

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5520928号
(P5520928)

(45) 発行日 平成26年6月11日(2014.6.11)

(24) 登録日 平成26年4月11日(2014.4.11)

(51) Int.Cl.		F I	
HO 4 L 12/741	(2013.01)	HO 4 L 12/741	
HO 4 L 12/66	(2006.01)	HO 4 L 12/66	A

請求項の数 13 (全 21 頁)

(21) 出願番号	特願2011-502421 (P2011-502421)	(73) 特許権者	591034154
(86) (22) 出願日	平成21年3月31日(2009.3.31)		オランジュ
(65) 公表番号	特表2011-517201 (P2011-517201A)		フランス・75015・パリ・リュ・オリ
(43) 公表日	平成23年5月26日(2011.5.26)		ヴィエ・ドゥ・セレ・78
(86) 国際出願番号	PCT/FR2009/050548	(74) 代理人	100108453
(87) 国際公開番号	W02009/125158		弁理士 村山 靖彦
(87) 国際公開日	平成21年10月15日(2009.10.15)	(74) 代理人	100064908
審査請求日	平成24年3月30日(2012.3.30)		弁理士 志賀 正武
(31) 優先権主張番号	0852108	(74) 代理人	100089037
(32) 優先日	平成20年3月31日(2008.3.31)		弁理士 渡邊 隆
(33) 優先権主張国	フランス (FR)	(74) 代理人	100110364
			弁理士 実広 信哉
		(72) 発明者	モハメッド・ブカデル
			フランス・35000・レンヌ・スコア
			ル・ルイ・アレル・ドゥ・ラ・ノエ・1
			最終頁に続く

(54) 【発明の名称】 ネットワークにおけるデータパケットのルーティング方法および関連デバイス

(57) 【特許請求の範囲】

【請求項1】

プライマリあて先アドレスとあて先ポート番号とを含むIPデータパケットを通信ネットワーク内でルーティングする方法において、

前記IPデータパケットの受信の際に、

・前記あて先ポート番号が属するポート番号の範囲を規定するポートマスクを決定するステップと、

・前記IPデータパケットのあて先装置の識別子を、前記プライマリあて先アドレスに関連する複数の装置の識別子から、前記ポートマスクに基づいて選択するステップと、

・前記IPデータパケットを、前記あて先装置の識別子に基づき前記あて先装置にルーティングするステップと

を有し、

前記識別子は、IPアドレス、または前記あて先装置に対応するルートを一意的に指定する前記あて先装置に特有のルート識別子であり、

前記プライマリあて先アドレスは、ルーティングされる前記IPデータパケット中に保持されることを特徴とするIPデータパケットルーティング方法。

【請求項2】

プライマリあて先アドレスとあて先ポート番号とを含むIPデータパケットを通信ネットワーク内でルーティングするデバイスであって、

前記IPデータパケットの受信に際して、

10

20

・前記あて先ポート番号が属するポート番号の範囲を規定するポートマスクを決定する手段と、

・前記IPデータパケットのあて先装置の識別子を、前記プライマリあて先アドレスに関連する複数の装置の識別子から、前記ポートマスクに基づいて選択する手段と、

・前記IPデータパケットを、前記あて先装置の識別子に基づき前記あて先装置にルーティングする手段と

を具備し、

前記識別子は、IPアドレス、または前記あて先装置に対応するルートを一意的に指定する前記あて先装置に特有のルート識別子であり、

前記プライマリあて先アドレスは、ルーティングされる前記IPデータパケット中に保持されることを特徴とするIPデータパケットルーティングデバイス。

10

【請求項3】

プライマリあて先アドレスとあて先ポート番号とを含むIPデータパケットを受信するように構成された通信ネットワーク装置であって、

少なくとも1つのルーティングデバイスを具備し、前記ルーティングデバイスは、

・前記あて先ポート番号が属するポート番号の範囲を規定するポートマスクを決定する手段と、

・前記IPデータパケットのあて先装置の識別子を、前記プライマリあて先アドレスに関連する複数の装置の識別子から、前記ポートマスクに基づいて選択する手段と、

・前記IPデータパケットを、前記あて先装置の識別子に基づき前記あて先装置にルーティングする手段と

20

を具備し、

前記識別子は、IPアドレス、または前記あて先装置に対応するルートを一意的に指定する前記あて先装置に特有のルート識別子であり、

前記プライマリあて先アドレスは、ルーティングされる前記IPデータパケット中に保持されることを特徴とする通信ネットワーク装置。

【請求項4】

通信ネットワークに接続された端末装置を構成する方法において、

前記端末装置から送信された構成要求の受信に際して、

・前記端末装置に、複数の端末装置で共有されるプライマリアドレスを割り当てるステップと、

30

・前記端末装置に、前記端末装置専用のポート番号の範囲を規定するポートマスクと、前記端末装置に対応するルートを一意的に指定するルート識別子とを割り当てるステップと、

・前記端末装置に、前記プライマリアドレスと前記ポートマスクと前記ルート識別子とを含む構成メッセージを送信するステップと

を有することを特徴とする端末装置構成方法。

【請求項5】

前記構成メッセージは、前記プライマリアドレスをあて先アドレスとして含むデータパケットを前記端末装置にルーティングするルーティングデバイスに、更に送信されることを特徴とする請求項4に記載の端末装置構成方法。

40

【請求項6】

通信ネットワーク内の構成サーバであって、

端末装置から送信された構成要求の受信に際して、

・前記端末装置に、複数の端末装置で共有されるプライマリアドレスを割り当てる手段と、

・前記端末装置に、前記端末装置専用のポート番号の範囲を規定するポートマスクと、前記端末装置に対応するルートを一意的に指定するルート識別子とを割り当てる手段と、

・前記端末装置に、前記プライマリアドレスと前記ポートマスクと前記ルート識別子とを含む構成メッセージを送信する手段と

50

を具備することを特徴とする構成サーバ。

【請求項 7】

通信ネットワークに接続された端末装置を構成する方法において、

プライマリアドレスと前記端末装置専用のポート番号の範囲を規定するポートマスクと前記端末装置に対応するルートを一意的に指定するルート識別子とを含む構成データを含む構成メッセージの受信に際して、

- ・前記構成データを格納するステップと、
- ・前記通信ネットワークヘデータパケットを送信する前に、前記ポートマスクにより規定されるポート番号の範囲内のポート番号を選択するステップと

を有し、

前記データパケットは、ソースアドレスとして前記端末装置の前記プライマリアドレスを含み、且つソースポート番号として前記選択されたポート番号を含むことを特徴とする構成方法。

【請求項 8】

前記プライマリアドレスをあて先アドレスとして含むデータパケットを前記端末装置へとルーティングするように構成されたルーティングデバイスの識別子を受信すると、前記構成データを前記ルーティングデバイスに送信するステップを更に有することを特徴とする請求項7に記載の構成方法。

【請求項 9】

あて先アドレスとポート番号とルート識別子とを含むデータパケットの受信に際して、前記ポート番号が前記端末装置の前記ポートマスクにより規定されるポート番号の範囲に属することを検証するステップと、

検証の結果が否である場合、前記データパケットを拒絶するステップと

を更に有することを特徴とする請求項7に記載の構成方法。

【請求項 10】

通信ネットワークに接続されたクライアント端末装置であって、

複数の端末装置で共有されるプライマリアドレスと前記クライアント端末装置専用のポート番号の範囲を規定するポートマスクと前記クライアント端末装置に対応するルートを一意的に指定するルート識別子とを含む構成データを含む構成メッセージの受信に際して

- ・前記構成データを格納する手段と、

- ・前記通信ネットワークヘデータパケットを送信する前に、前記ポートマスクにより規定されるポート番号の範囲内のポート番号を選択する手段と

を具備し、

前記データパケットは、ソースアドレスとして前記クライアント端末装置の前記プライマリアドレスを含み、且つソースポート番号として前記選択されたポート番号を含むことを特徴とするクライアント端末装置。

【請求項 11】

マイクロプロセッサにより実行可能なコンピュータプログラムであって、請求項1に記載のルーティング方法を実行するためのプログラムコード命令を含むことを特徴とするプログラム。

【請求項 12】

マイクロプロセッサにより実行可能なコンピュータプログラムであって、請求項4に記載の構成方法を実行するためのプログラムコード命令を含むことを特徴とするプログラム。

【請求項 13】

マイクロプロセッサにより実行可能なコンピュータプログラムであって、請求項7に記載の構成方法を実行するためのプログラムコード命令を含むことを特徴とするプログラム。

【発明の詳細な説明】

10

20

30

40

50

【技術分野】

【0001】

本発明の分野は、通信ネットワーク、特に、データの packets が送信元装置から、あて先アドレスにより特定される送信先装置に搬送される、IP通信ネットワークである。

【背景技術】

【0002】

このような通信ネットワークは、このネットワークに接続された端末装置からのデータを搬送するための複数の機器、接続、機能を集約している。具体的には、搬送機能は、ルーティングおよび送信プロトコルを起動することにより実行することができる。オペレータにより管理される通信ネットワークは、ドメインとも呼ばれる。

10

【0003】

IP接続サービスプロバイダは、端末装置のユーザと連絡を取れるようにする専用アーキテクチャを配備している。IP接続サービスへのアクセスは、オペレータの通信ネットワークを用いてサービスプロバイダにより管理され、端末装置により送信されたデータパケットはそれらの最終目的地へとルーティングされる。前記のサービスプロバイダは、時には、この通信ネットワークのオペレータでもあるということもある。

【0004】

本発明は、同じプライマリアドレスを通信ネットワークの複数の端末装置に割り当てることを可能にする、アドレスとポート番号の割り当てのメカニズムに関する。

【0005】

20

従って、本発明は、任意のタイプのパブリックまたはプライベートアドレッシングに適合するが、特に、インターネットプロトコルバージョン4(IPv4)により規定されるパブリックIPアドレスに適合する。しかしながら、これは本発明を限定するものではない。

【0006】

既知のやり方では、プライベートホームネットワークの端末とドメインとしても知られるオペレータのパブリック通信ネットワークとの間のホームゲートウェイは、プライベートIPアドレスとこの端末に関連付けられたポートとを、IPv4タイプのパブリックIPアドレスとパブリックネットワーク上の同じゲートウェイのポートとに関連付けるテーブルを備える。

【0007】

30

この表は、当業者には、NAT(Network Address Translation)テーブルとして知られている。

【0008】

IPサービスプロバイダの業界では、パブリックIPv4アドレスの枯渇は避けられないということが一般に認められている。この問題を避けるために、業界は既に行動を起こしており、新しいプロトコルであるインターネットプロトコルバージョン6(IPv6)を規定した。このIPv6は、多数のIPアドレスと、性能改善をもたらす階層的なルーティングメカニズムとを提供する。しかしながら、この解決法は、金銭的または戦略的理由により実際にはオペレータによって活発化されてはいない。同じプロバイダ達は、それでも、インターネット・エンジニアリング・タスクフォース(Internet Engineering Task Force:IETF)から、特にグローバル・ルーティング・オペレーションズ作業部会(Global Routing Operations Working Group:GROW)の中で提示された報告書において発せられた、2009年末までにIANA IPv4アドレスが枯渇する危険性に関する最近の警告に、無関心でいるというわけではない。

40

【0009】

IP接続サービスを提供するために必要なIPv4パブリックアドレスの数の歯止めをかけるために、デュアルNATすなわちオペレータNATによる解決策が提案され実行されている。これは、オペレータの通信ネットワーク内のNAT機能を作動させて、ホームゲートウェイが自らのNATテーブル内においてプライベートアドレッシングを用いるようにする。ここで、ホームネットワークRD内の1台の端末装置について考える。この端末装置は、自身と通

50

信ネットワークRTとの間のホームゲートウェイ220に接続されている(図1)。ゲートウェイは、端末装置120より送信されたデータパケットPTの第1のプライベートアドレスペアを第2のプライベートアドレスペア(@PRIV2、P2)に変換する第1のNAT機能NAT1を実行する。ゲートウェイは、その後、変換されたPTパケットを、通信ネットワークRTに送信する。このパケットは、ネットワーク装置N0により受信される。このネットワーク装置N0は、データパケットPTの第2のアドレスペア(@PRIV2、P2)を第3のパブリックアドレスペア(@PUB、P3)に変換するオペレータNAT機能NAT2を実行する。このように、ホームゲートウェイのプライベートアドレスをパブリックアドレスに変換するのがオペレータNAT機能であり、このことが無視できない数のIPv4パブリックアドレスを節約する。

【0010】

このオペレータNAT解法には、下記を含む欠点がある。

- ・IPデータパケットPTのルーティングはより複雑になる。つまり、第2のレベルのアドレス変換を導入するので、データパケットPTは2度の修正が必要となる。

- ・例えば、DNS(domain name system)、FTP(file transfer protocol)またはSIP(session initiation protocol)などの従来のアプリケーションシグナリングプロトコルまたはアプリケーションレベルのゲートウェイ(ALG)シグナリングプロトコルの実行を適合させる必要がある。例えば、SIPでは、そのNATテーブルを最新に維持するために、ボイスオーバーIPセッションのセットアップおよび維持により、SIPシグナリング経路内のホームゲートウェイが、周知の方法により加入者の端末とパブリックネットワークとの間でシグナリングの擬似的な交換を強いるように動作することを要求され、これにより、高頻度の再登録要求を強いることになる。デュアルネットワークアドレス変換が存在する場合、このようなメカニズムをオペレータNAT機能を担う装置の中にも配備する必要がある。

- ・パブリック通信ネットワークのオペレータにより提供されるデグレードしたIP接続サービスには非常に問題がある。その理由は、オペレータNATがあると、特に、ポートフォワーディングまたはDynDNSなどの機能がサポートできないためである。

【発明の概要】

【発明が解決しようとする課題】

【0011】

従って、従来技術のこれらの欠点を軽減する必要がある。

【0012】

具体的には、クライアント端末にデグレードしたサービスの提供をもたらすことなくパブリックIPアドレスの使用を節約する、新たな解決策を提供する必要がある。

【課題を解決するための手段】

【0013】

本発明はこの必要性に対して、通信ネットワーク内でプライマリあて先アドレスとあて先ポート番号とを含むデータパケットをルーティングする方法において、前記データパケットの受信の際に、

- ・あて先ポート番号が属するポート番号の範囲を規定するポートマスクを決定するステップと、

- ・データパケットのあて先装置のルーティング識別子を、前記あて先アドレスに関連する複数の端末装置ルーティング識別子から、決定されたポートマスクに基づいて選択するステップと、

- ・データパケットを、前記識別子に基づきあて先装置にルーティングするステップとを有する方法によって対処する。

【0014】

互いに関連付けられた形で、本発明は、プライマリあて先アドレスとあて先ポート番号とを含む通信ネットワーク内のIPデータパケットをルーティングするデバイスであって、前記IPデータパケットの受信に際して、

- ・あて先ポート番号が属するポート番号の範囲を規定するポートマスクを決定する手段と

10

20

30

40

50

・前記IPデータパケットのあて先装置の識別子を、前記プライマリあて先アドレスに関連する複数の装置識別子から、前記ポートマスクに基づいて選択する手段と、

・このIPデータパケットを、前記あて先装置識別子に基づきあて先装置にルーティングする手段と、を実現するように構成されていることを特徴とするデバイスを提供する。

【0015】

このように本発明は、パケットのあて先アドレスと、受信したパケットのあて先ポート番号を含むポート番号の範囲を規定するポートマスクと、あて先端末装置のルーティング識別子とから成る独特の組み合わせに依存する、全く新規且つ独創的なデータパケットのルーティングへの取り組み方に基づいている。本発明はこのようにして、通信ネットワークに接続された複数の端末装置に対して、この通信ネットワーク内の同じルーティング可能プライマリアドレスを割り当てることができ、よって、オペレータNAT解決手法に頼ることなくパブリックIPアドレスの使用を節約することができる。本発明は、このように、単純で効果的で且つこの分野における標準的な技法と連続性のある、IPv4アドレス枯渇に対する解決法を構成する。これにより、プロバイダは、その顧客数を大幅に増加することが可能となる。この方法は、大規模な投資を必要とせず、従って、資本的経費(CAPEX: capital expenditure)、および運用経費(OPEX: operative expenditure)を最適化することを可能にする。

【0016】

本発明は、任意のタイプのあて先端末装置(これがホームネットワークに接続されているか否かにかかわらず)へのデータパケットのルーティングに適用され、また、本発明を限定するものではないものの、とりわけホームネットワークとパブリック通信ネットワークとの間のホームゲートウェイへのデータパケットのルーティングに適用される。

【0017】

本発明のルーティング方法は、通信ネットワーク装置により実行される。結果として、本発明は、本発明のルーティングデバイスを備え、且つ、あて先アドレスとあて先ポート番号とを包むデータパケットを受信するように構成された、通信ネットワーク装置をも提供する。

【0018】

従って、端末装置に送られた全てのデータストリームは、上記の通信ネットワーク装置を通過するが、この装置はこの通信ネットワークのルータまたは専用装置であってもよい。

【0019】

プライマリアドレスは、パブリックアドレスであると有利である。パブリックアドレスを用いる利点は、サービスプロバイダにより管理されるドメインの周辺部でのアドレス変換やプロトコル補正が回避されることである。

【0020】

本発明の第1の実施形態においては、前記少なくとも1つの識別子は、あて先端末装置の二次アドレスである。このような二次アドレスは、プライベートアドレスとも呼ばれ、通信ネットワーク全体を通してルーティングされ得ない。二次アドレスは、制限された範囲を有し、ストリームを端末装置と通信ネットワーク装置間で、本発明の方法を用いてやりとりすることに限定されている。このアドレスは、特定のオペレータの通信ネットワークの境界ゲートウェイプロトコル(BGP: border gateway protocol)ドメインを超えて公開されることはない。

【0021】

本方法は、更に、パケットを変換して前記二次アドレスを追加するステップをルーティングステップの前に有すると好都合であり、このパケットはあて先端末装置に前記二次アドレスに基づいてルーティングされる。

【0022】

本発明の第1の実施形態の一態様によれば、この変換ステップは、このパケットを前記二次アドレスに送信される他のパケットの中にカプセル化する。

10

20

30

40

50

【0023】

このカプセル化の利点は、パケットの内部構造の変更を必要としないということである。これが、新たな書き込みやチェックサムの計算を回避する。

【0024】

本発明の第1の実施形態の他の態様によれば、この変換ステップは、あて先装置の二次アドレスをこのパケットのフィールドに追加する。

【0025】

これの第1の利点は、このような変換が帯域幅の使用を最適化することを可能とするということであるが、その理由は、カプセル化プロセスとは異なり、この変換が2つのヘッダの追加を必要としないからである。第2の利点は、例えば、インターネットプロトコルのソースルーティング・オプション(source routing option)の性能を十分に引き出すということである。

10

【0026】

本発明の第2の実施形態においては、識別子は、端末装置に特有のルート識別子であり、パケットは前記特有のルート識別子に基づきルーティングされる。ここで、特有のルートとは、この端末装置に接続するための専用のルートであり、同じプライマリアドレスを有する複数の装置の中でこの端末装置のみに働く。

【0027】

あて先端末装置に割り当てられたプライマリアドレスとポートマスクとを組み合わせることで、この特有ルート識別子は、あて先端末装置を一意的に特定することと、受信したデータパケットをルーティングすることと、の両方を可能にする。

20

【0028】

利点は、パケットの変換が不要なことである。本発明の本実施形態は、本発明を実施する装置の中に同じプライマリアドレスを有する複数の装置への分離されたルートを組み込むために、オペレータの基礎となる通信ネットワークへの作業を必要とする。

【0029】

本発明の特定の一実施形態においては、データパケットをルーティングする方法のステップは、コンピュータプログラム命令により決定される。

【0030】

従って、本発明はまた、データ媒体上に在って、ルーティングデバイスの中で、またはより一般的にはコンピュータの中で実行されるように構成されたコンピュータプログラムをも提供し、このプログラムは、上述のようなルーティング方法のステップを実行するように構成された命令を含んでいる。

30

【0031】

このプログラムは、任意のプログラム言語を用いてもよく、またソースコード、オブジェクトコード、若しくは部分的にコンパイルされた形態などのソースコードとオブジェクトコードとの中間のコード、または任意の他の望ましい形態であってもよい。

【0032】

本発明はまた、上述したコンピュータプログラムの命令を含むコンピュータで読み取り可能な媒体をも提供する。

40

【0033】

このデータ媒体は、このプログラムを格納することができる実体または装置であってもよい。例えば、媒体には、コンパクトディスク(CD)ROM若しくは超小型電子回路ROMなどのリードオンリーメモリ(ROM)、または、フロッピー(登録商標)ディスク若しくはハードディスクなどの磁気記憶手段などの記憶手段が含まれてもよい。

【0034】

データ媒体は、無線通信または他の手段により電氣的または光学的ケーブルを介して送られる電氣的または光学的信号などの、伝達性媒体であってもよい。本発明のプログラムは、とりわけ、インターネットタイプのネットワークを介してダウンロードしてもよい。

【0035】

50

あるいは、データ媒体は、プログラムが組み込まれた集積回路であってもよく、この集積回路は、当該の方法を実行するように構成されているか、またはこれの実行において使用される。

【0036】

本発明はまた、通信ネットワークに接続された端末装置を構成する方法も提供し、本方法は、前記端末装置から送信された構成要求の受信に際して、

- ・前記端末装置に、複数の端末装置で共有されるプライマリアドレスを割り当てるステップと、

- ・前記端末装置に、前記端末装置専用の番号の範囲を規定するポートマスクと、ルーティング識別子とを割り当てるステップと

- ・前記端末装置に、前記プライマリアドレスと前記ポートマスクと前記ルーティング識別子とを含む構成メッセージを送信するステップと、を有する。

10

【0037】

本発明に従って構成された複数の端末装置は、同じプライマリアドレスを受信する。これらの装置を個別に且つ一意的に特定することを可能とするのは、このプライマリアドレス、ルーティング識別子、ポートマスクの組み合わせである。

【0038】

本発明の一態様によれば、構成方法は、前記プライマリアドレスを前記あて先アドレスとして含むデータパケットを前記端末装置にルーティングするように構成されたルーティングデバイスの識別子を、前記端末装置に割り当てるステップを有し、構成メッセージは前記ルーティングデバイス識別子を更に含んでいる。

20

【0039】

このようにして、端末装置は、自らに向けられたデータパケットをルーティングするためのルーティングデバイスの身元を知る。

【0040】

本発明の一態様によれば、前記構成メッセージは、前記プライマリアドレスを前記あて先アドレスとして含むデータパケットを前記端末装置にルーティングすることができるルーティングデバイスを含む通信ネットワークに、更に送信される。

【0041】

本発明の構成方法は、前記端末装置により送信された構成要求を受信する際に、以下の手段を実現するように構成された通信ネットワーク内の構成サーバにより実行される。

30

- ・前記端末装置に、複数の端末で共有されるプライマリアドレスを割り当てる手段

- ・前記端末装置に、前記端末装置専用の番号の範囲を規定するポートマスクと、ルーティング識別子とを割り当てる手段

- ・前記端末装置に、前記プライマリアドレスと前記ポートマスクと前記ルーティング識別子とを含む構成メッセージを送信する手段

【0042】

本発明は更に、通信ネットワークに接続された端末装置を構成する方法において、プライマリアドレスと前記端末装置に専用の番号の範囲を規定するポートマスクとルーティング識別子とを含む構成データを含む構成メッセージの受信に際して、前記方法は、

40

- ・前記構成データを格納するステップと、

- ・通信ネットワークへとデータパケットを送信する前に、前記ポートマスクにより規定されるポート番号の範囲内のポート番号を選択するステップとを有し、前記データパケットは、ソースアドレスとして前記端末装置の前記プライマリアドレスを含み、且つソースポート番号として前記選択されたポート番号を含むことを特徴とする方法を提供する。

【0043】

本発明の一態様によれば、この構成方法は更に、構成データを、データパケットをルーティングする本発明のデバイスに送信するステップを有する。

【0044】

このルーティングデバイスは、端末装置の付属装置である。ルーティングデバイスは、

50

この端末装置に向けられた全てのデータパケットを通過中に見る。

【0045】

本発明の他の態様によれば、あて先アドレスとポート番号とルーティング識別子とを含むデータパケットの受信に際して、前記方法は、前記ポート番号が前記端末装置の前記ポートマスクにより規定される番号の範囲に属することを検証するステップと、検証結果が否である場合は前記データパケットを拒絶するステップとを更に有する。

【0046】

本構成方法は、通信ネットワークに接続されたクライアント端末装置により実行されると好都合であり、複数の端末装置を有するプライマリアドレスと前記端末装置に専用の番号の範囲を規定するポートマスクとルーティング識別子とを含む構成データを含む構成メ

10

ッセージの受信に際して、前記装置は、

- ・前記構成データを格納する手段と、
- ・前記通信ネットワークへとデータパケットを送信する前に、前記ポートマスクにより規定されるポート番号の範囲内のポート番号を選択する手段と、を実現するように構成され、前記データパケットは、ソースアドレスとして前記端末装置の前記プライマリアドレスを含み、且つソースポート番号として前記選択されたポート番号を含むことを特徴とする。

【0047】

本発明の特定の一実施形態においては、構成方法のステップは、コンピュータプログラム命令により決定される。

20

【0048】

従って、本発明はまた、データ媒体上にあり且つホームゲートウェイの中で、またはより一般的にはコンピュータの中で実行されるように構成されたコンピュータプログラムをも提供し、このプログラムは、上述のような構成方法のステップを実行するように構成された命令を含んでいる。

【0049】

本発明は更に、通信ネットワーク内のホームゲートウェイにより受信されたデータパケットのアドレスを変換する方法も提供し、このホームゲートウェイは、前記データパケットを送信した端末装置と前記パケットを受信する端末装置間にあり、前記パケットは第1のアドレスと送信端末装置の第1のポート番号とを含んでおり、前記方法は、前記第1のアドレスと前記第1のポート番号とをプライマリアドレスと第2のポート番号とに置き換える

30

ステップを有することを特徴とし、前記第2のポート番号は、前記ゲートウェイ専用の番号範囲に属しており、且つポート番号マスクにより決定される。

【0050】

端末装置が、本発明に従って構成されるホームゲートウェイにより管理されるホームネットワークの中に自らを見出すと、ホームゲートウェイは、この端末装置の第1のアドレスの該端末装置のプライマリアドレスへの置き換えだけでなく、該端末装置専用の範囲内のポート番号の選択をも引き起こす、アドレス変換メカニズムを実行する。

【0051】

本発明の特定の一実施形態においては、データパケットのアドレスの変換方法のステップは、コンピュータプログラム命令により決定される。

40

【0052】

従って、本発明はまた、データ媒体上にあり且つホームゲートウェイの中で、またはより一般的にはコンピュータの中で実行されるように構成されたコンピュータプログラムをも提供し、このプログラムは、上述のような構成方法のステップを実行するように構成された命令を含んでいる。

【0053】

本発明の他の利点および特徴は、説明に役立つ且つ限定を意図しない例示として与えられた本発明の特定の実施形態についての以下の記述を読むことにより、また添付の図面から、より明白になる。

50

【図面の簡単な説明】

【0054】

【図1】従来のオペレータNAT機能を実施する通信ネットワークを図式的に示す図である。

【図2A】本発明のポート番号マスクの一例を示す図である。

【図2B】本発明のポート番号マスクの一例を示す図である。

【図3】オペレータの通信ネットワークに接続された本発明の複数の端末装置を図式的に示す図である。

【図4】通信ネットワーク内でデータパケットをルーティングする本発明の方法を、図式的に示す図である。

【図5】本発明のルーティング方法を実行する通信ネットワーク装置が、その置かれた環境の中にある状態を示す図である。

【図6】ルーティング識別子がデータパケットのあて先端末装置専用のルート識別子である、本発明の一実施形態を図式的に示す図である。

【図7】端末装置を構成する本発明の方法を図式的に示す図である。

【図8】本発明の構成方法を実行する端末装置が、その置かれた環境の中にある状態を示す図である。

【図9】本発明の端末装置構成方法を示す図である。

【図10】本発明の構成方法を実行するホームゲートウェイが、その置かれた環境の中にある状態を示す図である。

【発明を実施するための形態】

【0055】

本発明の一般的な原理は、同じプライマリアドレスを通信ネットワーク内の複数の端末装置に割り当てし、これらの端末装置が、ルーティング識別子と、これらに専用のポート番号の範囲を規定するポートマスクとにより、一意的に特定されるということに依存している。

【0056】

端末装置という用語は一般的であり、通信ネットワークまたはホームゲートウェイに直接接続された端末装置をわけ隔てなく指すということに留意されたい。

【0057】

本発明者らは、端末装置が、利用可能な 2^{16} 個(すなわち65536個)のポート番号値の全てを同時には使用しないということを見出した。1人の顧客は、P2P(Peer to Peer)、FTP(File Transfer Protocol)、ウェブ閲覧、電話等のアプリケーションのために少数の接続しか用いないことから、上記の範囲は、顧客の実際の要求よりも大きい。

【0058】

本発明は、上記範囲の小部分を規定するポートマスクを端末装置に割り当てることによって、各アプリケーションのために端末装置が利用可能なポート数の範囲を削減する、というところに本質が存在する。このようにして特定の端末装置に割り当てられたポートマスクは、これに送信されるデータパケットをIPサービスをデグレードさせることなくルーティングするために、そのプライマリIPアドレスと共に用いられる。

【0059】

なお、ここで留意すべきは、IP接続サービスプロバイダは、同じプライマリアドレスを有する2つ端末装置が必ず異なるポートマスクを受け取るという制約を遵守する必要があるということである。

【0060】

例えば、接続サービスプロバイダは、特定の端末装置により送信されたIPパケットのソースポート番号に対応するフィールドの最上位ビットの値を強制してもよい。この端末装置はその結果、32768個の範囲の利用可能なポート番号を規定するポートマスクを利用できる。

【0061】

一変形例においては、プロバイダは、上から8つの上位ビットの値を強制して、端末装置が利用可能な256個のポート番号範囲を有するようになる。

【0062】

ポート番号は従って、依然として16ビットフィールドで符号化されるが、このフィールドの部分はIP接続サービスプロバイダにより強制される。本発明のポートマスクの2つの例を、連続的なマスクの一例と非連続的なマスクの一例である図2Aおよび図2Bを参照して説明する。

・連続的なマスクは、隣接した一連のビット(ポートフィールドの2進法表示)を用いる。この変形例は、実施が簡単であり、本発明を実施する装置に対する処理や実施についての知識は不要である。連続的なマスクに関連する範囲は、連続的且つ固有の範囲である。これらの認可された値は、1つの区間内に含まれる。

・非連続的なマスクは、非隣接ビットを用いる。結果としてのポートの範囲は、複数の「小さな」連続範囲を合わせるにより規定されてもよい。この2つ目の変形例の利点は、複数の端末装置に同時に、ポートのデフォルト範囲を割り当てることが可能であることである。

【0063】

サービスプロバイダがIP接続サービスアーキテクチャすなわちアクセスサービスアーキテクチャを展開するオペレータの通信ネットワークRTについて、図3を用いて説明する。複数の端末装置が、このネットワークにアクセスできる。以下、端末装置という用語は、端末装置110、120、130、140、160、170を平等に指し、例えば、通信ネットワークRTや、ホームネットワークと通信ネットワークRTとの間のホームゲートウェイ230、220に直接接続された、電話器またはコンピュータなどである。

【0064】

このようなゲートウェイは、自分のプライベートネットワークの端末装置のプライベートアドレスおよび第1のポート番号を、少なくとも自分のパブリックアドレスと第2のポート番号とに適合させるアドレス変換テーブルすなわちNATテーブルを有する。

【0065】

オペレータの通信ネットワークRTは、本発明のデータパケットルーティング方法を実施する少なくとも1つのルーティングデバイスAN300を含むことが好ましい。なお、このネットワークが、他のルーティングデバイス310のような、複数の他のデバイスを含んでもよいということに、留意すべきである。

【0066】

このルーティング方法を、図4を参照して説明する。あて先パブリックアドレス@PUBとあて先ポート番号P2とを含むデータパケットPTを受信すると、本発明のルーティング方法は、ポート番号P2が属するポート番号の範囲を規定するポートマスクを決定するステップE1を実行する。通信ネットワークのこれらの端末装置に割り当てられたポートマスクは、データベースBD1に有利に格納されてもよい。ステップE2においては、このポートマスクMPは、同じパブリックアドレスP2を有する複数の端末装置からパケットPTのあて先装置を選択するために、および、このあて先装置をこのルーティング識別子IDRを用いて特定するために用いられる。パケットはその後、ステップE3で、ルーティング識別子IDRに基づき選択されたあて先装置にルーティングされる。ルーティングデバイスAN300が、そのルーティングテーブルの中にエントリを何も持っていない場合には、当該パケットは削除される。

【0067】

図5を参照して説明する実施形態において、本発明のルーティングデバイスAN300は、在来型のコンピュータの中に通常見られる要素、すなわち、プロセッサ310、ランダムアクセスメモリ(RAM)320、リードオンリーメモリ(ROM)330、およびネットワーク1と通信するための通信手段340を備える。

【0068】

また、本発明によれば、ルーティングデバイスAN300は、パブリックアドレス@PUBおよ

10

20

30

40

50

びポートマスクMPと、端末装置100のルーティング識別子IDRとの間の関連性を格納するデータベースを含むメモリ350を備える。なお、もしルーティングデバイスが、受信されたデータパケットに対するあて先端末装置の識別データを回復するためにメモリにアクセスできるという条件が満足されるなら、このメモリは、このルーティングデバイスの外部に置くこともできる。

【0069】

リードオンリーメモリ330は、本発明の記憶媒体を構成し、図4を参照して上述した本発明のルーティング方法のステップを実行するための命令を含む、本発明のコンピュータプログラムを格納する。

【0070】

本発明のルーティングデバイスANは、複数の端末装置により共有されるあて先アドレス@PUBを含むデータパケットをどの端末装置に送信にしなければならないかということが明確に判断できるように、ルーティング識別子IDRと前述の対(パブリックIPアドレス@PUBとポートマスクMP)との間の対応のテーブルを維持するということを主機能として有する。ルーティングデバイスANは、通信ネットワークRTへのアクセスPoP(point of presence)内に配置してもよいし、または集中化(centralized)してもよい。また、ルーティングデバイスANは、ルータまたは専用装置によりホストされてもよい。

【0071】

端末装置のプライマリアドレス@PUBは、ルーティングデバイスANにより、例えばルーティング情報プロトコル(RIP: routing information protocol)、中間システム-中間システム(IS-IS: intermediate system to intermediate system)プロトコル、またはOSPF(open shortest path first)などの内部ゲートウェイプロトコル(IGP: interior gateway protocol)を用いて公開される。このことが、メインアドレスとして割り当てられた任意のパブリックIPアドレス向けのIPパケットの通行を、少なくとも2台の端末装置へと強制することを可能にする。

【0072】

本発明の第1の実施形態においては、ルーティング識別子IDRは、端末装置のプライベートアドレスであり、二次アドレスとしても知られている。このようなアドレスは、ルーティングデバイスANによって公開されることはない。従って、このアドレスはRTネットワークの中心部には、ルーティングされ得ない。また、インターネットからも接触できない。ルーティングデバイスANがネットワークRTへのアクセスPOP内に存在する場合、この範囲は、この端末装置と前記POPを構成する装置との間のやりとりに限定される。

【0073】

本発明のルーティング方法の第2の実施形態を、図6を参照して以下説明する。この実施形態においては、ルーティング識別子IDRは、端末装置に専用のルート識別子である。このような識別子は、この端末装置に一意的に且つ明確に対応するルートを、一意的に指定する。これは、例えば、分離されたルートの助けを借りて実現可能である。2つのルートR1とR2は、もしオペレータのネットワーク内のルートR1を構成するノードのどれかがルートR2により交差されていなければ、分離されていると見なされる。従って、ルートR1とR2は、一連のノードから成るが、これらノードのどれかが2つのルート間で共有されてはいない。このために、基礎をなす通信ネットワークのトポロジーは、本発明のルーティングデバイスANにより維持されるルートテーブル内に、分離されたルートを導入することができるように、構成されなければならない。

【0074】

本発明において、端末装置100およびルーティングデバイスAN300は、ネットワークに接続される前にはっきりと構成される必要がある。

【0075】

本発明の端末装置を構成する本発明の方法を、図7を参照して以下説明する。例えば電源投入後にオペレータの通信ネットワークRTに接続されると、端末装置100、200、210、220、130は、サービスプロバイダのIP接続サービスに対して構成要求を既知の方法で送信

10

20

30

40

50

する。このような要求RQ-CONFは、構成サーバSCにより受信され、構成サーバSCは応答としてそのIP接続サービスを実行するために必要な構成データを供給する。

【0076】

この要求は、例えば、IPサービスプロバイダの通信ネットワーク内におけるDHCP要求DHCP_DISCOVER()のブロードキャストであってもよい。また、このメッセージは、DHCPクライアントリレー(DHCP client relay)によりリレーしてもよいし、またはDHCP構成サーバにより直接受信してもよい。このメッセージを受信すると、DHCP構成サーバは、DHCPリースを含む専用のDHCP_OFFER()メッセージにより、DHCP_DISCOVER()メッセージの送信元に応答する。

【0077】

10

本発明の構成方法は、構成要求RQ-CONFの受信の際に、構成サーバSCにより用いられる。ステップE"1は、前記の端末装置に、複数の端末装置で共有される1つのパブリックアドレスを割り当てる。ステップE"2は、次に、前記端末装置にこの端末装置に専用の番号の範囲を規定するポートマスクMPとルーティング識別子IDRとを割り当てる。このような構成データ@PUB、IDR、およびMPは、構成メッセージMESS-CONFの中で最終的に前記端末装置に送信される。

【0078】

本発明の一態様によれば、構成サーバは、端末装置に対して付属(attachment)ルーティングデバイスAN300を指定する。構成データは、このルーティングデバイスAN300にも構成サーバSCによって送信される。構成メッセージMESS-CONFはこの結果、この付属ルーティングデバイスAN300の識別子を更に含める。

20

【0079】

DHCPサーバにより構成が成された場合は、構成メッセージMESS-CONFは、構成を要求した端末装置の構成に関連するIP構成データを含む、DHCP_OFFER()タイプのオファーである。このようなデータは、少なくとも以下を含んでいる。

- ・ IPv4二次アドレス@PRIV
- ・ IPv4プライマリアドレス@PUB
- ・ 以下のフォーマットを有する新規のDHCPオプションの対象であるポートマスクMP

【0080】

【表1】

30

Code	Len	Val
TBA	variable	MP

【0081】

・ Code: このフィールドは、オプションのコードを与える。このフィールドの値は、インターネット・アサインドナンバー・オーソリティ(IANA: Internet Assigned Numbers Authority)により割り当てられる必要があり、フィールドの長さは1バイトである。

・ Len: このフィールドは、オプションの値の長さを与え、ポートマスクオプションに対しては、このフィールドの値は「variable」と等しい。

40

・ Val: このフィールドは、ポートマスクの値を与える。この値は、IPトランスポートプロトコルの「port」フィールドとしてコード化される。また、値MPは、ホームゲートウェイが利用可能なポート番号の範囲を決定するために用いられる。

【0082】

付属ルーティングデバイスANの識別子は、この状況においては、そのIPアドレスまたはその省略されていないドメイン名(FQDN)と同じ識別子a.b.c.d.であってもよい。付属ルーティングデバイスANの識別子も、新規のDHCPオプションの対象である。

【0083】

付属ルーティングデバイスオプション(DAN)の形式は以下のとおりである。

50

【 0 0 8 4 】

【表 2】

Code	Len	Val
TBA	variable	MP

【 0 0 8 5 】

・Code:このフィールドは、オプションのコードを与える。このフィールドの値は、インターネット・アサインドナンバー・オーソリティ(IANA:Internet Assigned Numbers Authority)により割り当てられる必要があり、フィールドの長さは1バイトである。

・Len:このフィールドは、オプションの値の長さを与え、付属ルーティングデバイスオプション(DAN)に対しては、このフィールドの値は「4」と等しい。

・Val:このフィールドは、パラメータDANの値を与え、この値は、IPアドレスの形でコード化される。

【 0 0 8 6 】

DHCP構成サービスは、本発明を実行するために、とりわけ上記の新規の構成データを、例えばホームゲートウェイなどの、IP接続アクセスを要求する任意の装置に割り当てるために、修正されなければならない。

【 0 0 8 7 】

図8を参照して説明する本発明の実施形態において、本発明の構成サーバSC400は、在来型のコンピュータの中に通常見られるハードウェア要素、すなわち、プロセッサ410、ランダムアクセスメモリ(RAM)420、リードオンリーメモリ(ROM)430、ネットワーク1と通信するための通信手段440を備える。

【 0 0 8 8 】

本発明によれば、構成サーバSC400は、自らが管理する端末装置の構成データ、とりわけ、プライマリアドレス@PUBおよびポートマスクMPと端末装置100のルーティング識別子IDRとの関連性を格納させるデータベースを含む、メモリ450を備える。なお、もし構成サーバが、構成要求を送信した端末装置の構成データを回復するためにメモリにアクセスできるという条件が満足されるなら、このメモリは、この構成サーバの外部に置くこともできる。

【 0 0 8 9 】

構成サーバSC400に送信された構成要求への応答として、本発明の端末装置は、通信ネットワークRTへの該端末装置のIP接続性についての構成データを含む、構成メッセージMESSAGE-CONFを受信する。この構成メッセージを受信すると、端末装置は、図9を参照して以下説明する本発明の構成方法を実行する。ステップE"1において、端末装置は受信した構成データをデータベースBDTの中に格納する。通信ネットワークRTにデータパケットPTを送信したいと端末装置が望む場合は、端末装置は、ポートマスクMPにより規定されるポート番号の範囲内のポートP2を選択し(ステップE"3)、且つ、データパケットPTにこのポートP2に対応するソースポートを割り当てる。

【 0 0 9 0 】

通信ネットワークからデータパケットPT'を受信すると、端末装置は、前記パケットのポートP'2がポートマスクMPに属することを検証するステップE"4を実行し、検証の結果が否である場合は、このパケットを拒絶する(ステップE"5)。

【 0 0 9 1 】

一変形例では、本方法は、本発明のルーティングデバイスを含む通信ネットワークRTのルーティングデバイスAN300に、構成データを送信するステップE"2を更に含んでいる。

【 0 0 9 2 】

従って、本発明のルーティングデバイスを、端末装置を介してまたは直接構成サーバSC400により構成してもよいということは、明白である。

【 0 0 9 3 】

端末装置を介しての構成は、ルーティング識別子IDRが二次アドレス@PRIVである場合に適合する。構成メッセージMESS-CONF(これはDHCPリースである可能性がある)に含まれて受信された新規構成をアクティブにした後、端末装置は、本発明のルーティングデバイスANへの構成メッセージBIND()を生成する。このルーティングデバイスは、メッセージMESS-CONF内のアドレスDANによって特定される。構成メッセージBIND(@PRIV、@PUB、MP)は、少なくともこの端末装置のメインアドレスと、このルーティング識別子IDRと、このポートマスクとを含む。この構成メッセージが更に、この端末装置に宛てられたデータパケットをこの端末装置にルーティングできるルーティングデバイスの識別子を含んでいると有利である。

10

【 0 0 9 4 】

構成メッセージは、@PRIVと同じソースアドレスを持つ端末装置により送信される。このメッセージを受信すると、ルーティングデバイスANは、これを送信した端末装置に、肯定応答を確認メッセージ(acknowledgement message)によって送信する。

【 0 0 9 5 】

ルーティング識別子IDRが端末装置に専用のルート識別子である場合には、メッセージBIND()を送信するための2つの変化形が想定されよう。いずれの変化形においても、構成サーバSCは、ルーティングデバイスANにより維持される全てのルートを知っている。

・第1の変形例では、メッセージBIND()は、構成サーバSCによりルーティングデバイスANに有利に送信される。ここで留意すべきは、この事象において構成サーバSCはメッセージBIND()を送信するが、このメッセージはメインアドレス@PUBと、ポートマスクMPと、用いられるルートの識別子とを含んでいるということである。このメッセージを受信すると、本発明のルーティングデバイスは、あらかじめ組み込まれている分離されたルートを含んでいる自らのルーティングテーブルを調べることにより、特定のルート識別子を、受信された装置IDRおよび(@PUB、MP)に関連付けする。

20

・第2の変形例では、用いられるルートの識別子が構成サーバSCによって@PUBおよびMPと同じ表現で送信される。端末装置は、以下の情報を包含するメッセージBIND()を送信する。すなわち、@PUB、MP、およびIDRである。しかしながら、この第2の変形例は、顧客がサービスプロバイダにより組み込まれたルーティングポリシーについて知っているべきではないことから、推奨はされない。

30

【 0 0 9 6 】

以下の端末装置によりルーティングデバイスAN300に送信されるBIND()メッセージの内容を、図8を参照して考察する。

- ・ 端末装置110は、メッセージBIND(@PUB1、MP1、IDR1)を送信する。
- ・ 端末装置120のホームゲートウェイ220は、メッセージBIND(@PUB2、MP2、IDR2)を送信する。
- ・ 端末装置130のホームゲートウェイ230は、メッセージBIND(@PUB3、MP3、IDR3)を送信する。
- ・ 端末装置140は、メッセージBIND(@PUB、MP4、IDR4)を送信する。

【 0 0 9 7 】

メッセージBIND()が本発明のルーティングデバイスANにより受信されると、ルーティングデバイスANは、次に、関連付け(または結び付け)テーブルの中に新しいエントリをインスタンス化する。前記テーブルは、ルーティングデバイスANにより生成され且つ同じメインアドレス@PUBを有する全ての装置のどれに、メインアドレスとして割り当てされた前記特定のIPアドレス(すなわち@PUB)に宛てられたメッセージを送信する必要があるかを、明確に判断することを可能とする。

40

【 0 0 9 8 】

このために、ルーティングデバイスANは、関連付け(IDR、(@PUB、MP))を保持する。図8の例において、関連付けのテーブルは、以下の関連付けを含む。

- ・ IDR1(@PUB、MP1)

50

- ・ IDR2(@PUB、MP2)
- ・ IDR3(@PUB、MP3)
- ・ IDR4(@PUB、MP4)

【 0 0 9 9 】

一変形形態において、メッセージBIND()のシグネチャには、DHCPリースで与えられるようなライフタイムを含んでもよい。更に、関連付テーブルに組み込まれた関連付けは、他のメッセージBIND()によって更新してもよい。ライフタイムが満了する前に何も更新を受信しなかった場合は、対応するエントリはリストから削除される(正確性の許容範囲を想定してもよい)。

【 0 1 0 0 】

他の変形例では、メッセージBIND()は、構成されたばかりの端末装置によってではなく、構成サーバSC400によって送信してもよい。また、関連付けテーブル内の新規エントリを組み込むために必要な情報は、サービスプロバイダから直接ルーティングデバイスAN300に構成サーバSC400を介して送信してもよい。

【 0 1 0 1 】

端末装置110から端末装置120に送信されるデータパケットPT(@PUB、P2)の例を、図8を参照して考察する。IPメインアドレス@PUBに宛てられたこのパケットを受信すると、ルーティングデバイスANは次に、前記メッセージのあて先ポート番号P2を読み取り、対応するポートマスクMP2を推定する。このポートマスクとメインアドレス@PUBを用いて、ルーティングデバイスANは、自らの関連付けのテーブルをスキャンすることにより、ルーティン

【 0 1 0 2 】

グ識別子IDR2や、例えば(@PUB、MP2)の対に関連する二次アドレス@PRIV2を決定する。二次アドレスの決定を受けて、ルーティングデバイスANは、受信したIPパケットをパケットPT'(@PUB、P2、IDR2)へと変換する。セキュリティ上の理由のため、このパケットPT'に用いられるあて先ポート番号は、端末装置120とルーティングデバイスANとの間でネゴシエーションされる。

【 0 1 0 3 】

ここで、パケットPTは、さまざまなやり方で変換してもよいということに留意すべきである。例えば、本発明の第1の実施形態においては、これはあて先アドレスとしてあて先端末装置120の二次アドレス@PRIV2を含んでいるパケットPT'の中にカプセル化される。

【 0 1 0 4 】

本発明の第2の実施形態においては、パケットPTは、そのヘッダの特定のフィールド内に二次アドレス@PRIV2を含むように修正される。このデータパケット変換は、ソースルーティングモードを可能にする。なお、これは、通信ネットワークのノードにより常にサポートされるわけではない。

【 0 1 0 5 】

本発明の第3の実施形態では、パケットPTは完全に同じように変換され、ルーティングは専用ルート識別子IDR2に基づいてなされる。ここでは、パケットの修正は必要ない。

【 0 1 0 6 】

図8を参照して説明する本発明の実施形態において、本発明の端末装置100は、在来型のコンピュータの中に通常見られるハードウェア要素、すなわち、プロセッサ110、ランダムアクセスメモリ(RAM)120、リードオンリーメモリ(ROM)130、ネットワーク1と通信するための通信手段140を備える。

【 0 1 0 7 】

本発明によれば、端末装置100は、自らの構成データ、とりわけ、端末装置100のパブリックアドレス@PUBとポートマスクMPとルーティング識別子IDRとの間の関連性を格納するデータベースを含む、メモリ150を備える。なお、もし端末装置が、通信ネットワークRTへの自らのIP接続性を利用するために必要な構成データを回復するために、このメモリにアクセスできるという条件が満足されるなら、メモリは、この端末装置の外部に置くこともできる。

10

20

30

40

50

【 0 1 0 8 】

図10を参照して説明される本発明の一実施形態においては、端末装置120が考察され、この端末装置120は、これと通信ネットワークRTとの間のホームゲートウェイ220のホームネットワークに接続されている。本実施形態では、ホームゲートウェイ220は、本発明の端末装置を構成する。周知の方法により、ホームゲートウェイ220はアドレス変換テーブルすなわちNATテーブルを含み、このテーブルは、自らのホームネットワークの端末装置120により送信されるストリームに対して、このホームネットワークの端末のアドレスPRIV1とポートP1とを、少なくとも1つのパブリックアドレス@PUB2とオペレータの通信ネットワークRT内のホームゲートウェイ220のポートP2とに適合させる。ここで、P2は、ポートマスクMPにより規定される番号の範囲に属している。このテーブルNATは、例えば、データベースBDTに格納されるが、データベースは内部にあっても外部にあってもよい。

10

【 0 1 0 9 】

従って、本発明のホームゲートウェイは、そのホームネットワークの端末装置から送信され且つ通信ネットワークに宛てられたデータパケットPTを受信すると、また、この端末装置に宛てられたデータパケットPT'を受信すると、アドレス変換手段を用いる。

【 0 1 1 0 】

発信については、既存の慣行と比較した唯一の違いは、本発明の端末装置120またはホームゲートウェイ220は、サービスプロバイダにより割り当てされたポートマスクにより固定された範囲内でソースポートを選択することを余儀なくされるということである。BIND()メッセージを除く全てのメッセージは、これらのソースアドレスとして、サービスプロバイダにより割り当てされたメインアドレスすなわちパブリックアドレス@PUBを伴って送信される。BIND()メッセージに対しては、用いられるソースアドレスは二次アドレスID R2=@PRIV2である。

20

【 0 1 1 1 】

特定の端末装置から送信されたデータパケットは、途中でこの端末装置が帰属するルーティングデバイスAN300を通過することが有利である。ルーティングデバイスANは、次に、この特定の端末装置より送信されたデータパケットにマークを付ける。このIPパケットのDS(differentiated service)フィールドまたはToS(type of service)フィールドを、ポートのマスクが6ビットを超えないとき且つそのときに限り、マーキングのために用いてもよい。メッセージBIND()を受信すると、ルーティングデバイスANは、当該端末装置により送信されるメッセージのためのマーキングルールをあらかじめ組み込む。カプセル化プロセスは、その後、受信されたIPパケットのDSフィールドの値に導かれ、その結果、ルーティングデバイスANはもはやトランスポート層に関連する情報を調べる必要はない。これは、メッセージ処理時間を改善する。この変形例は、用いられるDS/ToSコードを端末装置が変更することはないということ、および応答パケットに対してこのコードが同じ値にリセットされるということを想定している。

30

【 0 1 1 2 】

本発明のルーティングデバイスは、伝統的なルータまたは専用装置にホストされてもよい。例えばDHCPプロトコルの下で、構成サーバを見出す段階での、本発明により要求される修正は大きなものではないことを考えれば、現在のアーキテクチャを採用してもよい。

40

【 0 1 1 3 】

本発明のルーティングデバイスANは、オペレータの通信ネットワーク内のどこでホストされてもよい。しかし、ルーティングデバイスANは、ネットワークアクセスPOP内に展開されると有利である。更に、1台または複数のルーティングデバイスANを、集中化または分散化された態様で、同じIPアクセスPOP内に展開してもよい。

【 符号の説明 】

【 0 1 1 4 】

110, 120, 130, 140, 150, 160, 170 端末装置
220, 230 ホームゲートウェイ
AN300 ルーティングデバイス

50

【 図 3 】

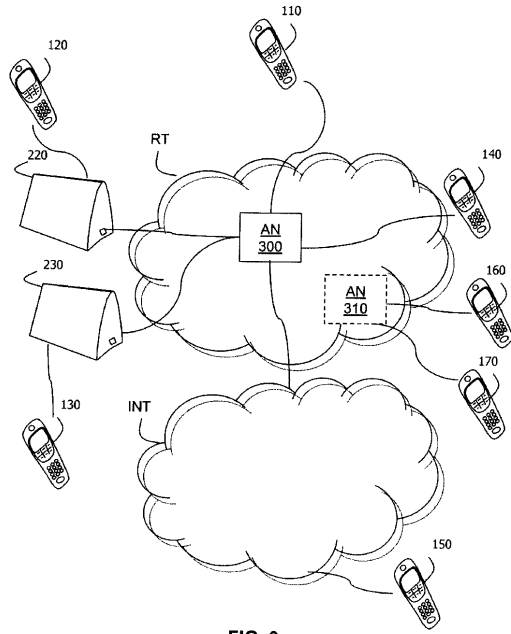


FIG. 3

【 図 4 】

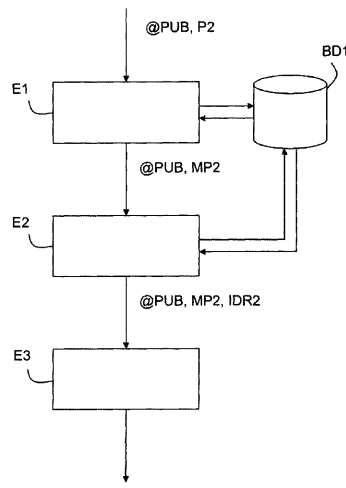


FIG. 4

【 図 5 】

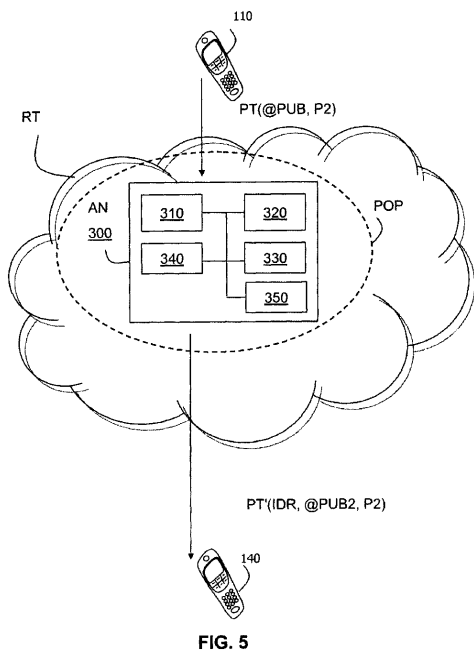


FIG. 5

【 図 6 】

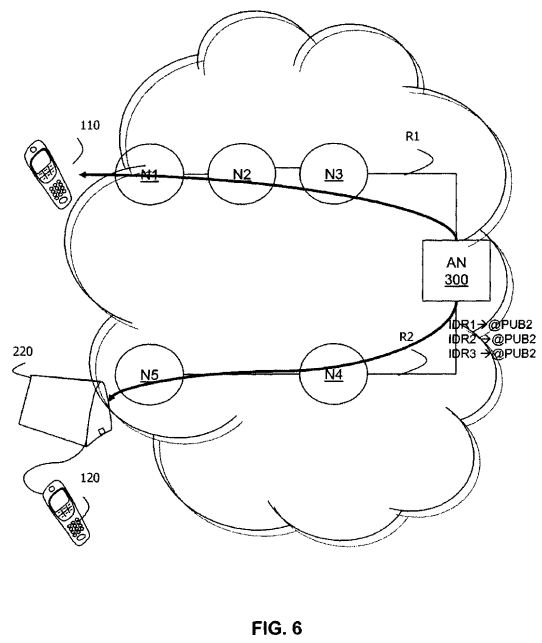


FIG. 6

【 図 7 】

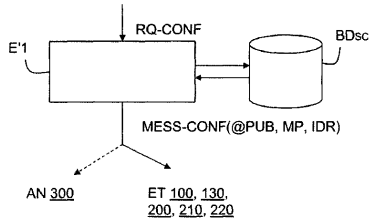


FIG. 7

【 図 8 】

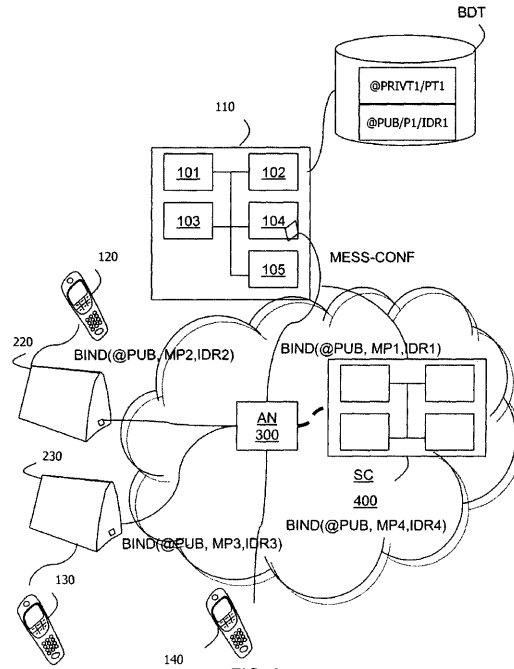


FIG. 8

【 図 9 】

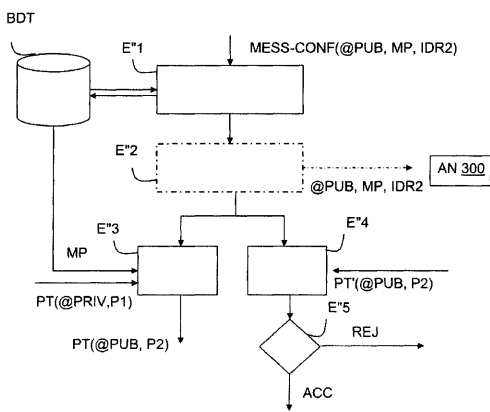


FIG. 9

【 図 10 】

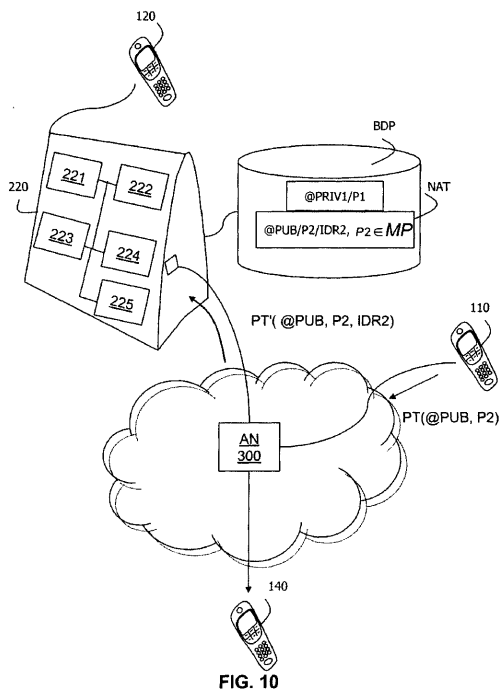


FIG. 10

フロントページの続き

審査官 山田 倍司

(56)参考文献 特表2008-527829(JP,A)
特表2004-533159(JP,A)
特開2003-218921(JP,A)

(58)調査した分野(Int.Cl., DB名)
H04L 12/00 - 12/955