(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4361270号
(P4361270)
(45)発行日　平成21年11月11日(2009.11.11)　(24)登録日　平成21年8月21日(2009.8.21)

(51)Int.Cl.　　F I
H04L 12/66 (2006.01)　　H04L 12/66　A
H04L 12/56 (2006.01)　　H04L 12/56　G
　　H04L 12/56　H

請求項の数 13　(全 12 頁)

(21)出願番号　特願2002-520510 (P2002-520510)
(86)(22)出願日　平成13年8月10日 (2001.8.10)
(65)公表番号　特表2004-507169 (P2004-507169A)
(43)公表日　平成16年3月4日 (2004.3.4)
(86)国際出願番号　PCT/US2001/025277
(87)国際公開番号　WO2002/015514
(87)国際公開日　平成14年2月21日 (2002.2.21)
審査請求日　平成16年9月27日 (2004.9.27)
審判番号　不服2007-7275 (P2007-7275/J1)
審判請求日　平成19年3月9日 (2007.3.9)
(31)優先権主張番号　09/638,351
(32)優先日　平成12年8月15日 (2000.8.15)
(33)優先権主張国　米国 (US)

(73)特許権者　500310339
アバイア　インコーポレーテッド
アメリカ合衆国．０７９２０　ニュージャーシイ．バスキング　リッジ．マウント　エアリー　ロード　２１１
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100096943
弁理士　臼井　伸一
(74)代理人　100101498
弁理士　越智　隆夫
(74)代理人　100104352
弁理士　朝日　伸光

最終頁に続く

(54)【発明の名称】網フロースイッチを用いてのＶＰＮデバイスのクラスタリング

(57)【特許請求の範囲】
【請求項１】
仮想プライベート網（ＶＰＮ）上にて、第１の複数のユーザ（１１０）と第２の複数のユーザ（１３２）の間でメッセージトラフィックをルーティングする方法であって、
各々が異なるメディア・アクセス・コントロール（ＭＡＣ）アドレスを有する複数のＶＰＮデバイスを含むクラスタ（１２４）を生成するステップであって、該クラスタ内に含まれるＶＰＮデバイスの一義的なＩＰアドレスと区別される論理インターネットプロトコル（ＩＰ）アドレスによって、クラスタがアドレスされるようになっているステップ（２００）と、
該クラスタに含まれる該ＶＰＮデバイスの中から選択される１つのＶＰＮデバイスを介して、該第１の複数のユーザと該第２の複数のユーザの間でトラフィックを分配するステップであって、該１つのＶＰＮデバイスがパケット宛先ＩＰアドレスとＶＰＮデバイスＭＡＣアドレスの両方に基づいて選択されるようになっているステップ（３００）と、を含むことを特徴とする方法。
【請求項２】
請求項１に記載の方法において、該クラスタを生成するステップが、さらに
単一のＭＡＣアドレスを該ＶＰＮデバイスのクラスタに割り当てる処理を含み、該トラフィックを分配するステップが、該単一のＭＡＣアドレスにアドレスされたトラフィックの単一のＭＡＣアドレスを、該選択されたＶＰＮデバイスの該ＭＡＣアドレスに置換する処理を含む方法。

【請求項３】
請求項１に記載の方法において、該生成するステップが
複数のＶＰＮデバイスクラスタのうちの各ＶＰＮデバイスクラスタに対して一義的ＭＡＣアドレスを割り当てる処理を含み、
該トラフィックを分配するステップが
該パケット宛先ＩＰアドレスに基づいて該ＶＰＮデバイスクラスタのうちの１つを選択する処理と
該選択されたＶＰＮデバイスクラスタの一義的なＭＡＣアドレスに宛てられたトラフィックの一義的なＭＡＣアドレスを、該選択されたＶＰＮデバイスクラスタのＭＡＣアドレスで置換する処理とを含む方法。
【請求項４】
請求項１に記載の方法において、該生成するステップが、さらに
異なる該論理的なＩＰアドレスを各ＶＰＮデバイスクラスタに割り当てる処理を含み、該トラフィックを分配するステップが
ＶＰＮクラスタを選択して、該トラフィックの宛先クラスタＩＰアドレスに基づいてトラフィックを転送する処理を含む方法。
【請求項５】
請求項１に記載の方法において、さらに
該ＶＰＮデバイスの動作の健全性を監視するステップと、
クラスタにおけるＶＰＮデバイスの故障の検出したことに応動して、該故障したＶＰＮデバイスに宛てられたトラフィックのＭＡＣ宛て先アドレスを同じ該クラスタにおける別のＶＰＮデバイスのＭＡＣアドレスに変更させるステップとを含む方法。
【請求項６】
請求項１に記載の方法において、該トラフィックを分配するステップが、さらに
あるＶＰＮユーザから別のＶＰＮユーザに対して市外トラフィックを分配するためのＶＰＮデバイスをクラスタ内に含まれる複数がＶＰＮデバイスの中から、該パケットＩＰ宛先アドレスおよびＶＰＮデバイスＭＡＣアドレスに基づいて選択して、クラスタを選択し、および該クラスタ内に含まれるＶＰＮデバイスの間の均衡をとるトラフィック負荷を実行する処理を含む方法。
【請求項７】
請求項１に記載の方法において、該トラフィックを分配するステップが、さらに
該クラスタ内に含まれる該複数のＶＰＮデバイスの中から、市外トラフィックをあるＶＰＮをユーザから別のＶＰＮユーザに対して分配するためのＶＰＮデバイスを選択して、いずれかの所与のＶＰＮユーザからユーザへの接続フローについて、該フローが動作したままである限り、同じＶＰＮデバイスがどの市外パケットに対しても用いられるようにする処理を含む方法。
【請求項８】
請求項１に記載の方法において、該トラフィックを分配するステップが、さらに
該クラスタ内に含まれる該複数のＶＰＮデバイスの中から、市外トラフィックをあるＶＰＮユーザから別のＶＰＮユーザに対して分配するためのＶＰＮデバイスを選択して、ＶＰＮユーザ間接続フロー転送について選択されているいずれか特定のＶＰＮデバイスの確立が同じになるようにする処理を含む方法。
【請求項９】
仮想プライベート網（ＶＰＮ）上のメッセージトラフィックをＶＰＮデバイスを介して第１の複数のユーザ（１１０）と第２の複数のユーザ（１３２）の間でルーティングするためのプロセッサ（１２０）上で実行するエンコーディングを含むコンピュータ読出し可能記憶媒体であって、
該エンコーディングは、各々が異なるメディア・アクセス・コントロール（ＭＡＣ）アドレスを有する複数のＶＰＮデバイス（１２６、１２８）を含むクラスタ（１２４）であって、該クラスタ内に含まれるＶＰＮデバイスの一義的なＩＰアドレスとは区別される論

理インターネット・プロトコル（ＩＰ）によってアドレスされるようになっているクラスタ（１２４）と、
パケット宛先ＩＰアドレスおよびＶＰＮデバイスＭＡＣアドレスの両方に基づいて該クラスタ内に含まれるＶＰＮデバイスの中から選択されるＶＰＮデバイスを介して該第１の複数のユーザと該第２の複数のユーザの間でトラフィックを分配するよう機能するトラフィック・ディストリビュータ（３００）と、を規定するようになっていることを特徴とするコンピュータ読出し可能記憶媒体。
【請求項１０】
請求項９に記載のコンピュータ読出し可能記憶媒体において
該エンコーディングが、
該クラスタ内に含まれるＶＰＮデバイス及びそれらのそれぞれの一義的なＭＡＣアドレスのリストと、
アクティブＶＰＮデバイスが故障したときに、その故障したＶＰＮデバイスにアドレスされたトラフィックのＭＡＣアドレスを同じ該クラスタ内の別のＶＰＮデバイスのＭＡＣアドレスに変更することにより、該クラスタの該アクティブＶＰＮデバイスから該クラスタの該別のＶＰＮデバイスに対してトラフィックを再指向させるよう機能する再指向ＶＰＮデバイスと、を規定するものであるコンピュータ読出し可能記憶媒体。
【請求項１１】
請求項１０に記載のコンピュータ読出し可能記憶媒体において、さらに
該クラスタに割り当てられた単一のＭＡＣアドレスと、
該トラフィックを送信するのに選択された該クラスタのいずれかのＶＰＮデバイスのＭＡＣアドレスで、該単一のＭＡＣアドレスに宛てられたトラフィックの該単一のＭＡＣアドレスを置換するよう機能するトラフィック・ディストリビュータを規定するエンコーティングとを含むコンピュータ読出し可能記憶媒体。
【請求項１２】
請求項１０に記載のコンピュータ読出し可能記憶媒体において、さらに
複数のクラスタの各クラスタに割り当てられた一義的なＭＡＣアドレスと、
パケット宛先ＩＰアドレスに基づいて該ＶＰＮデバイス・クラスタのうちの１つを選択するよう機能するトラフィック・ディストリビュータであって、該トラフィックを送信するために選択される選択されたクラスタのいずれかのＶＰＮデバイスのＭＡＣアドレスで、選択されたクラスタの該一義的なＭＡＣアドレスに宛られたトラフィックのＭＡＣアドレスを置換するよう機能するトラフィック・ディストリュビュータを規定するエンコーディングとを含むコンピュータ読出し可能記憶媒体。
【請求項１３】
請求項１０に記載のコンピュータ読出し可能記憶媒体において、さらに
該クラスタ内のＶＰＮデバイスの状態を決定し、および該クラスタ内の故障したＶＰＮデバイスに宛てられたトラフィックのＭＡＣ宛先アドレスを、該故障したＶＰＮデバイスの故障の検出に応答して同じ該クラスタ内の別のＶＰＮデバイスのＭＡＣアドレスで書き換えるよう機能する動作健全性プローブ・マネージャを規定するエンコーディングを含むコンピュータ読出し可能記憶媒体。
【発明の詳細な説明】
【０００１】
発明の背景
発明の技術分野
本発明は一般的にはコンピュータ網、より詳細には仮想プライベート網に係る。
【０００２】
関連技術の記載
コンピュータネットワーキングは、データ及びソフトウェアをこれら資源に対する共通の関心を有するユーザ間で共有するための広く普及したアプローチであり、今後も着実な発展が期待される。事実上、全ての企業、政府、その他の組織は、少なくても幾つかのコン

ピュータを有し、これらコンピュータは、個々のワークステーションが一つ或いは複数の共通のプロセッサ或いはサーバ資源を共有できるようにネットワーク化されている。単一のビル或いは比較的小さな地理的エリア内では、網コンピュータは、なんらかの形態のローカルエリア網（ＬＡＮ）を通じて接続することができる。

【０００３】

コンピュータとコンピュータ網間でより広い地理的エリアに渡って遠隔的にアクセスできる能力に対する需要はますます増加している。幾つかの支店を有する会社にとっては、これら支店間でコンピュータ資源を共有する能力を有することは必須である。ますます多くの社員が自宅で仕事を行うようになっていることや、会社の事務所から出張して働く社員もいることなどから、これら社員が会社のコンピュータ網に簡便に、しかも、データのアクセス及び転送に対する安全性が確保されるようなやり方にてアクセスできるようにする必要性が存在する。ある会社が他の会社と提携することもあり、この場合も、少なくとも幾つかのコンピュータ資源を共有することが必要となる。このような遠く離れたコンピュータを従来のアプローチを用いてネットワーク化することは、費用がかかり、困難で、場合によっては、不可能でさえある。

【０００４】

遠く離れたコンピュータを相互接続する問題に対する一つの解決策は、遠隔コンピューティングサイトを扱うために自社のみで使用する電気通信回線を所有或いはリースするやり方である。ワイドエリア網（Wide Area Network, ＷＡＮ）と呼ばれるこの技法は、回線をどの程度遠方までどの程度充実させて張るかによっては高価なものとなったり、或いは、これら電気通信回線は比較的使用が限られ、すなわち多くの容量が未使用となり、資源の浪費となることがある。加えて、ＷＡＮの確立、拡張、維持及び管理と関連して、かなりの組織上のオーバヘッドも存在する。

【０００５】

仮想プライベート網（virtual private network, ＶＰＮ）の概念が分散型コンピュータをより安価にかつ効率的にネットワーキングすることに対する必要性を満たすために開発された。仮想プライベート網は、公衆電気通信インフラストラクチャを活用するプライベートデータ網であり、タネリングプロトコル（tunneling protocol）及びセキュリティ手続き（security procedure）を使用することでプライバシーを維持する。ＶＰＮは、企業網を、遠方の事務所、家で仕事を行う社員、営業社員及びビジネスパートナへと延長する。ＶＰＮは、全世界的なＩＰネットワークサービスを、インターネットサービスプロバイダのバックボーンを含めて使用する。遠隔ユーザは、長距離料金にてダイヤリングする代りに、ローカルインターネット呼を掛けることができる。代替として、他のタイプの公衆網接続、例えば、フレームリレー（frame relay）を用いることもできる。

【０００６】

ＶＰＮシステムにとって重要な事項の一つは、データ或いはアプリケーションが許可されたユーザ間でのみ渡されるようなやり方にて公衆電気通信回線を「くぐり抜ける（tunnel）」ことができる能力である。トンネル（tunnels）は、仮想ポイント・ツウ・ポイント接続（virtual point-to-point connections）であり、トンネルのエンドポイント間に認証、暗号化、及びアクセス制御を提供する。トンネルは、様々なプロトコル層内に設けることができる。これは、「カプセル化（encapsulation）」、「タネリング（tunneling）」或いは「ＩＰタネリング（IP Tunneling）」とも呼ばれ、あるタイプのデータパケットを、通常はＴＣＰ／ＩＰとされる、別のプロトコルのパケット内に包み込む。ＶＰＮタネリングでは、カプセル化の前に、データが部外者には読めないようにパケットが暗号化される。カプセル化されたパケットは、インターネットを通じてそれらの意図される宛先へと送られ、宛先において分離（開封）され、元のフォーマットに戻される。認証技術（authentication technology）が、クライアントがサーバと接触する許可を有するか否かを確認するために採用される。

【０００７】

ＶＰＮは、ハードウェアに基づくことも、ソフトウェアに基づくこともできる。ハードウ

ェアに基づくシステムは、暗号化／復号及び認証などの必要とされるＶＰＮ機能を遂行する任意の数の、市販の或いは著作権を有する、ＶＰＮソフトウェアパッケージをランする専用のプロセッサから構成される。ハードウェアに基づくシステムは、特に、大きな企業に適する。これは、専用のＶＰＮプロセッサを用いることで、より厳重なセキュリティを確保でき、より多量のトラフィックを扱うことができるためである。より大きなＶＰＮユーザでは、さらに多くのトラフィックをより大きな速度、スケーラビリティ、冗長性及び信頼性にて処理するために、複数のＶＰＮデバイスを採用することもできる。

【０００８】

発明の概要

本発明は、仮想プライベート網（ＶＰＮ）の一方側の二つ或いはそれ以上のＶＰＮデバイスを、その網サイトの許可されたサーバ或いはユーザに接続するためのＶＰＮ網フロースイッチ及びこのための方法に係る。類似のクラスタリング構成がＶＰＮの他方側にも提供される。クラスタ化されたデバイスは、単一のＩＰアドレスを共有し、ＩＰアドレスの翻訳は要求されず、双方向クラスタリングを提供する。クラスタリングユニットは、ＩＳＯ層２及び３において透明的に動作することで、ＶＰＮデバイスのプラットホーム間クラスタリング（cross-platform clustering）を可能にする。これは、ある単一のクラスタ内のＶＰＮデバイスとして、いずれの製造業者のハードウェア或いはソフトウェアも用いることができることを意味する。

【０００９】

このＶＰＮデバイスクラスタリングシステムは、典型的には、一点の故障に起因して発生する問題を避けるための冗長として、複数のクラスタリングユニットを備える。例えば、２つのクラスタリングユニットが、作動・待機高アベイラビリティ構成（active-passive high-availability configuration）として用いられる。

【００１０】

このクラスタリングシステムは、出データパケットに関して、これらが送信ＶＰＮデバイスに送られる前に動作する。同様に、このクラスタリングシステムは、入りデータパケットに関して、ＶＰＮデバイスによる処理の後に動作する。こうして、このＶＰＮデバイスクラスタリングシステムは、ＶＰＮハードウェア及びソフトウェアとは独立なやり方にて動作する。このため、このクラスタリングシステムは、あらゆるＶＰＮハードウェア或いはソフトウェア構成と共に、ＶＰＮ認証、セキュリティ、或いは「タネリング（tunneling）」機能に影響を及ぼすことなく動作できる。

【００１１】

幾つかの実施例においては、ＶＰＮ網フロースイッチは、パケットのルーティングに加えて、負荷バランシング及びフォールトトレランス（fault tolerance）機能を遂行する。これら実施例においては、ＶＰＮ網フロースイッチのプロセッサは、定期的に負荷バランシングルーチンを遂行し、各ＶＰＮデバイスの相対作業負荷を決定する。ＶＰＮ網フロースイッチが、ＶＰＮデバイスのクラスタに向けられたパケットを受信すると、そのパケットは、作業負荷がＶＰＮデバイス間に等しく分配されるようなやり方にて、最適な作業負荷を有するＶＰＮデバイスに向けられる。加えて、あるＶＰＮデバイスの故障が検出されると、そのＶＰＮデバイスに向けられたパケットは、そのパケットのデータリンク層（ＭＡＣ）宛先アドレスを書き換えることで、別のＶＰＮデバイスに再ルーティングされる。このＶＰＮ網フロースイッチは、ＶＰＮデバイスの状態を絶えず監視しているために、あるＶＰＮデバイスが不能となった場合でも、ポイント・ツウ・ポイント通信に大きな時間遅延は導入されない。

【００１２】

クラスタのＩＰヘッダは修正されないために、本発明のＶＰＮ網フロースイッチは、どのようなＶＰＮプロトコルに従って符号化されたパケットに関しても動作できる。加えて、このＶＰＮ網フロースイッチは、暗号化されたパケットの再ルーティング、負荷バランシング及びフォールトトレランスを、ＶＰＮの両側のユーザには透明なやり方にて扱うことができる。

【００１３】
新規であると信じられる説明の実施例の特徴がより具体的にクレーム内に記載される。ただし、構造及び動作の方法の両方に係る本発明の幾つかの実施例は、以下の詳細な説明及び付録の図面を参照することで最も良く理解できるものである。
【００１４】
発明の詳細な説明
図１の略ブロック図は、二つ或いはそれ以上のＶＰＮデバイス、例えば、ＶＰＮデバイス１　１２６とＶＰＮデバイス２　１２８をインターネット１３０に、高‐アベイラビリティ、スケーラビリティ、及びトラフィック分配が完備されるような構成にて接続するＶＰＮデバイスクラスタリングシステム１００の一つの実施例を示す。詳細には示されないが、インターネット１３０の図１に詳細に示される構成要素の反対側にも類似の構成のＶＰＮデバイス、クラスタリングユニット、及びピア・ツウ・ピアデバイス１３２が配置される。この一例としてのＶＰＮデバイスクラスタリングシステム１００においては、網フローコントローラ１２０、すなわち、「ハイパフロー（hyperflow）」は、網フローコントローラ１２０を制御するための専用ソフトウェアを実行するためのプロセッサ（図示せず）及びメモリ（図示せず）を備える。網フローコントローラ１２０は、二つ或いはそれ以上のＶＰＮデバイス、例えば、ＶＰＮデバイス１　１２６及びＶＰＮデバイス２　１２８を、インターネット１３０を通じてＶＰＮ「トンネル（tunnel）」の他端に接続するために、一つのＶＰＮデバイスクラスタ１２４に構成する。網フローコントローラ１２０は、更に、ＶＰＮトンネルの一方の側に位置する支店サーバ及び他のクライアントデバイス１１２、１１４、１１６、１１８を、ＶＰＮトンネルの他方の端に配置される類似のピアデバイスとの安全な通信が確保されるようなやり方にて一つのクラスタ１１０に構成する。
【００１５】
ＶＰＮデバイスクラスタリングシステム１００は、一点の故障に起因して発生する問題を回避がするための冗長として、例えば、作動フローコントローラ１２０及び待機フローコントローラ１２２として動作する複数のクラスタリングユニット１２０、１２２を備える。作動網フローコントローラ１２０と待機フローコントローラ１２２は、作動・待機高アベイラビリティ構成（active-passive high-availability configuration）にて用いられる。
【００１６】
支店（或いはクライアント）Ａのクラスタ１１０から、インターネット１３０上の（１３２内に含まれる）支店（或いはクライアント）Ｂのクラスタデバイスに向けられる出トラフィックは、二つ或いはそれ以上のＶＰＮデバイス、例えば、ＶＰＮデバイス１　１２６とＶＰＮデバイス２　１２８の間に分配される。ＶＰＮデバイスクラスタリングシステム１００は、トラフィックをそのパケットの宛先クラスタＩＰアドレスに基づいて分配することで、全てのＩＰ－ベースのプロトコルをサポートする。各々の（クライアントＡ或いはクライアントＢの）クラスタ内の全てのＶＰＮデバイスに、単一のクラスタＩＰアドレスが割当てられる。
【００１７】
追加の帯域幅或いはより確実なフォールトトレランス（耐故障）を確保するために、クラスタ１２４に追加のＶＰＮデバイスをシームレスに追加することもできる。
網フローコントローラ１２０は、ＶＰＮデバイスクラスタを実現するために用いられるハードウェア及びソフトウェアとは独立に動作する。例えば、様々なＶＰＮデバイスが同一の接続性を有する限り、クラスタ１２４内にＶＰＮデバイスの様々な組合せを用いることができる。
【００１８】
ＶＰＮデバイスクラスタリングシステム１００は、作動網フローコントローラ１２０及び待機フローコントローラ１２２上で実行する複数の制御プロセスを備える。一つの制御プロセスは、ＶＰＮデバイスクラスタ１２４を形成或いは構成するＶＰＮデバイスクラスタクリエータ（VPN device cluster creator）である。

【００１９】
図２は、図１との関連で最も良く理解できるが、ＶＰＮデバイスクラスタクリエータのソフトウェアルーチン２００の動作を示す略流れ図である。ＶＰＮデバイスクラスタ１２４を形成するためには、クラスタＩＰ及びＶＰＮデバイス割当て動作（cluster IP and VPN device assignment operation）２１０において、管理者は、クラスタに論理インターネットプロトコルアドレス（logical Internet protocol address, ＩＰｖｐｎ）を割当て、ＶＰＮデバイスクラスタ１２４のメンバとなるべきＶＰＮデバイス、例えば、ＶＰＮデバイス１　１２６及びＶＰＮデバイス２　１２８を指定する。ＶＰＮデバイス健全性監視開始動作（begin monitoring VPN device health operation）２１２において、網フローコントローラ１２０は、ＶＰＮデバイス、例えば、ＶＰＮデバイス１　１２６及びＶＰＮデバイス２　１２８の健全性の監視を、典型的には、ある指定されたポーリング間隔にて行われる健全性チェック動作を用いて開始する。ＶＰＮデバイスクラスタアドレス構成動作（configure VPN device cluster address operation）２１４において、クライアントＡのデバイス１１０上で論理クラスタアドレスＩＰｖｐｎが構成される。

【００２０】
ＡＲＰリクエストに対する応答動作（respond to ARP request operation）２１６において、網フローコントローラ１２０はクライアントＡのデバイスクラスタ１１０内のサーバからのアドレス解決プロトコル（Address Resolution Protocol, ＡＲＰ）リクエストに応答して、ＶＰＮデバイスクラスタ１２４と関連する媒体アクセスコントロール（Media Access Control, ＭＡＣ）を識別する。ＭＡＣアドレスをＶＰＮデバイスクラスタ１２４と関連付けることで、クライアントＡのデバイス１１０が全ての出方向トラフィックを、インターネット１３０上の対応するＶＰＮデバイスクラスタに転送するために、ＶＰＮデバイスクラスタ１２４に送ることが確保される。

【００２１】
もう一つの制御プロセスは、インターネット１３０に向けられた出方向トラフィックを、ＶＰＮデバイス、例えば、ＶＰＮデバイス１　１２６及びＶＰＮデバイス２　１２８の間に分配するためのトラフィックディストリビュータである。図３は、図１との関連で最も良く理解できるが、トラフィックディストリビュータ３００の動作を示すの略流れ図である。トラフィックディストリビュータは、網フローコントローラ１２０から実行される。トラフィックディストリビュータ３００は、出トラフィックに対してＶＰＮデバイスを選択する動作（select VPN device for outbound traffic operation）３１０において、どのＶＰＮデバイスが出トラフィックを転送すべきかを、パケット宛先ＩＰアドレスに基づいて決定する。このパケット宛先ＩＰアドレスは、ＶＰＮ「トンネル（tunnel）」の受信端の対応するＶＰＮデバイスクラスタのクラスタＩＰアドレスであり得る。こうして宛先クラスタのＩＰアドレスを用いることで、ある特定のＶＰＮトンネル接続を指定するある与えられたフローに対して、同一のＶＰＮデバイスが、そのＶＰＮデバイスが動作を続けている限り、全ての出パケットに対して用いられることが確保される。フローが宛先クラスタＩＰアドレスに基づいて制御されるために、網フローコントローラ１２０による測定及び分析動作を低減することができる。これは、ＶＰＮデバイス上の負荷などのパラメータの測定が不要となるためである。こうして、ＶＰＮデバイスの負荷シェアリングは確率的或いは統計的に行われるが、この結果として負荷のバランスは若干悪くなる。この確率に基づく負荷管理は、ＶＰＮデバイスクラスタ１２４内の全てのＶＰＮデバイスが類似の転送能力を有することを想定する。

【００２２】
内部的には、作動中ＶＰＮデバイスのリストを維持する動作（maintain list of operational VPN devices operation）３１２において、トラフィックディストリビュータ３００は、作動中のＶＰＮデバイスのリストを維持する。パケットからのフィールドを用いてこのリストへのインデックスが計算され、作動中のＶＰＮデバイスが識別される。適当なＶＰＮデバイスクラスタにトラフィックを分配する動作（distribute traffic to appropriate VPN device cluster）３１４において、トラフィックが、クラスタに割当てられたＩ

Ｐアドレスに基づいて適当なピアＶＰＮクラスタに向けられる。

【００２３】

網フローコントローラ１２０は、トラフィックディストリビュータを識別するための特定のＭＡＣアドレスを有する。トラフィックディストリビュータは、置換の前はトラフィックディストリビュータのＭＡＣアドレスであったパケット宛先ＭＡＣアドレスを、そのフローを扱っているＶＰＮデバイスのＭＡＣアドレスと置換する。

【００２４】

各ＶＰＮデバイス、例えば、ＶＰＮデバイス１　１２６或いはＶＰＮデバイス２　１２８は、同一の確率にて出フローの転送のために割当てられる。これは、トラフィックディストリビュータは、ＶＰＮデバイス間の選択を行うために、パケットのＩＰヘッダ内の情報のみを用い、選択プロセスの部分としてＶＰＮデバイスの処理負荷或いは潜在的な処理能力は分析されないためである。

【００２５】

ＶＰＮデバイスクラスタ１２４は、網フローコントローラ１２０によってインターネット１３０から入来する入りトラフィックに対して遂行される処理には影響を与えない。任意のＶＰＮデバイスクラスタ１２４に向けられたトラフィックについては、変ることなく、ＶＰＮデバイスクラスタ１２４内に定義されるクライアントＡの作動中のサーバ及び他のデバイス間に分配される。入りトラフィックに対しては、最大でもたった一つのＶＰＮデバイスクラスタ１２４のみがサポートされる。

もう一つの制御プロセスは、ＶＰＮデバイスの「健全性（health）」を監視するためのＶＰＮデバイスモニタである。幾つかの実現においては、ＶＰＮデバイスクラスタリングシステム１００は、ＶＰＮデバイスの健全性を、所定のポーリング間隔及び健全性チェック方法を用いて監視する。健全性プローブは、ＶＰＮ間のフローの接続性を検証する。一つの実施例においては、網フローコントローラ１２０は、フローが正常に機能しているか確認するために、ＩＣＭＰエクステンションを用いて、定期的にピンパケット（Ping packet）をＶＰＮデバイス１　１２６に送る。ＶＰＮデバイス１　１２６は、ＶＰＮデバイスと網フローコントローラ１２０の個々のポートの間には一対一の対応が存在するために、同一ポート上で応答する。

【００２６】

幾つかの実現においては、ＶＰＮデバイスクラスタリングシステム１００は、絶えず、ＶＰＮデバイス及び関連するワイドエリア網（ＷＡＮ）リンクの動作の健全性を監視する。

【００２７】

幾つかの実現においては、ＶＰＮデバイスクラスタリングシステム１００は、様々な故障状態の一つ或いは複数を検出する。故障は、ＶＰＮデバイスとＬＡＮインタフェース及びリンクとの間で発生することも、ＶＰＮデバイス自身内で、停電、ソフトウェア障害、ハードウェア障害その他の原因で発生することもある。故障は、更に、ＶＰＮデバイスとＷＡＮインタフェース及びリンクとの間で発生することもある。ＶＰＮデバイスクラスタリングシステム１００が故障を検出すると、トラフィックは自動的に残りの作動中のＶＰＮデバイスに転送される。ＶＰＮデバイスクラスタリングシステムは、故障したＶＰＮデバイスをバイパスするために、クライアントＡのサーバの所での手作業による介入は必要としない。

【００２８】

図４の略ブロック図及び関連する遷移テーブルは、ＶＰＮデバイスクラスタリングシステムによってＶＰＮデバイス４１４を使用するように指定されたクライアントＡのデバイス４１０とクライアントＢのデバイス（図示せず）との間でパケットを転送するための技法を示す。出トラフィック４１６は、トラフィックディストリビュータのＭＡＣアドレスを指定する宛先ＭＡＣアドレスを有するが、ただし、この宛先ＩＰアドレスは、トラフィックディストリビュータも、トラフィックディストリビュータによってサポートされるクラスタも指定しない。ＶＰＮデバイスクラスタのトラフィックは、宛先ＶＰＮクラスタのＩＰアドレス以外には一意な属性は有さず、このため、宛先ＩＰアドレスを指定することで

、結果的に、現在のトラフィックディストリビュータは、単一のＶＰＮデバイスクラスタ４１８のみをサポートするように制限される。ＶＰＮデバイスクラスタリングシステム４００内には単一のＶＰＮデバイスクラスタ４１８しか含まれないが、ＶＰＮデバイスクラスタ４１８は、典型的には、ＶＰＮデバイス１　４１４及びＶＰＮデバイス２　４１５として示される複数のＶＰＮデバイスを備える。

【００２９】

単一のＶＰＮデバイスクラスタ４１８のみに制限することで、結果的にＶＰＮデバイスクラスタリングシステム４００は、ルーティング機能を遂行するための単一のクラスタのみを有することとなる。

【００３０】

ＶＰＮデバイスクラスタリングシステムの他の実現として、複数のＭＡＣアドレスをサポートし、追加のＶＰＮデバイスクラスタをサポートすることもできる。

ＶＰＮデバイスクラスタ４１８のクラスタＩＰアドレスはパケット内には現れない。これはＶＰＮデバイスクラスタ４１８が、実際のエンド宛先への経路上の唯一のゲートウェイであるためである。

【００３１】

網フローコントローラ４２０は、ＶＰＮプローブ法（ＡＲＰ　ｐｒｏｂｅ　ｍｅｔｈｏｄｓ）を用いて、ＶＰＮデバイスクラスタ４１８内のＶＰＮデバイスを監視する。網フローコントローラ４２０内で実行しているソフトウェアは、アドレス解決プロトコル（ＡＲＰ）を用いて、未使用のＩＰアドレスを探す。あるＶＰＮデバイスがＡＲＰプローブに応答した場合は、ソフトウェアは、次のＩＰアドレスを試みる。あるＡＲＰプローブからの応答が数回試みてもない場合は、ソフトウェアは、そのアドレスをそのＶＰＮデバイスのＩＰアドレスとして使用する。

【００３２】

図５の流れ図はトラフィック分配方法５００を示す。宛先ＩＰアドレスをチェックする動作（check destination IP address operation）５１０において、トラフィックディストリビュータは、パケットの宛先ＩＰアドレスをチェックすることで、宛先ＩＰアドレスがクラスタアドレスであるか否か決定する。

【００３３】

宛先ＩＰアドレスをチェックする動作５１０において、宛先ＩＰアドレスがクラスタアドレスではないことが決定された場合は、次に、宛先ＭＡＣアドレスをテストする動作（test destination MAC address operation）５１２において、トラフィックディストリビュータは、宛先ＭＡＣアドレスがクラスタアドレスであるか否か決定する。宛先ＭＡＣアドレスはクラスタアドレスと、プロキシＡＲＰ（Proxy ARP）を用いて、接続されているＶＰＮデバイスに対して、構成されているＩＰアドレスのいずれかにパケットを送るときは網フローコントローラのＭＡＣアドレスを使用すべきことが示されたときは一致する。

【００３４】

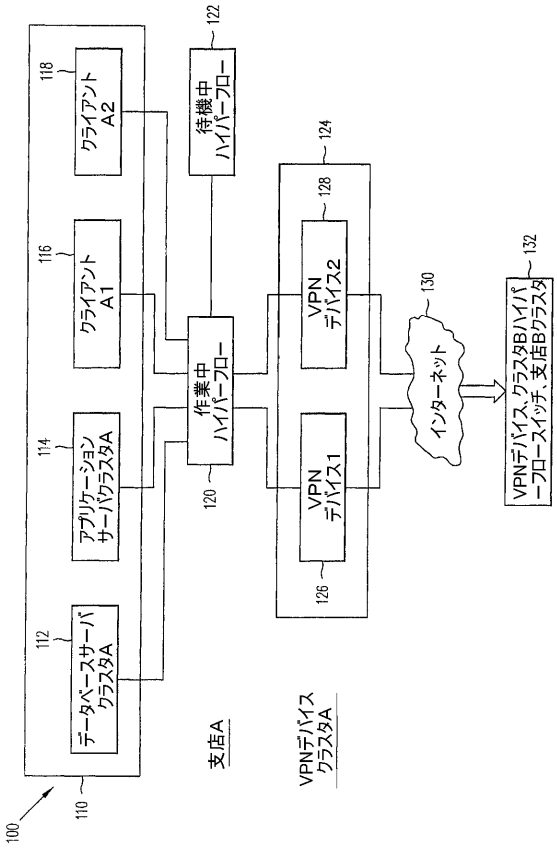
宛先ＭＡＣアドレスをテストする動作５１２において、そのＭＡＣアドレスがクラスタアドレスではないことが決定された場合は、次に、ＶＰＮの健全性をテストする動作（VPN health test operation）５１４において、トラフィックディストリビュータは、クラスタ内のＶＰＮデバイスに関して性能テストを遂行する。

【００３５】

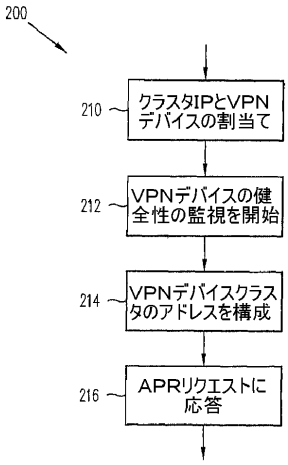
第一の再ダイレクション動作（redirection operation）は、ＶＰＮデバイスのクラスタ識別子を設定する動作（set VPN device cluster identifier operation）５１６から成るが、この動作において、ＭＡＣアドレス或いは宛先ＩＰアドレスのいずれかの形態でのクラスタアドレスが、クラスタデータ構造を識別するために設定される。次に、バケットをチェックする動作（bucket check operation）５１８は、クラスタデータ構造内に少なくとも１つのバケットが存在するか否かを決定する。存在しない場合は、バケットを作成する動作（create bucket operation）５２０において、１つのバケットが作成される。次に、負荷バランシング動作（load balancing operation）５２２において、負荷バラン

シングを達成できる適当なバケットが検索される。
【００３６】
フローテスト動作（flow test operation）５２４において、フローがバケットに割当てられているか否か決定され、割当てられてない場合は、フローを割当てる動作（flow assignment operation）５２６を遂行することで、バケットがサーバに割当てられる。次に、トラフィックディストリビュータは、パケットを割当てられたＶＰＮデバイスクラスタメンバに転送する動作（forward packet to assigned VPN device cluster member）５３２を、バケットを用いてクライアントＡからのデータリクエストをクライアントＢに転送することで実行する。
【００３７】
トラフィック分配及び負荷バランシングシステムの更なる詳細については、「Router Clustering for Multiple Network Service（マルチネットワークサービスに対するルータクラスタリング）」なる名称の同時係属出願第０９／５４０，２９６号において開示及び請求されているのでこれを参照されたい。
【００３８】
本発明が様々な実施例との関連で説明されたが、これら実施例は単に例示に過ぎず、本発明の範囲はこれらに制限されない。ここに説明された実施例に対する多くの変形、修正、追加及び改善が可能である。例えば、当業者においてはここに開示された構造及び方法を達成するために必要とされる様々な措置（ステップ）を容易に講ずることができるものである。加えて、説明のプロセスパラメータ、材料、及び寸法も単に一例として与えられたものであり、これらを変更しても所望の構造並びに修正物を容易に達成でき、これらも本発明の範囲に入るものと解される。上の詳細な説明からここに開示された実施例の様々な変形及び修正が明白であり、これらもクレームに記述される本発明の精神及び範囲から逸脱するものではない。
クレーム中、特に改めて記載されてない限り、不定冠詞「ａ」は「一つを指すことも複数を指すことも」ある。
【図面の簡単な説明】
【図１】　仮想プライベート網の一方の二つ或いはそれ以上のＶＰＮデバイスを、仮想プライベート網の他方の類似のＶＰＮデバイスクラスタリングシステムに接続するためのＶＰＮデバイスクラスタリングシステムの一つの実施例を示す略ブロック図である。
【図２】　ＶＰＮデバイスクラスタクリエータの動作を示す略流れ図である。
【図３】　トラフィックディストリビュータの動作を示す略流れ図である。
【図４】　ＶＰＮデバイスクラスタリングシステムを用いて２人の許可されたユーザ間でパケットを転送するための技法を示す略ブロック図及び関連する遷移テーブルである。
【図５】　トラフィック分配方法の更なる実現を示す流れ図である。
【符号の説明】
１００　ＶＰＮデバイスクラスタリングシステム
１２０　作動中網フローコントローラ
１２２　待機中網フローコントローラ
１１２、１１４、１１６、１１８　支店サーバ及び他のクライアントデバイス
１２６　ＶＰＮデバイス１
１２８　ＶＰＮデバイス２
１３０　インターネット
１３２　ピア・ツウ・ピアデバイス

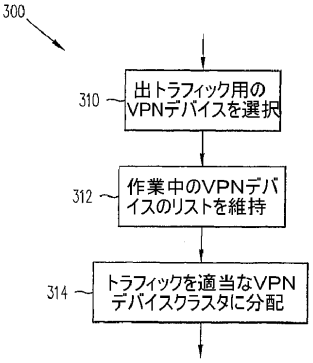
【図１】


100
110
支店A
VPNデバイス
クラスタA
データベースサーバ
クラスタA
112
アプリケーション
サーバクラスタA
114
クライアント
A1
116
クライアント
A2
118
作業中
ハイパーフロー
120
待機中
ハイパーフロー
122
VPN
デバイス1
126
VPN
デバイス2
128
124
インターネット
130
VPNデバイス、クラスタBハイパーフロースイッチ、支店Bクラスタ
132

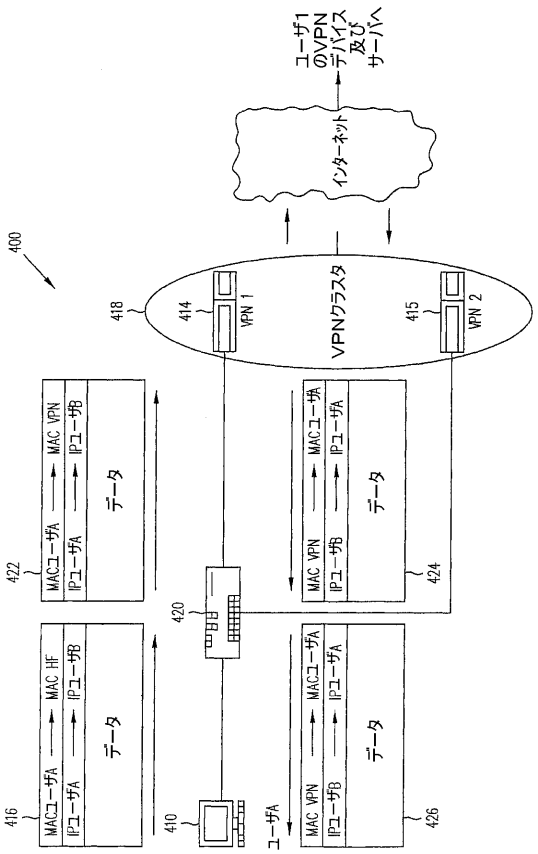
【図２】


200
クラスタIPとVPN
デバイスの割当て
210
VPNデバイスの健
全性の監視を開始
212
VPNデバイスクラス
タのアドレスを構成
214
APRリクエストに
応答
216

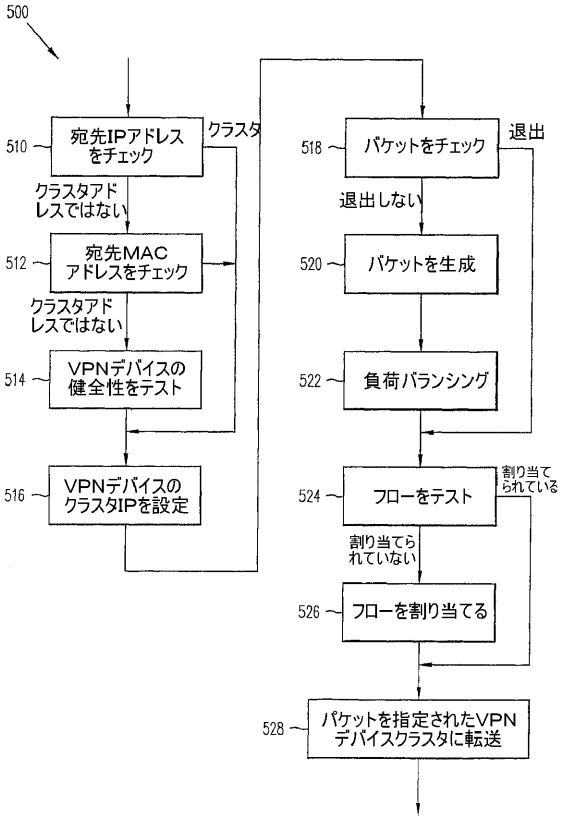
【図３】


300
出トラフィック用の
VPNデバイスを選択
310
作業中のVPNデバ
イスのリストを維持
312
トラフィックを適当なVPN
デバイスクラスタに分配
314

【図４】


400
ユーザ1
のVPN
デバイス
及び
サーバへ
インターネット
VPNクラスタ
418
414
VPN 1
415
VPN 2
422
MACユーザA
IPユーザA
MAC VPN
IPユーザB
データ
420
424
416
MAC HF
410
ユーザA
426

【図５】


500
宛先IPアドレス
をチェック
510
クラスタ
クラスタアド
レスではない
宛先MAC
アドレスをチェック
512
クラスタアド
レスではない
VPNデバイスの
健全性をテスト
514
VPNデバイスの
クラスタIPを設定
516
パケットをチェック
518
退出
退出しない
パケットを生成
520
負荷バランシング
522
フローをテスト
524
割り当て
られている
割り当てら
れていない
フローを割り当てる
526
パケットを指定されたVPN
デバイスクラスタに転送
528

フロントページの続き

(72)発明者 ボンマレディ，サティッシュ
アメリカ合衆国 ９５１２３ カルフォルニア，サン ジョゼ，コマンチェ ドライヴ ５８４３
(72)発明者 ケール，マカランド
アメリカ合衆国 ９４０８９ カルフォルニア，サニーヴェイル，ナンバー６１，ワイルドウッド アヴェニュー １２３５
(72)発明者 シャガンティ，スリニヴァス
アメリカ合衆国 ９５１３８ カルフォルニア，サン ジョゼ，ベリントン コート ２１８０

合議体
審判長 竹井 文雄
審判官 土居 仁士
審判官 萩原 義則

(56)参考文献 特開平８－８９７５（ＪＰ，Ａ）
セキュリティ大全，ＩＮＴＥＲＯＰ ＭＡＧＡＺＩＮＥ，第9巻，第１０号，ソフトバンクパブリッシング株式会社，第３３－４２頁，１９９９年１２月1日
小浅章，「サーバ負荷分散ツールの使い方アドバイス２「ＨＹＰＥＲＦＬＯＷ」」，コンピュータ&ネットワークＬＡＮ，第１６巻，第8号，株式会社オーム社，第１２－１８頁，１９９８年８月1日

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L12/46-12/66