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

特許第5152835号
(P5152835)

(45)発行日　平成25年2月27日(2013.2.27)　(24)登録日　平成24年12月14日(2012.12.14)

(51)Int.Cl.		F I		
H04L 12/46	(2006.01)	H04L	12/46	A
H04L 12/70	(2013.01)	H04L	12/56	B

請求項の数 1　(全 15 頁)

(21)出願番号　特願2007-218183 (P2007-218183)
(22)出願日　平成19年8月24日 (2007.8.24)
(65)公開番号　特開2009-55173 (P2009-55173A)
(43)公開日　平成21年3月12日 (2009.3.12)
審査請求日　平成22年8月13日 (2010.8.13)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(73)特許権者　504176911
国立大学法人大阪大学
大阪府吹田市山田丘１番１号
(74)代理人　100064621
弁理士　山川　政樹
(74)代理人　100098394
弁理士　山川　茂樹
(74)代理人　100153006
弁理士　小池　勇三
(72)発明者　八木　毅
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】多重アクセス装置

(57)【特許請求の範囲】
【請求項１】
複数の論理網を識別する論理網アドレスと前記論理網に所属する収容ユーザ端末を識別する論理網用端末アドレスとの対応を示す所属論理網用アドレスリストを備え、送信元の収容ユーザ端末より受信したパケットの前記送信元の収容ユーザ端末のユーザ端末アドレスに対応する論理網用端末アドレスを前記所属論理網用アドレスリストより検索する所属論理網管理手段と、
前記パケットの送信元アドレスを検索された前記論理網用端末アドレスに変更する送信元アドレス変更手段と
を備え、
収容している収容ユーザ端末に、収容ユーザ端末が所属する論理網識別子と前記収容ユーザ端末を識別する端末識別子とで階層化された前記論理網用端末アドレスを割り当て、
宛先の収容ユーザ端末が所属している論理網を宛先とした前記宛先の収容ユーザ端末に対して送出されたパケットの宛先アドレスを、前記宛先の収容ユーザ端末のユーザ端末アドレスに変更して前記宛先の収容ユーザ端末へ転送し、
前記送信元の収容ユーザ端末から送信されるパケットには、前記宛先の収容ユーザ端末が所属する論理網を識別する論理網識別子が備えられ、
宛先の収容ユーザ端末が受信したパケットには、送信元の収容ユーザ端末が所属する論理網を識別する論理網識別子が備えられている
ことを特徴とする多重アクセス装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数のＶＰＮに多重帰属している複数のユーザ端末の間の通信を制御する多重アクセス装置に関するものである。
【背景技術】
【０００２】
近年、ネットワーク技術の発展に伴い、様々な社会組織間の情報伝達が、インターネット通信網などのネットワークを介した通信により行われるようになっている。また、ネットワークの上に仮想組織（論理的な閉域網）を形成する試みもなされてきている。このような仮想組織のユーザは、セキュリティを維持した状態で、複数の仮想組織と通信可能な関係を確立する必要がある。
【０００３】
従来、このような、複数の仮想組織をユーザに提供する複数ＶＰＮ（Virtual Private Network）多重帰属サービスを提供する網では、まず、ユーザ端末に、各所属閉域網用のアドレスを割り当てている。加えて、ユーザ端末では、接続先の閉域網に応じ、パケットの送信元アドレスと宛先アドレスを決定してパケットを生成している。宛先アドレスは、論理網識別子と端末識別子とで階層化されており、ユーザ端末は、パケットを送信する際に、通信相手から宛先アドレスを決定した後、決定した宛先アドレスと同一の論理網識別子を有する保有アドレスを送信元アドレスとして記述してパケットを生成している（非特許文献１参照）。
【０００４】
また、ユーザ端末を収容する多重アクセス装置では、ユーザ端末からパケットを受信した際に、受信したパケットの宛先アドレスと送信元アドレスの論理網識別子が一致するか否かを確認し、不一致の際は前記パケットを廃棄している。この際、不正アクセスを防止するために、多重アクセス装置は、物理ポート識別子などの送信元アクセス回線識別子とパケットの宛先アドレスの論理網識別子を比較し、この論理網識別子が、前記アクセス回線識別子下のユーザ端末が接続を許可されている論理識別子であること確認している。
【０００５】
ここで、許可されていない論理識別子である場合は、パケットを廃棄する機能を保有することもある。さらに、この際、送信元アドレス詐称による不正アクセスを防止するために、多重アクセス装置は、物理ポート識別子などの送信元アクセス回線識別子とパケットの送信元アドレスを比較し、送信元アドレスが前記アクセス回線識別子下のユーザ端末に割り当てられたアドレスか否かを確認し、不一致の際はパケットを廃棄する機能を保有することもある。
【０００６】
これらは、ユーザ端末に、例えば、「ＯｐｅｎＶＰＮ」などのＳＳＬを用いたＶＰＮを構築するためのソフトウエアによるＶＰＮクライアントを配置し、多重アクセス装置にＯｐｅｎＶＰＮサーバ機能を配置することで、装置間でＶＰＮ毎にＳＳＬトンネルを設定するとともに、アドレス選択機能とアドレスチェック機能を各装置に配置することで実現できる。
【０００７】
この方式では、ユーザ端末が、ＶＰＮ毎に複数アドレスを保有する必要がある。しかし、通常、保有可能なアドレスに制限があるユーザ端末も多い。このため、一般的なユーザ端末に対して複数ＶＰＮ多重帰属サービスを実現する場合、上述した方式において、宛先アドレスを参照した転送制御のみを適用してサービスを実施する場合が多い。
【０００８】
これらの方式では、送信元のユーザ端末が、宛先のユーザ端末を指定するためのアドレスを特定できる必要がある。一方で、アドレス情報の漏えいに起因したスパム，フィッシング，及びＤＯＳ（Denial of Services）攻撃などのセキュリティ問題の発生を防止する

観点から、アドレス情報の公開は好ましくない。

【０００９】

従って、ユーザを収容する各多重アクセス装置に、収容ユーザの接続する閉域網毎に端末機能を保有させ、前記端末機能に閉域網毎のアドレスを保有させ、公開するアドレスを前記端末機能用アドレスとすることで、宛先ユーザ端末のアドレスを未公開としつつ通信を実現する方式が有効であると考えられる。この方式では、送信元ユーザ端末は、宛先アドレスとして、宛先ユーザを収容する多重アクセス装置上の端末機能のアドレスを指定する。送信元ユーザ端末からパケットを受信した多重アクセス装置上の端末機能は、受信したパケットの宛先アドレスを宛先ユーザ端末のアドレスに変換して転送する。これは、端末機能にＮＡＰＴ（Network Address Port Translation：RFC2663）機能を保有させることで実現できる。

【００１０】

【非特許文献１】八木 毅　他、「コミュニティ通信を支援するセキュアネットワーキングプラットホーム（ＳＰＸ）のアーキテクチャ設計」、電子情報通信学会、信学技法、ＩＮ２００６－１７３、ｐｐ．６５－７０、２００７。

【発明の開示】

【発明が解決しようとする課題】

【００１１】

しかしながら、上述した従来の技術では、宛先のユーザ端末では、受信したパケットの送信元アドレスを参照することで、送信元ユーザ端末のアドレスを特定することができる。前述したように、アドレス情報の漏えいに起因したスパム，フィッシングおよびＤＯＳ攻撃などのセキュリティ問題の発生を防止する観点から、アドレス情報が他者に漏えいすることは好ましくない。例えば、宛先ユーザ端末で参照が可能な送信元ユーザ端末のアドレスは、宛先ユーザ端末のインターネット接続で第三者に漏えいする可能性がある。このように送信元ユーザ端末のアドレスが漏洩すると、第三者による前述したようなセキュリティ問題が引き起こされ、送信元ユーザ端末が攻撃を受ける可能性がある。このように、従来の技術では、アドレス情報が他社に漏洩する可能性があるという問題があった。

【００１２】

本発明は、以上のような問題点を解消するためになされたものであり、送信元ユーザ端末のアドレスが隠蔽された状態で、複数の論理網にアクセスできるようにすることを目的とする。

【課題を解決するための手段】

【００１３】

本発明に係る多重アクセス装置は、複数の論理網を識別する論理網アドレスと論理網に所属する収容ユーザ端末を識別する論理網用端末アドレスとの対応を示す所属論理網用アドレスリストを備え、送信元の収容ユーザ端末より受信したパケットの送信元の収容ユーザ端末のユーザ端末アドレスに対応する論理網用端末アドレスを所属論理網用アドレスリストより検索する所属論理網管理手段と、パケットの送信元アドレスを検索された論理網用端末アドレスに変更する送信元アドレス変更手段とを少なくとも備えるようにしたものである。

【００１４】

ここで、収容している収容ユーザ端末に、収容ユーザ端末が所属する論理網識別子と収容ユーザ端末を識別する端末識別子とで階層化された論理網用端末アドレスを割り当て、宛先の収容ユーザ端末が所属している論理網を宛先とした宛先の収容ユーザ端末に対して送出されたパケットの宛先アドレスを、宛先の収容ユーザ端末のユーザ端末アドレスに変更して宛先の収容ユーザ端末へ転送し、送信元の収容ユーザ端末から送信されるパケットには、宛先の収容ユーザ端末が所属する論理網を識別する論理網識別子が備えられ、宛先の収容ユーザ端末が受信したパケットには、送信元の収容ユーザ端末が所属する論理網を識別する論理網識別子が備えられている。

【発明の効果】

【００１５】
以上説明したように、本発明によれば、送信元の収容ユーザ端末より受信したパケットの送信元のユーザ端末アドレスに対応する論理網用端末アドレスを所属論理網用アドレスリストに検索し、パケットの送信元アドレスを検索した論理網用端末アドレスに変更するようにしたので、送信元のユーザ端末のユーザ端末アドレスが隠蔽された状態で、複数の論理網にアクセスできるようになるという優れた効果が得られる。
【発明を実施するための最良の形態】
【００１６】
以下、本発明の実施の形態について図を参照して説明する。　図１は、本発明の実施の形態における多重アクセス装置、及び多重アクセス装置が適用可能なネットワークモデルの構成例を示す構成図である。このネットワークモデルは、多重アクセス装置Ａ１０１，多重アクセス装置Ｂ１０２，多重アクセス装置Ｃ１０３，多重アクセス装置Ｄ１０４，パケット転送装置１０６～１０９を備えている。また、ユーザ端末Ａ１１０，ユーザ端末Ｂ１１１，ユーザ端末Ｃ１１２，ユーザ端末Ｄ１１３，ユーザ端末Ｅ１１４，及びユーザ端末Ｆ１１５は、各アクセス網１１６～１１９を経由して、多重アクセス装置Ａ１０１，多重アクセス装置Ｂ１０２，多重アクセス装置Ｃ１０３，及び多重アクセス装置Ｄ１０４に収容されている。
【００１７】
一般に、多重アクセス装置は、例えば、エッジノードもしくはエッジルータと呼ばれ、パケット転送装置は、コアノードもしくはコアルータと呼ばれている。なお、多重アクセス装置は、ユーザ端末内にあってもよく、また、ホームゲートウェイとしてユーザ端末の側に配置されていても良い。
【００１８】
なお、多重アクセス装置Ａ１０１，多重アクセス装置Ｂ１０２，多重アクセス装置Ｃ１０３，多重アクセス装置Ｄ１０４，パケット転送装置１０６～１０９を備えるネットワークをコアネットワーク１２０とし、各ユーザ端末で構成されるネットワークをユーザネットワーク１２１とする。
【００１９】
次に、図２を用いて物理ネットワークの状態を説明する。図２は、図１に示した多重アクセス装置が適用されるネットワークにおける物理ネットワークの一例を示す構成図である。まず、ユーザ端末Ａ１１０はリンク２０１で多重アクセス装置Ａ１０１に収容され、ユーザ端末Ｂ１１１はリンク２０２で多重アクセス装置Ｂ１０２に収容され、ユーザ端末Ｃ１１２はリンク２０３で多重アクセス装置Ｃ１０３に収容され、ユーザ端末Ｄ１１３はリンク２０４で多重アクセス装置Ｃ１０３に収容され、ユーザ端末Ｅ１１４はリンク２０５で多重アクセス装置Ｄ１０４に収容され、ユーザ端末Ｆ１１５はリンク２０６で多重アクセス装置Ｄ１０４に収容されている。
【００２０】
また、多重アクセス装置Ａ１０１は、リンク２０７でパケット転送装置１０６と接続され、リンク２０８でパケット転送装置１０７と接続されている。多重アクセス装置Ｂ１０２は、リンク２０９でパケット転送装置１０６と接続され、リンク２１０でパケット転送装置１０７と接続されている。多重アクセス装置Ｃ１０３は、リンク２１１でパケット転送装置１０８と接続され、リンク２１２でパケット転送装置１０９と接続されている。多重アクセス装置Ａ１０１は、リンク２１３でパケット転送装置１０８と接続され、リンク２１４でパケット転送装置１０９と接続されている。
【００２１】
また、パケット転送装置１０６は、リンク２１５でパケット転送装置１０７と接続され、リンク２１６でパケット転送装置１０８と接続され、リンク２１７でパケット転送装置１０９と接続されている。パケット転送装置１０７は、リンク２１８でパケット転送装置１０８と接続され、リンク２１９でパケット転送装置１０９と接続されている。パケット転送装置１０８は、リンク２２０でパケット転送装置１０９と接続されている。なお、リ

ンクは、光ファイバや光波長のような光パスや、イーサネット（登録商標）ケーブルのような物理ケーブルである。

【００２２】

次に、本実施の形態における多重アクセス装置が適用されるネットワークの論理モデルについて図３を用いて説明する。図３は、図１に示した多重アクセス装置が適用されるネットワークにおける論理モデルの一例を示す構成図である。この論理モデルでは、ユーザ端末Ａ１１０は、ユーザ端末アドレスＵ＃１で識別され、ユーザ端末Ｂ１１１は、ユーザ端末アドレスＵ＃２で識別され、ユーザ端末Ｃ１１２は、ユーザ端末アドレスＵ＃３で識別され、ユーザ端末Ｄ１１３は、ユーザ端末アドレスＵ＃４で識別され、ユーザ端末Ｅ１１４はユーザ端末アドレスＵ＃５で識別され、ユーザ端末Ｆ１１５は、ユーザ端末アドレスＵ＃６で識別される。

【００２３】

また、各多重アクセス装置には、収容ユーザ端末用の論理網端末が設置され、この論理網端末は、接続先の論理網毎にアドレス（論理網用端末アドレス）を備える。このアドレスは、論理網識別子と端末識別子で階層化されている。本実施の形態では、各ユーザ端末の論理網用端末アドレスをＮ１－Ｃ１などと表現し、Ｎ１を論理網識別子、Ｃ１を端末識別子とする。

【００２４】

また、転送経路は論理網毎に分離され、論理網Ａの転送経路３０１，論理網Ｂの転送経路３０２，及び論理網Ｃの転送経路３０３は、論理網識別子で識別される。本実施の形態では、ユーザ端末Ａ１１０が論理網Ａ及び論理網Ｂへ所属し、ユーザ端末Ｂ１１１が論理網Ａ及び論理網Ｃへ所属し、ユーザ端末Ｃ１１２が論理網Ａ及び論理網Ｂへ所属し、ユーザ端末Ｄ１１３が論理網Ａ及び論理網Ｃへ所属し、ユーザ端末Ｆ１１５が論理網Ａ，論理網Ｂ，及び論理網Ｃへ所属している環境を想定している。

【００２５】

このとき、多重アクセス装置Ａ１０１は、ユーザ端末Ａ１１０が接続する論理網の論理網端末毎に、論理網Ａに対して論理網用端末アドレスＮ１－Ｃ１を備え、論理網Ｂに対しては論理網用端末アドレスＮ２－Ｃ３を備える。また、多重アクセス装置Ｂ１０２は、ユーザ端末Ｂ１１１が接続する論理網の論理網端末毎に、論理網Ａに対して論理網用端末アドレスＮ１－Ｃ２を備え、論理網Ｃに対しては論理網用端末アドレスＮ３－Ｃ１を備える。また、多重アクセス装置Ｃ１０３は、ユーザ端末Ｃ１１２が接続する論理網の論理網端末毎に、論理網Ａに対して論理網用端末アドレスＮ１－Ｃ３を備え、論理網Ｂに対しては論理網用端末アドレスＮ２－Ｃ２を備えている。加えて、多重アクセス装置Ｃ１０３は、ユーザ端末Ｄ１１３が接続する論理網の論理網端末毎に、論理網Ａに対しては論理網用端末アドレスＮ１－Ｃ４を備え、論理網Ｃに対しては論理網用端末アドレスＮ３－Ｃ３を保有する。また、多重アクセス装置Ｄ１０４は、ユーザ端末Ｆ１１５が接続する論理網の論理網端末毎に、論理網Ａに対して論理網用端末アドレスＮ１－Ｃ５を備え、論理網Ｂに対しては論理網用端末アドレスＮ２－Ｃ１を備え、論理網Ｃに対しては論理網用端末アドレスＮ３－Ｃ２を保有する。

【００２６】

上述した経路の中で、各々に到達するための経路は、ルーチングプロトコルにより管理されている。各アドレスは、ネットワークがＩＰｖ４ネットワークであればＩＰｖ４アドレスとなり、この場合のルーチングプロトコルとしてはＯＳＰＦ（Open Shortest Path First:RFC2328）などが挙げられる。また、ネットワークがＩＰｖ６ネットワークであればＩＰｖ６アドレスとなり、この場合のルーチングプロトコルとしては、ＯＳＰＦｖ６（Open Shortest Path First version 6:RFC2740）などが挙げられる。また、ネットワークがＭＰＬＳ（Multi-Protocol Label Switching）ネットワーク（:RFC3031）である場合、ルーチングプロトコルで経路を特定した後、ＲＳＶＰ－ＴＥ（ReSerVation Protocol with Traffic Engineering:RFC3209）やＣＲ－ＬＤＰ（Constrain-based Label Distribution Protocol:RFC3212）などのシグナリングプロトコルで、送信元と宛先のパケット転送装置

間にＬＳＰ（Label Switched Path）と呼ばれるパスを設定する。

【００２７】

次に、多重アクセス装置の構成例について説明する。図４は、図１に示した多重アクセス装置Ａ１０１の構成例を示す構成図である。多重アクセス装置Ａ１０１は、単一のユーザ端末Ａ１１０を収容している。多重アクセス装置Ａ１０１は、アクセス転送機能部４２２と、転送先端末特定機能部４２３と、論理網Ａ端末機能部４２４と、論理網Ｂ端末機能部４２５と、所属論理網管理機能部４２６と、コア転送機能部４２７とを備えている。なお、ユーザ端末Ａ１１０が、論理網Ｃにも所属している場合、論理網Ｃ端末機能部も備えることになる。

【００２８】

アクセス転送機能部４２２は、収容しているユーザ端末から送信されたパケットを受信する機能と、受信したパケットを後述する転送先端末特定機能部４２３へ転送する機能と、コアネットワークから受信して他機能部で処理されたパケットを収容しているユーザ端末へ送信する機能を有している。

【００２９】

転送先端末特定機能部４２３は、図５に例示する転送先端末特定テーブルを参照するなどして、受信したパケットの論理網識別子を参照し、上述したパケットの転送先の論理網を特定し、特定した論理網用の端末機能部（論理網用端末機能部）にパケットを転送する機能を有している。論理網用端末機能部は同じ機能を保有する。論理網Ａ端末機能部４２４は、アドレス変更機能として、送信元アドレス変更機能部４２８及びＮＡＰＴ機能部４２９を備えている。

【００３０】

送信元アドレス変更機能部４２８は、パケットの送信元アドレス（ユーザ端末アドレス）を変更する機能を有している。ＮＡＰＴ機能部４２９は、図７に例示する論理網Ａ端末ＮＡＰＴテーブルを参照するなどして、パケットの宛先アドレス（論理網用端末アドレス）を変換用アドレス（ユーザ端末アドレス）に変換する機能（ＮＡＰＴ機能）を有している。ここで、論理網Ａ端末ＮＡＰＴテーブルの宛先アドレスには、論理網Ａ端末機能部４２４に割り当てられたアドレスが記述されていることを想定する。

【００３１】

論理網Ａ端末機能部４２４は、転送先端末特定機能部４２３からパケットを受信した際に、図７に例示する論理網ＡＮＡＰＴテーブルを参照し、参照の結果、宛先アドレスがヒットした際は（宛先アドレスの存在を確認した場合は）、ＮＡＰＴ機能部４２９を用いて宛先アドレスを変更し、この後、アクセス転送機能部に受信したパケットを転送する。

【００３２】

一方、論理網Ａ端末機能部４２４は、宛先アドレスがヒットしなかった際（受信したパケットの宛先アドレスを、論理網ＡＮＡＰＴテーブルに確認できなかった場合）は、所属論理網管理機能部４２６に論理網Ａ端末用のアドレスを問い合わせ、送信元アドレス変更機能部４２８により所属論理網管理機能部４２６からの応答通知に記述されたアドレスに受信したパケットの送信元アドレスを変更する。また、このように変更した後、後述するコア転送機能部４２７に受信したパケットを転送する機能を有している。

【００３３】

なお、所属論理網管理機能部４２６からの応答通知に記述されていたアドレスを記憶し、これ以降、パケット受信時に、論理網ＡＮＡＰＴテーブルを参照し、宛先アドレスがヒットしなかった際は、記憶していたアドレスに上記パケットの送信元アドレスを変更し、この後、後述するコア転送機能部４２７に上記パケットを転送する機能を、論理網Ａ端末機能部４２４に備えるようにしても良い。この場合、後述する所属論理網管理機能部４２６から、アドレスを変更する通知を受信した際に記憶しているアドレスを通知されたアドレスに変更する機能も備えてるようにしてもよい。

【００３４】

次に、論理網Ｂ端末機能部４２５は、上述同様に、送信元アドレス変更機能部４３０及

びＮＡＰＴ機能部４３１を備える。送信元アドレス変更機能部４３０は、パケットの送信元アドレスを変更する機能を有している。ＮＡＰＴ機能部４３１は、図８に例示する論理網Ｂ端末ＮＡＰＴテーブルを参照するなどし、パケットの宛先アドレス（論理網用端末アドレス）を変換用アドレス（ユーザ端末アドレス）に変換する機能を有している。なお、論理網Ｂ端末ＮＡＰＴテーブルの宛先アドレスには、論理網Ｂ端末機能部４２５に割り当てられたアドレスが記述されていることを想定する。

【００３５】

論理網Ｂ端末機能部４２５は、転送先端末特定機能部４２３からパケットを受信すると、図８に示す論理網ＢＮＡＰＴテーブルを参照し、宛先アドレスがヒットした場合は、ＮＡＰＴ機能部４２９を用いて宛先アドレスを変更し、この後、アクセス転送機能部に上記パケットを転送し、宛先アドレスがヒットしなかった場合は、後述する所属論理網管理機能部４２６に論理網Ｂ端末用のアドレスを問い合わせ、所属論理網管理機能部４２６からの応答通知に記述されたアドレスに上記パケットの送信元アドレスを変更し、この後、後述するコア転送機能部４２７に上記パケットを転送する機能を有している。

【００３６】

なお、所属論理網管理機能部４２６からの応答通知に記述されていたアドレスを記憶し、これ以降、パケット受信時に、論理網ＢＮＡＰＴテーブルを参照し、宛先アドレスがヒットしなかった場合は、記憶していたアドレスに上記パケットの送信元アドレスを変更し、この後、後述するコア転送機能部４２７に上記パケットを転送する機能を有してもよい。この場合、後述する所属論理網管理機能部４２６から、アドレスを変更する通知を受信した際に記憶しているアドレスを通知されたアドレスに変更する機能も備えている。

【００３７】

これらの論理網用端末機能部は、統合して１つの機能部としてもよい。このように１つの機能部とした場合には、転送先端末特定機能部は不要となる。さらに、１つの機能部とした場合は、ＮＡＰＴテーブルは全論理網の情報を統合した形となる。また、統合された１つの機能部は、ＮＡＰＴテーブルを検索して宛先アドレスがヒットしなかった場合に、受信パケットのアドレスに記載された論理網識別子からパケットを転送する論理網を特定することで、前述の手順を用いて変更すべき送信元アドレスを特定する。

【００３８】

所属論理網管理機能部４２６は、所属論理網用アドレスリスト４３２を備えている。所属論理網用アドレスリスト４３２は、図６に例示するアドレスリストのように、収容ユーザ（ユーザ端末）が所属する論理網に対して、収容ユーザ端末に割り当てられている各論理網用のアドレスを管理する機能を有している。言い換えると、所属論理網用アドレスリスト４３２は、複数の論理網を識別する論理網アドレスと、各論理網に所属するユーザ端末を識別する論理網用端末アドレスとの対応を示すアドレスリストを備え、これを管理している。

【００３９】

所属論理網管理機能部４２６は、各論理網用端末機能部からのアドレス問い合わせに対し、問い合わせ元の端末の所属する論理網に対応する論理網用端末アドレスを所属論理網用アドレスリスト４３２から特定し、上記論理網用端末アドレスを記述した応答通知を生成して送信元の論理網用端末機能部に送信する機能を有している。

【００４０】

コア転送機能部４２７は、論理網識別子確認機能部４３３と、出力インタフェース特定機能部４３４を備えている。論理網識別子確認機能部４３３は、受信パケットの宛先アドレスの論理網識別子と送信元アドレスの論理識別子を抽出し、同一か否かを確認する機能を有している。

【００４１】

出力インタフェース特定機能部４３４は、図９に例示する出力インタフェース特定テーブルを参照するなどして、各論理網端末機能部から受信したパケットの宛先アドレスから、出力先を特定する機能を有している。

【００４２】
コア転送機能部４２７は、論理網識別子確認機能部４３３により、受信パケットの宛先アドレスの論理識別子と送信元アドレスの論理識別子とが異なる場合はパケットを廃棄し、同一の場合は、出力インタフェース特定機能部４３４により出力先を特定してパケットを転送する機能を有している。
【００４３】
上述したように、本実施の形態の多重アクセス装置は、まず、終端する論理網毎に端末としてのアドレスを割り当てるとともに、これをアドレスリストとして管理する機能を備える。また、本多重アクセス装置は、アクセス網から受信した論理網宛のパケットについて、宛先アドレスの論理網識別子を参照してアドレスリストを検索し、同一の論理網識別子を有するアドレスを特定するとともに、送信元アドレスを上記アドレスに書き換える機能を備えている。
【００４４】
これらの機能部により、本多重アクセス装置では、転送先の論理網に応じて送信元アドレスを変更することが可能となり、宛先ユーザに対して送信元ユーザ端末のアドレスを隠蔽することが可能となる。
【００４５】
次に、図１に示した、複数のユーザ端末を収容する多重アクセス装置Ｃ１０３（多重アクセス装置Ｄ１０４）について説明する。図１０は、複数のユーザ端末を収容する多重アクセス装置Ｃ１０３の構成例を示す構成図である。本例において、多重アクセス装置Ｃ１０３が収容する端末は、ユーザ端末Ｃ１１２及びユーザ端末Ｄ１１３である。このように、複数のユーザ端末を収容する場合、収容しているユーザ端末（ユーザＣとユーザＤと）を識別（区別）する機能が必要となる。
【００４６】
多重アクセス装置Ｃ１０３は、複数ユーザアクセス転送機能部１０３５と、ユーザＣ用多重アクセス機能部１０３６と、ユーザＤ用多重アクセス機能部１０３７と、各ユーザ所属論理網管理機能部１０３８と、複数ユーザコア転送機能部１０３９を保有している。このように、収容ユーザが増加すると、各ユーザ端末用の多重アクセス機能部が追加されることとなる。
【００４７】
複数ユーザアクセス転送機能部１０３５は、コア転送先ユーザ特定機能部１０４０と、アクセス側出力インタフェース特定機能部１０４１を備えている。コア転送先ユーザ特定機能部１０４０は、図１１に例示するコア転送先ユーザ特定テーブルを参照するなどして、パケットの送信元ユーザを特定する機能を有している。アクセス側出力インタフェース特定機能部１０４１は、図１７に例示する出力先インタフェース特定テーブルを参照するなどして、パケットの宛先アドレスから出力先を特定する機能を有している。
【００４８】
複数ユーザアクセス転送機能部１０３５は、まず、収容しているユーザ端末からパケットを受信した場合に、コア転送先ユーザ特定機能部１０４０によりパケット送信元のユーザを特定し、この後、ユーザＣ用多重アクセス機能部１０３６もしくはユーザＤ用多重アクセス機能部１０３７の該当する方に、上記パケットを転送する機能を備えている。また、複数ユーザアクセス転送機能部１０３５は、ユーザＣ用多重アクセス機能部１０３６もしくはユーザＤ用多重アクセス機能部１０３７からパケットを受信した際に、アクセス側出力インタフェース特定機能部４１により上記パケットの宛先アドレスから出力先のリンクを特定してパケットを転送する機能を有している。
【００４９】
次に、ユーザＣ用多重アクセス機能部１０３６及びユーザＤ用多重アクセス機能部１０３７は、同様の構成を備え、転送先端末特定機能部１０４２，論理網Ａ端末機能部１０４３，及び論理網Ｂ端末機能部１０４４を備えている。転送先端末特定機能部１０４２と、各論理網端末機能部である論理網Ａ端末機能部１０４３及び論理網Ｂ端末機能部１０４４

とは、送信元アドレス変更機能部１０４５，ＮＡＰＴ機能部１０４６及び送信元アドレス変更機能部１０４７，ＮＡＰＴ機能部１０４８を備え、多重アクセス装置Ａ１０１が備える同一名称の機能部と同じ機能を保有する。

【００５０】

なお、多重アクセス装置Ａ１０１においてコア転送機能部４２７に送信されていたパケットは、多重アクセス装置Ｃ１０３では、複数ユーザコア転送機能部１０３９へ送信される。また、多重アクセス装置Ａ１０１においてアクセス転送機能部４２２に送信されていたパケットは、多重アクセス装置Ｃ１０３では、複数ユーザアクセス転送機能部１０３５へ送信されることとなる。

【００５１】

各ユーザ所属論理網管理機能部１０３８は、各ユーザ所属論理網用アドレスリスト１０４９を備えている。各ユーザ所属論理網用アドレスリスト１０４９は、図１４に例示するようなユーザ識別子と、上記ユーザ識別子を備えているユーザが所属する論理網に対して上記ユーザに割り当てられている各論理網用のアドレスとを管理する機能を有している。

【００５２】

各ユーザ所属論理網管理機能部１０３８は、ユーザＣ用多重アクセス機能部１０３６又はユーザＤ用多重アクセス機能部１０３７からのアドレス問い合わせに対し、アドレス問い合わせ元から対応するユーザ識別子を特定するとともに、問い合わせ元の端末の所属する論理網に対応するアドレスを、各ユーザ所属論理網用アドレスリスト１０４９から特定する。また、この特定の後、各ユーザ所属論理網管理機能部１０３８は、上記アドレスを記述した応答通知を生成し、問い合わせ送信元のユーザ識別子を備えているユーザＣ用多重アクセス機能部１０３６又はユーザＤ用多重アクセス機能部１０３７の、問い合わせ送信元の論理網用端末機能部に送信する機能を有している。

【００５３】

次に、複数ユーザコア転送機能部１０３９は、複数ユーザ論理網識別子確認機能部１０５０と、コア側出力インタフェース特定機能部１０５１と、アクセス転送先ユーザ特定機能部１０５２を備えている。

【００５４】

複数ユーザ論理網識別子確認機能部１０５０は、受信パケットの宛先アドレスの論理網識別子と送信元アドレスの論理識別子を抽出し、同一か否かを確認する機能を有している。コア側出力インタフェース特定機能部１０５１は、図１７に例示する出力インタフェース特定テーブルを参照するなどして、パケットの宛先アドレスから出力先を特定する機能を有している。アクセス転送先ユーザ特定機能部１０５２は、図１２に例示するアクセス転送先ユーザ特定テーブルを参照するなどして、パケットの送信先ユーザを特定する機能を有している。

【００５５】

複数ユーザコア転送機能部１０３９は、まず、複数ユーザ論理網識別子確認機能部１０５０により、受信パケットの宛先アドレスの論理識別子と送信元アドレスの論理識別子が異なる場合はパケットを廃棄する機能を備える。また、複数ユーザコア転送機能部１０３９は、各ユーザ用多重アクセス機能部の各論理網端末機能部から受信したパケットの宛先アドレスからコア側出力インタフェース特定機能部１０５１を用いて出力先を特定する機能を備える。また、複数ユーザコア転送機能部１０３９は、コアネットワークからパケットを受信すると、アクセス転送先ユーザ特定機能部１０５２によりパケット送信先のユーザを特定し、この後、ユーザＣ用多重アクセス機能部１０３６もしくはユーザＤ用多重アクセス機能部１０３７の該当する方にパケットを転送する機能を有している。

【００５６】

以上に説明したように、本実施の形態における多重アクセス装置（多重アクセス装置Ｃ１０３，多重アクセス装置Ｄ１０４）では、複数ユーザを収容する場合においても、終端する論理網毎に端末としてのアドレスを割り当てることができるとともに、これをアドレスリストとして管理する機能を備えている。また、アクセス網から受信した論理網宛のパ

ケットについて、図１３に例示する転送先端末特定手テーブルの宛先アドレスの論理網識別子を参照し、図１４に例示するアドレスリストを検索し、同一の論理網識別子を有するアドレスを特定するとともに、送信元アドレスを上記アドレスに書き換える機能を備えている。これらのことにより、本実施の形態によれば、複数ユーザを収容する場合においても、転送先の論理網に応じて送信元アドレスを変更することが可能となり、宛先ユーザに対して送信元ユーザ端末のアドレスを隠蔽することが可能となる。

【００５７】

次に、上述した本実施の形態における多重アクセス装置の動作例について説明する。図１８は、ユーザ端末Ａ１１０がユーザ端末Ｃ１１２宛のパケットを生成した際の動作例を示す構成図である。なお、図１８において、図１と同一の符号は同じ構成を示している。この例では、ユーザ端末Ａ１１０とユーザ端末Ｃ１１２は、論埋網Ａに所属しており、ユーザ端末Ａ１１０は多重アクセス装置Ａ１０１上にアドレスＮ１－Ｃ１が割り当てられた論埋網Ａ用端末機能部を保有し、ユーザ端末Ｃ１１２は多重アクセス装置Ｃ１０３上にアドレスＮ１－Ｃ３が割り当てられた論理網Ａ用端末機能部を備えている。

【００５８】

また、ユーザ端末Ａ１１０は、自身が備えているアドレスＵ＃３を送信元アドレスとし、宛先アドレスとしては、ユーザ端末Ｃ１１２が多重アクセス装置Ｃ１０３上に備えている論理網Ａ用端末（Ｎ１－Ｃ３）を指定してパケット１８０１を生成して送信する。

【００５９】

パケットを受信した多重アクセス装置Ａ１０１では、図１９に矢視線で示すように、アクセス転送機能部４２２を経由して転送先端末特定機能部４２３にパケットを転送し、転送先端末特定機能部４２３において、受信パケットの論理網識別子Ｎ１を参照し、転送先の論理網を論理網Ａと特定し、論理網Ａ端末機能部４２４にパケットを転送する。このようにして転送されたパケットを受け付けた論理網Ａ端末機能部４２４は、図７のＮＡＰＴテーブルを参照するなどし、宛先アドレスがヒットしないため、所属論理網管理機能部４２６に論理網Ａ端末用のアドレスを問い合わせ、応答通知に記載されていたアドレスＮ１－Ｃ１を送信元アドレスとするようパケットの送信元アドレスを変更し、コア転送機能部４２７にパケットを転送する。

【００６０】

コア転送機能部４２７は、送信元アドレスの論理網識別子Ｎ１と宛先アドレスの論理網識別子Ｎ１を参照し、両者が同一であるため、図９の出力インタフェース特定テーブルを参照するなどし、パケットの宛先アドレスから出力先としてリンク２０７（図２）を特定してパケットを送信する。ここで送信されるパケットは、図２０のパケット２００１に示すように、送信元アドレスが「Ｎ１－Ｃ１」に変更される。

【００６１】

上記パケットを受信した多重アクセス装置Ｃ１０３は、図２１に矢視線で示すように、複数ユーザコア転送機能部１０３９でパケットを受信した後、複数ユーザ論理網識別子確認機能部１０５０により受信パケットの宛先アドレスの論理網識別子Ｎ１と送信元アドレスの論理識別子Ｎ１が同一であることを確認し、図１２に例示するアクセス転送先ユーザ特定テーブルを参照するなどして、パケットの宛先アドレスから送信先ユーザであるユーザ端末Ｃ１１２を特定し、ユーザ端末Ｃ用多重アクセス機能部１０３６へパケットを転送する。

【００６２】

ユーザ端末Ｃ用多重アクセス機能部１０３６では、転送先端末特定機能部１０４２において、受信パケットの論理網識別子Ｎ１を参照し、転送先の論理網を論理網Ａと特定し、論理網Ａ端末機能部１０４３にパケットを転送する。論理網Ａ端末機能部１０４３は、図１５のＮＡＰＴテーブルを参照し、宛先がヒットした際に、ＮＡＰＴ機能部１０４６により宛先アドレス（論理網用端末アドレス）をテーブルに記載されたアドレスＵ＃３（ユーザ端末アドレス）に変更し、複数ユーザアクセス転送機能部１０３５へパケットを転送する。複数ユーザアクセス転送機能部１０３５は、アクセス側出力インタフェース機能部１

０４１により、出力先のリンク２０３（図２）を特定してパケットを送信する。以上のようにして多重アクセス装置Ｃ１０３より送信されるパケットは、図２２のパケット２２０１に示すように、宛先アドレスが「Ｕ＃３」に変更される。

【００６３】

以上に説明したように、本実施の形態における多重アクセス装置を配置するパケット通信網では、送信元ユーザ端末は宛先ユーザ端末のアドレス（ユーザ端末アドレス）を知ることなくパケットを送信でき、かつ、宛先ユーザ端末は送信元ユーザ端末のアドレス（ユーザ端末アドレス）を知ることなくパケットを受信できる。さらに、宛先ユーザ端末は、受信パケットの送信元アドレス（論理網用端末アドレス）を宛先アドレスとしてパケットを返送すれば、上記パケットは送信元ユーザ端末に到達する。これにより、ユーザ端末のアドレスを隠蔽した状態で、双方向の通信が実現できる。

【００６４】

上述のように、本発明によれば、ユーザ端末のアドレス情報（ユーザ端末アドレス）を隠蔽しつつユーザに複数ＶＰＮへの多重帰属機能を提供するために、送信元ユーザを収容する多重アクセス装置において、終端する論理網毎に端末としてのアドレス（論理網用端末アドレス）を割り当て、これをアドレスリストとして管理し、さらに、アクセス網から受信した論理網宛のパケットについて、宛先アドレスの論理網識別子を参照し、アドレスリストを検索し、同一の論理網識別子を有するアドレス（論理網用端末アドレス）を特定するとともに、送信元アドレスをこのアドレスに書き換えるようにした。

【００６５】

これにより、宛先ユーザ端末に対して送信元ユーザ端末のアドレスを隠蔽することが可能となり、各ユーザ端末は複数の論理網にセキュアにアクセスできる。この結果、本発明により、ネットワーク事業者は、ユーザ端末のアドレスを隠蔽しつつ、一般的なユーザ端末に対して、複数ＶＰＮ多重帰属サービスを提供でき、安心・安全・便利なネットワークサービスが実現できるようになる。

【図面の簡単な説明】

【００６６】

【図１】本発明の実施の形態における多重アクセス装置、及び多重アクセス装置が適用可能なネットワークモデルの構成例を示す構成図である。

【図２】図１に示した多重アクセス装置が適用されるネットワークにおける物理ネットワークの一例を示す構成図である。

【図３】図１に示した多重アクセス装置が適用されるネットワークにおける論理モデルの一例を示す構成図である。

【図４】図１に示した多重アクセス装置Ａ１０１の構成例を示す構成図である。

【図５】転送先端末特定テーブルの構成例を示す構成図である。

【図６】アドレスリストの構成例を示す構成図である。

【図７】論理網Ａ端末ＮＡＰＴテーブルの構成例を示す構成図である。

【図８】論理網Ｂ端末ＮＡＰＴテーブルの構成例を示す構成図である。

【図９】出力インタフェース特定テーブルの構成例を示す構成図である。

【図１０】複数のユーザ端末を収容する多重アクセス装置Ｃ１０３の構成例を示す構成図である。

【図１１】コア転送先ユーザ特定テーブルの構成例を示す構成図である。

【図１２】アクセス転送先ユーザ特定テーブルの構成例を示す構成図である。

【図１３】転送先端末特定テーブルの構成例を示す構成図である。

【図１４】アドレスリストの構成例を示す構成図である。

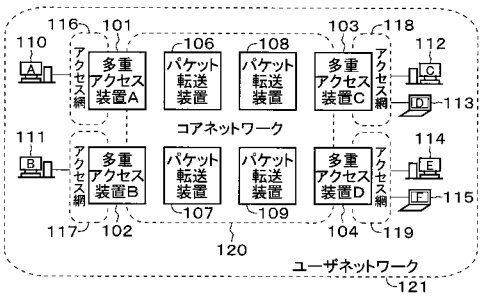
【図１５】ユーザＣ用多重アクセス機能論理網Ａ端末ＮＡＰＴテーブルの構成例を示す構成図である。

【図１６】ユーザＣ用多重アクセス機能論理網Ｂ端末ＮＡＰＴテーブルの構成例を示す構成図である。

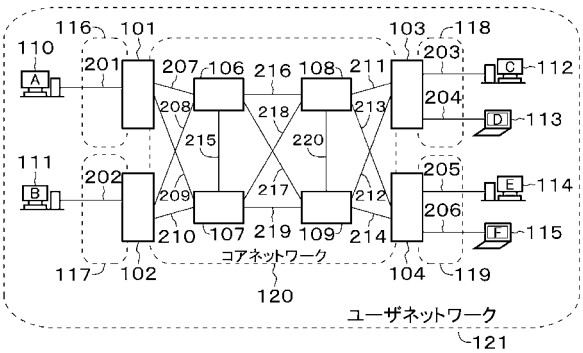
【図１７】出力先インタフェース特定テーブルの構成例を示す構成図である。

【図１８】ユーザ端末Ａ１１０がユーザ端末Ｃ１１２宛のパケットを生成した際の動作例を示す構成図である。
【図１９】多重アクセス装置Ａ１０１によるパケット転送の動作例を矢視線で示す構成図である。
【図２０】多重アクセス装置Ａ１０１によるユーザ端末Ｃ１１２宛のパケットを生成した際の動作例を示す構成図である。
【図２１】多重アクセス装置Ｃ１０３によるパケット転送の動作例を矢視線で示す構成図である。
【図２２】多重アクセス装置Ｃ１０３によるユーザ端末Ｃ１１２宛のパケットを生成した際の動作例を示す構成図である。
【符号の説明】
【００６７】
１０１…多重アクセス装置Ａ、１０２…多重アクセス装置Ｂ、１０３…多重アクセス装置Ｃ、１０４…多重アクセス装置Ｄ、１０６～１０９…パケット転送装置、１１０…ユーザ端末Ａ、１１１…ユーザ端末Ｂ、１１２…ユーザ端末Ｃ、１１３…ユーザ端末Ｄ、１１４…ユーザ端末Ｅ、１１５…ユーザ端末Ｆ、１１６～１１９…アクセス網、１２０…コアネットワーク、１２１…ユーザネットワーク。

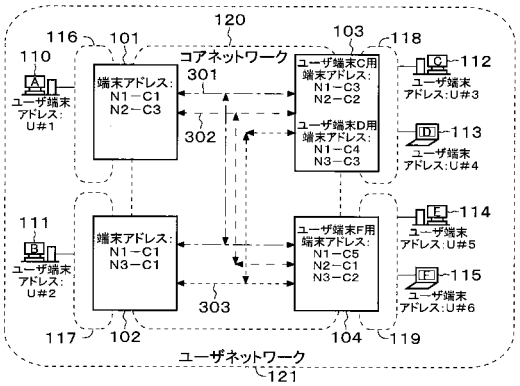
【図１】



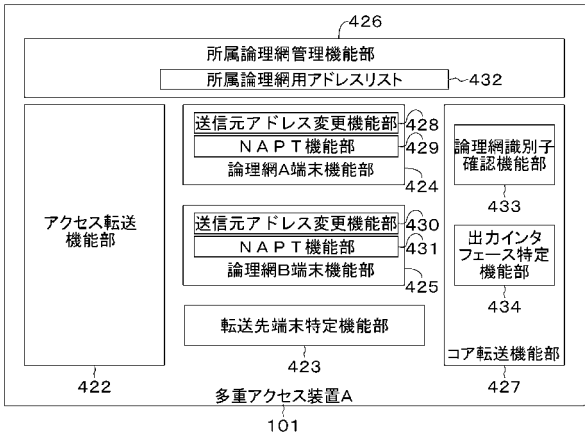
【図２】



【図３】



【図４】



【図５】

宛先アドレス 論理網識別子	端末機能識別子
N1	論理網A
N2	論理網B

【図６】

所属論理網管理リスト	論理網用端末アドレス
論理網A	N1－C1
論理網B	N2－C3

【図７】

宛先アドレス	変換用アドレス
N1－C1	U#1

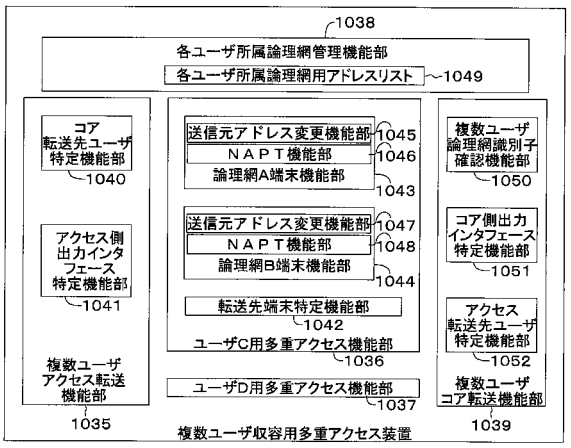
【図８】

宛先アドレス	変換用アドレス
N2－C3	U#1

【図９】

宛先アドレス	出力先
N1－C2	リンク208
N1－C3	リンク207
N1－C4	リンク207
N1－C5	リンク208
N2－C1	リンク207
N2－C2	リンク207

【図１０】



【図１１】

送信先アドレス	ユーザ識別子
U#3	ユーザC
U#4	ユーザD

【図１２】

宛先アドレス	端末機能別識別子
N1－C2	ユーザC
N1－C3	ユーザD
N1－C4	ユーザC
…	…

【図１３】

宛先アドレス 論理網識別子	端末機能識別子
N1	論理網A
N2	論理網B

【図１４】

ユーザ識別子	論理網用管理リスト	論理網用端末アドレス
ユーザC	論理網A	N1－C3
ユーザC	論理網B	N2－C2
ユーザD	論理網A	N1－C4
ユーザD	論理網C	N3－C3
…		

【図１５】

宛先アドレス	変換用アドレス
N1－C3	U#3

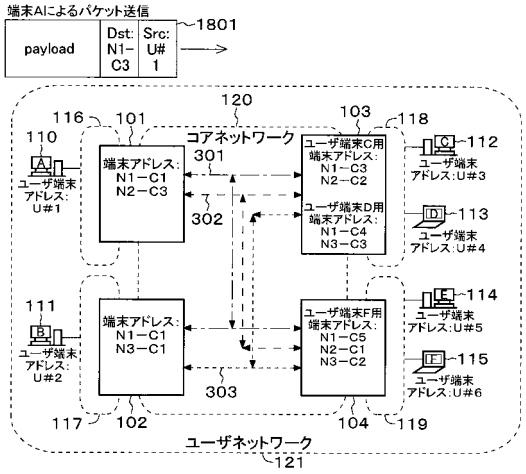
【図１６】

宛先アドレス	変換用アドレス
N2－C2	U#3

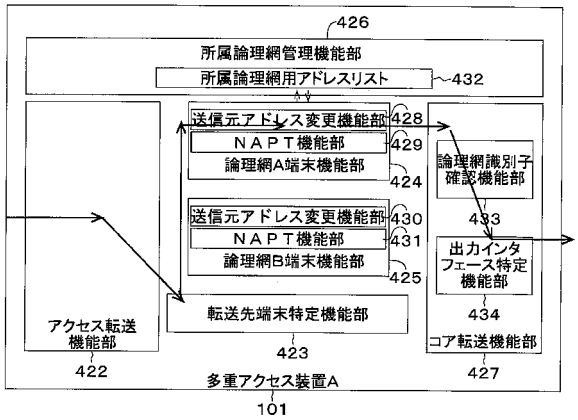
【図１７】

宛先アドレス	出力先
N1－C1	リンク211
N1－C2	リンク211
N1－C5	リンク212
N1－C1	リンク212
…	…
U#3	リンク203
U#4	リンク204

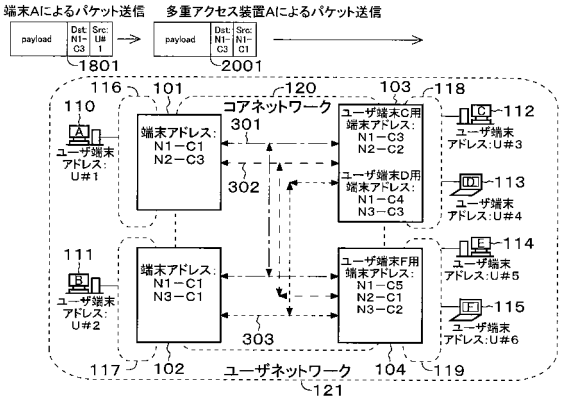
【図１８】



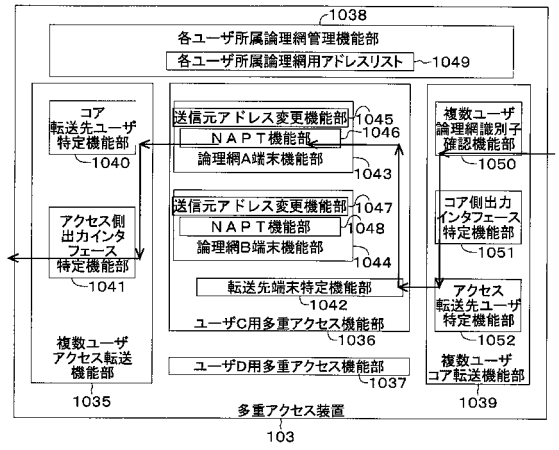
【図１９】



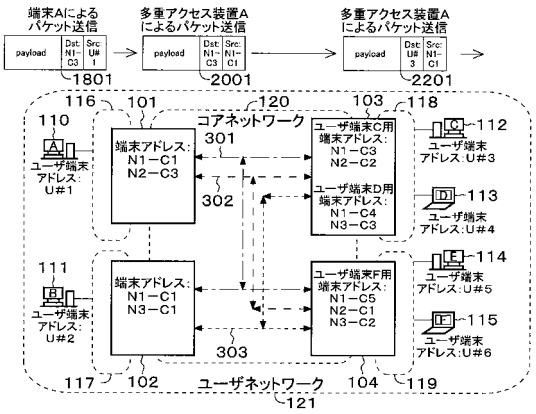
【図２０】



【図２１】



【図２２】



フロントページの続き

(72)発明者　近藤　努
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　桑原　健
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　村山　純一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　大崎　博之
大阪府吹田市山田丘１番１号　国立大学法人大阪大学内
(72)発明者　今瀬　真
大阪府吹田市山田丘１番１号　国立大学法人大阪大学内

審査官　中木　努

(56)参考文献　特開２００６－１２８８０３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／２８－４６、５６，６６