

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2008-219530

(P2008-219530A)

(43) 公開日 平成20年9月18日(2008.9.18)

(51) Int.Cl.
H04L 12/56 (2006.01)

F I
H04L 12/56

テーマコード(参考)
5K030

審査請求 未請求 請求項の数 9 O L (全 17 頁)

(21) 出願番号 特願2007-54970 (P2007-54970)
(22) 出願日 平成19年3月6日(2007.3.6)

(71) 出願人 000208891
KDDI株式会社
東京都新宿区西新宿二丁目3番2号
(74) 代理人 100135068
弁理士 早原 茂樹
(72) 発明者 堀 賢治
埼玉県ふじみ野市大原二丁目1番15号
株式会社KDDI研究所内
(72) 発明者 堀内 浩規
埼玉県ふじみ野市大原二丁目1番15号
株式会社KDDI研究所内
(72) 発明者 内川 亘
東京都新宿区西新宿二丁目3番2号 KDDI株式会社内

最終頁に続く

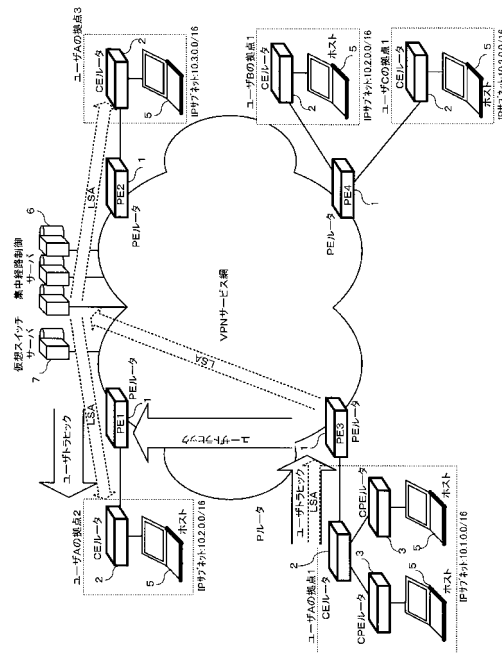
(54) 【発明の名称】 仮想閉域網にユーザ経路広告を転送するシステム及びプログラム

(57) 【要約】

【課題】VPN(Virtual Private Network)に複数のPEルータ(Provider Edge Router)が接続されており、その網側エッジルータを介してユーザ側ルータに接続されるシステムについて、ユーザが自由にVPN経路を設定することができるVPNサービス網のためのシステム及びプログラムを提供する。

【解決手段】PEルータから受信したユーザ経路広告に基づいてユーザリンクステートを生成し、ユーザVPN識別子毎にユーザリンクステートを保持し、ユーザリンクステートから、PEルータ毎のVPN経路表を算出し、VPN経路表を保持する集中経路制御サーバ(MR)を更に有する。PEルータは、MRからVPN経路表を取得し、そのVPN経路表を用いて、ユーザトラフィックの経路を制御する。また、PEルータは、ユーザ側ルータから受信したユーザ経路広告をそのまま、集中経路制御サーバへ転送する。

【選択図】図3



【特許請求の範囲】

【請求項 1】

仮想閉域網（VPN:Virtual Private Network）に複数の網側エッジルータ（PEルータ:Provider Edge Router）が接続されており、該網側エッジルータを介してユーザ側ルータに接続されるシステムにおいて、

集中経路制御サーバ（MR）を更に有し、該集中経路制御サーバは、前記網側エッジルータから受信したユーザ経路広告に基づいてユーザリンクステートを生成するユーザ経路広告処理手段と、ユーザVPN識別子毎に、ユーザリンクステートを保持するリンクステート保持手段と、

前記ユーザリンクステートから、前記網側エッジルータ毎のVPN経路表を算出するVPN経路表計算手段と、

前記VPN経路表を保持するVPN経路表保持手段とを有し、

前記網側エッジルータは、

前記集中経路制御サーバから前記VPN経路表を取得するVPN経路表取得手段と、

前記VPN経路表を用いて、ユーザトラヒックの経路を制御するVPN経路制御手段と

前記ユーザ側ルータから受信したユーザ経路広告をそのまま、前記集中経路制御サーバへ転送するユーザ経路広告転送手段とを有することを特徴とするシステム。

【請求項 2】

前記集中経路制御サーバが、複数備えられており、

仮想スイッチサーバを更に有し、該仮想スイッチサーバは、

前記集中経路制御サーバのMR識別子と、該集中経路制御サーバによって保持されたユーザリンクステートに対応するユーザVPN識別子との対応関係情報を保持する対応関係保持手段と、

前記網側エッジルータから、ユーザVPN識別子を含むMR識別子要求を受信した際に、前記対応関係保持手段を用いて該ユーザVPN識別子に対応するMR識別子を返信するPE側送信手段とを有することを特徴とする請求項 1 に記載のシステム。

【請求項 3】

仮想閉域網（VPN）とユーザ側ルータとの間に接続されており、VPN経路表を保持する集中経路制御サーバ（MR）と通信可能な網側エッジルータ（PEルータ）であって、

前記集中経路制御サーバから前記VPN経路表を取得するVPN経路表取得手段と、

前記VPN経路表を用いて、ユーザトラヒックの経路を制御するVPN経路制御手段と

前記ユーザ側ルータから受信したユーザ経路広告をそのまま、前記集中経路制御サーバへ転送するユーザ経路広告転送手段と

を有することを特徴とする網側エッジルータ。

【請求項 4】

前記集中経路制御サーバのMR識別子と、該集中経路制御サーバによって保持されたユーザリンクステートに対応するユーザVPN識別子との対応関係情報を保持する仮想スイッチサーバと更に通信可能であって、

前記仮想スイッチサーバへ、ユーザVPN識別子を含むMR識別子要求を送信し、該仮想スイッチサーバから前記ユーザVPN識別子に対応するMR識別子を受信するMR識別子取得手段を更に有し、

前記VPN経路表取得手段は、取得された前記MR識別子に基づく集中経路制御サーバから、前記VPN経路表を取得し、

前記ユーザ経路広告転送手段は、取得された前記MR識別子に基づく集中経路制御サー

10

20

30

40

50

バへ、前記ユーザ経路広告を送信することを特徴とする請求項 3 に記載の網側エッジルータ。

【請求項 5】

請求項 3 又は 4 に記載の網側エッジルータ（PE ルータ）と通信可能な集中経路制御サーバ（MR）であって、

前記網側エッジルータから受信したユーザ経路広告に基づいてユーザリンクステートを生成するユーザ経路広告処理手段と、

ユーザVPN 識別子毎に、ユーザリンクステートを保持するリンクステート保持手段と、

前記ユーザリンクステートから、前記網側エッジルータ毎のVPN 経路表を算出するVPN 経路表計算手段と、

前記VPN 経路表を保持するVPN 経路表保持手段とを有することを特徴とする集中経路制御サーバ。

【請求項 6】

前記網側エッジルータへ、前記VPN 経路表保持手段に保持した前記VPN 経路表を送信するVPN 経路表送信手段を更に有することを特徴とする請求項 5 に記載の集中経路制御サーバ。

【請求項 7】

請求項 3 又は 4 に記載の網側エッジルータと、請求項 5 又は 6 に記載の複数の集中経路制御サーバと通信可能な仮想スイッチサーバであって、

前記集中経路制御サーバのMR 識別子と、該集中経路制御サーバによって保持されたユーザリンクステートに対応するユーザVPN 識別子との対応関係情報を保持する対応関係保持手段と、

前記網側エッジルータから、ユーザVPN 識別子を含むMR 識別子要求を受信した際に、前記対応関係保持手段を用いて該ユーザVPN 識別子に対応するMR 識別子を返信するPE 側送信手段と

を有することを特徴とする仮想スイッチサーバ。

【請求項 8】

仮想閉域網（VPN）とユーザ側ルータとの間に接続されており、VPN 経路表を保持する集中経路制御サーバ（MR）と通信可能な網側エッジルータ（PE ルータ）に搭載されるコンピュータを機能させるプログラムであって、

前記集中経路制御サーバから前記VPN 経路表を取得するVPN 経路表取得手段と、

前記VPN 経路表を用いて、ユーザトラヒックの経路を制御するVPN 経路制御手段と

前記ユーザ側ルータから受信したユーザ経路広告をそのまま、前記集中経路制御サーバへ転送するユーザ経路広告転送手段と

してコンピュータを機能させることを特徴とする網側エッジルータ用のプログラム。

【請求項 9】

前記集中経路制御サーバのMR 識別子と、該集中経路制御サーバによって保持されたユーザリンクステートに対応するユーザVPN 識別子との対応関係情報を保持する仮想スイッチサーバと更に通信可能であって、

前記仮想スイッチサーバへ、ユーザVPN 識別子を含むMR 識別子要求を送信し、該仮想スイッチサーバから前記ユーザVPN 識別子に対応するMR 識別子を受信するMR 識別子取得手段を更に有し、

前記VPN 経路表取得手段は、取得された前記MR 識別子に基づく集中経路制御サーバから、前記VPN 経路表を取得し、

前記ユーザ経路広告転送手段は、取得された前記MR 識別子に基づく集中経路制御サーバへ、前記ユーザ経路広告を送信する

ようにコンピュータを機能させることを特徴とする請求項 8 に記載の網側エッジルータ用のプログラム。

10

20

30

40

50

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、仮想閉域網（VPN:Virtual Private Network）にユーザ経路広告を転送するシステム及びプログラムに関する。

【背景技術】

【0002】

企業のような組織は、地理的に分散する複数の拠点を有し、これら拠点間でネットワークを構築する場合がある。このような秘匿性を要するネットワークは、仮想閉域網（以下「VPN」という）によって構築される場合が多い。VPNサービスは、通常、プロバイダ（通信事業者）の設備であるVPNサービス網を用いて提供される。

10

【0003】

図1は、従来技術におけるVPNサービス網のシステム構成図である。

【0004】

図1によれば、プロバイダは、VPNサービス網を、プロバイダエッジルータ（Provider Edge Router、以下「PEルータ」という）1と、プロバイダルータ（Provider Router、以下「Pルータ」という）4とによって構成する。PEルータは、ユーザ拠点をVPNサービス網へ収容する装置である。Pルータは、VPNサービス網内で、VPN専用のパケットラベルを用いて、PEルータ間のユーザトラヒックを転送する。

20

【0005】

一方で、ユーザは、各拠点に1台以上のユーザ側ルータ（Customer Router、以下「CEルータ」という）2を配置する。CEルータ2は、通常、IP(Internet Protocol)ルータである。また、CEルータ2の下流ネットワークにユーザ宅内ルータ（Customer Premises Equipment router、以下「CPEルータ」という）3を更に配置していてもよい。

【0006】

図1によれば、ユーザAは、拠点1～3を有し、ユーザBは拠点1を有し、ユーザCは拠点1を有する。ユーザの各拠点に配置されたCEルータ2は、アクセス回線を介して、PEルータ1に接続する。CEルータ2は、転送すべきユーザトラヒックをPEルータ1へ送信すると共に、その拠点のユーザ経路広告もPEルータ1へ送信する。逆に、CEルータ2は、PEルータ1から、そのユーザの他の拠点からのユーザ経路広告も受信する。このユーザ経路広告は、例えば、RIPv2(Routing Information Protocol Version 2)、OSPF(Open Shortest Path First)、BGP(Border Gateway Protocol)等のダイナミックルーティングプロトコルのユーザ経路広告である。

30

【0007】

VPNサービス網には、複数のユーザVPNが相乗りする。図1によれば、ユーザA～CのユーザVPNが構成されている。ここで、ユーザVPNは、必ずしも相互に固有のIPアドレス体系を用いるとは限らない。図1によれば、ユーザAの拠点2と、ユーザBの拠点1と、ユーザCの拠点1とは、同一のIPプレフィックス(10.2.0.0/16)を利用している。従って、VPNサービス網におけるユーザトラヒックは、ユーザパケットの宛先IPアドレスと無関係であって、且つ、特定のユーザVPNの中でのみ転送されなければならない。

40

【0008】

ホスト端末5は、各ユーザVPN内に閉じたIPアドレス体系を用いる。このため、CEルータ2（又はCPEルータ3）は、ユーザパケットの宛先IPアドレスに基づいて経路制御をする。従って、CEルータ2が、そのユーザの他の拠点やIPサブネットへの経路を学習できるように、VPNサービス網は、CEルータ間で交換されるユーザ経路広告の転送を、サポートする必要がある。

【0009】

ユーザVPN経路用の経路制御プロトコルとして、「IGP」(Interior Gateway Protocol)が用いられ、PEルータ（又はPルータ）間での転送用の経路制御プロトコルとし

50

て「EGP」(Exterior Gateway Protocol)が用いられる。CEルータ間で交換されるIGPのユーザ経路広告は、「LSA」(Link State Advertisement)である。

【0010】

従来のVPNサービス網の代表的な実現方式として、BGP/MPLS(Border Gateway Protocol / Multi Protocol Label Switching)VPN(例えば非特許文献1及び2参照)がある。BGP/MPLSVPNの場合、Pルータ間及びPルータ-PEルータ間のパケット転送にMPLSを用いることにより、ユーザパケットの宛先IPアドレスと無関係なパケット転送を実現している。BGP/MPLSVPNはまた、PEルータ間でBGPセッションを確立し、その中にIGPのユーザ経路広告を格納して転送することにより、拠点間のLSAの転送をサポートしている。

10

【0011】

図1によれば、BGP/MPLSVPNにおけるユーザトラヒック及びユーザ経路広告(LSA)の流れが表されている。BGP/MPLSVPNによれば、各PEルータが、CEルータ(及びCPEルータ)及び他のPEルータから到着するLSAを受信し、且つ処理する必要がある。

【0012】

図2は、BGP/MPLSVPNにおけるPEルータの機能構成図である。

【0013】

図2によれば、PEルータ1は、経路広告検出部10と、経路広告処理部11と、リンクステート保持部13と、VPN経路表計算部14と、VPN経路制御部15とを有する。

20

【0014】

経路広告検出部10は、CEルータから、ユーザ経路広告を含むユーザトラヒックを受信し、ユーザ経路広告(LSA)のみを検出する。検出されたユーザ経路広告は、経路広告処理部11へ通知される。また、ユーザ経路広告を除くユーザトラヒックは、VPN経路制御部15へ通知される。

【0015】

経路広告処理部11は、網側エッジルータから受信したユーザ経路広告に基づいてユーザリンクステートを生成する。例えば、OSPFは、リンクステート型のプロトコルであって、ユーザVPN内の全てのCEルータ(及びCPEルータ)が、完全なネットワーク

30

【0016】

経路広告変換部12は、経路広告処理部11から通知されたユーザ経路広告を、BGPを通じて転送可能な格納形式(以下「BGP格納形式ユーザ経路広告」という)に変換して、隣接PEルータへ転送する。BGPによれば、ユーザ経路広告は、ユーザから受信した原形のままで、転送できない仕様となっているためである。

【0017】

リンクステート保持部13は、ユーザVPN識別子毎に、ユーザリンクステートを保持する。

【0018】

VPN経路表計算部14は、ユーザリンクステートから、網側エッジルータ毎のVPN経路表を算出する。算出されたVPN経路表は、VPN経路制御部15へ通知される。

40

【0019】

VPN経路制御部15は、VPN経路表を用いて、ユーザトラヒックの経路を制御する。

【0020】

【非特許文献1】E. Rosen及びY.Rekhter、「BGP/MPLS IP Virtual Private Networks (VPNs)」、IETF RFC4364、2006年2月

【非特許文献2】E. Rosen、P.Psenak及びP. Pillay-Esnault、「OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)」、IETF

50

RFC4577、2006年6月

【発明の開示】

【発明が解決しようとする課題】

【0021】

しかし、BGP/MPLS VPNでは、ユーザがVPN経路を必ずしも自由に新規設定や更新することができないという問題がある。第1の問題点は、ユーザ経路広告(LSA)を処理するPEルータに、過大な処理負荷が係ることにある。第2の問題点は、PEルータにかかるそのような処理負荷の制約を避けるために、プロバイダがユーザにVPN経路数の制約を課すことにある。第3の問題点は、ユーザはプロバイダの想定外のIGPを使用できない点にある。

10

【0022】

例えばOSPFのようなリンクステート型IGPの場合、ユーザ経路広告(LSA)を処理することは、以下の3つの意味を持つ。

(1) 各PEルータは、CEルータを介して接続されるユーザ拠点のリンクステート情報と、CPEルータを介して接続されるサブネットワークと、そのユーザの他の拠点のリンクステート情報とを、更新し且つ保持しなければならない。

(2) 受信したユーザ経路広告を、そのユーザの他のPEルータへ転送しなければならない。

(3) リンクステート情報が更新された際に、そのリンクステート情報を用いて、PEルータのユーザリンクステートを更新しなければならない。

20

【0023】

PEルータの処理負荷を増大させる理由は、主に(1)(3)である。

【0024】

第1の問題点について、PEルータに処理負荷が集中しやすい例として、あるユーザが全ての拠点を単一のOSPFエリアに収容した場合を考える。この場合、OSPFリンクステート(PEルータ/CEルータ/CPEルータ間の接続トポロジ及びメトリック)の大きさは、OSPFエリア内のCEルータ(及びCPEルータ)の合計数の2乗に比例することとなる。これに加え、大きなリンクステートに対して、ダイクストラ法等の経路計算アルゴリズムを実施して経路表を求める処理によって、PEルータの処理負荷が増大する。

30

【0025】

第1の問題点を回避するために、プロバイダは、PEルータの処理容量を考慮して、ユーザにVPN経路数(即ち、ユーザ経路広告を発するCEルータ(及びCPEルータ)の数)に制約を設ける。これが第1の問題点である。

【0026】

尚、第1及び第2の問題点1及び2を解決するために、単純にPEルータの処理容量を増大させることもできる。しかしながら、この解決策は、設備投資が非常に非効率となり、サービスコストの低減を望むプロバイダにとって非現実的である。なぜなら、ユーザ経路広告の処理と、ユーザ拠点のVPNサービス網への収容処理とを、同一装置即ちPEルータのみで行うためである。

40

【0027】

PEルータの処理負荷は、その収容するユーザ拠点の数と、ユーザの使用するIGPの種類と、ユーザの広告するVPN経路数等に応じて変動する。しかし、その変動幅は、プロバイダがVPNサービス網を構築する時点では必ずしも明らかではない。このような場合、将来的な処理負荷の増加を見越して、全てのPEルータに処理容量の大きい装置を用いてVPNサービス網を構築する対策が考えられる。しかし、一般に処理容量の大きいPEルータほど高価であるため、VPNサービス網構築の初期投資が高額となる。また、PEルータの実際の処理負荷に大きな格差が生じる可能性が否定できず、結果的に処理容量に余裕のあるPEルータへの投資が無駄になってしまう。従って、全てのPEルータに処理容量の大きい装置を用いてVPNサービス網を構築することは、投資効率が必ずしも良

50

いとはいえない。

【 0 0 2 8 】

また、初期投資の抑制、投資効率の向上を求めて、VPNサービス網の運用中、処理容量の需要に応じて一部のPEルータのみを設備更新することもできる。しかし、ユーザがプロバイダの求める制限を越えてVPN経路数を増加させようと希望しても、プロバイダにその希望を伝え、プロバイダがPEルータの設備更新（処理容量の拡大）を決定し、それを完了するまで相当な期間、待たなければならない。また、設備が更新されない可能性もある。なぜなら、当該ユーザがVPN経路数を減少させたり、収容するPEルータが移動したりして、PEルータの処理容量に余裕ができたとしても、一旦拡大した処理容量は必ずしも再利用できるとは限らないからである。この場合、ユーザがVPN経路を自由に設定できるとはいえない。

10

【 0 0 2 9 】

このように、BGP/MPLS VPNでは、ユーザ経路広告(LSA)の処理と、ユーザ拠点のVPNサービス網への収容とを、同一装置で行わなければならない。このため、PEルータに収容されるユーザ拠点数と、ユーザの使用するIGPの種類と、ユーザの広告するLSAの数等（各種パラメータ）によっては、いずれのPEルータにおいても、ユーザ経路広告の処理負荷が増大する可能性がある。一方、これらのパラメータは、PEルータの設置前には、必ずしも正確に予測できない。

【 0 0 3 0 】

従って、プロバイダは、設備投資時点での平均的な見積りに基づいて、処理能力を決定し、PEルータの設備投資を行わざるを得ない。この結果、プロバイダは準備したPEルータの処理能力で収まるように、ユーザのVPN経路数を制約せざるを得ない。また、そのようなVPN経路数の制約のために、ユーザは、自由にVPN経路を設定できない。

20

【 0 0 3 1 】

第1及び第2の問題点が解決されたとしても、更に、第3の問題点が残る。これについて以下に説明する。

【 0 0 3 2 】

第3の問題点は、前述した(2)（「受信したユーザ経路広告を他のPEルータにも転送する」）の処理について発生する。図1によれば、PEルータ1に流入したユーザ経路広告は、BGP格納形式ユーザ経路広告に変換されて、他のPEルータ1へと転送されている。

30

【 0 0 3 3 】

また、例えば非特許文献2のような、IGP個別のBGP格納形式ユーザ経路広告の定義によれば、各IGPに対応するPEルータの経路広告変換部が、IGPの種類毎に必要なことを意味する。

【 0 0 3 4 】

このため、もし、プロバイダがPEルータを準備した時点で、ユーザが、プロバイダによって想定されないIGPをCEルータ間で交換させようとしても、VPNサービス網を透過できない。即ち、CEルータ又はCPEルータの発するユーザ経路広告は、VPNサービス網を全く透過できない。このユーザ経路広告をVPNサービス網を透過させるためには、プロバイダが、PEルータの経路広告変換部を機能拡張する必要がある。

40

【 0 0 3 5 】

更に、PEルータが対応しないIGPに対応するように、経路広告変換部を機能拡張するためには、BGP格納形式ユーザ経路広告への変換仕様を、製造者の異なるCEルータ及びPEルータを包含するユーザVPNの中で、矛盾無く動作するように規定しなければならない。このため、変換仕様は、非特許文献2のように、標準化団体による標準化手続きを経て承認されなければならない、その手続きには多大な時間を要する。

【 0 0 3 6 】

このため、プロバイダが、VPNサービス網を、あるIGPに対応させるまでの時間及びコストを考慮すると、ユーザが、プロバイダ想定外のIGPを使うことは非常に困難と

50

なるという課題がある。これが、第3の問題点であり、BGP/MPLS VPNでは、ユーザがVPN経路を自由に設定できない理由の1つである。

【0037】

そこで、本発明は、ユーザが自由にVPN経路を設定することができるVPNサービス網のためのシステム及びプログラムを提供することを目的とする。

【課題を解決するための手段】

【0038】

本発明によれば、仮想閉域網(VPN:Virtual Private Network)に複数の網側エッジルータ(PEルータ:Provider Edge Router)が接続されており、該網側エッジルータを介してユーザ側ルータに接続されるシステムにおいて、

集中経路制御サーバ(MR)を更に有し、該集中経路制御サーバは、網側エッジルータから受信したユーザ経路広告に基づいてユーザリンクステートを生成するユーザ経路広告処理手段と、

ユーザVPN識別子毎に、ユーザリンクステートを保持するリンクステート保持手段と、ユーザリンクステートから、網側エッジルータ毎のVPN経路表を算出するVPN経路表計算手段と、

VPN経路表を保持するVPN経路表保持手段とを有し、

網側エッジルータは、集中経路制御サーバからVPN経路表を取得するVPN経路表取得手段と、VPN経路表を用いて、ユーザトラヒックの経路を制御するVPN経路制御手段と、ユーザ側ルータから受信したユーザ経路広告をそのまま、集中経路制御サーバへ転送するユーザ経路広告転送手段と

を有することを特徴とする。

【0039】

本発明のシステムにおける他の実施形態によれば、集中経路制御サーバが、複数備えられており、仮想スイッチサーバを更に有し、該仮想スイッチサーバは、集中経路制御サーバのMR識別子と、該集中経路制御サーバによって保持されたユーザリンクステートに対応するユーザVPN識別子との対応関係情報を保持する対応関係保持手段と、

網側エッジルータから、ユーザVPN識別子を含むMR識別子要求を受信した際に、対応関係保持手段を用いて該ユーザVPN識別子に対応するMR識別子を返信するPE側送信手段とを有することも好ましい。

【0040】

本発明によれば、仮想閉域網(VPN)とユーザ側ルータとの間に接続されており、VPN経路表を保持する集中経路制御サーバ(MR)と通信可能な網側エッジルータ(PEルータ)であって、

集中経路制御サーバからVPN経路表を取得するVPN経路表取得手段と、VPN経路表を用いて、ユーザトラヒックの経路を制御するVPN経路制御手段と、ユーザ側ルータから受信したユーザ経路広告をそのまま、集中経路制御サーバへ転送するユーザ経路広告転送手段と

を有することを特徴とする。

【0041】

本発明の網側エッジルータにおける他の実施形態によれば、集中経路制御サーバのMR識別子と、該集中経路制御サーバによって保持されたユーザリンクステートに対応するユーザVPN識別子との対応関係情報を保持する仮想スイッチサーバと更に通信可能であって、

仮想スイッチサーバへ、ユーザVPN識別子を含むMR識別子要求を送信し、該仮想ス

10

20

30

40

50

イチサーバからユーザVPN識別子に対応するMR識別子を受信するMR識別子取得手段を更に有し、

VPN経路表取得手段は、取得されたMR識別子に基づく集中経路制御サーバから、VPN経路表を取得し、

ユーザ経路広告転送手段は、取得されたMR識別子に基づく集中経路制御サーバへ、ユーザ経路広告を送信する

ことを特徴とする。

【0042】

本発明によれば、前述した網側エッジルータ（PEルータ）と通信可能な集中経路制御サーバ（MR）であって、

網側エッジルータから受信したユーザ経路広告に基づいてユーザリンクステートを生成するユーザ経路広告処理手段と、

ユーザVPN識別子毎に、ユーザリンクステートを保持するリンクステート保持手段と、

ユーザリンクステートから、網側エッジルータ毎のVPN経路表を算出するVPN経路表計算手段と、

VPN経路表を保持するVPN経路表保持手段と

を有することを特徴とする。

【0043】

本発明の集中経路制御サーバにおける他の実施形態によれば、

網側エッジルータへ、VPN経路表保持手段に保持したVPN経路表を送信するVPN経路表送信手段を更に有することも好ましい。

【0044】

本発明によれば、前述した網側エッジルータと、前述した複数の集中経路制御サーバと通信可能な仮想スイッチサーバであって、

集中経路制御サーバのMR識別子と、該集中経路制御サーバによって保持されたユーザリンクステートに対応するユーザVPN識別子との対応関係情報を保持する対応関係保持手段と、

網側エッジルータから、ユーザVPN識別子を含むMR識別子要求を受信した際に、対応関係保持手段を用いて該ユーザVPN識別子に対応するMR識別子を返信するPE側送信手段と

を有することを特徴とする。

【0045】

本発明によれば、仮想閉域網（VPN）とユーザ側ルータとの間に接続されており、VPN経路表を保持する集中経路制御サーバ（MR）と通信可能な網側エッジルータ（PEルータ）に搭載されるコンピュータを機能させるプログラムであって、

集中経路制御サーバからVPN経路表を取得するVPN経路表取得手段と、

VPN経路表を用いて、ユーザトラヒックの経路を制御するVPN経路制御手段と、

ユーザ側ルータから受信したユーザ経路広告をそのまま、集中経路制御サーバへ転送するユーザ経路広告転送手段と

してコンピュータを機能させることを特徴とする。

【0046】

本発明の網側エッジルータ用のプログラムにおける他の実施形態によれば、

集中経路制御サーバのMR識別子と、該集中経路制御サーバによって保持されたユーザリンクステートに対応するユーザVPN識別子との対応関係情報を保持する仮想スイッチサーバと更に通信可能であって、

仮想スイッチサーバへ、ユーザVPN識別子を含むMR識別子要求を送信し、該仮想スイッチサーバからユーザVPN識別子に対応するMR識別子を受信するMR識別子取得手段を更に有し、

VPN経路表取得手段は、取得されたMR識別子に基づく集中経路制御サーバから、V

10

20

30

40

50

P N 経路表を取得し、

ユーザ経路広告転送手段は、取得された M R 識別子に基づく集中経路制御サーバへ、ユーザ経路広告を送信する

ようにコンピュータを機能させることも好ましい。

【発明の効果】

【0047】

本発明によれば、ユーザ経路広告の処理は、各 P E ルータから分離され、集中経路制御サーバで一括して集中的に実行される。これにより、プロバイダは、どの P E ルータのユーザ経路広告の処理負荷が大きくなるかを、V P N サービス網構築段階で適切に推測する必要がなくなる。本発明によれば、運用中に、集中経路制御サーバにおけるユーザ経路広告の処理負荷が増大してきた場合、集中経路制御サーバの台数又はその処理容量を増やすこともできる。これにより、V P N 経路数の増加、即ち、ユーザ経路広告の処理負荷の増加に対応することができる。

10

【0048】

また、本発明によれば、あるユーザの V P N 経路数が増加され、ユーザ経路広告の処理負荷が高まってきた場合、プロバイダ運用者は、仮想スイッチサーバにおける当該ユーザと集中経路制御サーバとの対応関係を解除して、処理容量に余裕のある他の集中経路生業サーバへ新たに設定することができる。このため、任意の集中経路制御サーバに収容したユーザの V P N 経路数が増加しても、仮想スイッチサーバに対する対応関係の操作によって容易に対応できる。従って、B G P / M P L S V P N のように、P E ルータの処理容量に応じて、ユーザに V P N 経路数の制約を課す必要もなくなり、ユーザは自由に V P N 経路を設定することができる。

20

【発明を実施するための最良の形態】

【0049】

以下では、図面を用いて、本発明を実施するための最良の形態について詳細に説明する。

【0050】

図3は、本発明における V P N サービス網のシステム構成図である。

【0051】

図3によれば、図1と比較して、複数の集中経路制御サーバ(M R)6と、1つの仮想スイッチサーバ(V S W - O S)7と更に備える。また、図1と比較して、ユーザトラヒックの流れは同じであるものの、ユーザ経路広告(L S A)の流れが異なる。ユーザ拠点からユーザ経路広告を受信した P E ルータは、いずれか1つの集中経路制御サーバ6へ転送される。ユーザ経路広告を受信した集中経路制御サーバは、そのユーザの他の拠点へ転送するために、他の P E ルータへ転送する。

30

【0052】

図4は、本発明における P E ルータの機能構成図である。

【0053】

P E ルータ1は、V P N サービス網と C E ルータとの間に接続されており、V P N 経路表を保持する集中経路制御サーバ6と通信可能である。図4によれば、本発明における P E ルータ1は、図2と比較して、経路広告処理部11と、リンクステート保持部13と、V P N 経路表計算部14とを有さない。それに代えて、本発明の P E ルータ1は、経路広告転送部16と、M R 識別子取得部17とを有する。尚、本発明によれば、経路広告処理部11と、リンクステート保持部13と、V P N 経路表計算部14とは、集中経路制御サーバ6に備えられる。

40

【0054】

経路広告検出部10は、C E ルータから、ユーザ経路広告を含むユーザトラヒックを受信し、ユーザ経路広告のみを検出する。検出されたユーザ経路広告は、経路広告転送部16へ通知される。また、ユーザ経路広告を除くユーザトラヒックは、V P N 経路制御部15へ通知される。

50

【 0 0 5 5 】

経路広告転送部 1 6 は、C E ルータから受信したユーザ経路広告 (L S A : Link State Advertisement) をそのまま、M R 識別子取得部 1 7 によって指定される集中経路制御サーバ 6 へ転送する。本発明における P E ルータ 1 は、ユーザ経路広告をそのまま、指定された集中経路制御サーバ 6 へ転送するだけであるので、極めて処理負荷が小さい。

【 0 0 5 6 】

V P N 経路制御部 1 5 は、B G P / M P L S V P N と同様に、V P N 経路表に従って、ユーザトラヒックの経路を制御する。この V P N 経路表は、V P N 経路表取得部 1 8 から受信する。

【 0 0 5 7 】

M R 識別子取得部 1 7 は、仮想スイッチサーバ 7 へ、ユーザ V P N 識別子を含む M R 識別子要求を送信する。これに対し、M R 識別子取得部 1 7 は、仮想スイッチサーバ 7 から、そのユーザ V P N 識別子に対応する M R 識別子を受信する。M R 識別子は、経路広告転送部 1 6 へ通知される。これにより、経路広告転送部 1 6 は、ユーザ経路広告を、その M R 識別子に対応する集中経路制御サーバ 6 へ送信する。

【 0 0 5 8 】

また、M R 識別子取得部 1 7 は、仮想スイッチサーバ 7 から受信した M R 識別子を、V P N 経路表取得部 1 8 へ通知する。

【 0 0 5 9 】

V P N 経路表取得部 1 8 は、M R 識別子に対応する集中経路制御サーバ 6 へ、V P N 経路表要求を送信する。これに対し、V P N 経路表取得部 1 8 は、集中経路制御サーバ 6 から、V P N 経路表を受信する。受信された V P N 経路表は、V P N 経路制御部 1 5 へ通知される。尚、V P N 経路表が、集中経路制御サーバ 6 から定期的に送信されるものであってもよい。また、P E ルータ 1 の V P N 経路表取得部 1 8 が、仮想スイッチサーバ 7 から特定のシグナルを受信した際に、集中経路制御サーバ 6 へ V P N 経路表要求を送信するものであってもよい。

【 0 0 6 0 】

尚、経路広告検出部 1 0 と、V P N 経路制御部 1 5 と、経路広告転送部 1 6 と、M R 識別子取得部 1 7 と、V P N 経路表取得部 1 8 とは、P E ルータに搭載されたコンピュータを機能させるプログラムを実行することによっても実現できる。

【 0 0 6 1 】

図 5 は、本発明における集中経路制御サーバ及び仮想スイッチサーバの機能構成図である。

【 0 0 6 2 】

図 5 によれば、集中経路制御サーバ 6 は、経路広告処理部 6 1 と、リンクステート保持部 6 2 と、V P N 経路表計算部 6 3 と、V P N 経路表保持部 6 4 と、V P N 経路表送信部 6 5 とを有する。

【 0 0 6 3 】

経路広告処理部 6 1 は、網側エッジルータからユーザ経路広告 (L S A) を受信する。そして、そのユーザ経路広告に基づいてユーザリンクステートが生成される。生成されたユーザリンクステートは、リンクステート保持部 6 2 へ通知される。

【 0 0 6 4 】

リンクステート保持部 6 2 は、ユーザ V P N 識別子毎に、ユーザリンクステートを保持する。

【 0 0 6 5 】

V P N 経路表計算部 6 3 は、ユーザリンクステートから、網側エッジルータ毎の V P N 経路表を算出する。

【 0 0 6 6 】

V P N 経路表保持部 6 4 は、ユーザ V P N 識別子毎に、必要な P E ルータ毎の V P N 経路表を保持する。図 3 によれば、ユーザ A 用の V P N 経路表には、P E 1 用、P E 2 用及

10

20

30

40

50

びPE 3用のVPN経路表が保持される。どの集中経路制御サーバ6が、どのユーザのVPN経路表を保持するかの対応関係は、仮想スイッチサーバ7からの指示に基づく。従って、仮想スイッチサーバ7からの指示によって、集中経路制御サーバ6によって保持されるユーザVPN経路表は異なる。

【0067】

VPN経路表送信部65は、PEルータへ、VPN経路表保持部64に保持したVPN経路表を送信する。

【0068】

図5によれば、仮想スイッチサーバ7は、対応関係保持部71と、PE側送信部72と、MR側送信部73とを有する。

【0069】

対応関係保持部71は、集中経路制御サーバ6のMR識別子と、その集中経路制御サーバ6によって保持されたユーザリンクステートに対応するユーザVPN識別子との対応関係情報を保持する。この対応関係情報は、プロバイダ運用者によって自由に設定することができる。

【0070】

PE側送信部72は、網側エッジルータから、ユーザVPN識別子を含むMR識別子要求を受信した際に、対応関係保持部71を用いて該ユーザVPN識別子に対応するMR識別子を返信する。

【0071】

MR側送信部73は、対応関係保持部71の対応関係が更新された際に、各集中経路制御サーバ6へ、その旨を指示する。例えば、ユーザC用VPN経路表を、MR1からMR2へ変更したとする(後述する図6及び図7を参照)。このとき、ユーザC用VPN経路表の管理終了をMR1へ送信し、ユーザC用VPN経路表の管理開始をMR2へ送信する。

【0072】

尚、PE側送信部72も、対応関係保持部71の対応関係が更新された際に、各PEルータ1へ、その旨を指示する。

【0073】

図6は、仮想スイッチサーバの対応関係情報と、集中経路制御サーバが保持するVPN経路表との第1の関係図である。

【0074】

図6によれば、仮想スイッチサーバ7は、ユーザA及びユーザCのVPN識別子は、MR識別子MR1に対応付けられており、ユーザBのVPN識別子は、MR識別子MR2に対応付けられている。このとき、集中経路サーバMR1は、ユーザA用VPN経路表と、ユーザC用VPN経路表とを保持する。ユーザA用VPN経路表には、PEルータPE1、PE2及びPE3それぞれに対するVPN経路表を保持する。一方、集中経路サーバMR2は、ユーザB用VPN経路表を保持する。ユーザB用VPN経路表には、PEルータPE4に対するVPN経路表を保持する。

【0075】

ここで、集中経路制御サーバMR1について、ユーザ経路広告の処理負荷が大きくなってきたとする。このとき、プロバイダ運用者は、仮想スイッチサーバ7の対応関係情報を、任意の時点で変更することができる。

【0076】

図7は、仮想スイッチサーバの対応関係情報と、集中経路制御サーバが保持するVPN経路表との第2の関係図である。

【0077】

図7によれば、仮想スイッチサーバ7は、ユーザAのVPN識別子のみを、MR識別子MR1に対応付け、ユーザCのVPN識別子を、MR識別子MR2に変更されている。このとき、集中経路サーバMR1は、ユーザA用VPN経路表のみを保持する。一方、集中

10

20

30

40

50

経路サーバMR2は、ユーザB用VPN経路表及びユーザC用VPN経路表を保持する。

【0078】

以上、詳細に説明したように、本発明によれば、ユーザ経路広告の処理は、各PEルータから分離され、集中経路制御サーバで一括して集中的に実行される。これにより、プロバイダは、どのPEルータのユーザ経路広告の処理負荷が大きくなるかを、VPNサービス網構築段階で適切に推測する必要がなくなる。本発明によれば、運用中に、集中経路制御サーバにおけるユーザ経路広告の処理負荷が増大してきた場合、集中経路制御サーバの台数又はその処理容量を増やすこともできる。これにより、VPN経路数の増加、即ち、ユーザ経路広告の処理負荷の増加に対応することができる。

【0079】

また、本発明によれば、あるユーザのVPN経路数が増加され、ユーザ経路広告の処理負荷が高まってきた場合、プロバイダ運用者は、仮想スイッチサーバにおける当該ユーザと集中経路制御サーバとの対応関係を解除して、処理容量に余裕のある他の集中経路生業サーバへ新たに設定することができる。このため、任意の集中経路制御サーバに収容したユーザのVPN経路数が増加しても、仮想スイッチサーバに対する対応関係の操作によって容易に対応できる。従って、BGP/MPLS VPNのように、PEルータの処理容量に応じて、ユーザにVPN経路数の制約を課す必要もなくなり、ユーザは自由にVPN経路を設定することができる。

【0080】

更に、本発明によれば、PEルータ上にIGP固有なユーザ経路広告変換仕様に順ずる経路広告変換部を設ける必要がなくなるため、ユーザから新たなIGP利用開始の要望があった場合も、当該IGPに対応する経路広告処理部、リンクステート保持部及びVPN経路表計算部のみを集中経路制御サーバ上に備えるだけで、対応することができる。

【0081】

ここで、経路広告処理部、リンクステート保持部及びVPN経路表計算部を、集中経路制御サーバに備えることは、PEルータ上に経路広告変換部を備えるよりも極めて簡単である。その理由は、以下のとおりである。

【0082】

まず、ユーザが、当該IGPを利用できるということは、当該IGPに対応するセルータやCPEルータが既に存在していることを意味する。即ち、当該IGPに対応する経路広告処理部、リンクステート保持部及びVPN経路表計算部が、既にセルータやCPEルータの機能として備えられていることになる。従って、セルータやCPEルータの経路広告処理部、リンクステート保持部及びVPN経路表計算部を、そのままMRに備えるだけで済むからである。

【0083】

また、そのようなセルータやCPEルータを集中経路制御サーバの機能部品として流用してもよい。即ち、ある集中経路制御サーバから、ユーザ経路広告を（機能部品として利用される）セルータやCPEルータに通知する。そして、それらの経路広告処理部、リンクステート保持部及びVPN経路表計算部に処理させる。その処理結果を集中経路制御サーバが取得する。この形態によれば、当該IGPに対応する経路広告処理部、リンクステート保持部及びVPN経路表計算部を、集中経路制御サーバに備える必要性も無くなる。

【0084】

前述した本発明における種々の実施形態によれば、当業者は、本発明の技術思想及び見地の範囲における種々の変更、修正及び省略を容易に行うことができる。前述の説明はあくまで例であって、何ら制約しようとするものではない。本発明は、特許請求の範囲及びその均等物として限定するもののみ制約される。

【図面の簡単な説明】

【0085】

【図1】従来技術におけるVPNサービス網のシステム構成図である。

10

20

30

40

50

【図 2】 B G P / M P L S V P Nにおける P E ルータの機能構成図である。

【図 3】 本発明における V P N サービス網のシステム構成図である。

【図 4】 本発明における P E ルータの機能構成図である。

【図 5】 本発明における集中経路制御サーバ及び仮想スイッチサーバの機能構成図である。

【図 6】 仮想スイッチサーバの対応関係情報と、集中経路制御サーバが保持する V P N 経路表との第 1 の関係図である。

【図 7】 仮想スイッチサーバの対応関係情報と、集中経路制御サーバが保持する V P N 経路表との第 2 の関係図である。

【符号の説明】

10

【 0 0 8 6 】

1 P E ルータ、網側エッジルータ

1 0 経路広告検出部

1 1 経路広告処理部

1 2 経路広告変換部

1 3 リンクステート保持部

1 4 V P N 経路表計算部

1 5 V P N 経路制御部

1 6 経路広告転送部

1 7 M R 識別子取得部

20

1 8 V P N 経路表取得部

2 C E ルータ、ユーザ側ルータ

3 C P E ルータ

4 P ルータ

5 ホスト

6 集中経路制御サーバ

6 1 経路広告処理部

6 2 リンクステート保持部

6 3 V P N 経路表計算部

6 4 V P N 経路表保持部

30

6 5 V P N 経路表送信部

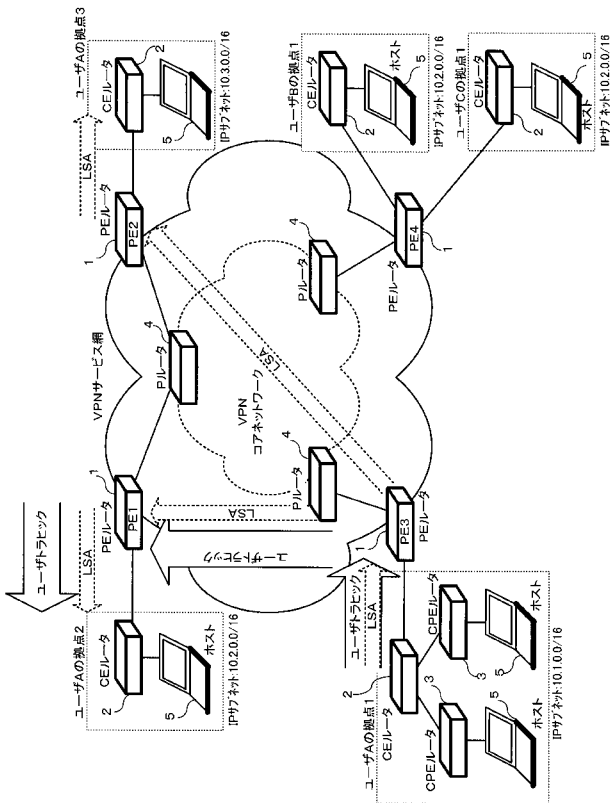
7 仮想スイッチサーバ

7 1 対応関係保持部

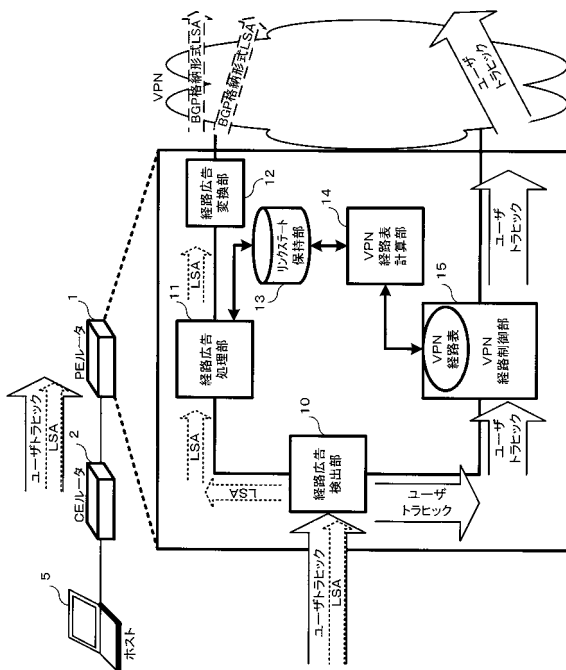
7 2 P E 側送信部

7 3 M R 側送信部

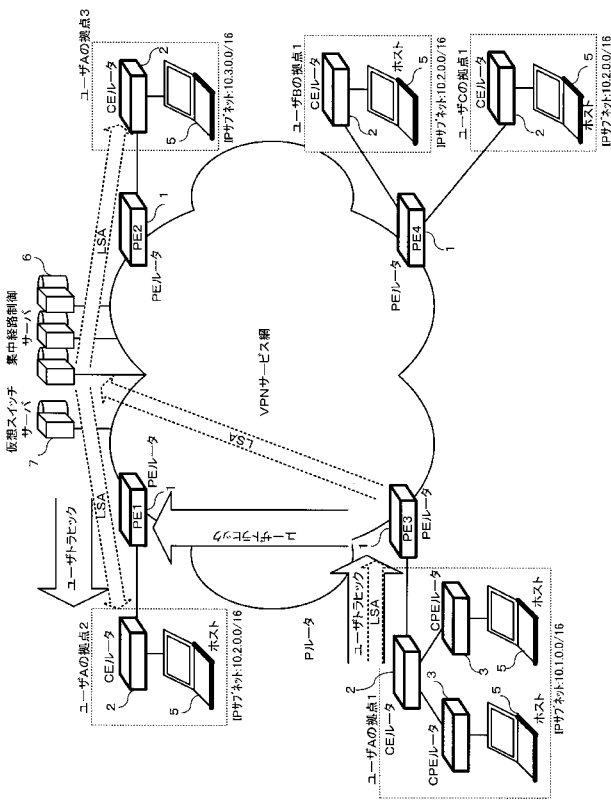
【 図 1 】



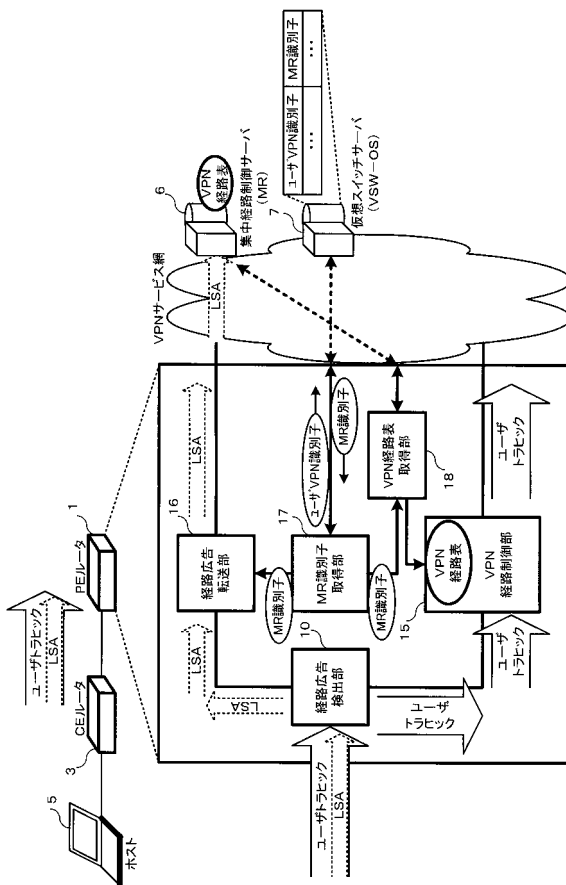
【 図 2 】



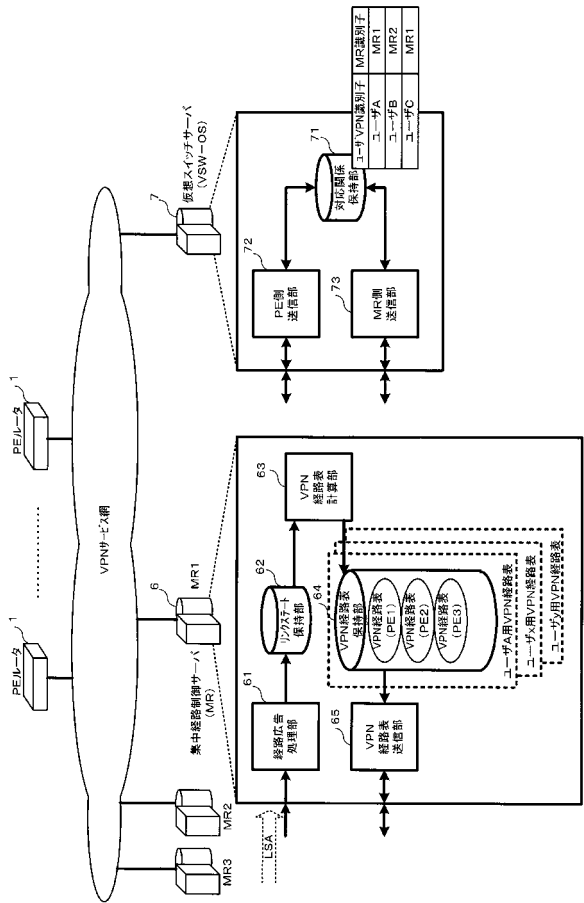
【 図 3 】



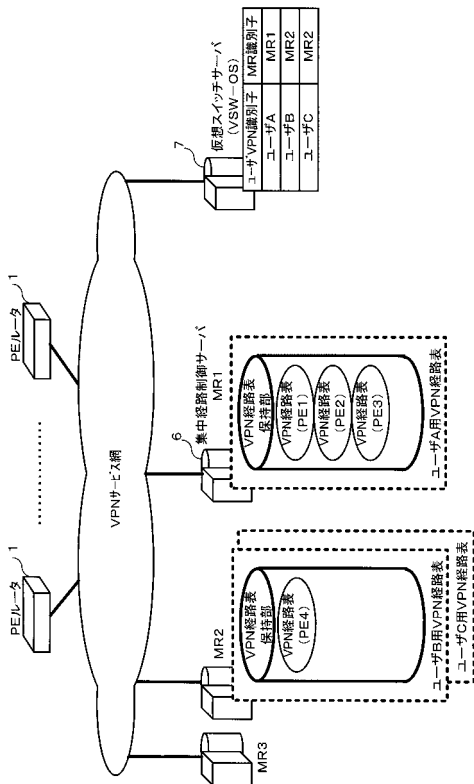
【 図 4 】



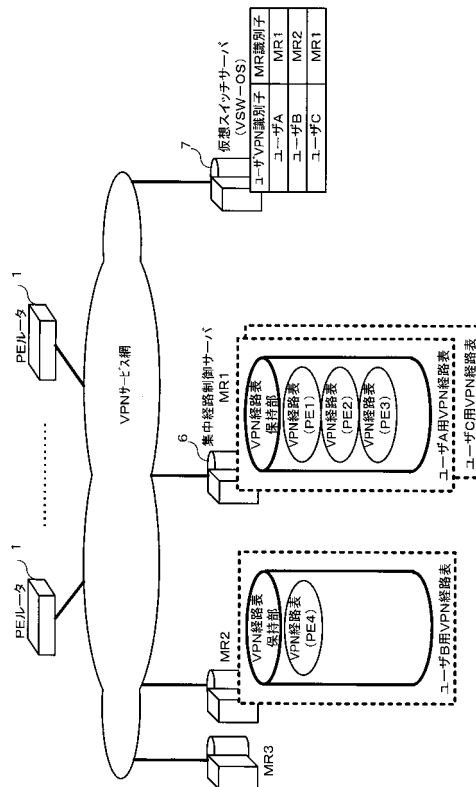
【 図 5 】



【 図 7 】



【 図 6 】



フロントページの続き

(72)発明者 安藤 雅人

東京都新宿区西新宿二丁目3番2号 KDDI株式会社内

(72)発明者 大野 泰伸

東京都新宿区西新宿二丁目3番2号 KDDI株式会社内

Fターム(参考) 5K030 GA11 HA08 HB11 HC01 HC13 HD03 KA05 LB05