

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4038221号

(P4038221)

(45) 発行日 平成20年1月23日(2008.1.23)

(24) 登録日 平成19年11月9日(2007.11.9)

(51) Int. Cl.	F I
<b>H O 4 L 12/46 (2006.01)</b>	H O 4 L 12/46 E
	H O 4 L 12/46 M
	H O 4 L 12/46 V

請求項の数 16 (全 15 頁)

(21) 出願番号	特願2005-354886 (P2005-354886)	(73) 特許権者	500260296
(22) 出願日	平成17年12月8日(2005.12.8)		フリービット株式会社
(65) 公開番号	特開2007-159012 (P2007-159012A)		東京都渋谷区円山町3番6号
(43) 公開日	平成19年6月21日(2007.6.21)	(74) 代理人	100104411
審査請求日	平成19年10月3日(2007.10.3)		弁理士 矢口 太郎
早期審査対象出願		(74) 代理人	100104215
			弁理士 大森 純一
		(74) 代理人	100099656
			弁理士 山口 康明
		(72) 発明者	北村 淳
			東京都渋谷区円山町3番6号 フリービッ
			ト株式会社内
		(72) 発明者	屋島 新平
			東京都渋谷区円山町3番6号 フリービッ
			ト株式会社内

最終頁に続く

(54) 【発明の名称】 中継装置及びクライアント機器とサーバとの接続方法

(57) 【特許請求の範囲】

【請求項1】

L A N上のクライアント機器を、インターネット上のサーバを通した仮想ネットワークに接続するために、前記L A N上の前記クライアント機器の上流側に設置される中継装置であって、

この中継装置は、ブリッジモジュールを有し、このブリッジモジュールは、ローカル通信プロトコルスタックとネットワークデバイスとの間に設けられ、自己宛、ブロードキャスト及び仮想ネットワークのアドレス宛の要求パケット以外のパケットはローカル通信プロトコルスタックに渡さずに単に前記L A Nの上流側と下流側とをブリッジするものであり、

この中継装置は、さらに、

前記インターネット上のサーバのグローバルアドレスを記憶するサーバアドレス記憶部と、

前記サーバのグローバルアドレスに基づき、この中継装置とサーバとの間にトンネリング接続を確立するためのトンネリング接続確立部と、

前記ブリッジモジュールにより前記クライアント機器からの上記仮想ネットワーク上の仮想ネットワークアドレスを含む要求パケットを捕捉し、発信元アドレスとして前記クライアント機器の仮想ネットワークアドレスを付したものをカプセリングし、前記トンネリング接続を介して前記サーバへ送出するカプセリング処理部と、

前記ローカル通信プロトコルスタックを通して受け取ったトンネリング接続における自

己宛パケットをディカプセリングすると共に、このディカプセリングしたパケットに含まれる宛先仮想ネットワークアドレスを前記クライアント機器のLAN上のプライベートIPアドレスに変換し、このパケットをブリッジモジュールにより当該クライアント機器に送出するディカプセリング処理部と

を有することを特徴とする中継装置。

【請求項2】

請求項1記載の中継装置において、

前記中継装置は、前記LANにおいて、クライアント機器からルータに至る経路の途中に設置されるものであることを特徴とする中継装置。

【請求項3】

請求項1記載の中継装置において、

前記中継装置は、インターネット上に設けられたトンネル仲介サーバに接続し、この仲介サーバから前記サーバのグローバルアドレスを受け取るものである

ことを特徴とする中継装置。

【請求項4】

請求項1記載の中継装置において、

前記中継装置は、

クライアント機器に割り当てる仮想ネットワークアドレスを前記サーバから受け取り、各クライアント機器のLAN上のプライベートIPアドレスとこのクライアントに割り当てた仮想ネットワークアドレスを関連付けて記憶するものである

ことを特徴とする中継装置。

【請求項5】

請求項4記載の中継装置において、

前記LAN下流側のネットワークデバイスに到達する全てのパケットを監視することで前記クライアント機器のプライベートIPアドレス及びMACアドレスを検出する下流側クライアント機器検出部を有するものである

ことを特徴とする中継装置。

【請求項6】

請求項5記載の中継装置において、

前記下流側クライアント機器検出部は、ブロードキャストの応答要求を定期的若しくは任意にLANの下流側に送信し、前記クライアント機器の応答を促す機能を有する

ことを特徴とする中継装置。

【請求項7】

請求項1記載の中継装置において、

前記クライアント機器は、ネットワーク対応の家電であるが、ユーザが仮想ネットワークドライバ等をインストールできない家電を含むことを特徴とする中継装置。

【請求項8】

請求項1記載の中継装置において、

前記クライアント機器は、前記中継装置とは通信可能であるが、自らはインターネットに接続することができない周辺装置を含むものであることを特徴とする中継装置。

【請求項9】

請求項1記載の中継装置において、

前記ブリッジモジュールは、ブロードキャストの要求パケットは、前記通信プロトコルスタックに渡すと共に、前記ブリッジするものであることを特徴とする中継装置。

【請求項10】

LAN上のクライアント機器と、このLAN上の前記クライアント機器の上流側に接続された中継装置と、前記クライアント機器がインターネットを介して接続されるサーバと、を有するインターネット接続環境において実行される、前記クライアント機器とサーバとの接続方法であって、

(a)前記中継装置が前記サーバのグローバルIPアドレスを受け取り格納する工程と

10

20

30

40

50

、  
 (b) 前記中継装置が、前記で通知されたグローバルIPアドレスを使用して前記中継装置と前記サーバとの間で、トンネリング接続によるTCP/IPセッションを確立する工程と、

(c) 前記中継装置が、前記クライアント機器に仮想ネットワークIPアドレスを割り当て、前記サーバから前記トンネリング接続を通して受け取った仮想ネットワークIPアドレス宛の packets を前記クライアント機器のLAN上のプライベートIPアドレス宛に書き換えて前記LANの下流側に送出する工程と、

(d) 前記中継装置が、前記クライアント機器からの上記仮想ネットワークIPアドレスを含む packets を捕獲し、前記トンネリング接続を通して前記サーバへ送出する工程とを有することを特徴とする接続方法。 10

【請求項11】

請求項10記載の接続方法において、

前記中継装置は、前記クライアント機器の属するLAN上に設置されるものであり、この方法は、この中継装置宛、ブロードキャスト及び仮想ネットワークのアドレス宛の要求 packets 以外の packets は前記(c)、(d)工程を行わずにLAN上で単にブリッジするものであることを特徴とする方法。

【請求項12】

請求項10記載の方法において、 20

さらに、前記サーバが前記中継装置に前記クライアント機器用の仮想ネットワークIPアドレスを通知する工程を有することを特徴とする方法。

【請求項13】

請求項10記載の方法において、

前記中継装置が、インターネット上に設けられたトンネル仲介サーバに接続し、この仲介サーバから前記サーバのグローバルアドレスを受け取る工程をさらに有することを特徴とする方法。

【請求項14】

請求項10記載の方法において、

前記中継装置が、前記クライアント機器に割り当てる仮想ネットワークアドレスを前記サーバから受け取り、各クライアント機器のLAN上のプライベートIPアドレスとこのクライアントに割り当てた仮想ネットワークアドレスを関連付けて記憶する工程をさらに有するものである 30

ことを特徴とする方法。

【請求項15】

請求項14記載の方法において、

前記中継装置が、前記LAN下流側のネットワークデバイスに到達する全ての packets を監視することで前記クライアント機器のプライベートIPアドレス及びMACアドレスを検出する工程をさらに有する

ことを特徴とする方法。 40

【請求項16】

請求項15記載の方法において、

前記中継装置が、ブロードキャストの応答要求を定期的若しくは任意にLANの下流側に送信し、前記クライアント機器の応答を促す機能を有する

ことを特徴とする方法。

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、IPv4 (Internet Protocol version 4) が普及した現状のインフラ環境の下で、比較的簡易な手段により異なるLANに属する端末同士を、インターネットを 50

通してかつセキュリティの高い方法で双方向の通信を可能とする、中継装置及びクライアント機器とサーバとの接続方法に関するものである。

【背景技術】

【0002】

一般に、インターネットを中心とした公衆ネットワークを通じたサービス提供環境においては、全ての情報の価値は、クライアント側ではなく、サーバ側に集まるようになって

いる。

【0003】

すなわち、各クライアントである端末機器は、基本的にインターネット上の情報を閲覧するための単なるビューワーにしか過ぎない。また、各クライアントはインターネット側

10

【0004】

このような状況を変えるためには、アクセス方向を逆行させ、サーバとクライアントの立場を逆転させることが必要である。すなわち、インターネットに接続される家庭内ネットワークがある場合、インターネット側から家庭内ネットワークへのアクセスが開始され、家庭内ネットワーク側からインターネット側へサービスが提供されるような状態を作り出す必要がある。

20

【0005】

このためには、ホームネットワークに接続された機器のそれぞれが、インターネット側からユニークに特定できること、家庭内のルーティングの問題、セキュリティの問題を解決する必要がある。このような課題に対応し、ひとつの解決を見出せる技術として、IP

v 6 (Internet Protocol version 6: 第6世代インターネットプロトコル)がある。

【0006】

しかしながら、現在の日本のキャリアやインターネットサービスプロバイダを取り巻く環境を鑑みると、IP v 6の普及にはかなりの時間がかかるものと考えられる。例えば、現在使用しているIP v 4の機材償却に最低2年～3年は必要であり、テスト的なサービスが行われているのみである。

30

【0007】

今すぐにメーカーがIP v 6対応ネットワークを実現するには、ISPレベルのサービスにまで手を出すしかないが、非常にコストがかかることであり、多くのメーカーにとって現実的ではない。家庭内ネットワークの事情が様々で非常に大きく異なることや、キャリアやISPによって接続の仕組みが大きく異なることもあり、これらの差を吸収して画一的なアプローチでIP v 6環境を実現するための仕組みが必要である。

【0008】

この出願に係る発明の新規性や進歩性を否定するものではないが、上述した事情に関連する先行技術文献として以下のものがある。

【特許文献1】特開2001-274845号公報

40

【0009】

従来IP v 4環境下で、IP v 6ネットワークで実現されるような家庭内ネットワークとインターネットとの間の双方向のアクセスを実現しようとする場合、以下のような問題がある。

【0010】

例えば、現在のIP v 4環境下においては、自宅にネットワーク家電を設置する場合、自宅ネットワークを通して、インターネットに接続されたルータに繋げて使用する。このため、ネットワーク家電のIPアドレスは、プライベートアドレスになってしまい、自宅ネットワーク以外からはアクセスすることはできない。

【0011】

50

そこで、従来は、自宅のネットワーク家電にアクセスするために、ネットワーク家電をコントロールする機能を有する専用のルータを使用したり、ネットワーク家電をコントロールするための情報を一度インターネット上に設置されたデータセンターに蓄積し、ネットワーク家電からポーリングを行って取りに行く必要があった。

【0012】

しかし、専用のルータを使用した場合、汎用性が低くなりコストも嵩む。ポーリングを行ってコントロール情報を取りに行く場合、リアルタイムでのアクセスは行えず、ネットワークやサーバへの負荷も高くなる。

【0013】

このような課題を解決するため、本出願人が2005年5月20日に提出した国際出願PCT/JP2005/9280号に開示されたネットワーク接続方法及び中継装置がある(PCT/JP2005/9280号は、この言及によりこの明細書に組み込まれる)。この発明によれば、プライベートネットワーク内のコンピュータシステムとインターネット上のInterServerとの間にトンネリング接続のセッションを確立することにより比較的簡易な手段により家庭内ネットワークとインターネット間の双方向の通信が可能になる。

10

【0014】

しかしながら、この出願に開示された中継装置は主にルータとして動作するもの若しくは各クライアント機器に仮想デバイスドライバ及びプログラムの形でインストールされるものであったため、以下のような改善の余地がある。すなわち、ルータとして動作するようなものではなく、かつ、仮想デバイスドライバ等としてインストールできない機器、例えばプリンタ、カメラ、スキャナなどが接続されたネットワーク上でも上記出願と同様の接続が確立できる手段を提供することである。

20

【0015】

この発明はこのような事情に鑑みてなされたもので、仮想デバイスドライバがインストールできない機器が接続されたプライベートネットワーク環境において、ルータを取り替える必要がなく、比較的簡易な手段により家庭内ネットワークとインターネットを介した仮想ネットワーク通信を可能とするインターネット接続システムを提供することを目的とするものである。

【発明の開示】

30

【課題を解決するための手段】

【0016】

上記目的を達成するため、この発明の主要な観点によれば、LAN上のクライアント機器を、インターネット上のサーバを通じた仮想ネットワークに接続するために、前記LAN上の前記クライアント機器の上流側に設置される中継装置であって、この中継装置は、ブリッジモジュールを有し、このブリッジモジュールは、ローカル通信プロトコルスタックとネットワークデバイスとの間に設けられ、自己宛、ブロードキャスト及び仮想ネットワークのアドレス宛の要求パケット以外のパケットはローカル通信プロトコルスタックに渡さずに単に前記LANの上流側と下流側とをブリッジするものであり、この中継装置は、さらに、前記インターネット上のサーバのグローバルアドレスを記憶するサーバアドレス記憶部と、前記サーバのグローバルアドレスに基づき、この中継装置とサーバとの間にトンネリング接続を確立するためのトンネリング接続確立部と、前記ブリッジモジュールにより前記クライアント機器からの上記仮想ネットワーク上の仮想ネットワークアドレスを含む要求パケットを捕捉し、発信元アドレスとして前記クライアント機器の仮想ネットワークアドレスを付したものをカプセリングし、前記トンネリング接続を介して前記サーバへ送出手続をカプセリング処理部と、前記ローカル通信プロトコルスタックを通して受け取ったトンネリング接続における自己宛パケットをディカプセリングすると共に、このディカプセリングしたパケットに含まれる宛先仮想ネットワークアドレスを前記クライアント機器のLAN上のプライベートIPアドレスに変換し、このパケットをブリッジモジュールにより当該クライアント機器に送出するディカプセリング処理部とを有することを特

40

50

徴とする中継装置が提供される。

【0017】

このような構成によれば、LAN上のクライアント機器と、他の特定のLAN上にある他のクライアント機器を、前記サーバを通じた仮想ネットワークにより双方向通信可能に接続することができる。この中継装置によれば、上記クライアント機器やルータを含むLANの構成要素はなんら変更することなく、この中継装置を設置するだけで上記仮想ネットワークによる通信が可能になる。

【0018】

また、この中継装置は、仮想ネットワークアドレスを含むパケットのみを捕捉し、その他のパケット（ブロードキャストも含む）は単にブリッジ（透過）させるのみであるので、この中継装置を挟んで位置するネットワーク下流側機器と上流側機器は同じLANにある機器としてシームレスに通信することができるし、下流側機器は上流側にあるルータを介してインターネットに接続することもできる。

10

【0019】

このような特徴を備えているため仮想ネットワークドライバをインストールできないプリンタやWebカメラなどの機器を、上記仮想ネットワークドライバをインストールすることなく仮想ネットワークに参加させることができ、かつ、今までのLAN環境を全く損なわないというものである。すなわち、この中継装置は、LANネットワークの配線の一本のケーブルをこの中継装置に置き換えるだけで動作するものである。

好ましい1の実施形態によれば、前記中継装置は、インターネット上に設けられたトンネル仲介サーバに接続し、この仲介サーバから前記サーバのグローバルアドレスを受け取るものである。

20

また、1の実施形態によれば、前記中継装置は、クライアント機器に割り当てる仮想ネットワークアドレスを前記サーバから受け取り、各クライアント機器のLAN上のプライベートIPアドレスとこのクライアントに割り当てた仮想ネットワークアドレスを関連付けて記憶するものである。ここで、この中継装置は、前記LAN下流側のネットワークデバイスに到達する全てのパケットを監視することで前記クライアント機器のプライベートIPアドレス及びMACアドレスを検出する下流側クライアント機器検出部を有することが好ましい。また、この下流側クライアント機器検出部は、ブロードキャストの応答要求を定期的若しくは任意にLANの下流側に送信し、前記クライアント機器の応答を促す機能を有することがさらに好ましい。

30

また、別の好ましい1の実施形態によれば、前記クライアント機器は、ネットワーク対応の家電であるが、ユーザが仮想ネットワークドライバ等をインストールできない家電を含むものである。また、前記クライアント機器は、前記中継装置とは通信可能であるが、自らはインターネットに接続することができない周辺装置を含むものであっても良い。

さらに、この発明の他の主要な観点によれば、LAN上のクライアント機器と、このLAN上の前記クライアント機器の上流側に接続された中継装置と、前記クライアント機器がインターネットを介して接続されるサーバと、を有するインターネット接続環境において実行される、前記クライアント機器とサーバとの接続方法であって、

(a) 前記中継装置が前記サーバのグローバルIPアドレスを受け取り格納する工程と、  
(b) 前記中継装置が、前記で通知されたグローバルIPアドレスを使用して前記中継装置と前記サーバとの間で、トンネリング接続によるTCP/IPセッションを確立する工程と、

40

(c) 前記中継装置が、前記クライアント機器に仮想ネットワークIPアドレスを割り当て、前記サーバから前記トンネリング接続を通して受け取った仮想ネットワークIPアドレス宛のパケットを前記クライアント機器のLAN上のプライベートIPアドレス宛に書き換えて前記LANの下流側に送出する工程と、

(d) 前記中継装置が、前記クライアント機器からの上記仮想ネットワークIPアドレスを含むパケットを捕獲し、前記トンネリング接続を通して前記サーバへ送出する工程とを有することを特徴とする接続方法が提供される。

50

この場合、前記中継装置は、前記クライアント機器の属するLAN上に設置されるものであり、この方法は、この中継装置宛、ブロードキャスト及び仮想ネットワークのアドレス宛の要求パケット以外のパケットは前記(c)、(d)工程を行わずにLAN上で単にブリッジするものである。

また、好ましい1の実施形態によれば、この方法は、さらに、前記サーバが前記中継装置に前記クライアント機器用の仮想ネットワークIPアドレスを通知する工程を有する。さらに、好ましい1の実施形態によれば、この方法は、前記中継装置が、インターネット上に設けられたトンネル仲介サーバに接続し、この仲介サーバから前記サーバのグローバルアドレスを受け取る工程をさらに有するものである。

また、更なる他の好ましい1の実施形態によれば、この方法は、前記中継装置が、前記クライアント機器に割り当てる仮想ネットワークアドレスを前記サーバから受け取り、各クライアント機器のLAN上のプライベートIPアドレスとこのクライアントに割り当てた仮想ネットワークアドレスを関連付けて記憶する工程をさらに有するものである。この場合、前記中継装置が、前記LAN下流側のネットワークデバイスに到達する全てのパケットを監視することで前記クライアント機器のプライベートIPアドレス及びMACアドレスを検出する工程をさらに有し、この工程では、前記中継装置が、ブロードキャストの応答要求を定期的若しくは任意にLANの下流側に送信し、前記クライアント機器の応答を促す機能を有することが好ましい。

なお、この発明の更なる他の特徴と顕著な効果は次の発明を実施するための最良の形態の項に記載された実施形態及び図面を参照することによって当業者にとって理解される。

#### 【発明を実施するための最良の形態】

##### 【0020】

以下、この発明の一実施形態を図面を参照して説明する。

##### 【0021】

図1は、この実施形態に係るネットワーク構成の例を示したものである。

##### 【0022】

図中1は、IPv4(第1の通信プロトコル)で通信を行う各種クライアント機器(PC、カメラ、プリンタ、スキャナ)が接続されてなるLANである。

##### 【0023】

このLAN1は、ゲートウェイとなるルータ2と、このルータ2に接続された上流側イーサネット(登録商標)3と、この上流側イーサネット(登録商標)3の下流側に接続された中継装置4と、この中継装置4の下流側に接続された下流側イーサネット(登録商標)5とからなる。そして、下流側イーサネット(登録商標)5に、仮想ネットワークに接続したい各種クライアント機器6a~6dが接続されている。このようなクライアント機器としては、それぞれネットワーク接続に対応したプリンタ6a、カメラ6b、スキャナ6cがある。また、上記PCT出願に開示したような仮想デバイスをインストールしないPC6dもこれに含まれる。

##### 【0024】

すなわち、各クライアント機器6a~6dには、仮想ネットワーク接続をするための機能はなんらインストールされていないものである。

##### 【0025】

したがって、このLAN1は、前記中継装置4を除けば、職場や家庭に見られるような通常の構成であり、ただ単に、前記中継装置4が前記クライアント機器6a~6dが接続されたイーサネット(登録商標)5の上流側、すなわちルータ2との間に位置するように導入されているだけである。

##### 【0026】

したがって、各クライアント機器6a~6dは、前記ルータ2及び通信キャリア/ISP(インターネットサービスプロバイダ:図示せず)を介してインターネット7に接続することができ、このインターネット7上の各種コンピュータとIPv4を用いて通信が行なわれるようになっている。

10

20

30

40

50

## 【0027】

そして、このインターネット7上には、前記仮想ネットワーク上の通信を制御するためのELサーバ8（この発明の「サーバ」、ELは発明者らが考案した識別符号、PCT出願のInterServerに対応するもので同様の構成を有するもの）が接続されている。このELサーバ8は、後で詳しく説明するように、このLAN1上の前記クライアント機器6a～6dと、他のLAN9上のクライアント機器（図示せず）との間の仮想ネットワークを通じた双方向通信、及びインターネット7上からの前記クライアント機器6a～6dとの間の双方向通信すべてを仲介する機能を有するものである。

## 【0028】

ここで、中継装置4とELサーバ8は、同じメーカー若しくは統一された規格の下に製造されることが意図されており、予め連動するように設計されたものである。そして、中継装置4には、後で説明するように、ELサーバ8から仮想ネットワーク接続用のプライベートアドレス/グローバルアドレスが付与され、ISPやキャリアを問わず前記ELサーバ8にトンネリング接続によるTCP/IPセッションが確立されて通信ができるようになっている。また、この中継装置4は、前記ELサーバ8から割り当てられたクライアント機器用の仮想ネットワーク接続用アドレスを記憶するようになっている。

## 【0029】

なお、前記クライアント機器6a～6dのアドレスが常にユニークに生成できるのであれば、この中継装置4によって生成されるようになっていても構わない。

## 【0030】

また、前記クライアント機器6a～6dが自らはインターネットに接続できないビデオやテレビのような家電である場合には、前記中継装置4とそのクライアント機器は所定の通信インタフェース（IEEE1394）を介して接続され、それぞれに仮想IPアドレスを割り付けておけば良い。

## 【0031】

図2は、中継装置4を示す概略構成図である。

## 【0032】

この中継装置4は、この実施形態では、OSとしてリナックス（商品名、以下同じ）がインストールされてなるものである。

## 【0033】

図中10、11は、パケットを送受信する通信インタフェースとしてのイーサネット（登録商標）ワークデバイスである。ここではeth0が上流ネットワーク3、eth1が下流ネットワーク5に接続されている。

## 【0034】

また、図中12は、ELブリッジモジュール（この発明のブリッジモジュール）である。このブリッジモジュール12は、リナックスのカーネルに組み込まれるものであり、パケットを解釈し所定の場所に届けるネットワーク・プロトコルスタック13より先にパケットを受け取り、以下の動作を行う。

（1）イーサネット（登録商標）のパケットをeth0から受信した場合、

・パケットの形式がIPではない場合はそのままブリッジ（一点鎖線で示す経路を参照）してeth1から送信する。

## 【0035】

・あて先のIPアドレスが自分（中継装置4）と関係ないアドレスの場合、ブリッジしてeth1から送信する。

## 【0036】

・あて先のIPアドレスが自分宛であればネットワーク・プロトコルスタック13にパケットを返す。

## 【0037】

・あて先のパケットがブロードキャストであれば、パケットを複製して、eth1から送信するとともに、受け取ったパケットをネットワーク・プロトコルスタック13に返す。従

10

20

30

40

50

ってこのブリッジモジュール12はブロードキャストを通過させるとともに、自身もパケットを受け取る。

(2) イーサネット(登録商標)のパケットをeth1から受信した場合

・パケットの形式がIPでない場合はそのままeth0から送信する。

【0038】

・あて先のIPアドレスが仮想ネットワークのものであれば、そのようなパケットが来たことを上位層15へ伝えパケットの内容を蓄える。

【0039】

・あて先のIPアドレスが自分宛であればネットワーク・プロトコルスタック13にパケットを返す。

【0040】

・あて先のパケットがブロードキャストであれば、パケットを複製して、eth1から送信するとともに、受け取ったパケットをネットワーク・プロトコルスタック13に返す。従ってこのブリッジモジュール12はブロードキャストを通過させるとともに、自身もパケットを受け取る。

(3) 上位層15からパケットを渡された場合は、内容を確認せずeth1から送信する。

(4) 上位層15から要求があった場合は、蓄えてあった仮想ネットワークアドレス向けのパケットを渡す。

(5) eth1から受信したパケットのIPアドレスとMACアドレスの対の一覧を持ち、上位層から要求があった場合は、その一覧を渡す。

【0041】

そして、上位層15には、プログラムもしくは記憶領域として、前記ELサーバのIPv4でのグローバルアドレスを記憶するサーバアドレス記憶部17と、この中継装置4に割り当てられた仮想ネットワーク上でのプライベートアドレス(仮想IPアドレス)を記憶する中継装置アドレス記憶部18と、仮想プライベートネットワークを構成するための、前記ELサーバ8から割当られたクライアント機器の仮想IPアドレス(1若しくはそれ以上)を記憶するクライアント機器用仮想IPアドレス記憶部19と、ELサーバ8のアドレスに基づいてELサーバ8との間でトンネリング接続を確立するトンネリングセッション(接続)確立部20と、IPv4/IPv6でのパケットをIPv4でカプセリング/デカプセリングして前記ELサーバ8との間でトンネリング送受信を行うためのカプセリング処理部21と、クライアント機器6a~6dの仮想IPアドレスとLAN上のプライベートIPアドレスとを変換する仮想IPアドレス・プライベートIPアドレス変換部22と、前記LAN下流側のクライアント機器6a~6dのプライベートIPアドレス及びMACアドレスを検出するクライアント機器検出部23とを有する。前記ELサーバ8との間で送受信されるパケットは、このアドレス変換部22を介して前記ブリッジモジュール12/ネットワーク・プロトコルスタック13との間で受け渡される。

【0042】

このような構成によれば、ブリッジモジュール12はリナックスカーネルのネットワーク・プロトコルスタックの間にデータの受信口と送信口を持つので、リナックスのネットワーク機能を使わずにパケットの送受信を行うことができる。

【0043】

そして、eth0とeth1との間のパケットの転送はアドレスのみを判断基準として行われるので、もしパケットの中身が壊れていてもそのことには中継装置は一切関知しない。このため通常は、この中継装置4は、通常ネットワークにとってケーブルと全く同じ機能のもの(すなわちブリッジ)となる。

【0044】

また上位層15からの送信要求されたパケットは中身を解釈せず送信するので、パケットの発信元アドレスが自分自身ではないパケットも自由に送信できる。ただし、ネットワーク・プロトコルスタック13を通さないため、規格に則ったパケットを作成するのは全

10

20

30

40

50

て上位層 15 のアプリケーションの責任となる。

【 0 0 4 5 】

また、このブリッジモジュール 1 2 は、eth1 で受信したパケットの IP アドレスと MAC アドレスの一覧を保持しているため、下流側ネットワーク 5 に繋がる機器 6 a ~ 6 d のアドレスを検知することができる。

【 0 0 4 6 】

指定の条件に合致するパケットは蓄えて、そのパケットを受信したことを上位層 15 に伝える機能があるため、仮想ネットワーク向けのパケットを横取りすることで仮想ネットワークを構成することができる。この機能のため下流側に繋がっている機器は従来の VLAN ルータと異なり、機器の存在を知る必要が無く特別な設定を行わずに仮想ネットワークの構成要素となることができる。

10

【 0 0 4 7 】

また、ブロードキャストを通過させるため下流側機器と上流側機器は同じ LAN にある機器としてシームレスに使用することができる。

【 0 0 4 8 】

そして、以上のような特徴を備えているため、仮想ネットワークドライバをインストールできないプリンタやウェブカメラなどの機器を設定なしで仮想ネットワークに参加させることができるとともに、今までの LAN 環境を全く損なわないという利点がある。

【 0 0 4 9 】

なお、ここで、上記「トンネリング」とは、IP v 4 や IP v 6 のネットワーク（ルータ）同士を IP v 4 ネットワークを介して接続するための技術であり、特に、ここでは、異なるネットワークに属する機器同士を仮想ネットワーク（VPN：バーチャル・プライベート・ネットワーク）で終端するためにトンネリングするものをいう。そして、この実施形態では、機器間で通信される IP v 4 パケットを IP v 4 でカプセルリングしてやり取りする。

20

なお、上記では、IP プロトコルのみブリッジするように記載されているが、ether 上で動作する appletalk 等の IP も素通しするように構成されている。

【 0 0 5 0 】

また、上記中継装置 4 の前記各構成要素は、実際には例えば、コンピュータシステムに設けられたハードディスク等の RAM 若しくは ROM 等のメモリに確保された一定の領域及びそこにインストールされたコンピュータソフトウェアプログラム、これらのメモリを制御して前記プログラムを読み出して実行するための CPU、一時記憶装置その他入出力装置等の周辺機器から構成される。また、OS 等のプログラムは表示していないが、実際にはこの実施形態の各構成要素は OS と協働して動作する場合がある。

30

【 0 0 5 1 】

また、前記 EL サーバ 8 は、負荷を分散するために互いに接続された複数のコンピュータシステムから構成されていることが好ましい。1 つの EL サーバ 8 で複数の異なる仮想ネットワークに対応する場合は通常であると考えられるからである。

【 0 0 5 2 】

次に、上記中継装置 4 の各構成の詳細な構成及び機能を、図 3 の通信例を参照して詳しく説明する。

40

【 0 0 5 3 】

図 3 は、中継装置 4 が接続されている LAN 1 上のクライアント機器 6 a ~ 6 d と、他の LAN 9 にある他のクライアント機器（これに限られないが）とが、前記 EL サーバ 8 を介して通信を行う場合を示したものである。上記他の LAN 9 にも、当該 LAN 1 と同様の構成で中継装置が設けられているものとする。

【 0 0 5 4 】

まず、中継装置 4 と EL サーバ 8 との間でトンネリングセッションが確立される。

【 0 0 5 5 】

この場合、前記中継装置 4 は、まず、通常のインターネット接続方法で、図に 2 5 で示

50

すトンネルブローカーに接続する。このトンネルブローカー 25 は、アドレスデータベースからトンネル接続を確立する先の E L サーバ 8 を選択し、前記中継装置 4 にこの E L サーバ 8 の I P v 4 アドレスを通知する。このことで、前記中継装置 4 は E L サーバ 8 を識別可能になり、ユーザ認証を行った後、E L サーバ 8 から受け取った仮想 I P アドレスを用いてトンネリングセッションを確立し通信を行うことができる。

**【 0 0 5 6 】**

すなわち、前記中継装置 4 が E L サーバ 8 に接続すると接続確立のための認証が行われ、これに基づいて E L サーバ 8 から中継装置 4 に対して特定の仮想プライベートネットワーク用の仮想 I P アドレスの割り当てが行われる。また、このとき、E L サーバ 8 からは、前記クライアント機器 6 a ~ 6 d のための数個の仮想 I P アドレスの割り当ても行なわれ、このクライアント機器用仮想 I P アドレスはクライアント機器用仮想 I P アドレス記憶部 19 に格納される。

また、前記アドレス変換部 22 は、このクライアント機器用仮想 I P アドレスと、各クライアント機器に割り当てられたこの L A N 1 上の I P アドレスとの変換表（変換ルール）を保持する。この変換表は、この実施形態では、前記クライアント機器検出部 23 が前記クライアント機器を検出することで自動的に作成されるようになっている。すなわち、前記中継装置のブリッジモジュールは、前記クライアント機器のブロードキャスト通信を含む下流側のパケットをすべて監視できるので、このクライアント機器検出部 23 は、前記クライアント機器の L A N 1 上の I P アドレス及び M A C アドレスを検出することができる。また、このクライアント機器検出部 23 は、さらに、ブロードキャストの応答要求（ICMP ECHO）を定期的若しくは任意に L A N の下流側に送信し、前記クライアント機器の応答（ICMP REPLY パケット）を促すことで、確実に下流側のクライアント機器を検出する機能を有する。なお、このような自動検出を使用しない場合には、ユーザが手動で前記 L A N 1 の I P アドレスを入力し、かつ仮想アドレスとの割り当てを行って前記変換ルールを生成できるようになっていても良い。また、この場合、前記割り当てのみを自動で行なうようにしても良いし、自動/手動をユーザが選択できるように構成されていても良い。なお、各クライアント機器への L A N 1 上の I P アドレスは、前記ルータ 2 によって割り当てられたものである。

**【 0 0 5 7 】**

図 3 の符号 26 で示す経路は、前記 E L サーバ 8 のアドレス、中継装置 4 に割り当てられた仮想 I P アドレスに基づき、前記トンネリングセッション確立部 20 により前記中継装置 4 との間でトンネリング接続内の通信セッションを確立されている状態を示している。また、他の L A N 9 との間にも同様にトンネリング接続による通信セッションが確立されている（経路 27）。そして、この L A N 1 と L A N 9 とは、同一の仮想ネットワーク（V L A N）に属するものとしてグループ化されるものとする。

**【 0 0 5 8 】**

この状態において、前記クライアント機器 6 a ~ 6 d へのパケットは、前記カプセリング処理部 21 によって前記中継装置 4 向けの I P v 4 パケットでカプセリングされて送信される。中継装置 4 は、カプセリング処理部 21 がそのパケットをデカプセリングすると共に、前記変換部 22 が送信先アドレスを当該プライベートネットワークのプライベート I P アドレスに変換して前記ブリッジモジュール 12 に受け渡す。ブリッジモジュール 12 は、受け取ったパケットをそのまま eth0 から下流側に流す。このようにして、例えば家庭内の L A N 1 上のクライアント機器 6 a ~ 6 d への接続を、外部にあるサーバ 8 や他の L A N 9 側からの起動により行うことができる。

**【 0 0 5 9 】**

また、前記クライアント機器 6 a ~ 6 d からの仮想ネットワークへの通信は、仮想 I P アドレス宛に送出される。この仮想 I P アドレスを含むパケットが下流側のデバイス eth1 から中継装置 4 に入ると、このパケットは前記ブリッジモジュール 12 に捕捉され、前記上位層 15 で前記 E L サーバ宛のパケットにカプセリングされ、前記ローカル通信プロトコルスタック、eth0 を介してトンネリング接続により前記サーバ 8 に送出される。

## 【 0 0 6 0 】

このような構成によれば、例えば、前記クライアント機器 6 a ~ 6 d が自宅の LAN に接続されたネットワーク対応の家庭内監視カメラであるとする、前記中継装置 4 により前記カメラに仮想 IP アドレスが割り当てられ、他のネットワークの中継装置 4 との間に形成された仮想ネットワークにより他のネットワーク上から直接操作できるようになる。

## 【 0 0 6 1 】

また、この中継装置 4 は、前記 EL サーバ 8 が仮想ネットワーク上のハブのように動作する場合であっても、ハブを介さない PPP 接続の場合であっても同じように対応することができる。

## 【 0 0 6 2 】

以上のような構成によれば、仮想ネットワークを通したクライアント機器 6 a ~ 6 d との通信は、すべて、キャリアや ISP に関らず、前記 EL サーバ 8 を通して行われることになるから、家庭や職場のホームネットワーク上のクライアント機器 6 a ~ 6 d を EL サーバ 8 側から自由に設定・制御することが可能になる。これにより、従来問題であった、インターネット上のサーバからのプライベートネットワーク中のネットワーク家電の個体認識、家庭内ルーティング及びセキュリティの問題を全て解決でき、極めてオープンかつ、クローズドなネットワークの構築を実現することが可能になる。

## 【 0 0 6 3 】

なお、以上説明した実施形態は、この発明の一つの実施形態に過ぎないのであって、その要旨を変更しない範囲で種々の形態をとりうることはいうまでもない。

## 【 0 0 6 4 】

例えば、上記一実施形態では、IPv4・OVER・IPv4 によるカプセリングであったが、LAN のプロトコルが IPv6 であってもよい。また、他の LAN のプロトコルも IPv6 であってもよい。さらに、両方ともに上記以外のプロトコルであっても良い。

また、上記一実施形態では、前記中継装置は、独立した装置として開示されていたが、LAN 1 上のいずれかのコンピュータにソフトウェアとしてインストールされたものであっても良い。

さらに、上記一実施形態では、中継装置の OS はリナックスであったが、これに限定されるものではないことは当然である。

## 【 図面の簡単な説明 】

## 【 0 0 6 5 】

【 図 1 】 この発明の一実施形態に係るネットワーク構成の例を示す図。

【 図 2 】 同じく中継装置の例を示す概略構成図。

【 図 3 】 同じく通信例を示す図。

## 【 符号の説明 】

## 【 0 0 6 6 】

- 1 ... LAN
- 2 ... ルータ
- 3 ... 上流側イーサネット（登録商標）
- 4 ... 中継装置
- 5 ... 下流側イーサネット（登録商標）
- 6 a ... プリンタ
- 6 b ... カメラ
- 6 c ... スキャナ
- 6 d ... PC
- 7 ... インターネット
- 8 ... EL サーバ
- 9 ... LAN
- 10 ... イーサネット（登録商標）ワークデバイス
- 11 ... イーサネット（登録商標）ワークデバイス

10

20

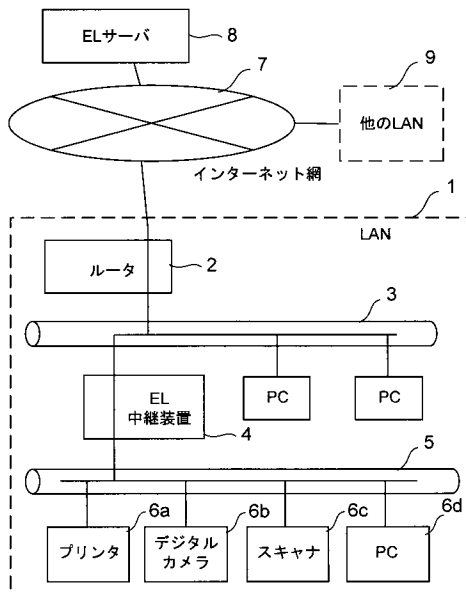
30

40

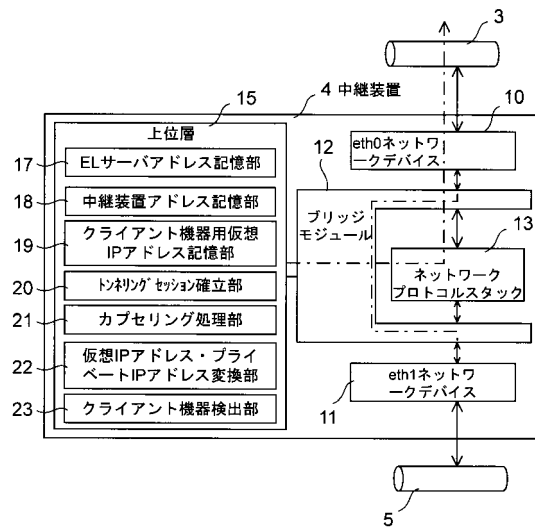
50

- 1 2 ...ブリッジモジュール
- 1 3 ...ネットワーク・プロトコルスタック
- 1 5 ...上位層
- 1 7 ...サーバアドレス記憶部
- 1 8 ...中継装置アドレス記憶部
- 1 9 ...IPアドレス記憶部
- 2 0 ...トンネリングセッション確立部
- 2 1 ...カプセリング処理部
- 2 2 ...仮想IPアドレス・プライベートIPアドレス変換部
- 2 3 ...クライアント機器検出部
- 2 5 ...トンネルブロッカー
- 2 6、2 7 ...経路

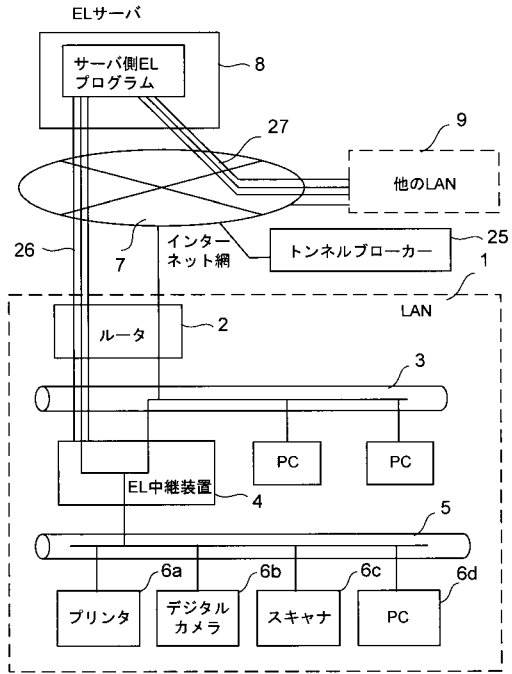
【図1】



【図2】



【 図 3 】



---

フロントページの続き

(72)発明者 石田 宏樹  
東京都渋谷区円山町3番6号 フリービット株式会社内

審査官 岩田 玲彦

(56)参考文献 携帯電話で制御するホーム・セキュリティ レイヤー2VPN技術の組み込みで実現, 日経コミュニケーション, 日本, 日経BP社, 2005年 9月15日, 第446号, P.114  
ASPサービス「どこでもLAN」を使う, NETWORK MAGAZINE 2005年1月号, 日本, 株式会社アスキー, 2005年 1月 1日, 第10巻 第1号, pp.86-87  
三輪芳久・平野亜矢, SoftEther大研究, 日経NETWORK 2005年8月号, 日本, 日経BP社, 2005年 7月22日, 第64号, pp.43-61

(58)調査した分野(Int.Cl., DB名)

H04L 12/46

H04L 12/66

H04L 12/56