワークインタフェースとして動作する。

なお、ネットワークインタフェースの初期化処理では、まず、ＤＨＣＰクライアント部５１が、使用すべき論理ポートのためにＩＰアドレスを取得する。続いて、ＩＰ処理部５４が、ルーティングテーブル５４およびＡＲＰテーブル

５６を初期化する。さらに、その後、ＩＥＥＥ８０２．１ｘ要求部２１は、使用すべき論理ポートを介して行う通信のためのセッションの確立を要求する。そして、セッションの確立が許可されると、ＩＥＥＥ８０２．１ｘ要求部２１は、その許可されたセッションに係わるセッション情報をセッション管理テーブル３０に書き込む。なお、セッション確立手順は、後述するが、ＩＥＥＥ８０２．１ｘの仕様に準拠するものとする。

図１１は、セッション管理テーブル３０の実施例である。図１１において、「割当て条件」としては、送信フレームを接続すべきセッションを選択するためのキーワードが記述される。具体的には、たとえば、認証システムにより許可された通信を特定する情報（通信条件：送信元ＩＰアドレス、ポート番号など）が格納される。「セッションＩＤ」は、各セッションを識別する識別番号である。ただし、このセッションＩＤは、ＩＥＥＥ８０２．１ｘにおいて定義されているものではなく、ユーザ端末１の内部で使用される。

「論理ポート番号」は、選択したセッションを割り当てるべき論理ポートを識別する。「ＭＡＣアドレス」には、確立されたＩＥＥＥ８０２．１ｘセッションに割り当てるべきＭＡＣアドレスが記述される。

「有効／無効表示」は、登録されているＭＡＣアドレスが有効であるか否かを表示する（有効：１、無効：０）。また、「セッション確立表示」は、各セッションの利用状況を表示する（使用中：１、未使用：０）。

図１２は、セッション管理テーブル３０を作成する処理を示すフローチャートである。ここでは、ユーザ端末１が新たな通信を開始するものとする。そして、新たな通信を開始する際には、上位レイヤのソフトウェアにより、セッション確立要求が生成されるものとする。

ステップＳ１１においてセッション確立要求の発生を検出すると、ステップＳ１２以降の処理が実行される。ステップＳ１２～Ｓ１６では、セッション管

理テーブル３０を先頭から順番に各エントリを参照してゆき、ＭＡＣアドレスが有効であり且つセッションが確立されていないエントリを探す。すなわち、ステップＳ１２において、先頭エントリが参照される。続いて、ステップＳ１３およびＳ１４では、それぞれ「有効／無効表示」および「セッション確立表示」が調べられる。なお、ステップＳ１５およびＳ１６は、テーブル内のエントリを順番に参照する処理である。また、ＭＡＣアドレスが有効であり且つセッションが確立されていないエントリが検出されなかった場合は、ステップＳ２２において、新たなセッションを確立することができないと判断する。

ＭＡＣアドレスが有効であり且つセッションが確立されていないエントリが検出されると、ステップＳ１７において、このエントリ内にセッション確立要求に係わる「割当て条件」を設定する。続いて、ステップＳ１８では、ＩＥＥＥ８０２．１ｘ認証を行う。なお、ＩＥＥＥ８０２．１ｘ認証自体は、公知のプロトコルである。ただし、ここでは、ステップＳ１２～Ｓ１６において検出したエントリに登録されているＭＡＣアドレスを用いて論理ポートが作成され、その論理ポートを介してユーザ認証のためのメッセージの送受信が行われる。したがって、このＩＥＥＥ８０２．１ｘ認証においてユーザ端末１から認証システムに送信されるフレームの送信元ＭＡＣアドレスとしては、上記エントリに登録されているＭＡＣアドレスが使用されることになる。

ステップＳ１９では、認証システムからＩＥＥＥ８０２．１ｘ認証の結果を受信する。そして、認証に成功した旨の通知を受信した場合は、ステップＳ２０において、ステップＳ１８の認証手順で使用した論理ポートを識別する情報を、セッション管理テーブル３０の「論理ポートＩＤ」に設定する。さらに、ステップＳ２１において「セッション確立表示＝使用中（確立)」を設定する。なお、認証に失敗した旨の通知を受信した場合は、ステップＳ２２において、新たなセッションを確立することができないと判断する。

次に、図１３Ａ～図１３Ｃを参照しながら、新たなセッションの確立に伴ってセッション管理テーブル３０を更新する手順を説明する。なお、ここでは、図１３Ａに示すように、ユーザ端末１が３個のＭＡＣアドレス（a0b0c0d0e0f0、a1b1c1d1e1f1、a2b2c2d2e2f2）を使用できるものとする。また、現時点では、まだ、セッションが１つも確立されていないものとする。したがって、各エントリの「セッション確立表示」には、それぞれ「０」が書き込まれている。また、各エントリの「割当て条件」および「論理ポートＩＤ」には、それぞれ未設定であることを表す値として「－１」が書き込まれている。

この状態において、ユーザが、ホームページの閲覧を開始するものとする。この場合、ＩＥＥＥ８０２．１ｘ要求部２１は、まず、図１３Ａに示すセッション管理テーブルから「有効／無効表示＝１」かつ「セッション確立表示＝０」であるエントリを検出する。ここでは、第１番目のエントリが検出されたものとする。続いて、そのエントリの「割当て条件」として、ホームページを閲覧するためのプロトコルに対応するポート番号「８０：ｈｔｔｐ」を書き込む。さらに、認証システムに対してユーザ認証を依頼する。このとき、ＩＥＥＥ８０２．１ｘ認証に係わるメッセージを認証システムに送るためのフレームの送信元ＭＡＣアドレスとして、上記エントリに登録されているＭＡＣアドレス「a0b0c0d0e0f0」が設定される。

ユーザ認証が成功すると、セッションが確立される。そして、上記エントリにおいて「論理ポートＩＤ」が設定されると共に、「セッション確立表示」に「１」が書き込まれる。この結果、セッション管理テーブル３０は、図１３Ｂに示す状態に更新される。

この後、ユーザは、ｈｔｔｐに係わるセッションを維持したままメール送信を行う場合には、同様のセッション確立手順が実行される。ただし、今回は、ＩＥＥＥ８０２．１ｘ認証に係わるメッセージを認証システムに送るためのフ

レームの送信元ＭＡＣアドレスとして、第２番目のエントリに登録されているＭＡＣアドレス「a1b1c1d1e1f1」が使用される。また、そのエントリの「割当て条件」として、「２５：ｓｍｔｐ」が書き込まれる。そして、この結果、セッション管理テーブル３０は、図１３Ｃ示す状態に更新される。このように、セッション管理テーブル３０は、同時に存在する複数のセッションを管理できる。

図１４は、ユーザ認証手順におけるメッセージ交換を示す図である。なお、この手順は、基本的に、ＩＥＥＥ８０２．１ｘの仕様に従う。また、この処理は、図１２のステップＳ１８に相当する。

ユーザ端末１は、ＩＳＰ－１にアクセスするために第１番目のセッションを確立する際には、例えば、論理ポート０を介して認証システム（プロキシＲＡＤＩＵＳサーバ１３２、および対応するＩＳＰ－１のＲＡＤＩＵＳサーバ）との間でメッセージを送受信する。

ユーザ端末１から認証システムへＥＡＰＯＬ（Extensible Authentication Protocol over LAN）開始メッセージが送信されると、プロキシＲＡＤＩＵＳ１３２は、ＥＡＰ要求メッセージを用いてユーザＩＤを要求する。これに対して、ユーザ端末１がユーザＩＤを送信すると、プロキシＲＡＤＩＵＳサーバ１３２およびＲＡＤＩＵＳサーバは、そのユーザＩＤをチェックする。続いて、プロキシＲＡＤＩＵＳサーバ１３２は、ＥＡＰ要求メッセージを用いてパスワード（ＯＴＰ：One Time Password）を要求する。これに対して、ユーザ端末１がパスワードを送信すると、プロキシＲＡＤＩＵＳサーバ１３２およびＲＡＤＩＵＳサーバは、そのパスワードをチェックする。そして、これらのユーザＩＤおよびパスワードについてのユーザ認証が成功すると、プロキシＲＡＤＩＵＳサーバ１３２は、ユーザ端末１へＥＡＰ成功メッセージを送る。

上記認証手順において、ユーザ端末１は、論理ポート０を介してＥＡＰＯＬ

開始メッセージおよびＥＡＰ応答メッセージをプロキシＲＡＤＩＵＳサーバ１３２へ送信する。このため、これらのメッセージを格納するフレームの送信元ＭＡＣアドレスとしては、論理ポート０に割り当てられているＭＡＣアドレスが使用される。そして、プロキシＲＡＤＩＵＳサーバ１３２は、送信元ＭＡＣアドレスとしてこのＭＡＣアドレスが設定されているフレームをＩＳＰ－１転送するための情報をレイヤ２スイッチ１３１に設定する。

続いて、ユーザ端末１は、ＩＳＰ－２にアクセスするために第２番目のセッションを確立する際には、例えば、論理ポート１を介して認証システム（プロキシＲＡＤＩＵＳサーバ１３２、および対応するＩＳＰ－２のＲＡＤＩＵＳサーバ）との間でメッセージを送受信する。

この手順は、基本的に、第１番目のセッションを確立するための手順と同じである。しかし、今回は、ユーザ端末１は、論理ポート１を介してＥＡＰＯＬ開始メッセージおよびＥＡＰ応答メッセージをプロキシＲＡＤＩＵＳ１３２へ送信する。このため、これらのメッセージを格納するフレームの送信元ＭＡＣアドレスとしては、論理ポート１に割り当てられているＭＡＣアドレスが使用される。そして、プロキシＲＡＤＩＵＳ１３２サーバは、送信元ＭＡＣアドレスとしてこのＭＡＣアドレスが設定されているフレームをＩＳＰ－２転送するための情報をレイヤ２スイッチ１３１に設定する。

尚、認証システム（特に、プロキシＲＡＤＩＵＳサーバ１３２）の動作は、ＩＥＥＥ８０２．１ｘの仕様に従っており、本発明を実施するうえで特に変更を加える必要はない。

次に、既に確立されているセッションを利用してフレームを送信する手順について説明する。

図１５は、フレームを送信する処理を示すフローチャートである。なお、ここでは、図１２～図１３を参照しながら説明した手順によってセッション管理

テーブル３０に１以上のセッションに係わるセッション情報が既に登録されているものとする。また、上位レイヤのソフトウェアにより、セッション接続要求が生成されるものとする。なお、「セッション確立」が新たなセッションを確立することを意味するのに対し、「セッション接続」は、既に確立されているセッションを利用してフレームを送受信することを意味するものとする。

ステップＳ２１においてセッション接続要求の発生を検出すると、ステップＳ２２以降の処理が実行される。ステップＳ２２～Ｓ２７では、セッション管理テーブル３０を先頭から順番に各エントリを参照してゆき、ＭＡＣアドレスが有効であり、セッションが既に確立されており、且つ割当て条件を満たすエントリを探す。ここで、ステップＳ２３、Ｓ２４、Ｓ２６、Ｓ２７の処理は、基本的に図１２に示したステップＳ１３、Ｓ１４、Ｓ１５、Ｓ１６と同じなので、説明を省略する。

ステップＳ２５では、送信フレームの内容を解析し、割当て条件を満たしているか否かを調べる。ここで、送信フレームは、例えば、図１６に示すフォーマットであるものとする。すなわち、イーサネットフレームのペイロードにＩＰデータグラムが格納されており、さらにそのＩＰデータグラムのデータ領域にＴＣＰデータグラムが格納されている。そして、「割当て条件」として「送信元ＩＰアドレス」が設定されている場合には、ＩＰデータグラムのヘッダに設定されている「送信元アドレス」が抽出され、その抽出したアドレスと同じアドレスがセッション管理テーブル３０に登録されているか否かが調べられる。あるいは、「割当て条件」として「ポート番号」が設定されている場合には、ＴＣＰデータグラムのヘッダに設定されている「送信ポート番号または宛先ポート番号」が抽出され、その抽出したポート番号と同じポート番号がセッション管理テーブル３０に登録されているか否かが調べられる。

そして、ＭＡＣアドレスが有効であり、セッションが既に確立されており、

且つ割当て条件を満たすエントリが検出されると、ステップＳ２８において、そのエントリに登録されている論理ポートに送信フレームを渡す。なお、該当するエントリが検出されなかったときは、ステップＳ３２において、接続要求を拒否する。ステップＳ２９では、送信フレームにＭＡＣヘッダを付与する。なお、この処理は、論理ポートにより行われる。また、この処理は、単に、送信元ＭＡＣアドレスを挿入するだけであってもよい。

ステップＳ３０では、ＭＡＣヘッダが付与された送信フレームを物理ポートに渡す。そして、ステップＳ３１において、送信フレームがネットワークに送出される。

このように、ユーザ端末１は、フレームを送信する毎にセッション管理テーブル３０を参照し、そのフレームに対応するセッションを検出する。そして、そのフレームを検出したセッションに対応する論理ポートを介してネットワークに送出する。したがって、各フレームの送信元アドレスとして、それぞれ、接続すべきセッションに対応するＭＡＣアドレスが設定される。

よって、送信元ＭＡＣアドレスに基づいてセッションが識別されるネットワークにおいて、ユーザ端末１は、１つの物理ポートを用いて同時に複数のセッションを確立できる。すなわち、マルチセッションを実現できる。

図１７は、送信フレームに送信元ＭＡＣアドレスを設定する方法を説明する図である。ここでは、送信フレームのＩＰアドレスに基づいてセッションを選択する例を示す。すなわち、ここでは、セッション管理テーブル３０の割当て条件として、ユーザ認証において許可された送信元ＩＰアドレスが登録されているものとする。

ＩＰ処理部５４から出力された送信フレームは、いったんフレームバッファ６０に格納される。そして、ＩＰアドレス解析部７１は、フレームバッファ６０に格納されている送信フレームの送信元ＩＰアドレスを抽出する。なお、送

信元ＩＰアドレスは、例えば、図１６に示すＩＰデータグラムのヘッダに格納されている。続いて、テーブル検索部７２は、ＩＰアドレス解析部７１により抽出されたＩＰアドレスと同じアドレスが「割当て条件」として登録されているエントリを検出する。さらに、フレーム振分け部７３は、テーブル検索部７２により検出されたエントリに登録されている論理ポートに対して、インタフェース処理命令を与える。

インタフェース処理命令を受け取った論理ポートのＭＡＣアドレス挿入部７４は、自分に割り当てられているＭＡＣアドレスをセッション管理テーブル３０に問い合わせる。そして、フレームバッファ６０から送信フレームを読み出し、そのフレームの送信元アドレス領域にセッション管理テーブル３０から取得したＭＡＣアドレスを格納する。インタフェース処理部７５は、ＦＣＳ（Frame Check Sequence）の再計算等を行った後、物理ポートを介して送信フレームをネットワークへ送出する。

このように、この実施例では、送信フレームの送信元ＭＡＣアドレスとして、送信フレームのＩＰアドレスに基づいて一意に決まるＭＡＣアドレスが設定される。

図１８は、送信フレームに送信元ＭＡＣアドレスを設定する他の方法を説明する図である。ここでは、送信フレームのポート番号に基づいてセッションを選択する例を示す。即ち、「割当て条件」として、ユーザ認証において許可されたポート番号がセッション管理テーブル３０に登録されているものとする。

セッション選択部２２および論理ポート４０の構成および動作は、基本的には図１７に示した例と同じである。ただし、ＩＰアドレス解析部７１の代わりに設けられているアプリケーション解析部８１は、フレームバッファ６０に格納されている送信フレームのポート番号を抽出する。ここで、ポート番号は、たとえば、図１６に示すＴＣＰデータグラムのヘッダに格納されている。そし

て、テーブル検索部７２は、アプリケーション解析部８１により抽出されたポート番号と同じポート番号が「割当て条件」として登録されているエントリを検出する。

このように、この実施例においては、送信フレームの送信元ＭＡＣアドレスとして、送信フレームのＴＣＰポート番号に基づいて一意に決まるＭＡＣアドレスが設定される。

図１９および図２０は、論理ポートの実現方法を説明する図である。図１９に示す例では、ＭＡＣアドレスを保持するためのレジスタ９１が設けられている。このとき、ＩＰ処理部５４により送信フレームが生成されると、そのフレームの送信元ＩＰアドレスに対応するＭＡＣアドレスがセッション管理テーブル３０から取り出され、そのＭＡＣアドレスがレジスタ９１に書き込まれる。そして、このレジスタ９１に保持されているＭＡＣアドレスが送信フレームの送信元ＭＡＣアドレス領域に書き込まれる。

このように、この形態では、送信元ＩＰアドレスに応じてレジスタ９１が保持するＭＡＣアドレスを更新することにより複数の論理ポートが実現される。したがって、この形態では、物理ポート内に設けられているＭＡＣアドレスを保持するためのレジスタを図１９に示すレジスタ９１として利用することもできる。ただし、この場合、レジスタ９１を書き換えるためのソフトウェアプログラムまたはハードウェア回路が必要になる。

図２０に示す例では、ＭＡＣアドレスを保持するための複数のレジスタ９２－０～９２－３が設けられている。そして、これらのレジスタ９２－０～９２－３には、それぞれ、ユーザ端末１に割り当てられている複数のＭＡＣアドレスが予め書き込まれている。また、セッション管理テーブル３０には、論理ポートＩＤとして、レジスタ９２－０～９２－３を識別する情報が登録されている。

ＩＰ処理部５４により送信フレームが生成されると、そのフレームの送信元ＩＰアドレスに対応する論理ポートＩＤがセッション管理テーブル３０から取り出され、その論理ポートＩＤにより識別されるレジスタが指定される。図２０に示す例では、レジスタ９２－０が指定されている。そして、このレジスタ９２－０に保持されているＭＡＣアドレスが送信フレームの送信元ＭＡＣアドレス領域に書き込まれる。

このように、この形態では、送信元ＩＰアドレスに応じて互いに異なるＭＡＣアドレスを保持するレジスタを選択することにより複数の論理ポートが実現される。

図２１は、本発明の通信装置を利用した通信の実施例である。

現在、多くのサービスプロバイダがネットワークを介してコンテンツを提供するサービスを展開しているが、一般に、これらのサービスは、サービスプロバイダと契約しているユーザに対してのみ提供される。このため、サービスプロバイダは、ユーザ認証を行い、非契約ユーザからのフレームの流入や、非契約ユーザに対するデータの送出を遮断する必要がある。そして、今後、このようなユーザ認証として、装置導入コストが安価で処理速度の高いＩＥＥＥ８０２．１ｘの導入が進むことが予想されている。

一方、ネットワークを利用するユーザの端末装置は、通常、ネットワークインタフェース（すなわち、物理ポート）を１つだけ備え、そのネットワークインタフェースを介してネットワークに接続する。しかし、ＩＥＥＥ８０２．１ｘ認証においては、上述したように、物理ポートまたはフレーム中の送信元ＭＡＣアドレスのみによりセッションが識別される。このため、従来、ＩＥＥＥ８０２．１ｘ認証が行われる環境下では、ユーザは、異なるサービスプロバイダが提供するコンテンツ等を同時に利用することができなかった。

そこで、本発明では、ユーザが使用する端末装置（以下、ユーザ装置）のネ

ットワークインタフェースに対して互いに異なる複数のＭＡＣアドレスを付与しておき、必要に応じてそれら複数のＭＡＣアドレスを使い分けられるように機能を拡張した。このとき、このユーザを認証する認証システムは、図１４に示したように、各送信元ＭＡＣアドレスについて個々に公知のＩＥＥＥ８０２．１ｘを実行する。すなわち、認証システムは、このユーザ装置を認証する際に、複数のインタフェースを認証することになる。従って、このユーザ装置に割り当てられている複数のＭＡＣアドレスに対応する複数のセッションを並列に確立できる。

図２１に示す例では、ユーザ装置に「ＭＡＣアドレスＡ」および「ＭＡＣアドレスＢ」が割り当てられている。そして、「ＭＡＣアドレスＡ」により識別されるセッションにより、ユーザ装置とサービスプロバイダＡとが接続されている。また、「ＭＡＣアドレスＢ」により識別されるセッションも同時に確立されており、そのセッションによりユーザ装置とサービスプロバイダＢとが接続されている。すなわち、マルチセッションが実現されており、ユーザは、複数のサービスプロバイダから同時に異なるサービスを受けることができる。

なお、上述の実施例は、ユーザ認証方式としてＩＥＥＥ８０２．１ｘを使用するシステムを前提としているが、本発明はこれに限定されるものではない。すなわち、本発明は、少なくとも、送信元アドレス（特に、送信元ＭＡＣアドレス）に基づいてセッションが識別されるネットワークを介して通信を行う端末装置に適用可能である。

また、本発明は、ネットワークインタフェース（物理ポート）を１つだけ有するユーザ端末に好適であるが、複数のネットワークインタフェースを備える端末装置に適用することを排除するものではない。

さらに、上述の実施例では、本発明がユーザ宅等に設けられている端末装置に適用されているが、これに限定されるものではない。すなわち、本発明は、

例えば、図２２に示すように、端末装置とネットワークとの間に設けられる通信装置（ルータ装置など）に適用されるようにしてもよい。

本発明によれば、ネットワークインタフェースを１つしか持たない通信装置であっても、送信元アドレスに基づいてセッションを識別するネットワークを介して、同時に複数のセッションを利用して通信を行うことができる。

請求の範囲

1． フレームに設定されている送信元アドレスに基づいてセッションが識別されるネットワークを介して通信を行う通信装置であって、

上記ネットワークに接続するインタフェース手段と、

複数のアドレスを管理する管理手段と、

セッション確立要求を含むフレームを上記インタフェース手段を介して上記ネットワーク上に設けられている認証システムに送信する確立要求手段と、

上記セッション確立要求を含むフレームの送信元アドレスとして上記管理手段により管理されている複数のアドレスの中の１つを設定するアドレス設定手段、

を有する通信装置。

2． 請求項１に記載の通信装置であって、

上記管理手段は、上記セッション確立要求を用いて要求したセッションが上記認証システムにおいて許可された場合に、そのセッション確立要求において指定した通信条件を、上記セッション確立要求を含むフレームに設定したアドレスに対応づけて管理する

ことを特徴とする通信装置。

3． 請求項２に記載の通信装置であって、

送信フレームの内容を解析する解析手段と、

上記解析手段の解析結果を利用して上記管理手段により管理されている通信条件を検索し、その検索結果に対応するアドレスを選択する選択手段、

をさらに有し、

上記アドレス設定手段は、上記送信フレームの送信元アドレスとして上記選択手段により選択されたアドレスを設定する

ことを特徴とする通信装置。

4． 請求項２に記載の通信装置であって、

上記通信条件として送信元ＩＰアドレスが使用される

ことを特徴とする通信装置。

5． 請求項２に記載の通信装置であって、

上記通信条件としてポート番号が使用される

ことを特徴とする通信装置。

6． 請求項１に記載の通信装置であって、

上記管理手段により管理される複数のアドレスは、それぞれＭＡＣアドレスである

ことを特徴とする通信装置。

7． フレームに設定されている送信元アドレスに基づいてセッションが識別されるネットワークを介して通信を行う通信装置であって、

上記ネットワークに接続する物理ポートと、

それぞれ互いに異なるアドレスが付与されている複数の論理ポートと、

送信フレームの内容を解析する解析手段と、

上記解析手段の解析結果に基づいて上記複数の論理ポートの中から１つの論理ポートを選択する選択手段、

を有し、

上記選択手段により選択された論理ポートは、上記送信フレームの送信元アドレスとしてその論理ポートに付与されているアドレスを設定し、上記物理ポートを介して上記ネットワークへ送出する

ことを特徴とする通信装置。

8． 請求項７に記載の通信装置であって、

上記ネットワーク上に設けられている認証システムにより許可されたセッシ

ョンと、上記複数の論理ポートとの対応関係を管理する管理手段をさらに有し、

上記選択手段は、上記管理手段により管理されている対応関係に従って論理ポートを選択する

ことを特徴とする通信装置。

９．　請求項７に記載の通信装置であって、

使用すべき送信元ＩＰアドレスを指定したセッション確立要求を含むフレームを、上記複数の論理ポートの中の任意の論理ポートを介して上記ネットワーク上に設けられている認証システムに送信する要求手段と、

上記セッション確立要求を含むフレームを送信する際に使用した論理ポートとそのセッション確立要求において指定した送信元ＩＰアドレスとの対応関係を管理する管理手段、

をさらに有し、

上記解析手段は、送信フレームの送信元ＩＰアドレスを検出し、

上記選択手段は、上記管理手段を参照し、上記解析手段により検出された送信元ＩＰアドレスに対応する論理ポートを選択する

ことを特徴とする通信装置。

１０．　請求項７に記載の通信装置であって、

使用すべきポート番号を指定したセッション確立要求を含むフレームを、上記複数の論理ポートの中の任意の論理ポートを介して上記ネットワーク上に設けられている認証システムに送信する要求手段と、

上記セッション確立要求を含むフレームを送信する際に使用した論理ポートとそのセッション確立要求において指定した送信元ポート番号との対応関係を管理する管理手段、

をさらに有し、

上記解析手段は、送信フレームのポート番号を検出し、

上記選択手段は、上記管理手段を参照し、上記解析手段により検出されたポート番号に対応する論理ポートを選択する

ことを特徴とする通信装置。

１１．　請求項７に記載の通信装置であって、

上記複数の論理ポートには、それぞれ互いに異なるＭＡＣアドレスが付与されている

ことを特徴とする通信装置。

１２．　ＩＥＥＥ８０２．１ｘを利用してユーザ認証を行うネットワークを介して通信を行う通信装置であって、

上記ネットワークに接続する物理ポートと、

それぞれ互いに異なるアドレスが付与されている複数の論理ポートと、

送信フレームの内容を解析する解析手段と、

上記解析手段の解析結果に基づいて上記複数の論理ポートの中から１つの論理ポートを選択する選択手段、

を有し、

上記選択手段により選択された論理ポートは、上記送信フレームの送信アドレスとしてその論理ポートに付与されているアドレスを設定し、上記物理ポートを介して上記ネットワークへ送出する

ことを特徴とする通信装置。

１３．　フレームに設定されている送信元アドレスに基づいてセッションが識別されるネットワークにおけるセッション確立方法であって、

複数のＭＡＣアドレスが割り当てられている通信装置において、セッション確立要求を含むフレームの送信元アドレスとして上記複数のＭＡＣアドレスの中の１つを選択して設定し、そのフレームを、当該通信装置が備える唯一のネ

ットワークインタフェースを介して上記ネットワーク上に設けられている認証システムに送信し、

上記認証システムにおいて、上記セッション確立要求により要求されたセッションを許可するか否かを判断し、

上記通信装置において、上記認証システムにより許可されたセッションと上記セッション確立要求を含むフレームに付与したＭＡＣアドレスとを対応づけて管理することにより、ＭＡＣアドレス毎にセッションを生成する

ことを特徴とするセッション確立方法。

１４．フレームに設定されている送信元アドレスに基づいてセッションが識別されるネットワークにおける通信方法であって、

送信フレームの内容を解析し、

それぞれ互いに異なるＭＡＣアドレスが付与されている複数の論理ポートの中から、上記解析の結果に対応する論理ポートを選択し、

上記選択された論理ポートにおいて、その論理ポートに付与されているＭＡＣアドレスを上記送信フレームの送信元アドレスとして設定し、

上記送信フレームを、当該通信装置が備える唯一のネットワークインタフェースを介して上記ネットワーク送出する

ことを特徴とする通信方法。

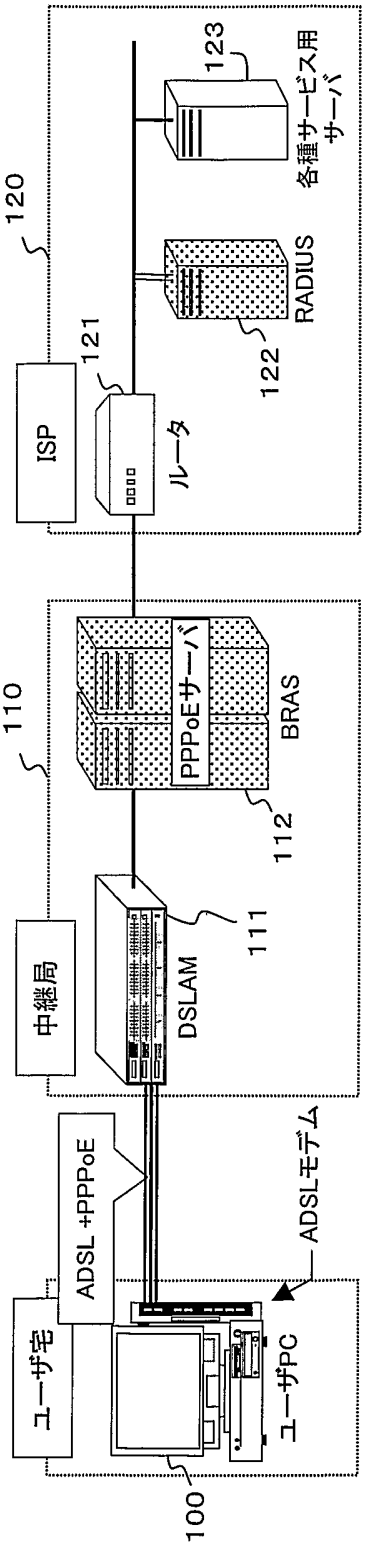

120
123
各種サービス用
サーバ
RADIUS
122
121
ISP
ルータ
110
PPPoEサーバ
BRAS
112
中継局
DSLAM
111
ADSL +PPPoE
ADSLモデム
ユーザ宅
ユーザPC
100

図1

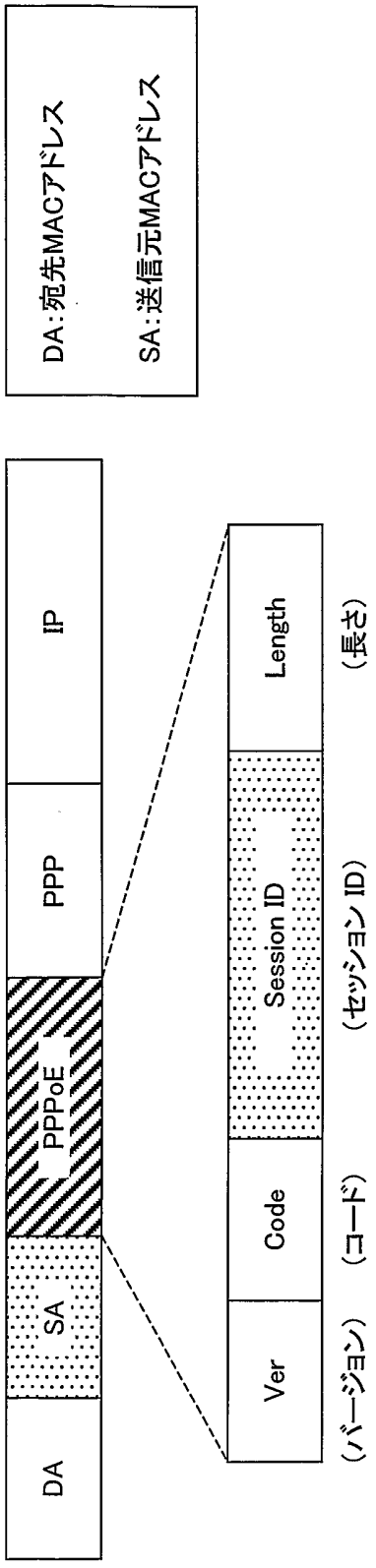

DA:宛先MACアドレス
SA:送信元MACアドレス
IP
PPP
PPPoE
SA
DA
Length
Session ID
Code
Ver
（長さ）
（セッションID）
（コード）
（バージョン）

図2

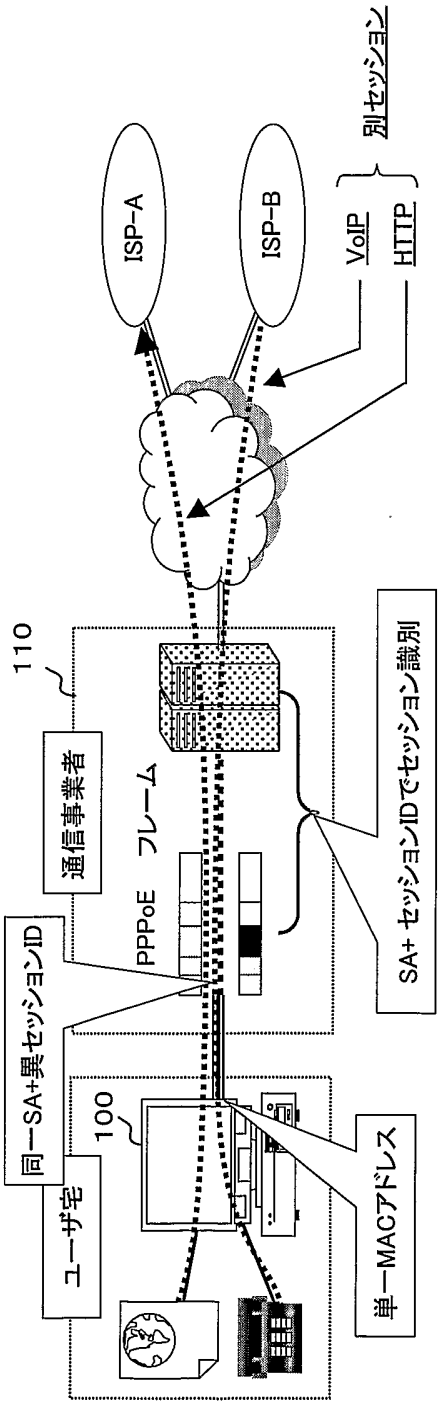

別セッション
ISP-A
ISP-B
VoIP
HTTP
110
通信事業者
PPPoE フレーム
SA+ セッションIDでセッション識別
同一SA+異セッションID
100
ユーザ宅
単一MACアドレス

図3

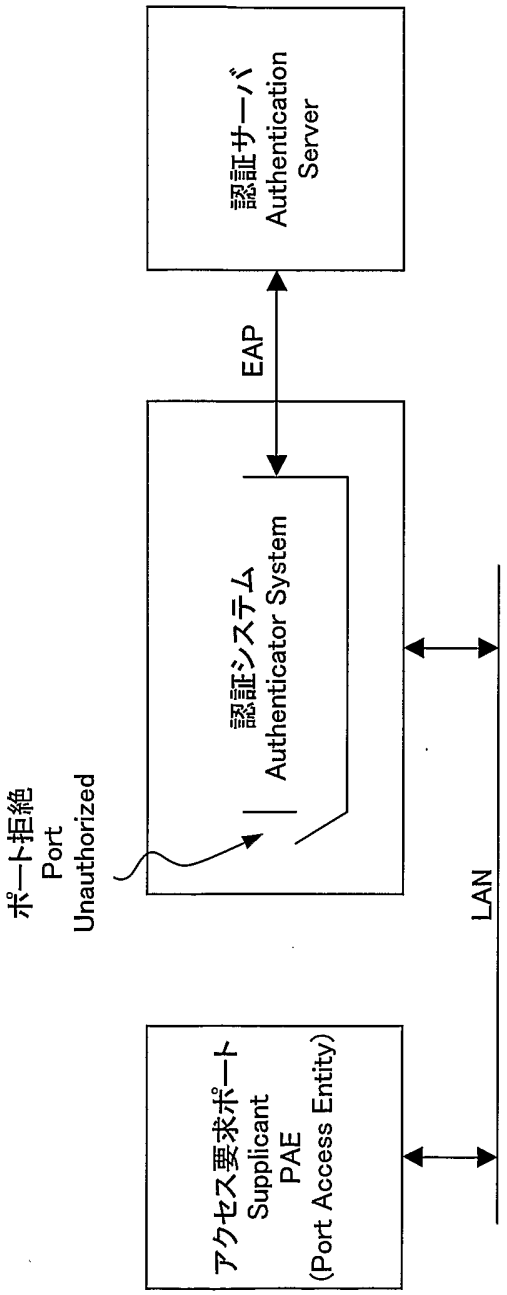

認証サーバ
Authentication
Server
EAP
認証システム
Authenticator System
ポート拒絶
Port
Unauthorized
LAN
アクセス要求ポート
Supplicant
PAE
(Port Access Entity)

図4

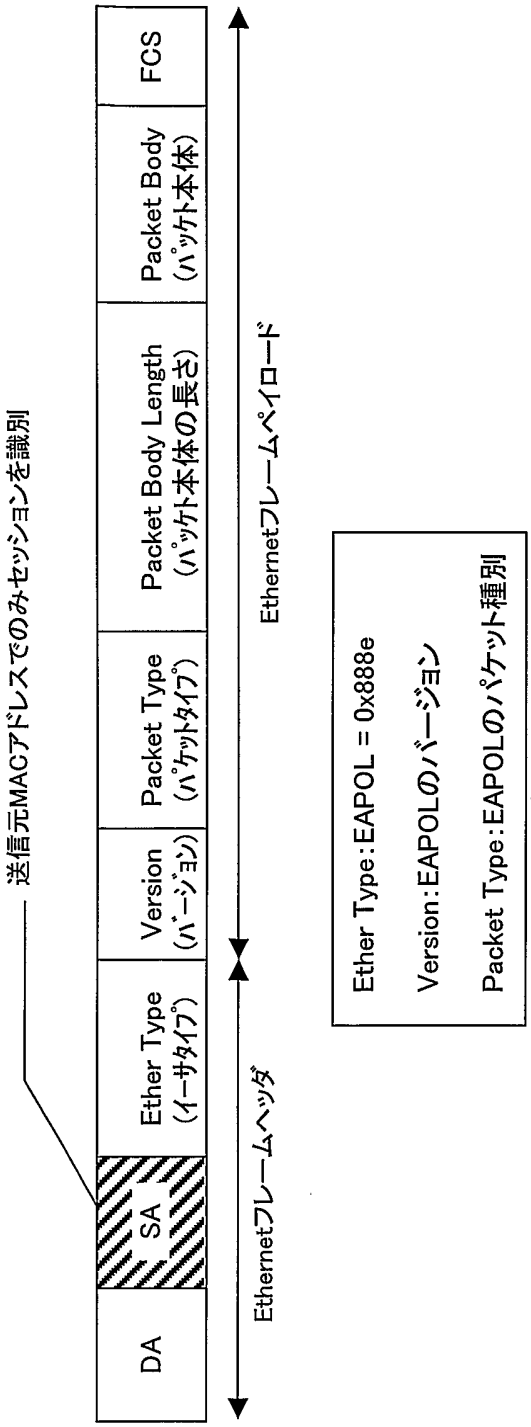

DA
SA
Ether Type
(イーサタイプ)
Version
(バージョン)
Packet Type
(パケットタイプ)
Packet Body Length
(パケット本体の長さ)
Packet Body
(パケット本体)
FCS
送信元MACアドレスでのみセッションを識別
Ethernetフレームヘッダ
Ethernetフレームペイロード
Ether Type:EAPOL = 0x888e
Version:EAPOLのバージョン
Packet Type:EAPOLのパケット種別

図5

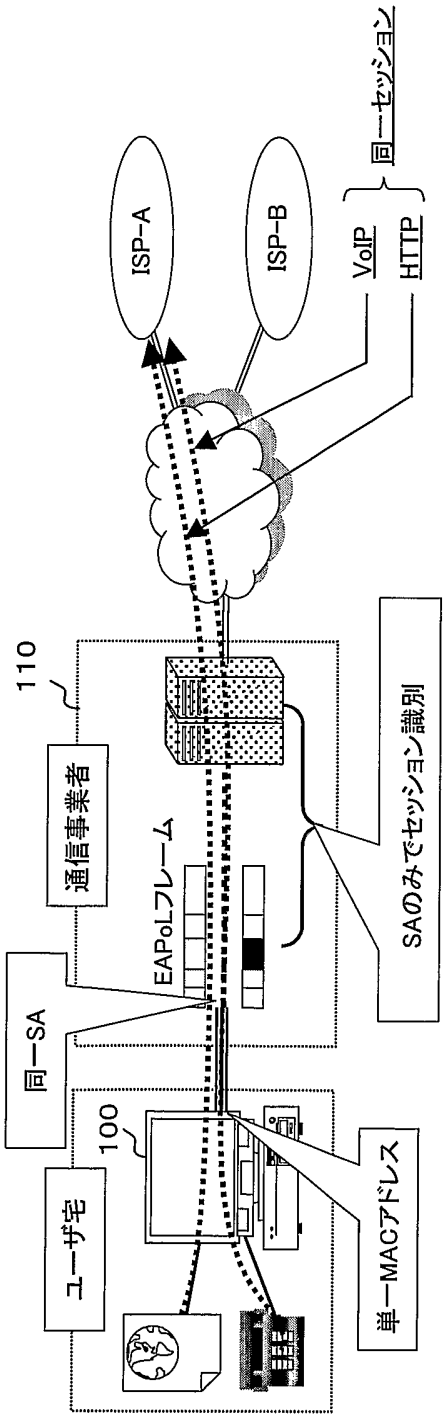

ISP-A
ISP-B
VoIP
HTTP
同一セッション
110
通信事業者
EAPoLフレーム
SAのみでセッション識別
同一SA
100
ユーザ宅
単一MACアドレス

図6

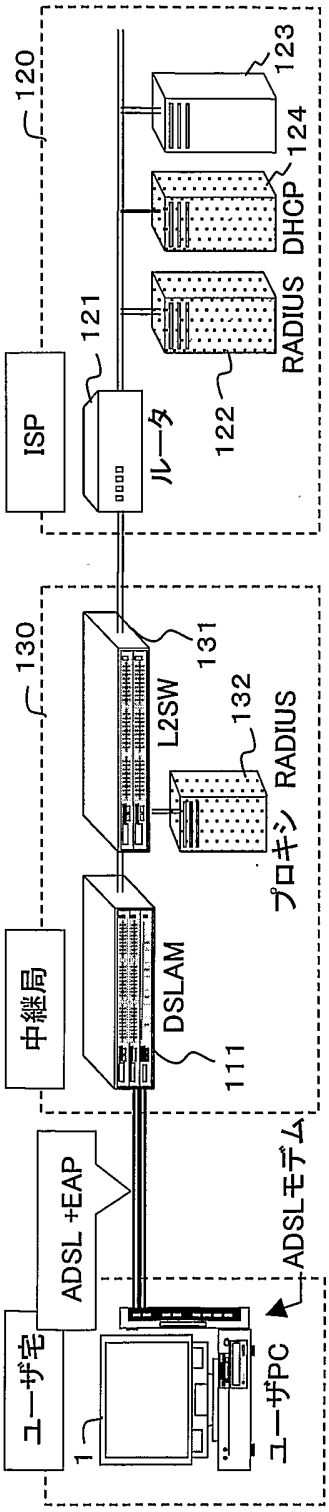

120
123
124
DHCP
RADIUS
121
ISP
ルータ
122
130
131
L2SW
132
RADIUS
プロキシ
中継局
DSLAM
111
ADSL +EAP
ADSLモデム
ユーザ宅
1
ユーザPC

図7

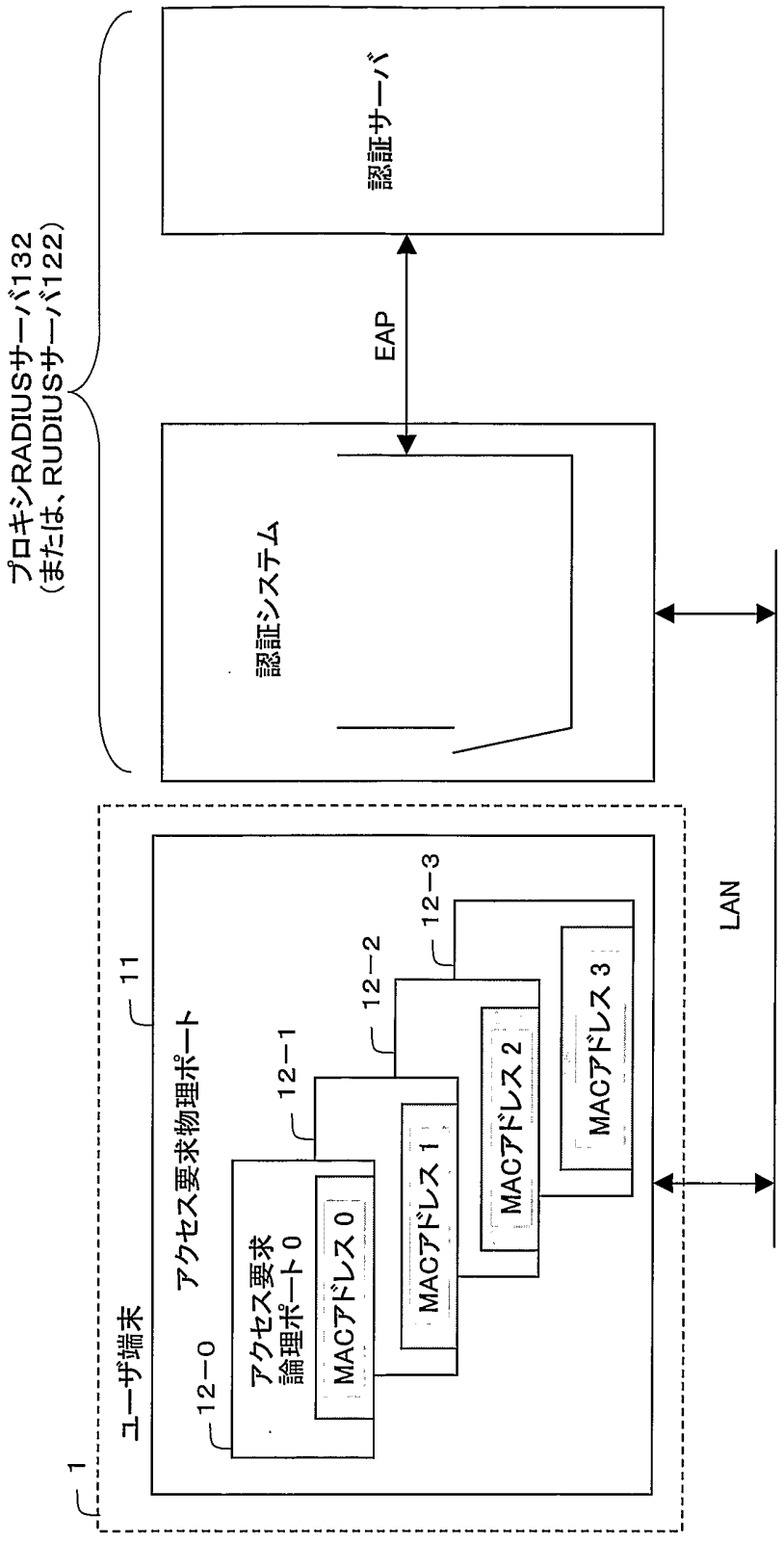

プロキシRADIUSサーバ132
(または、RUDIUSサーバ122)
認証サーバ
EAP
認証システム
LAN
1
ユーザ端末
11
アクセス要求物理ポート
12−0
アクセス要求
論理ポート0
12−1
MACアドレス0
12−2
MACアドレス1
12−3
MACアドレス2
MACアドレス3

図8

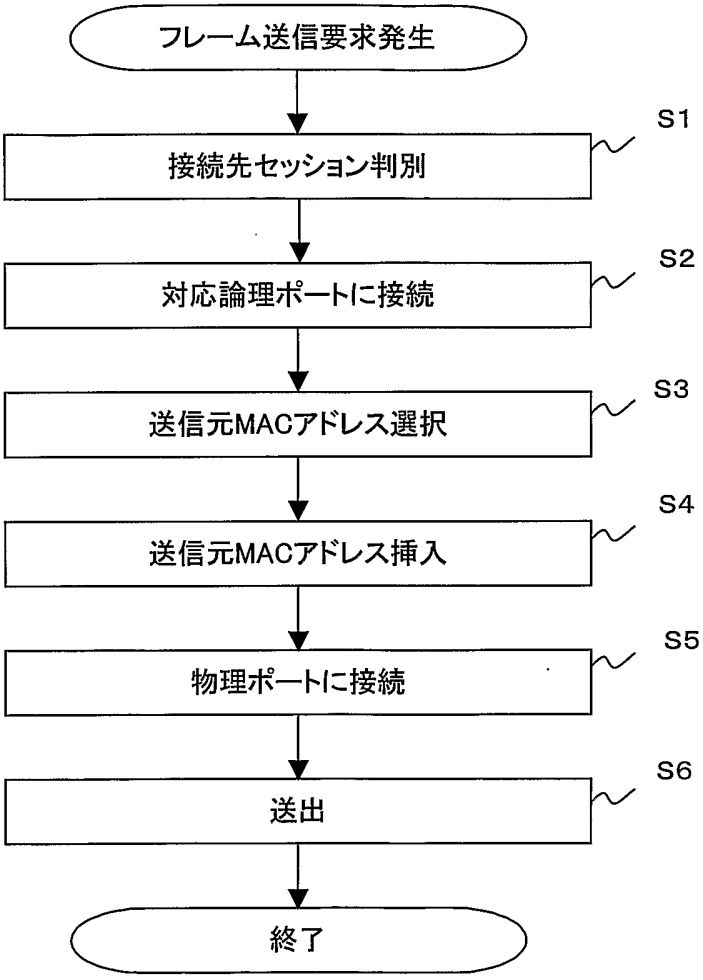

フレーム送信要求発生
S1
接続先セッション判別
S2
対応論理ポートに接続
S3
送信元MACアドレス選択
S4
送信元MACアドレス挿入
S5
物理ポートに接続
S6
送出
終了

図9

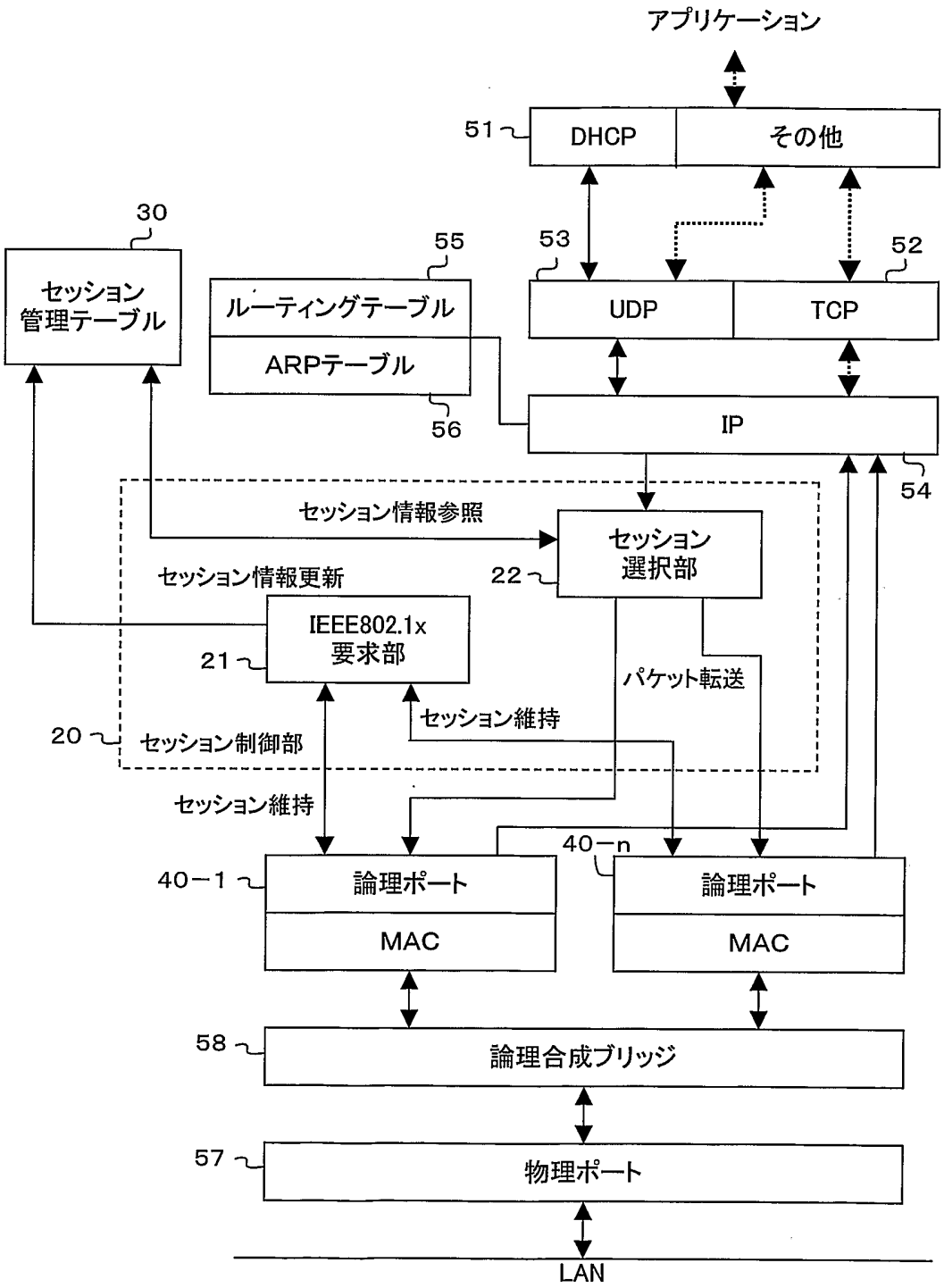

アプリケーション
51
DHCP
その他
30
セッション
管理テーブル
55
ルーティングテーブル
ARPテーブル
56
53
52
UDP
TCP
IP
54
セッション情報参照
セッション情報更新
22
セッション
選択部
IEEE802.1x
要求部
21
パケット転送
セッション維持
20
セッション制御部
セッション維持
40−n
40−1
論理ポート
MAC
論理ポート
MAC
58
論理合成ブリッジ
57
物理ポート
LAN

図10

割当て条件	セッションID	論理ポートID	MACアドレス	有効無効表示	セッション確立
条件 1	0	0	a0-b0-c0-d0-e0-f0	1	1
条件 2	1	1	a1-b1-c1-d1-e1-f1	1	0
条件 3	2	3	a2-b2-c2-d2-e2-f2	1	0
条件 4	3	0	0	0	0
条件 5	0	0	0	0	0
条件 6	0	0	0	0	0

図11

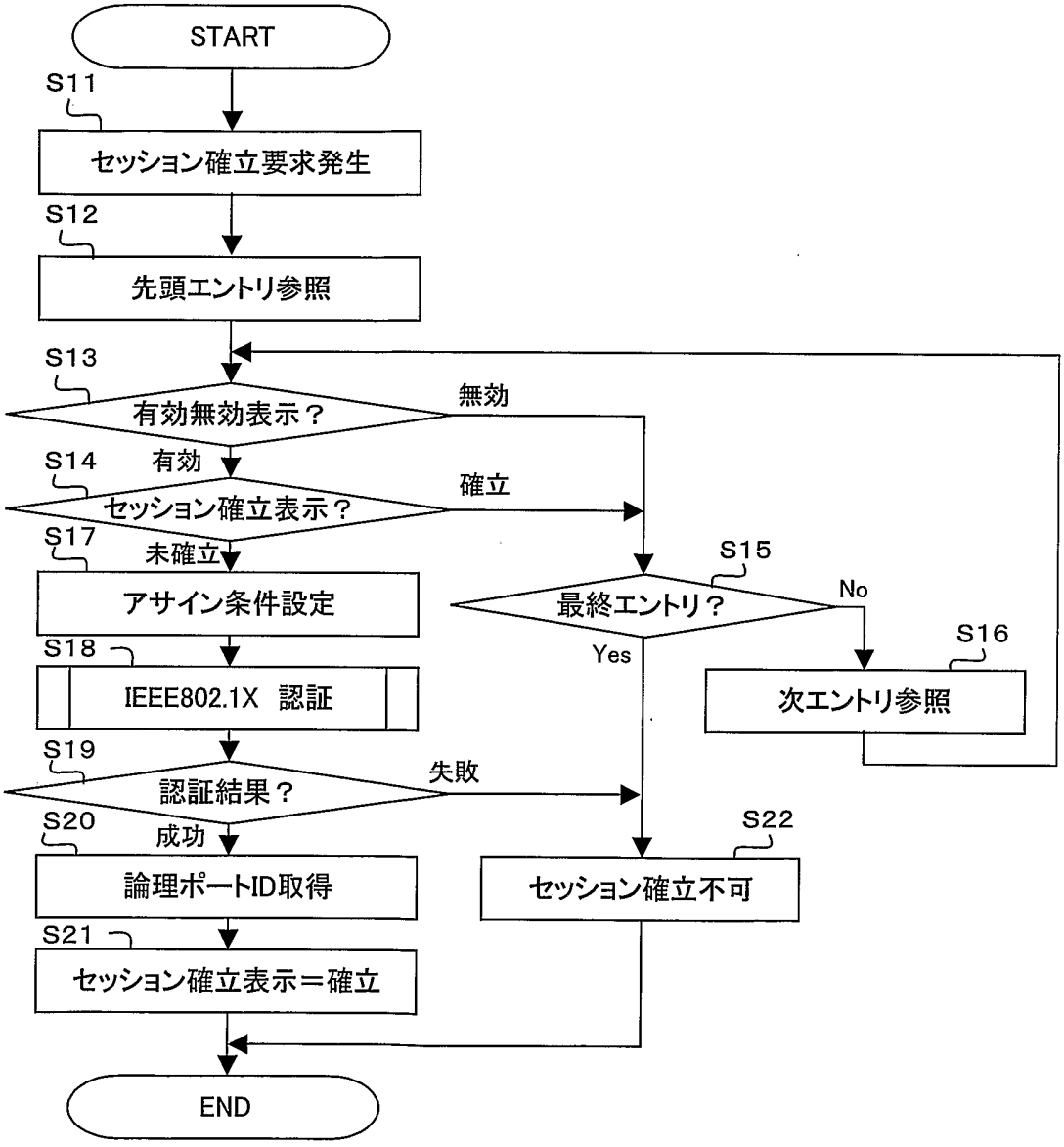

START
S11
セッション確立要求発生
S12
先頭エントリ参照
S13
有効無効表示？
無効
S14
有効
セッション確立表示？
確立
S17
未確立
アサイン条件設定
S15
最終エントリ？
No
S16
次エントリ参照
Yes
S18
IEEE802.1X 認証
S19
認証結果？
失敗
S20
成功
論理ポートID取得
S22
セッション確立不可
S21
セッション確立表示＝確立
END

図12

図13A

割当て条件	セッションID	論理ポートID	MACアドレス	有効無効表示	セッション確立
(-1)	0	(-1)	a0-b0-c0-d0-e0-f0	1	0
(-1)	1	(-1)	a1-b1-c1-d1-e1-f1	1	0
(-1)	2	(-1)	a2-b2-c2-d2-e2-f2	1	0
(-1)	3	(-1)	(-1)	0	0
(-1)	0	(-1)	(-1)	0	0
(-1)	0	(-1)	(-1)	0	0

図13B

割当て条件	セッションID	論理ポートID	MACアドレス	有効無効表示	セッション確立
80	0	0	a0-b0-c0-d0-e0-f0	1	1
(-1)	1	(-1)	a1-b1-c1-d1-e1-f1	1	0
(-1)	2	(-1)	a2-b2-c2-d2-e2-f2	1	0
(-1)	3	(-1)	(-1)	0	0
(-1)	0	(-1)	(-1)	0	0
(-1)	0	(-1)	(-1)	0	0

図13C

割当て条件	セッションID	論理ポートID	MACアドレス	有効無効表示	セッション確立
80	0	0	a0-b0-c0-d0-e0-f0	1	1
25	1	1	a1-b1-c1-d1-e1-f1	1	1
(-1)	2	(-1)	a2-b2-c2-d2-e2-f2	1	0
(-1)	3	(-1)	(-1)	0	0
(-1)	0	(-1)	(-1)	0	0
(-1)	0	(-1)	(-1)	0	0

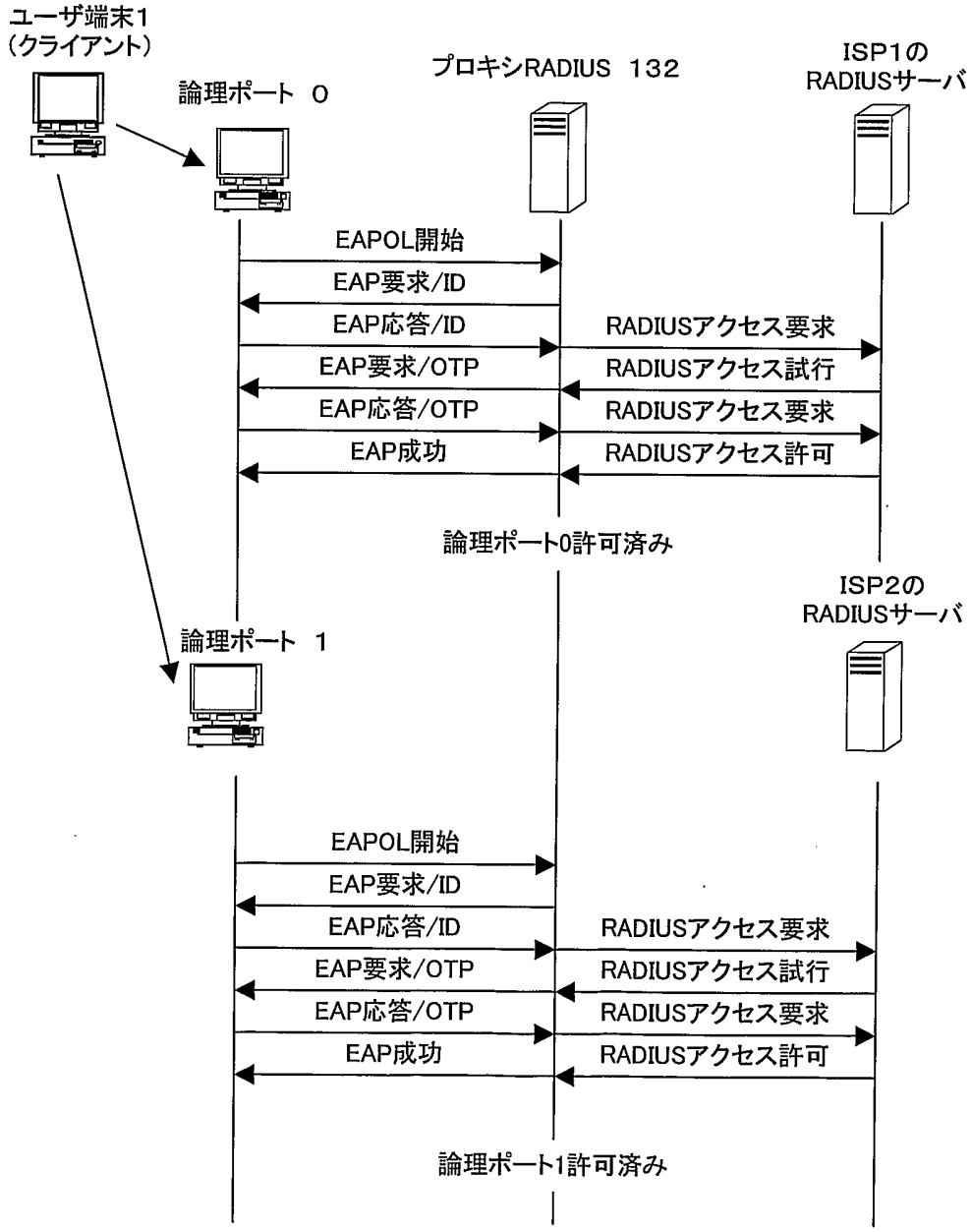

ユーザ端末1
(クライアント)
論理ポート 0
プロキシRADIUS 132
ISP1の
RADIUSサーバ
EAPOL開始
EAP要求/ID
EAP応答/ID
RADIUSアクセス要求
EAP要求/OTP
RADIUSアクセス試行
EAP応答/OTP
RADIUSアクセス要求
EAP成功
RADIUSアクセス許可
論理ポート0許可済み
ISP2の
RADIUSサーバ
論理ポート 1
EAPOL開始
EAP要求/ID
EAP応答/ID
RADIUSアクセス要求
EAP要求/OTP
RADIUSアクセス試行
EAP応答/OTP
RADIUSアクセス要求
EAP成功
RADIUSアクセス許可
論理ポート1許可済み

図14

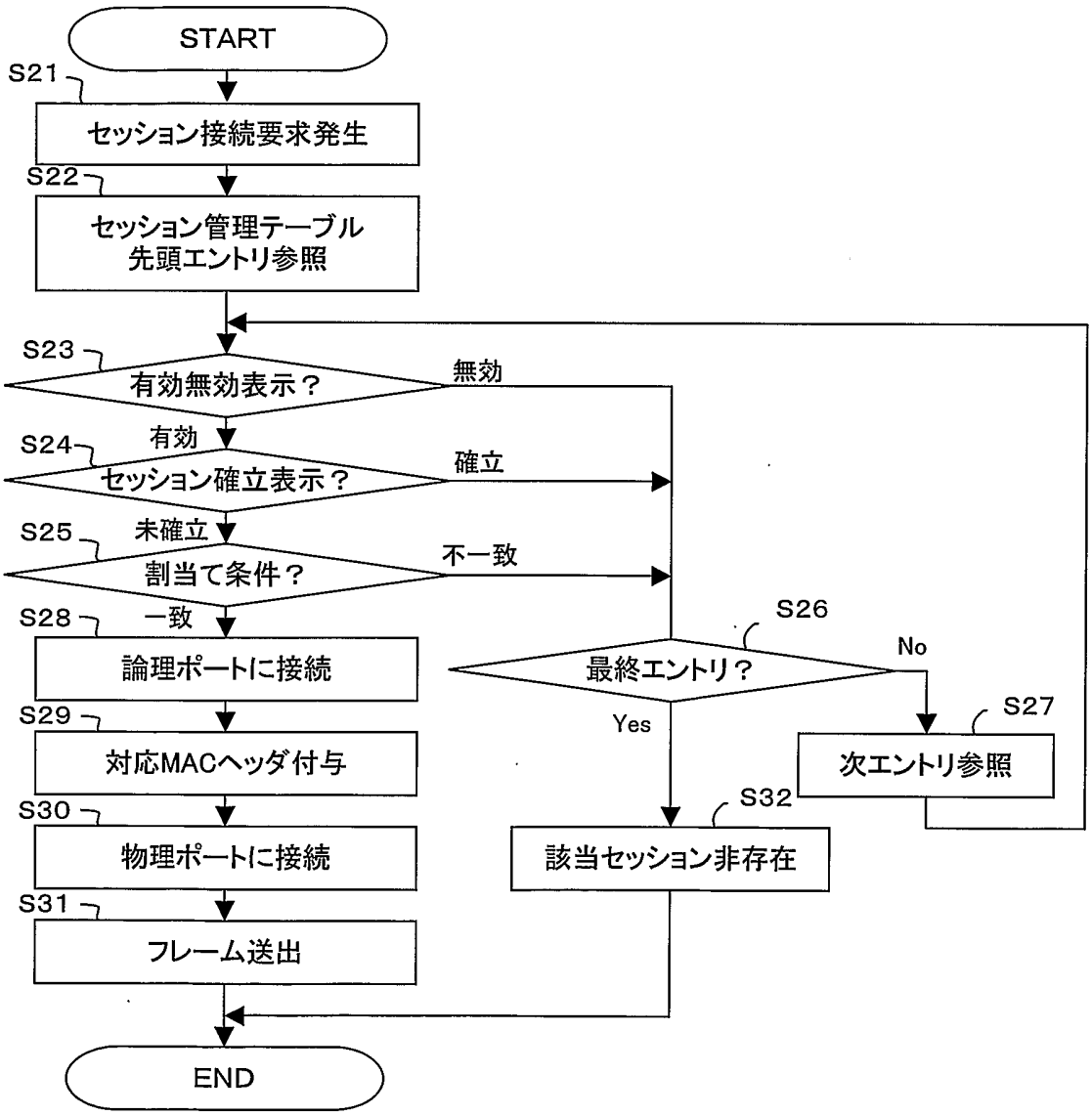

START
S21
セッション接続要求発生
S22
セッション管理テーブル
先頭エントリ参照
S23
有効無効表示？
無効
有効
S24
セッション確立表示？
確立
未確立
S25
割当て条件？
不一致
一致
S28
論理ポートに接続
S29
対応MACヘッダ付与
S30
物理ポートに接続
S31
フレーム送出
END
S26
最終エントリ？
No
Yes
S27
次エントリ参照
S32
該当セッション非存在

図15

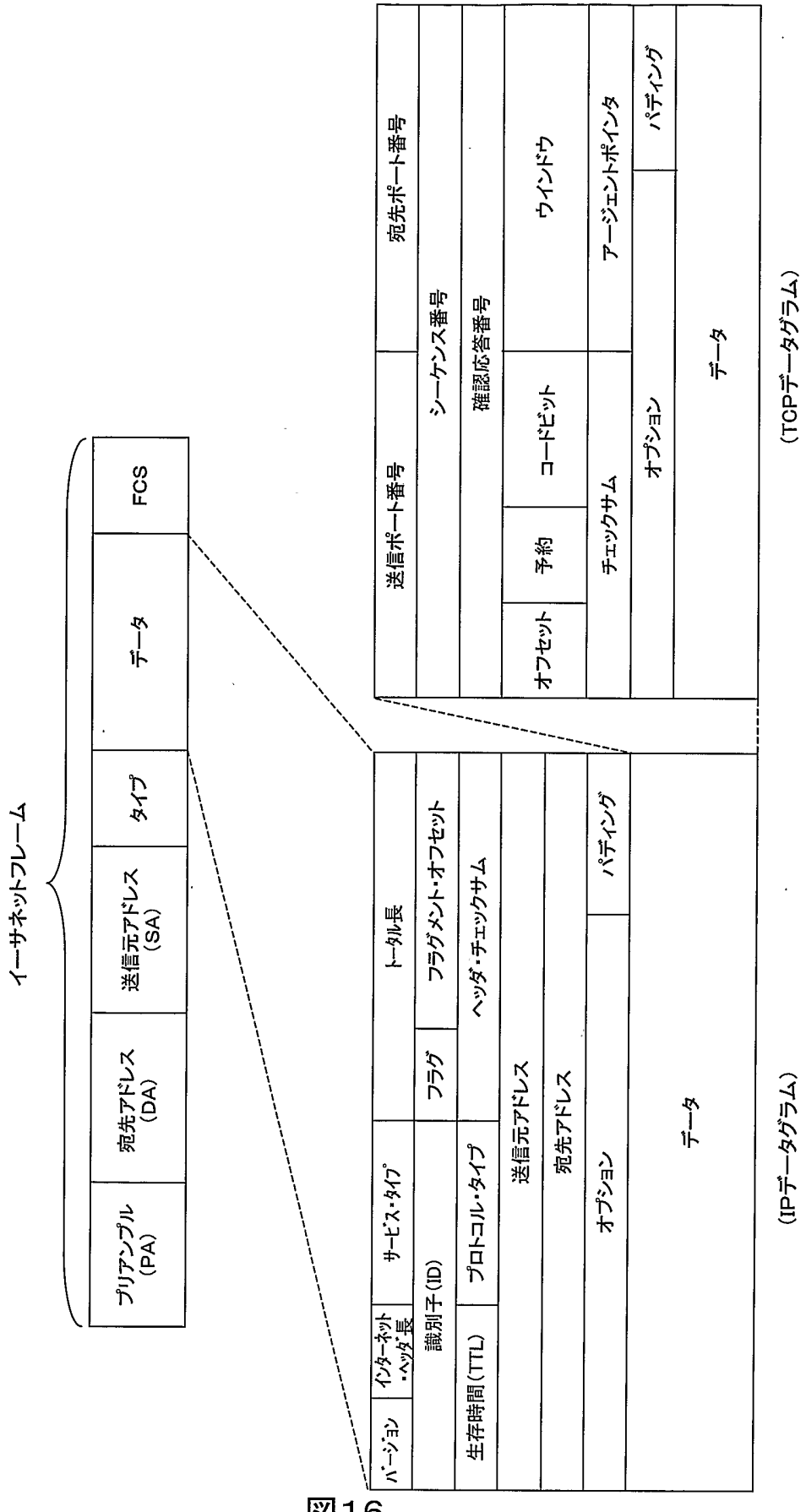

イーサネットフレーム
プリアンブル (PA)
宛先アドレス (DA)
送信元アドレス (SA)
タイプ
データ
FCS
バージョン
インターネット・ヘッダ長
サービス・タイプ
トータル長
識別子(ID)
フラグ
フラグメント・オフセット
生存時間(TTL)
プロトコル・タイプ
ヘッダ・チェックサム
送信元アドレス
宛先アドレス
オプション
パディング
データ
(IPデータグラム)
送信ポート番号
宛先ポート番号
シーケンス番号
確認応答番号
オフセット
予約
コードビット
ウインドウ
チェックサム
アージェントポインタ
オプション
パディング
データ
(TCPデータグラム)

図16

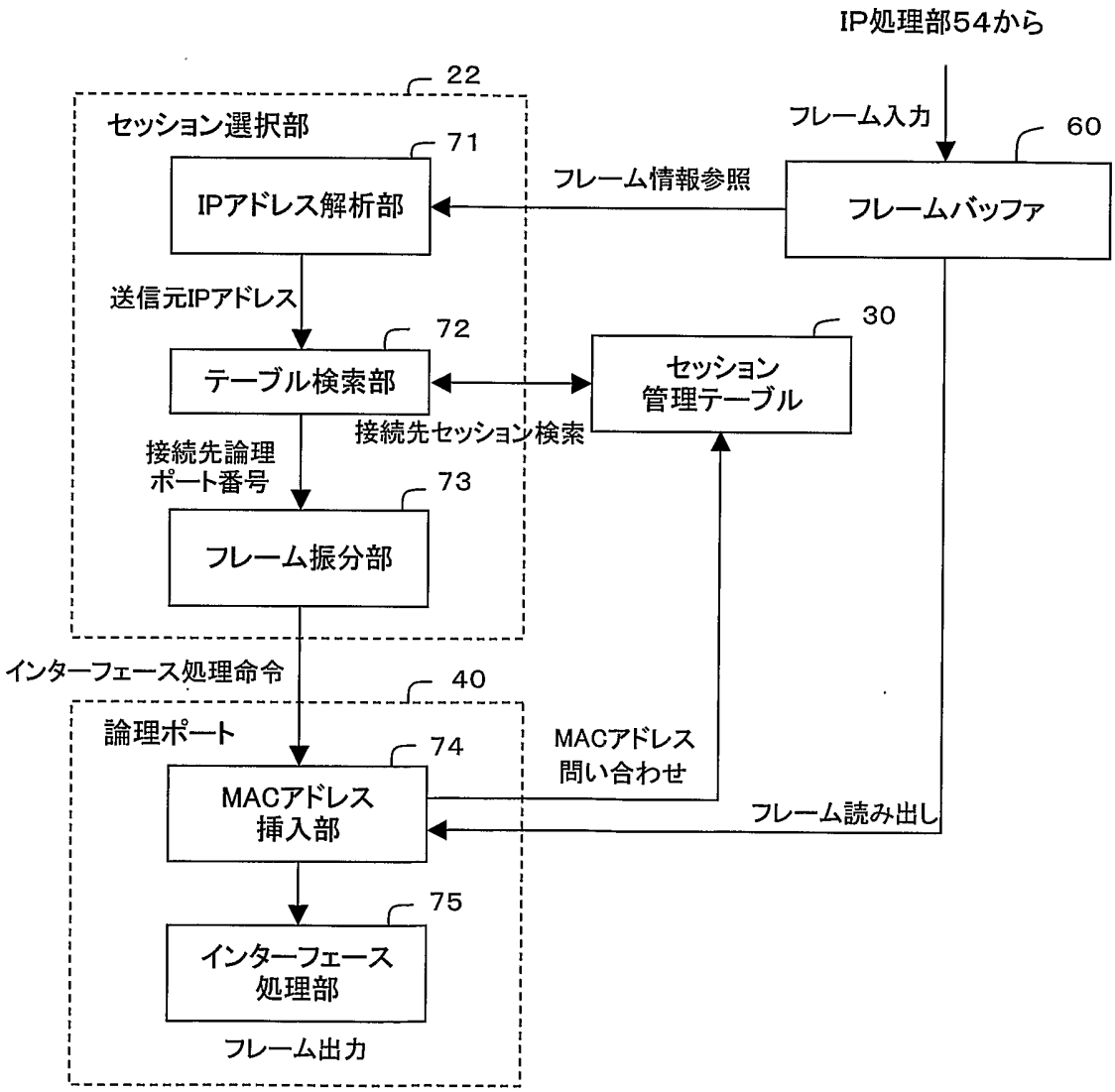

IP処理部54から
22
セッション選択部
71
IPアドレス解析部
フレーム入力
60
フレーム情報参照
フレームバッファ
送信元IPアドレス
72
テーブル検索部
30
セッション
管理テーブル
接続先セッション検索
接続先論理
ポート番号
73
フレーム振分部
インターフェース処理命令
40
論理ポート
74
MACアドレス
挿入部
MACアドレス
問い合わせ
フレーム読み出し
75
インターフェース
処理部
フレーム出力

図17

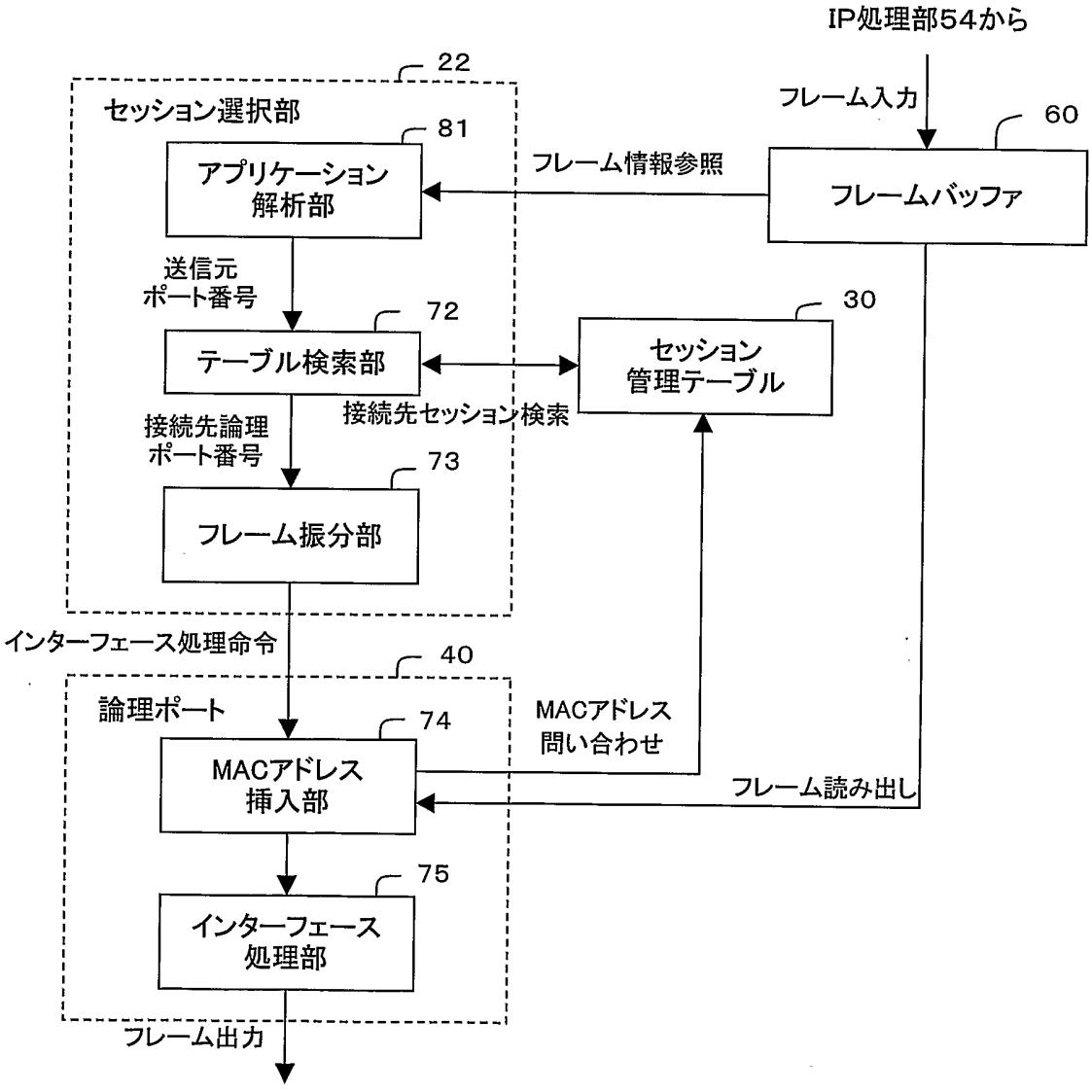

IP処理部54から
フレーム入力
60
フレームバッファ
フレーム情報参照
22
セッション選択部
81
アプリケーション
解析部
送信元
ポート番号
72
テーブル検索部
30
セッション
管理テーブル
接続先セッション検索
接続先論理
ポート番号
73
フレーム振分部
インターフェース処理命令
40
論理ポート
74
MACアドレス
挿入部
MACアドレス
問い合わせ
フレーム読み出し
75
インターフェース
処理部
フレーム出力

図18

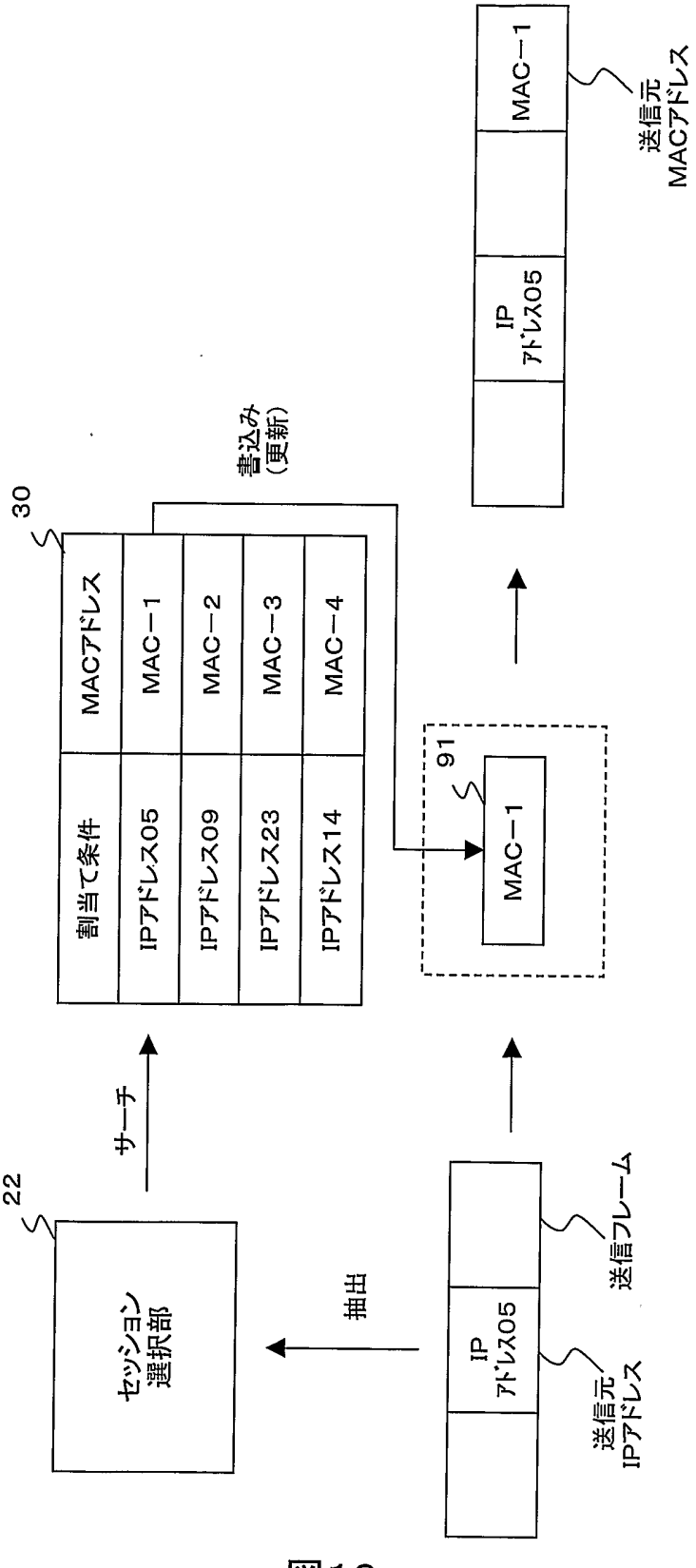

22
セッション
選択部
サーチ
抽出
IP
アドレス05
送信元
IPアドレス
送信フレーム
30
割当て条件
IPアドレス05
IPアドレス09
IPアドレス23
IPアドレス14
MACアドレス
MAC－1
MAC－2
MAC－3
MAC－4
書込み
(更新)
91
MAC－1
IP
アドレス05
MAC－1
送信元
MACアドレス

図19

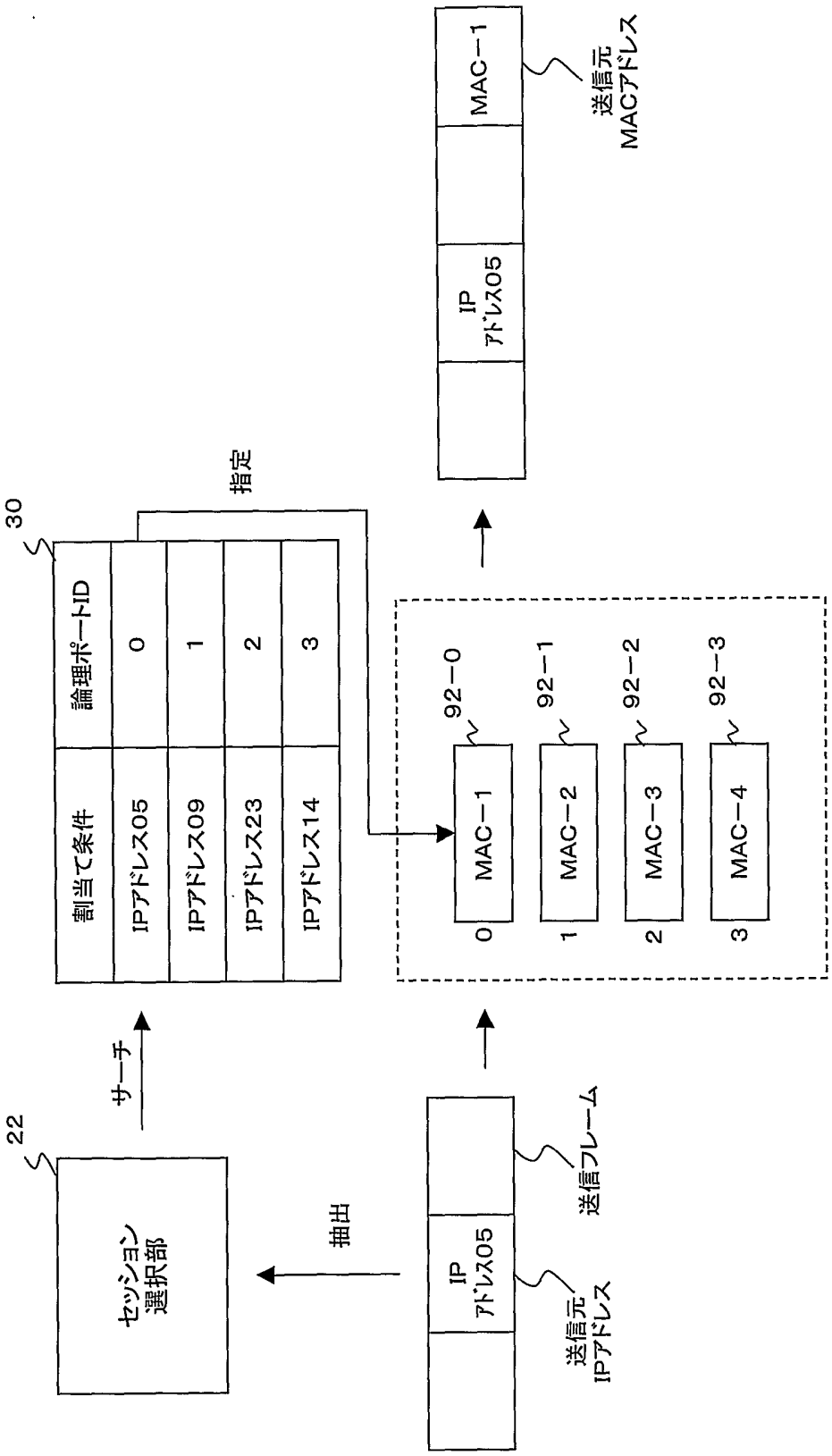

22
セッション
選択部
サーチ
30
割当て条件
論理ポートID
IPアドレス05
IPアドレス09
IPアドレス23
IPアドレス14
0
1
2
3
指定
抽出
IP
ｱﾄﾞﾚｽ05
送信元
IPアドレス
送信フレーム
92−0
92−1
92−2
92−3
MAC−1
MAC−2
MAC−3
MAC−4
0
1
2
3
IP
ｱﾄﾞﾚｽ05
MAC−1
送信元
MACアドレス

図20

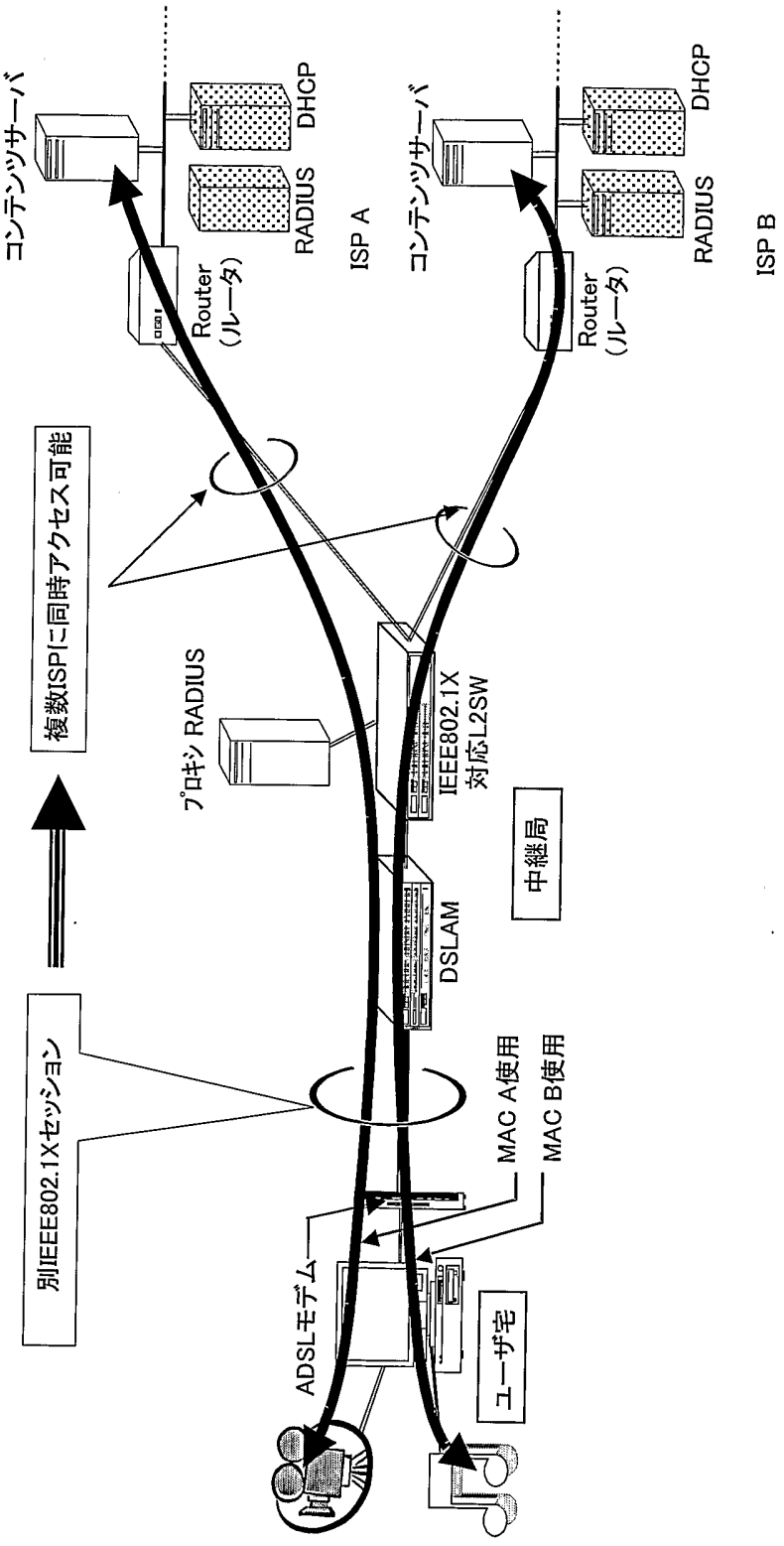

コンテンツサーバ
DHCP
RADIUS
ISP A
Router
(ルータ)
コンテンツサーバ
DHCP
RADIUS
ISP B
Router
(ルータ)
複数ISPに同時アクセス可能
プロキシ RADIUS
IEEE802.1X
対応L2SW
DSLAM
中継局
別IEEE802.1Xセッション
MAC A使用
MAC B使用
ADSLモデム
ユーザ宅

図21

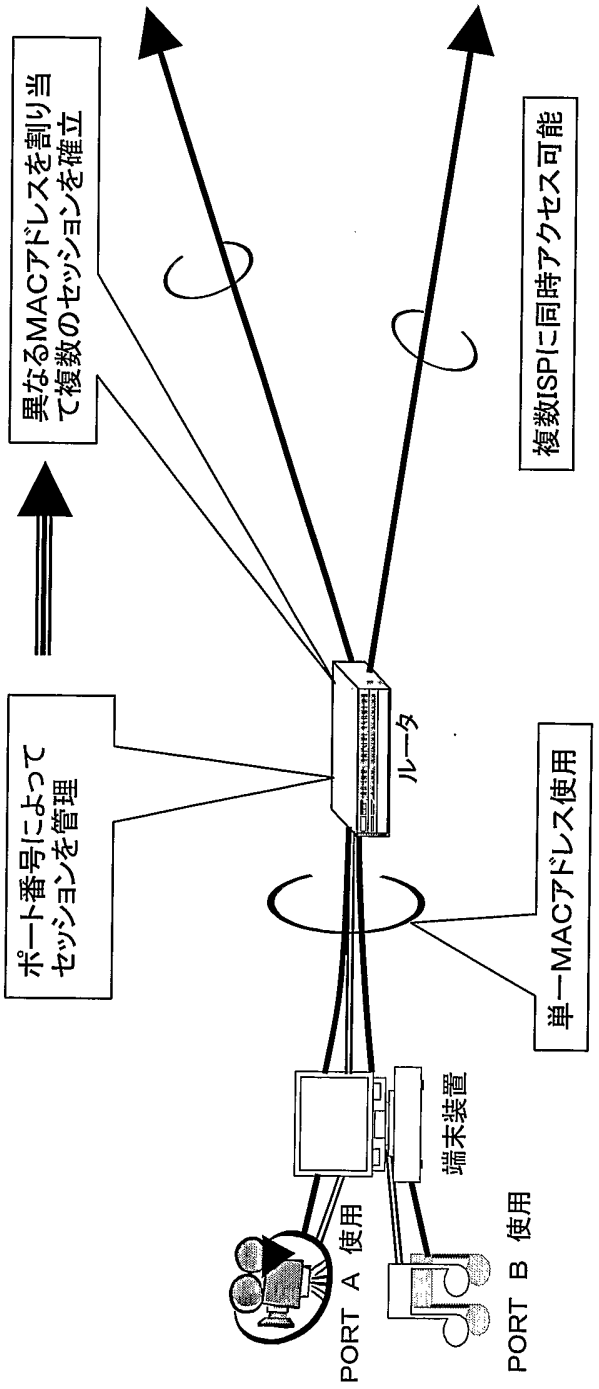

異なるMACアドレスを割り当て複数のセッションを確立
ポート番号によってセッションを管理
ルータ
複数ISPに同時アクセス可能
単一MACアドレス使用
端末装置
PORT A 使用
PORT B 使用

図22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/06609

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/46, G06F13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/00-12/66, H04L13/00-13/18, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Toroku Jitsuyo Shinan Koho 1994-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DENSHIJOHOTSUSHINGAKKAISOGOTAIKAI,
DENSHIJOHOTSUSHINGAKKAITSUSHINSOSAIETEITAIKAI
DENSHIJOHOTSUSHINGAKKAIGIJUTSUKENKYUHOKOKU CS, NS, IN (in Japanese)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-45058 A (Nippon Telegraph And Telephone Corp.), 16 February, 2001 (16.02.01), Full text; Figs. 1 to 8 (Family: none)	1-14
A	JP 2000-332813 A (NEC Corp.), 30 November, 2000 (30.11.00), Full text; Figs. 1 to 7 (Family: none)	1-14
A	JP 2002-64523 A (Fujitsu Ltd.), 28 February, 2002 (28.02.02), Full text; Figs. 1 to 7 (Family: none)	1-14

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 August, 2003 (22.08.03)	09 September, 2003 (09.09.03)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

国際調査報告

国際出願番号　PCT／JP03／06609

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁷ H04L12／46
Int. Cl⁷ G06F13／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁷ H04L12／00－12／66　　Int. Cl⁷ H04L13／00－13／18
Int. Cl⁷ G06F13／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1922－1996
日本国公開実用新案公報　1971－2003
日本国実用新案登録公報　1996－2003
日本国登録実用新案公報　1994－2001

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
電子情報通信学会総合大会
電子情報通信学会通信ソサイエティ大会
電子情報通信学会技術研究報告 CS, NS, IN

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP　2001－45058　A（日本電信電話株式会社）2001．02．16，全文，第1－8図（ファミリーなし）	1－14
A	JP　2000－332813　A（日本電気株式会社）2000．11．30，全文，第1－7図（ファミリーなし）	1－14
A	JP　2002－64523　A（富士通株式会社）2002．02．28，全文，第1－7図（ファミリーなし）	1－14

☐ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
22．08．03	09.09.03

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	宮島郁美	5X	8523
	電話番号　03－3581－1101　内線　3595		

様式PCT／ISA／210（第2ページ）（1998年7月）