

(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2008-236212

(P2008-236212A)

(43) 公開日 平成20年10月2日(2008.10.2)

(51) Int.Cl. F I テーマコード(参考)
 H O 4 L 12/56 (2006.01) H O 4 L 12/56 1 O O Z 5 K O 3 O
 H O 4 L 12/56 H

審査請求 未請求 請求項の数 7 O L (全 25 頁)

(21) 出願番号 特願2007-71145 (P2007-71145)
 (22) 出願日 平成19年3月19日(2007.3.19)

(71) 出願人 000005223
 富士通株式会社
 神奈川県川崎市中原区上小田中4丁目1番1号
 (74) 代理人 100090516
 弁理士 松倉 秀実
 (74) 代理人 100113608
 弁理士 平川 明
 (74) 代理人 100105407
 弁理士 高田 大輔
 (74) 代理人 100089244
 弁理士 遠山 勉
 (72) 発明者 官部 正剛
 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

最終頁に続く

(54) 【発明の名称】 V P N 装置

(57) 【要約】

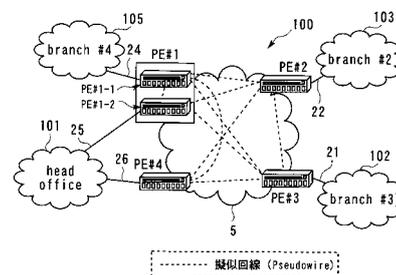
【課題】冗長化された拠点に係るV P Nを通じたループの発生を防止する。

【解決手段】第1拠点105のアクセス回線24及び第2拠点101の二つのアクセス回線の一つ25が接続されるV P N装置(PE#1)であって、アクセス回線24が接続され、第1拠点105を

含む二つの拠点間で送受信すべきフレーム用の第1フォワーディングテーブル38Aに従っ

てフレーム転送を行う第1仮想V P N装置(PE#1-1)と、アクセス回線25が接続され、第2拠点101を含む二つの拠点間で送受信すべきフレーム用の第2フォワーディングテーブル38Bに従ってフレーム転送を行う第2仮想V P N装置(PE#1-2)であって、上記二つのアクセス回線の他方26が接続された他のV P N装置(PE#4)へのフレーム転送を行わない設定を有する第2仮想V P N装置とを含む。

【選択図】 図 1 3



本発明に係るV P L Sシステムにおいて、仮想P Eを有するP Eが一つの場合

【特許請求の範囲】**【請求項 1】**

単一のアクセス回線を夫々有する複数の第 1 の拠点、及び少なくとも二つのアクセス回線を有する第 2 の拠点を含む複数の拠点間を相互に結ぶ仮想プライベート網(VPN)サービスを提供するための複数の VPN 装置を備える VPN システムにおいて、前記複数の第 1 の拠点の 1 つが有する単一のアクセス回線、及び前記第 2 の拠点が有する少なくとも二つのアクセス回線の一方が接続される VPN 装置であって、

前記複数の第 1 の拠点の 1 つが有する単一のアクセス回線が接続され、前記第 1 の拠点を含む少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第 1 のフォワーディングテーブルに従ってフレーム転送処理を行う第 1 の仮想 VPN 装置と、

10

前記第 2 の拠点が有する少なくとも二つのアクセス回線の一方が接続され、前記第 2 の拠点を含む少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第 2 のフォワーディングテーブルに従ってフレーム転送処理を行う第 2 の仮想 VPN 装置であって、前記少なくとも二つのアクセス回線の他方が接続された他の VPN 装置へのフレーム転送を行わない設定を有する第 2 の仮想 VPN 装置とを含む VPN 装置。

【請求項 2】

前記第 1 の仮想 VPN 装置は、他の VPN 装置の総てと擬似回線を介してフルメッシュ状に接続されており、

前記第 2 の仮想 VPN 装置は、前記少なくとも二つのアクセス回線の他方が接続された他の VPN 装置を除く他の VPN 装置の総てと擬似回線を介してフルメッシュ状に接続されており、

20

前記第 1 の仮想 VPN 装置と前記第 2 の仮想 VPN 装置とは擬似回線を介して接続されており、

前記第 1 及び第 2 の仮想 VPN 装置の夫々は、対応するアクセス回線から受信されたフレームを他のアクセス回線及び擬似回線へ転送することを許容されており、且つ擬似回線から受信されたフレームを他の擬似回線を除くアクセス回線に転送することを許容されている

請求項 1 記載の VPN 装置。

【請求項 3】

30

前記少なくとも二つのアクセス回線の他方が接続された他の VPN 装置が、前記複数の第 1 の拠点の 1 つと異なる第 1 の拠点が有する単一のアクセス回線が接続され、前記第 2 の拠点を含まない少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第 1 のフォワーディングテーブルに従ってフレーム転送処理を行う第 3 の仮想 VPN 装置、及び前記第 2 の拠点が有する少なくとも二つのアクセス回線の他方が接続され、前記第 2 の拠点を含む少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第 2 のフォワーディングテーブルに従ってフレーム転送処理を行う第 4 の仮想 VPN 装置を含む場合には、前記第 2 の仮想 VPN 装置は、前記第 4 の仮想 VPN 装置へのフレーム転送を行わず、且つ前記第 4 の仮想 VPN 装置からフレームを受信しない構成となっている

請求項 1 記載の VPN 装置。

40

【請求項 4】

前記第 1 の仮想 VPN 装置は、前記第 3 及び第 4 の仮想 VPN 装置、及び前記他の VPN 装置を除く残りの他の VPN 装置の総てと擬似回線を介してフルメッシュ状に接続されており、

前記第 2 の仮想 VPN 装置は、前記第 4 の仮想 VPN 装置、及び前記第 4 の仮想 VPN 装置を含む他の VPN 装置を除く残りの他の VPN 装置の総てと擬似回線を介してフルメッシュ状に接続されており、

前記第 1 の仮想 VPN 装置と前記第 2 の仮想 VPN 装置とは擬似回線を介して接続されており、

前記第 1 の仮想 VPN 装置及び第 2 の仮想 VPN 装置の夫々は、対応するアクセス回線

50

から受信されたフレームを他のアクセス回線及び擬似回線へ転送することを許容されており、且つ擬似回線から受信されたフレームを他の擬似回線を除くアクセス回線に転送することを許容されている

請求項 3 に記載の V P N 装置。

【請求項 5】

単一のアクセス回線を夫々有する複数の第 1 の拠点と、少なくとも二つのアクセス回線を有する第 2 の拠点とを含む複数の拠点間を結ぶ仮想プライベート網(V P N)サービスを提供するための複数の V P N 装置を備える V P N システムにおいて、前記第 2 の拠点が有する少なくとも二つのアクセス回線の一方が接続される V P N 装置であって、

フレーム送信元からフレームを受信するための二つの擬似回線を収容し、二つの擬似回線ではほぼ同時に同一のフレームが受信された場合に、これらのフレームがフレーム送信元でのフラッディングによって到着したフラッディングフレームであることを検出する検出部と、

前記第 2 の拠点を含む少なくとも二つの拠点間で送受信すべきフレーム転送処理用のフォーワーディングテーブルに従ってフラッディングフレームの転送先を決定するフォーワーディング部と、

決定されたフラッディングフレームの転送先が前記少なくとも二つのアクセス回線の一方を含む場合に、該フラッディングフレームを所定のフィルタ条件に従って廃棄するフィルタ部であって、前記少なくとも二つのアクセス回線の他方が接続された他の V P N 装置から前記第 2 の拠点へ当該フラッディングフレームと同一のフレームが転送される場合に、当該フラッディングフレームを廃棄するフィルタ部とを含む V P N 装置。

【請求項 6】

前記少なくとも二つのアクセス回線の他方の状態を示すアクセス回線状態メッセージを受信する受信部と、

前記受信部で前記少なくとも二つのアクセス回線の他方の異常を示すアクセス回線状態メッセージが受信された場合に、前記フィルタ部に設定されているフィルタ条件を変更するフィルタ制御部と

をさらに含む請求項 5 記載の V P N 装置。

【請求項 7】

前記フィルタ制御部は、周期的に受信すべきアクセス回線状態メッセージが所定時間前記受信部で受信されなかった場合に、前記他の V P N 装置に異常が発生したと判断して、前記フィルタ条件の変更を行う

請求項 6 記載の V P N 装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、複数の拠点を有する顧客に V P N サービスを提供するための通信装置(V P N 装置)に関し、例えば、V P L S (Virtual Private LAN Service)を用いて、Ethernet (登録商標) LAN サービスを提供する V P N 装置に関する。

【背景技術】

【0002】

例えば、Ethernet (登録商標) L A N サービス(以下、“E - L A N”サービス)を提供する通信装置において、収容拠点を冗長化する技術としては E S R P (登録商標) (Extreme Standby Router Protocol (登録商標))がよく知られている。E S R P (登録商標)とは、Externe Networks社によって開発されたEthernet (登録商標) / I P レイヤの冗長化技術である。

【0003】

図 1 に E S R P (登録商標)の動作概要を示す。図 1 に示す例では、顧客ネットワーク(customer Ethernet (登録商標) network) 1 は、2 台のプロバイダエッジスイッチ(以

10

20

30

40

50

下、“PE”と表記)2及び3に2つのアクセス回線(access line)A1, A2を介して収容されている。各PE2及び3は、プロバイダネットワーク(provider Ethernet(登録商標)network)4に接続されている。図1では、PE2がアクティブ(active)になっており、PE3がスタンバイ(standby)になっている。

【0004】

PE2及び3の間でESRP(登録商標)が実行される。ESRP(登録商標)を実行しているPE及び3の間では、ESRP(登録商標)helloと呼ばれる特殊なEthernet(登録商標)フレーム(以下“helloフレーム”と称する)がやりとりされる。各PE2及び3は、helloフレーム中の設定情報や障害情報などを元に、PEの状態(アクティブとスタンバイとの一方)を認識する。

10

【0005】

アクティブ状態のPE2は、スタンバイ状態のPE3とhelloフレームのメッセージ交換を行うことを除き、通常のEthernet(登録商標)スイッチ(以下、“E-スイッチ”と表記)として動作する。これにより、顧客ネットワーク1とプロバイダネットワーク4との間でPE2を通じて通信を行うことができる(図1の顧客トラフィック(customer traffic)参照)。

【0006】

一方、スタンバイ状態のPE3は、アクティブ状態のPE2とhelloフレームのメッセージ交換を行うことを除き、PE3自身に入力されるEthernet(登録商標)フレーム(以下、“E-フレーム”と称する)を廃棄する(図1のブロック(block)参照)。これによって、E-フレームのループが防止される。

20

【0007】

図2に示すように、アクティブ状態を有するPE2に障害が発生すると、スタンバイ状態を有するPE3は、helloフレームを通じてこの障害を認識し、自らの状態をスタンバイからアクティブに変更し、E-フレームのブロックを解除する。これによって、ユーザトラフィック(customer traffic)が新たにアクティブ状態になったPE3を通過する状態となる。

【0008】

E-LANサービスを提供する方法として、VPLSと呼ばれる技術が、IETF(Internet Engineering Task Force)を中心に議論されている。現在、“draft-ietf-l2vpn-vpls-ldp-09.txt”や“draft-ietf-l2vpn-vpls-bgp-08.txt”のようなインターネットドラフトが発行されており、VPLSの標準化が進められている。

30

【0009】

図3にVPLSの動作を示す。VPLSは、VPLS網として機能するプロバイダのMPLS(Multi-Protocol Label Switching)網の上にユーザ(顧客)のEthernet(登録商標)VPN(Virtual Private Network)(以下、“E-VPN”と表記)を構築する。顧客は複数の拠点(この例では、customer head office及びcustomer branch)を有し、各拠点はアクセス回線(access line)によってPEに収容される。

【0010】

図3に示す例では、プロバイダMPLS網(プロバイダ網)5に、PE6, PE7及びPE8が接続されている。PE6は、3つの顧客拠点(ヘッドオフィス, ブランチ#3及び#4)の夫々を、個別のアクセス回線Aを介して収容している。PE7は、拠点(ブランチ#2)をアクセス回線Aを介して収容している。PE8は、拠点(ブランチ#1)をアクセス回線Aを介して収容している。

40

【0011】

PE6~8は、Pseudowireと呼ばれる擬似回線でフルメッシュ状に接続されている。Pseudowireとは、パケット網上でEthernet(登録商標)、ATM(非同期転送モード)、FR(フレームリレー)などの回線をエミュレートする技術である。PseudowireもIETFで標準化が進められており、RFC3985などにおいて説明されている。本明細書におけるPseudowireは、MPLS網上でE-回線をエミュレートするような擬似回線を指す。以下

50

、Pseudowireを「擬似回線」と表記する。

【0012】

図3に示す各PE6～8は、アクセス回線Aあるいは擬似回線PWから受信したE-フレームを、通常のE-スイッチと同様の処理によりフォワーディングする。但し、擬似回線PWから受信したE-フレームは、擬似回線PWに対してフォワーディング又はフラッディングを行わない。この点が、唯一通常のE-スイッチとは異なる。これは、“split horizon (スプリットホライゾン)”と呼ばれている。

【0013】

図3を用いてスプリットホライゾンを説明する。例えば、PE7は、ブランチ#2から受信されるE-フレームについて、PE6及び/又はPE8へのフォワーディングを許容する。これに対し、PE7は、PE6から受信されるE-フレームについて、ブランチ#2へのフォワーディングを許容するが、PE8へのフォワーディングは許容しない(フォワーディングを行わない)。さらに、PE7は、PE8から受信されるE-フレームについて、ブランチ#2へのフォワーディングを許容するが、PE6へのフォワーディングを行わない。このようなスプリットホライゾンによって、プロバイダ網5内のE-フレームのループが防止される。

【非特許文献1】“コンフィギュレーションガイド ESRP(登録商標)”, [2006年11月15日検索]、インターネット URL: <http://www.extremenetworks.co.jp/technology/configure#guide/ESRP/index.htm>

【非特許文献2】"Virtual Private LAN Service (VPLS) Using BGP for Auto-discovery and Signaling", Network Working Group, Internet-Draft, K. Kompella, Ed., Y. Rekhter, Ed., Juniper Networks, June 21, 2006, "draft-ietf-l2vpn-vpls-bgp-08.txt"

【非特許文献3】"Virtual Private LAN Services Using LDP", Internet Draft Document, L2VPN Working Group, Marc Lasserre, Vach Kompella (Editors), June 2006, "draft-ietf-l2vpn-vpls-ldp-09.txt"

【発明の開示】

【発明が解決しようとする課題】

【0014】

ESRP(登録商標)では、冗長化されたPEのうちの一つだけがアクティブ状態になることによって、E-フレームのループが防止される。このため、例えば、2本のアクセス回線を用いて2つのPEで1つのユーザ拠点を収容した場合でも、ユーザトラフィックは、常にアクティブ状態のPEだけに流れる。スタンバイ状態のPEに繋がっている側のアクセス回線の帯域は、そのPEの状態がアクティブになるまで使われない。このため、2つのアクセス回線に関する帯域は、その半分しか常に使われない。

【0015】

また、VPLSでは、ESRP(登録商標)のように2つのアクセス回線の片方をスタンバイとしない方法で一つのユーザ拠点を複数のPEに収容した場合、以下の二つの問題が発生する。

【0016】

一つ目の問題は、E-フレームのループの発生である。図4は、E-フレームのループの様子を示している。顧客(ユーザ)が、ヘッドオフィスとE-VPNとの接続に対して耐障害性を向上させるため、2本のアクセス回線A1及びA2を用いてヘッドオフィスを冗長化しようとした場合を考える。図4において、E-VPNは、顧客拠点をそれぞれ収容する複数のPE#1～#4を有するプロバイダMPLS網5で構成される。

【0017】

この場合、図4に示すように、ヘッドオフィスとE-VPNとの間でループが発生する。すなわち、ヘッドオフィスからPE#4へ送信したE-フレームは、PE#4から擬似回線PWを通じてPE#1へフォワーディングされる。このとき、PE#1とヘッドオフィスとを結ぶアクセス回線は擬似回線ではないので、PE#1は、E-フレームのヘッドオフィスへのフォワーディングを許容する。この結果、E-フレームがヘッドオフィスに

10

20

30

40

50

戻ってしまう。ヘッドオフィスからPE#1へE-フレームを送信した場合にも、PE#1及びPE#4を介してE-フレームがヘッドオフィスに戻ってしまう。このようなループは、プロバイダ網5内でのループと異なり、擬似回線から擬似回線へのフォワーディングを禁止するスプリットホライゾンでは解消されない。

【0018】

二つ目の問題は、他の拠点からのE-フレームが二重に到着する可能性があることである。E-フレームの二重到着の様子を図5に示す。図5では、図4に示したネットワーク構成において、複数の拠点の一つであるブランチ#1内の端末(図示せず)がヘッドオフィス内の端末(図示せず)に向けてE-フレームを送信した場合を示している。

【0019】

さらに、図5では、E-VPNが、E-フレームの宛先ノード(ヘッドオフィス内の端末)に関してフォワーディング先をまだ学習していない場合を想定している。PE#3で受信されたヘッドオフィス向けのE-フレームの宛先がまだ学習されていない場合には、PE#3は、全ての擬似回線(図5中のPW1, PW2及びPW3)に対してフラッディングを行う。これによって、PE#1とPE#4は、E-フレームを受信する。すると、PE#1は、ヘッドオフィスを含む総てのアクセス回線A1及びA3に向けてフラッディングを行う。一方、PE#4は、アクセス回線A2及びA4に向けてフラッディングを行う。従って、ヘッドオフィスは、ブランチ#1から送出されたE-フレームをアクセス回線A1及びA2を通じて二重に受信してしまう。

【0020】

本発明の目的は、複数のアクセス回線を有する拠点に関してVPNを介したループが発生することを防止することができる技術を提供することである。

【0021】

また、本発明の他の目的は、複数のアクセス回線を介してVPNに収容される特定の拠点へ同一のフレームが重複して到着することを防止することができる技術を提供することである。

【課題を解決するための手段】

【0022】

本発明は、上記した目的を達成するために以下の手段を採用する。

【0023】

即ち、本発明の第1の態様は、単一のアクセス回線を夫々有する複数の第1の拠点、及び少なくとも二つのアクセス回線を有する第2の拠点を含む複数の拠点間を相互に結ぶ仮想プライベート網(VPN)サービスを提供するための複数のVPN装置を備えるVPNシステムにおいて、前記複数の第1の拠点の1つが有する単一のアクセス回線、及び前記第2の拠点が有する少なくとも二つのアクセス回線の一方が接続されるVPN装置であって、

前記複数の第1の拠点の1つが有する単一のアクセス回線が接続され、前記第1の拠点を含む少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第1のフォワーディングテーブルに従ってフレーム転送処理を行う第1の仮想VPN装置と、

前記第2の拠点が有する少なくとも二つのアクセス回線の一方が接続され、前記第2の拠点を含む少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第2のフォワーディングテーブルに従ってフレーム転送処理を行う第2の仮想VPN装置であって、前記少なくとも二つのアクセス回線の他方が接続された他のVPN装置へのフレーム転送を行わない設定を有する第2の仮想VPN装置とを含むVPN装置である。

【0024】

本発明の第1の態様によれば、第2の拠点が有する少なくとも二つのアクセス回線の一方が接続された第2の仮想VPN装置が、第2の拠点用の第2のフォワーディングテーブルに従ってフレーム転送処理を行う。このとき、第2の仮想VPN装置は、第2の拠点が有する少なくとも二つのアクセス回線の他方を収容する他のVPN装置へフレーム転送を

10

20

30

40

50

行わない。これによって、第2の拠点から第2の仮想VPN装置が受信したフレームが他のVPN装置を経由して第2の拠点に戻ることを(ループ)を防止することができる。

【0025】

この場合、第2の仮想VPN装置が上記他のVPN装置からのフレームを受信しないように構成することも可能である。この場合、他のVPN装置が第2の拠点から受信したフレームが第2の仮想VPN装置を経由して第2の拠点に戻ることを(ループ)を防止することができる。

【0026】

また、本発明の第1の態様では、上述した手段でループの発生が防止されるため、第2の拠点が有する二つのアクセス回線を並列に使用することができる。これによって、二つのアクセス回線の帯域が無駄になるのを防止できる。

10

【0027】

好ましくは、本発明の第1の態様は、前記第1の仮想VPN装置は、他のVPN装置の総てと擬似回線を介してフルメッシュ状に接続されており、

前記第2の仮想VPN装置は、前記少なくとも二つのアクセス回線の他方が接続された他のVPN装置を除く他のVPN装置の総てと擬似回線を介してフルメッシュ状に接続されており、

前記第1の仮想VPN装置と前記第2の仮想VPN装置とは擬似回線を介して接続されており、

前記第1及び第2の仮想VPN装置の夫々は、対応するアクセス回線から受信されたフレームを他のアクセス回線及び擬似回線へ転送することを許容されており、且つ擬似回線から受信されたフレームを他の擬似回線を除くアクセス回線に転送することを許容されている、ように構成することができる。

20

【0028】

また、好ましくは、本発明の第1の態様は、前記少なくとも二つのアクセス回線の他方が接続された他のVPN装置が、前記複数の第1の拠点の1つと異なる第1の拠点が有する単一のアクセス回線が接続され、前記第2の拠点を含まない少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第1のフォワーディングテーブルに従ってフレーム転送処理を行う第3の仮想VPN装置、及び前記第2の拠点が有する少なくとも二つのアクセス回線の他方が接続され、前記第2の拠点を含む少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第2のフォワーディングテーブルに従ってフレーム転送処理を行う第4の仮想VPN装置を含む場合には、前記第2の仮想VPN装置は、前記第4の仮想VPN装置へのフレーム転送を行わず、且つ前記第4の仮想VPN装置からフレームを受信しない構成となっている。

30

【0029】

また、好ましくは、本発明の第1の態様は、前記第1の仮想VPN装置は、前記第3及び第4の仮想VPN装置、及び前記他のVPN装置を除く残りの他のVPN装置の総てと擬似回線を介してフルメッシュ状に接続されており、

前記第2の仮想VPN装置は、前記第4の仮想VPN装置、及び前記第4の仮想VPN装置を含む他のVPN装置を除く残りの他のVPN装置の総てと擬似回線を介してフルメッシュ状に接続されており、

40

前記第1の仮想VPN装置と前記第2の仮想VPN装置とは擬似回線を介して接続されており、

前記第1の仮想VPN装置及び第2の仮想VPN装置の夫々は、対応するアクセス回線から受信されたフレームを他のアクセス回線及び擬似回線へ転送することを許容されており、且つ擬似回線から受信されたフレームを他の擬似回線を除くアクセス回線に転送することを許容されている、構成を採用することができる。

【0030】

本発明の第2の態様は、単一のアクセス回線を夫々有する複数の第1の拠点と、少なくとも二つのアクセス回線を有する第2の拠点とを含む複数の拠点間を結ぶ仮想プライベート

50

ト網(VPN)サービスを提供するための複数のVPN装置を備えるVPNシステムにおいて、前記第2の拠点が有する少なくとも二つのアクセス回線の一方が接続されるVPN装置であって、

フレーム送信元からフレームを受信するための二つの擬似回線を収容し、二つの擬似回線でほぼ同時に同一のフレームが受信された場合に、これらのフレームがフレーム送信元でのフラッディングによって到着したフラッディングフレームであることを検出する検出部と、

前記第2の拠点を含まず少なくとも二つの拠点間で送受信すべきフレーム転送処理用のフォワーディングテーブルに従ってフラッディングフレームの転送先を決定するフォワーディング部と、

決定されたフラッディングフレームの転送先が前記少なくとも二つのアクセス回線の一方を含む場合に、該フラッディングフレームを所定のフィルタ条件に従って廃棄するフィルタ部であって、前記少なくとも二つのアクセス回線の他方が接続された他のVPN装置から前記第2の拠点へ当該フラッディングフレームと同一のフレームが転送される場合に、当該フラッディングフレームを廃棄するフィルタ部を含むVPN装置である。

【0031】

本発明の第2の態様によれば、フラッディングフレームが検出され、このフラッディングフレームの転送先として第2の拠点が決定された場合において、このフラッディングフレームと同一のフレームが他のVPN装置から第2の拠点へ転送されるときには、フィルタ部がフラッディングフレームを廃棄する。これによって、同一のフレームが重複して第2の拠点に到着するのを防止することができる。

【0032】

好ましくは、本発明の第2の態様は、前記少なくとも二つのアクセス回線の他方の状態を示すアクセス回線状態メッセージを受信する受信部と、

前記受信部で前記少なくとも二つのアクセス回線の他方の異常を示すアクセス回線状態メッセージが受信された場合に、前記フィルタ部に設定されているフィルタ条件を変更するフィルタ制御部とをさらに含むことができる。

【0033】

このようにすれば、例えば、他方のアクセス回線の異常時にフィルタ条件が変更されることで、フラッディングフレームを廃棄することなく第2の拠点へ転送することが可能となる。これによって、フレームが第2の拠点に届かなくなることを防止できる。

【0034】

また、好ましくは、本発明の第2の態様において、フィルタ制御部は、周期的に受信すべきアクセス回線状態メッセージが所定時間前記受信部で受信されなかった場合に、前記他のVPN装置に異常が発生したと判断して、前記フィルタ条件の変更を行う構成を採用することができる。

【発明の効果】

【0035】

本発明によれば、複数のアクセス回線を有する拠点に関してVPNを介したループが発生することを防止することができる。

【0036】

また、本発明によれば、複数のアクセス回線を介してVPNに収容される特定の拠点へ同一のフレームが重複して到着することを防止することができる。

【発明を実施するための最良の形態】

【0037】

以下、図面を参照して本発明の実施形態を説明する。実施形態の構成は例示であり、本発明は実施形態の構成に限定されない。

【0038】

〔実施形態の概要〕

10

20

30

40

50

最初に、図4に示したVPLSシステムにおける問題点(ループの発生)の解決(ソリューション)について説明する。アクセス回線の帯域を無駄にすることなくループの発生を抑止するには、ループ中のアクセス回線ではない部分(区間)に対するE-フレームのフォワーディングを止めればよい。

【0039】

図4に示した例では、PE#1とPE#4との間を結ぶ擬似回線(pseudowire)が、ループ中のアクセス回線ではない区間に該当する。しかしながら、この擬似回線を単純に削除すると、ブランチ#4とブランチ#3との間で通信ができなくなってしまう。

【0040】

ここで、ヘッドオフィスからE-VPNを通過してヘッドオフィスへ戻るトラフィックのみをブロックするため、図4のPE#1及びPE#4の夫々が、VPNに冗長収容されているヘッドオフィス用のフォワーディングテーブル(第2のフォワーディングテーブル)とその他の拠点向けのフォワーディングテーブル(第1のフォワーディングテーブル)とを有するように構成する。

10

【0041】

通常のVPLSでは、PEはVPN毎にフォワーディングテーブルを有し、同一のVPNに属する拠点は、同一のフォワーディングテーブルを用いてフォワーディング処理される。これに対し、本発明に係るPE(VPN装置)は、通常のフォワーディングテーブル(第1のフォワーディングテーブル)に加えて、同一のVPNに属する拠点に含まれる冗長化収容された拠点(少なくとも二つのアクセス回線を有する第2の拠点)に対する専用のフォワーディングテーブル(第2のフォワーディングテーブル)を持つ。

20

【0042】

本明細書では、このような第1及び第2のフォワーディングテーブルの一方を用いてフォワーディング処理(転送処理)を行う機能を仮想PEと呼び、それぞれの仮想PEは、通常のVPLSにおけるPEと同様に、他のPE及び仮想PEとフルメッシュ(full-mesh)の擬似回線で接続される。

【0043】

但し、E-VPNに冗長化収容された拠点(第2の拠点：図4ではヘッドオフィス)を収容している二つの仮想PEの間は、擬似回線で接続されない。以上説明した本発明に係るVPN(ここではE-VPN)のネットワーク構成例を図6に示す。

30

【0044】

図6に示すネットワーク構成例は、図4に示したネットワーク構成と次のように異なっている。PE#1は、冗長化収容された拠点(第2の拠点：ヘッドオフィス)を含まない少なくとも二つの拠点間で送受信すべきフレームの転送処理用のフォワーディングテーブル(第1のフォワーディングテーブル)を用いる仮想PE#1-1(第1の仮想VPN装置)と、冗長化収容された拠点(ヘッドオフィス)を含む少なくとも二つの拠点間で送受信すべきフレームの転送処理用のフォワーディングテーブル(第2のフォワーディングテーブル)を用いる仮想PE#1-2(第2の仮想VPN装置)とを備える。仮想PE#1-1は、ブランチ#4のアクセス回線A3を収容し、仮想PE#1-2は、ヘッドオフィスのアクセス回線A1を収容する。

40

【0045】

また、PE#4は、冗長化収容された拠点(ヘッドオフィス)を含まない少なくとも二つの拠点間で送受信されるフレームの転送処理用のフォワーディングテーブル(第1のフォワーディングテーブル)を用いる仮想PE#4-2(第4の仮想VPN装置)と、冗長化収容された拠点(ヘッドオフィス)を含む少なくとも二つの拠点間で送受信されるフレームの転送処理用のフォワーディングテーブル(第2のフォワーディングテーブル)を用いる仮想PE#4-1(第3の仮想VPN装置)とを備える。仮想PE#4-2は、ブランチ#3のアクセス回線A4を収容し、仮想PE#4-1は、ヘッドオフィスのアクセス回線A2を収容する。

【0046】

50

さらに、各仮想PE#1-1, #1-2, #4-1及び#4-2は、仮想PE#1-2と仮想PE#4-1との間を除き、他のPE(PE#2, #3)及び他の仮想PEとフルメッシュの擬似回線で接続される。

【0047】

このように、本発明では、冗長化拠点を収容するPEが二つの仮想PEに分割される。また、本発明では、冗長化拠点を収容する仮想PE間を除きフルメッシュ状に擬似回線が設定され、スプリットホライズンによりループが回避される。

【0048】

仮に、図6に示すPE及び仮想PEの総てが擬似回線で相互に接続された状態を想定する。この場合、例えばブランチ#3からブランチ#4へ向かうトラフィックは、仮想PE#4-2及び仮想PE#1-1を通過してブランチ4に到達する。即ち、当該トラフィックは、ヘッドオフィスとE-VPNとの間のループトラフィックと異なる経路を通過する。一方、仮想PE#1-2と仮想PE#4-1との間を流れるトラフィックは、ループトラフィックのみとなる。

【0049】

ここで、上述した様に、仮想PE#1-2と仮想PE#4-1の間には擬似回線が設定されない。このため、仮想PE#1-2と仮想PE#4-1の間でのE-フレームのフォワーディングは行われない。従って、E-VPNに冗長化収容されている拠点(ヘッドオフィス)とE-VPNとの間でのループが回避される。

【0050】

次に、図5に示したVPLSシステムにおける問題点(E-フレームの二重到着)の解決について説明する。アクセス回線を冗長化している拠点(冗長化拠点)へのE-フレームの二重到着を回避するには、各PEで受信されるE-フレームがE-VPN中の他のPEによってフラッディングされたのか、ユニキャスト(unicast)フォワーディングされたのかを判断(識別)する必要がある。このような判断を行うための手段として、PE間を複数の擬似回線(Pseudowire)で接続することが考えられる。

【0051】

背景技術で説明したように、VPLSでは、アクセス回線から宛先を学習していないE-フレームを受信したノード(PE)は、自身に接続されている総ての擬似回線及びアクセス回線に向けてそのE-フレームをフラッディング(ブロードキャスト)する。このため、PE間が2本の擬似回線で接続されていれば、フラッディングされたフレームは両方の擬似回線を通じて受信側のPEにほぼ同時に到着する。これに対し、送信側のPEからユニキャストフォワーディングされたフレームは、受信側のPEにおいて、片側の擬似回線でしか受信されない。

【0052】

このような、2本の擬似回線からのE-フレームの受信状況を示す情報に基づき、フラッディングされたE-フレームをフィルタリング(排除)することができる。図7は、フラッディングされたE-フレームをフィルタリングするためのPEの構成例を示す図である。

【0053】

図7において、PE#1は、フラッディング検出部(検出部)11と、フラッディング検出部11に接続されたMAC(Media Access Control)フォワーディング部(フォワーディング部)12と、MACフォワーディング部12に接続され、フラッディング検出部11によって制御されるフレームフィルタ部(フィルタ部)13とを備えている。フラッディング検出部11は、他のPE(PE#2:フレーム送信元)と、2本の擬似回線(pseudowires)#1及び#2を介して接続されている。フレームフィルタ部13は、アクセス回線Aを介して、冗長収容された顧客拠点(例えば、図4に示すヘッドオフィス)に接続される。

【0054】

図7において、PE#2からフラッディングされたE-フレーム(フレーム)は、擬似回線#1及び擬似回線#2の双方を通過してPE#1に到着する。PE#1のフラッディング

10

20

30

40

50

検出部 11 は、擬似回線 # 1 及び # 2 の双方から同一の E - フレームをほぼ同時に受信したとき、PE # 2 が E - フレームをフラッディングしたと認識する(フラッディングを検出する)。

【0055】

この場合、フラッディング検出部 11 は、この E - フレームを擬似回線 # 1 及び # 2 のいずれか一方のみから受信したものと擬制し、E - フレームを受信したと擬制した側の擬似回線の情報を、MAC フォワーディング部 12 に通知する。これによって、MAC フォワーディング部 12 は、その E - フレームがフラッディング検出部 11 から通知された側の擬似回線から到着したと認識し、この送信元アドレス(source address)に対するフォワーディングテーブルエントリを学習する。即ち、MAC フォワーディング部 12 は、フォワーディングテーブルを有しており、フォワーディングテーブル内に、E - フレームの送信元アドレスと受信擬似回線との関係を示すエントリを登録する。

10

【0056】

MAC フォワーディング部 12 は、学習後、この E - フレームを更にフラッディングする。これによって、E - フレームは、アクセス回線 A と MAC フォワーディング部 12 との間に設けられたフレームフィルタ部 13 に送られる。フレームフィルタ部 13 は、フラッディング検出部 11 からの制御により、フラッディングを検出(認識)した E - フレームのフィルタリング(ブロック)を行う。

【0057】

図 7 に示した PE # 1 の構成を有する PE が、冗長化収容される拠点から伸びる複数のアクセス回線(少なくとも 2 本のアクセス回線)を夫々収容する。そして、2 本のアクセス回線を夫々収容する二つの PE の一方が、フラッディングされた E - フレームをアクセス回線にフォワーディングし、他方の PE がフラッディングされた E - フレームをフィルタリングするようなフィルタリング処理を行う。これによって、アクセス回線を冗長化した拠点宛に同一の E - フレームが二重到着することが防止される。

20

【0058】

本発明によれば、VPN へのアクセス回線が冗長化された顧客拠点に対してアクセス回線の帯域を効率的に利用しつつ、E - フレームのループや二重到着を防止することができる。

【0059】

具体例

図 8 は、本発明の実施形態に係る VPLS 網(VPN システム)の構成例を示す図である。図 8 には、顧客が有する複数の拠点を複数のアクセス回線を介して収容する VPLS 網が示されている。複数の拠点として、図 8 では、顧客のヘッドオフィス 101 と、ブランチ # 1 (102)、# 2 (103)、# 3 (104) 及び # 4 (105) からなる 5 つのユーザ拠点が VPLS 網に接続されている。複数の拠点 101 ~ 105 は、VPLS 網により提供される同一の VPN (仮想プライベート網) に属し、VPN を通じてあたかも同一の Ethernet (登録商標) に接続された状態にされる。

30

【0060】

図 8 に示す例では、VPLS 網として、VPLS プロバイダの MPLS 網(プロバイダ網) 5 が適用されている。プロバイダ網 5 は、複数の拠点を収容するための複数のプロバイダエッジスイッチ(PE: VPLS 装置、VPN 装置に相当)を備えている。各 PE は、プロバイダ網 5 のエッジ部分に配置され、各拠点が有するアクセス回線を収容している。

40

【0061】

図 8 に示す例では、プロバイダ網 5 は、ヘッドオフィス 101 及びブランチ 102 ~ 105 (# 1 ~ # 4) を収容するための PE # 1、# 2、# 3 及び # 4 を備えている。ブランチ 102 は、単一のアクセス回線 21 を介して PE # 3 に接続されている。ブランチ 103 は、単一のアクセス回線 22 を介して PE # 2 に接続されている。ブランチ 104 は、単一のアクセス回線 23 を介して PE # 4 に接続されている。ブランチ 105 は、単一のアクセス回線 24 を介して PE # 1 に接続されている。

50

【0062】

ヘッドオフィス101は、VPLS網(VPN)との接続に対して耐障害性を向上させるため、アクセス回線25を介してPE#1に接続(収容)されるとともに、アクセス回線26を介してPE#4に接続されている。ブランチ102~105の夫々が、本発明に係る複数の第1の拠点に相当し、ヘッドオフィス101が本発明に係る少なくとも1つの第2の拠点に相当する。

【0063】

ここで、VPLS網(VPN)に冗長収容される拠点(ヘッドオフィス101)を収容するPE#1及びPE#4は、単一のアクセス回線を介してVPNに接続された複数の拠点102~105中の少なくとも二つの拠点間で送受信されるべきE-フレーム(以下、単に「フレーム」と表記)に係るフォワーディング(通常のフォワーディング)を行うための第1のフォワーディングテーブルを用いてフォワーディング/フラッディング処理を行う第1の仮想PE(第1の仮想VPN装置)と、VPNに冗長収容された(少なくとも二つのアクセス回線を介してVPNに収容された)第2の拠点を含む少なくとも二つの拠点間で送受信されるべきフレームのフォワーディングを行うための第2のフォワーディングテーブルを用いてフォワーディング/フラッディング処理を行う第2の仮想PE(第2の仮想VPN装置)とを含む装置として機能する。

10

【0064】

図8において、PE#1は、第1の仮想PE(第1の仮想VPN装置)に相当する仮想PE#1-1と、第2の仮想PE(第2の仮想VPN装置)に相当する仮想PE#1-2とを備えている。ブランチ#4(105)用のアクセス回線24は、仮想PE#1-1に接続される。ヘッドオフィス101用のアクセス回線の一方(アクセス回線25)は、仮想PE#1-2に接続される。

20

【0065】

また、PE#4は、第2の仮想PE(第4の仮想VPN装置)に相当する仮想PE#4-1と、第1の仮想PE(第3の仮想VPN装置)に相当する仮想PE#4-2とを備えている。ブランチ#3(104)用のアクセス回線23は、仮想PE#4-2に接続される。ヘッドオフィス101用のアクセス回線の他方(アクセス回線26)は、仮想PE#4-1に接続される。

30

【0066】

プロバイダ網5内において、PE及び仮想PEの夫々は、原則として、同一のVPNに属する総てのPE及び仮想PEとPseudowire(PW:擬似回線)を介して接続される(プロバイダ網5上に複数の擬似回線が設定される)。即ち、PE間、仮想PE間、及びPE-仮想PE間は、冗長化されたアクセス回線をそれぞれ収容する仮想PE間を除き、擬似回線でフルメッシュ状に接続される。図8において、アクセス回線21~26は実線で示され、擬似回線は破線で示されている。

40

【0067】

例えば、PE#2は、PE#3と、仮想PE#1-1、#1-2、#4-1及び#4-2と擬似回線で接続される。或いは、仮想PE#1-1は、PE#2及び#3と、仮想PE#1-2、#4-1及び#4-2と擬似回線で接続される。但し、冗長化されたアクセス回線(アクセス回線25及び26)を夫々収容する仮想PE間(仮想PE#1-2と仮想PE#4-1との間)は擬似回線で接続されない。

40

【0068】

PE及び仮想PEの夫々は、擬似回線を用いたスプリットホライズンを適用することにより、プロバイダ網5内でのループ発生を抑制する。即ち、PE及び仮想PEの夫々は、擬似回線から受信されるフレームを他の擬似回線へフォワーディング及びフラッディングしない。

【0069】

以上のような構成によって、ヘッドオフィス101に関するループの発生が抑制される。

50

例えば、仮想PE#1-2がヘッドオフィス101からのフレームをアクセス回線25を介して受信し、このフレームをフラッディングした場合を想定する。この場合、フラッディングフレームが、擬似回線を介してPE#2, PE#3, 仮想PE#1-1及び仮想PE#4-2に転送される。

【0070】

しかし、仮想PE#1-2と仮想PE#4-1の間には擬似回線が設定されないため、フラッディングフレームは仮想PE#4-1に到着しない。従って、仮想PE#4-1が、仮想PE#1-2からのフラッディングフレームを受信し、そのフラッディングフレームの転送先が未学習であるが故に、このフラッディングフレームを再度フラッディングし、フラッディングフレームがヘッドオフィス101に戻ってしまうことがない。

10

【0071】

図8に示す具体例によれば、ヘッドオフィス101から送信されたE-フレームが、PE#1とPE#4との間を経由してヘッドオフィス101に戻ることを防止することができる。一方で、各拠点からE-VPNへ送信されるフレームは、スプリットホライズンによりVPN内でループすることなく、フレームの宛先の拠点を収容するPE又は仮想PEを介して、宛先拠点到達することができる。

【0072】

図9は、図8に示したPE#1の機能ブロック構成例を示す図である。但し、図8に示したPE#4も、図9に示す構成を有する。図9において、仮想PE#1-1(第1の仮想PE)は、仮想PE#1-1に接続されるアクセス回線及び複数の擬似回線(PW)から受信されるフレームに対するフォワーディング/フラッディング処理を行うMACフォワーディング部31Aを有している。

20

【0073】

ここに、MACフォワーディング部31Aは、ブランチ#4(105)のアクセス回線24と接続されている。また、MACフォワーディング部31Aは、PE#2に接続される1本の擬似回線(PW#9)と、PE#3に接続される1本の擬似回線(PW#10)と、仮想PE#4-1に接続される2本の擬似回線(PW#11及び#12)と、仮想PE#4-2に接続される1本の擬似回線(PW#13)とを収容している。

【0074】

さらに、MACフォワーディング部31Aは、仮想PE#4-1のフラッディングを検出するためのフラッディング検出部32Aを含んでいる。フラッディング検出部32Aは、PW#11及び#12と接続されている。

30

【0075】

一方、仮想PE#1-2(第2の仮想PE)は、仮想PE#1-2が収容するアクセス回線25及び擬似回線で受信されたフレームに対するフォワーディング/フラッディング処理を行うMACフォワーディング部31B(本発明のフォワーディング部に相当)を有している。

【0076】

また、仮想PE#1-2は、PE#2及び#3並びに仮想PE#4-2のそれぞれでフラッディングされたフレームを検出するための複数のフラッディング検出部32B, 32C及び32Dを備えている(夫々が本発明の検出部に相当する)。フラッディング検出部32B, 32C及び32Dの夫々は、MACフォワーディング部31Bに接続されている。

40

【0077】

フラッディング検出部32Bは、PE#2に接続される2本の擬似回線(PW#1及び#2)を収容している。フラッディング検出部32Cは、PE#3に接続される2本の擬似回線(PW#3及び#4)を収容している。フラッディング検出部32Dは、仮想PE#4-2に接続される2本の擬似回線(PW#7及び#8)を収容している。

【0078】

仮想PE#1-2は、冗長化されたアクセス回線25及び26を有するヘッドオフィス101を収容している。このため、仮想PE#1-2は、ヘッドオフィス101に同一の

50

フレームが二重に到着することを防ぐためのフレームフィルタ部 3 3 (本発明のフィルタ部に相当)を備えている。

【 0 0 7 9 】

さらに、仮想 P E # 1 - 2 は、アクセス回線障害等を検出するアクセス回線障害検出部 3 4 (本発明の監視部に相当)と、アクセス回線障害メッセージ送信部 3 5 (本発明の送信部に相当)と、アクセス回線障害メッセージ受信部 3 6 (本発明の受信部に相当)と、フィルタ制御部 3 7 (本発明のフィルタ制御部に相当)とを備えている。仮想 P E # 1 - 1 は、冗長化されていないブランチ # 4 (1 0 5) を収容している。このため、仮想 P E # 1 - 1 は、これらのブロック 3 4 ~ 3 7 を持たない。

【 0 0 8 0 】

また、仮想 P E # 1 - 2 は、アクセス回線 2 5 及び 2 6 を有するヘッドオフィス 1 0 1 を収容している。このため、上述したように、仮想 P E # 1 - 2 と P E # 2 , # 3 及び仮想 P E # 4 - 2 の夫々との間において、それぞれ 2 本の擬似回線が設定され、これらの P E # 2 , # 3 及び仮想 P E # 4 - 2 に対応するフラッディング検出部 3 2 B , 3 2 C , 3 2 D が設けられている。

【 0 0 8 1 】

これに対し、仮想 P E # 1 - 1 は、フレームフィルタ部 3 3 を有しないので、基本的にフラッディングを検出する必要がない。このため、顧客ヘッドオフィスを収容している仮想 P E # 4 - 1 を除く P E # 2 , # 3 及び仮想 P E # 4 - 2 の夫々と 1 本の擬似回線で接続される。但し、上述したように、仮想 P E # 1 - 1 は、仮想 P E # 4 - 1 からのフラッディングフレームを検出するために、仮想 P E # 4 - 1 と 2 本の擬似回線 (P E # 1 1 及び # 1 2) を収容するフラッディング検出部 3 2 A を持つ。

【 0 0 8 2 】

M A C フォワーディング部 3 1 A 及び 3 1 B の夫々は、フォワーディングテーブル 3 8 の登録内容に基づいて、フォワーディング/フラッディング処理を行う。図 1 0 は、P E # 1 が有するフォワーディングテーブル 3 8 の例を示す図である。

【 0 0 8 3 】

フォワーディングテーブル 3 8 中の上半分のエントリ群 3 8 A が仮想 P E # 1 - 1 の M A C フォワーディング部 3 1 A で参照される第 1 のフォワーディングテーブルに相当し、下半分のエントリ群 3 8 B が仮想 P E # 1 - 2 の M A C フォワーディング部 3 1 B で参照される第 2 のフォワーディングテーブルに相当する。

【 0 0 8 4 】

通常の V P L S 装置では、V P N 毎にフォワーディングテーブルを持つ。しかしながら、本発明は、同じ V P N に属する顧客拠点であっても、特定の拠点に関して、通常のフォワーディングテーブルと異なる専用のフォワーディングテーブルを持つことを特徴の一つとする。

【 0 0 8 5 】

ヘッドオフィス 1 0 1 がフォワーディングテーブル 3 8 中の仮想 P E 番号 “ # 1 - 2 ” に対応し、ブランチ # 4 (1 0 5) がフォワーディングテーブル 3 8 中の仮想 P E 番号 “ # 1 - 1 ” に対応する。言い換えれば、図 1 0 には、アクセス回線 2 4 から受信されるフレーム用のエントリ群と、アクセス回線 2 5 から受信されるフレーム用のエントリ群とが例示登録された状態となっている。

【 0 0 8 6 】

P E # 1 によって収容される複数のアクセス回線及び複数の擬似回線 (P W) は、図 9 中に示したように、仮想 P E # 1 - 1 及び # 1 - 2 の一方に属する。M A C フォワーディング部 3 1 A 及び 3 1 B の夫々 (3 1 A と 3 1 B を区別しない場合には、「M A C フォワーディング部 3 1」と表記)に接続される各回線と仮想 P E 番号とは予め関連付けられ、受信回線に対応する仮想 P E 番号が登録されたエントリが参照される。

【 0 0 8 7 】

具体的には、M A C フォワーディング部 3 1 は、フレームを受信したアクセス回線又は

10

20

30

40

50

擬似回線に対応する仮想PE番号を有するエントリを参照し、受信フレームの宛先MACアドレスが登録されたエントリを検索する。エントリが検索された場合には、MACフォワーディング部31は、検索されたエントリ内で送出先として規定された回線へフレームをフォワーディングする。

【0088】

これに対し、フレームの宛先MACアドレスに対応するエントリがフォワーディングテーブル38から検索されない場合には、MACフォワーディング部31は、自身に接続された総てのアクセス回線及び擬似回線へ向けて当該フレームのフラッディングを行う。但し、擬似回線から受信されたフレームは他の擬似回線に対してフラッディングされない(スプリットホライゾン)。

10

【0089】

同一のPE中の仮想PE間(例えば、PE#1中の仮想PE#1-1と仮想PE#1-2との間)のフォワーディングは、異なる論理PE間のフォワーディングに該当するので、これらの間に擬似回線(PW)が設定されているものとして取り扱われる。即ち、MACフォワーディング部31A(仮想PE#1-1)とMACフォワーディング部31B(仮想PE#1-2)とは、擬似回線PWxで接続される。

【0090】

但し、図9に示す例では、仮想PE#1-2はヘッドオフィス101を収容しており、仮想PE#1-1で行われたフラッディングの情報を必要とする。ここに、仮想PE#1-2のフラッディング検出部32B、32C及び32Dの夫々(これらを区別しない場合には、「フラッディング検出部32」と表記)は、フレームのフラッディングを検出すると、フラッディング情報を制御線40を通じてフレームフィルタ部33に通知するように構成されている。MACフォワーディング部31Aがフラッディングを行った場合には、フラッディング情報が、制御線40を介してフレームフィルタ部33に通知される。

20

【0091】

また、MACフォワーディング部31は、フレームの受信時に、受信フレームのソースMACアドレスを確認し、このソースMACアドレスと同一のアドレスがフォワーディングテーブル38中に登録されているか否かを判断する。もし、ソースMACアドレスと同一のアドレスが登録されていない場合には、MACフォワーディング部31は、通常のE-スイッチと同様に、このフレームのアドレスを学習する。即ち、MACフォワーディング部31は、フレームを受信したアクセス回線又は擬似回線がフレームの送出先として規定され、且つソースMACアドレスが宛先MACアドレスとして規定された新たなエントリをフォワーディングテーブル38に登録する。

30

【0092】

仮想PE#1-2は、特定のユーザ拠点(ヘッドオフィス101)にフレームが二重到着することを防ぐために、他のPE又は仮想PEでフラッディングが行われたか否かを検出する必要がある。この目的のために、仮想PE#1-2は、フラッディング検出部32B、32C及び32Dを有する。各フラッディング検出部32は、2本の擬似回線(図7のPEW#1及び#2に相当)で他のPE又は仮想PEと接続されている。

【0093】

フラッディング検出部32は、自身が収容する2本の擬似回線からほぼ同時に同一のフレームを受信した場合には、このフレームの送出元(送信元)のPEあるいは仮想PEでフラッディングが行われたと判断する(フラッディングを検出する)。この場合、フラッディング検出部32は、受信された二つのフレームのいずれか片方を廃棄し、残りの片方を、受信した擬似回線の情報とともに対応するMACフォワーディング部31(MACフォワーディング部31A及び31Bの一方)に送ると共に、フラッディングが行われたこと(フラッディング情報)をフレームフィルタ部33に伝える。

40

【0094】

これに対し、フラッディング検出部32は、2本の擬似回線の一方のみからフレームを受信した場合には、このフレームを受信擬似回線の情報とともに対応するMACフォー

50

ディング部 3 1 に送る。

【 0 0 9 5 】

また、フラディング検出部 3 2 は、M A C フォワーディング部 3 1 からユニキャストのフレームを受信した場合には、フォワーディングテーブル 3 8 の送出先情報に従って、フレームを 2 本の擬似回線の一方に送出する。

【 0 0 9 6 】

さらに、フラディング検出部 3 2 は、対応する M A C フォワーディング部 3 1 からフラディングのフレームを受け取った場合において、擬似回線の宛先 P E あるいは仮想 P E が冗長化された拠点(ヘッドオフィス 1 0 1)を収容している設定を有するときには、2 本の擬似回線の双方に同一のフレームを送出し、そうでない場合には、2 本の擬似回線のいずれか片方のみフレームを送出する。

10

【 0 0 9 7 】

フレームフィルタ部 3 3 は、フラディングによってアクセス回線 2 5 を収容する仮想 P E # 1 - 2 とアクセス回線 2 6 を収容する仮想 P E # 4 - 1 に夫々到着する 2 つの同一のフレームの一方をフィルタリングする機能を有し、フラディング検出部 3 2 からの制御信号に従って動作する。

【 0 0 9 8 】

フレームフィルタ部 3 3 は、冗長化したアクセス回線を収容している全ての P E 及び仮想 P E に夫々設けられ、これらの P E 及び仮想 P E 中の 1 つのフレームフィルタ部 3 3 のみがフラディングが検出されたフレームを透過し、残りの P E 又は仮想 P E のフレームフィルタ部 3 3 ではフレームを廃棄するように構成される。

20

【 0 0 9 9 】

フレームをフィルタリングするアルゴリズムの一例として、以下を考えることができる。例えば、冗長化された複数のアクセス回線を有する拠点を収容している総ての P E 又は仮想 P E のフレームフィルタ部 3 3 (複数のフレームフィルタ部 3 3)で、同一のハッシュ(hash)関数を用いてフレームからハッシュ値を夫々計算する。その後、ハッシュ値と所定の閾値とが比較され、その比較結果に基づいて、複数のフレームフィルタ部 3 3 の 1 つのみがフレームを透過し、残りのフレームフィルタ部 3 3 がフレームを廃棄する。例えば、複数のフレームフィルタ部 3 3 の 1 つのみが閾値より大きいハッシュ値を持つフレームを廃棄することなく透過させ、残りのフレームフィルタ部 3 3 が閾値以下のハッシュ値を持つフレームを廃棄するように構成される。

30

【 0 1 0 0 】

図 1 1 は、図 8 に示したフレームフィルタ部 3 3 の構成例を示す図である。仮想 P E # 1 - 2 及び # 4 - 1 の双方には、図 1 1 に示した構成を有するフレームフィルタ部 3 3 が設けられる。なお、フレームフィルタ部 3 3 の説明の便宜のため、図 1 1 に示すフレームフィルタ部 3 3 は、仮想 P E # 1 - 2 に搭載されていると仮定して説明する。

【 0 1 0 1 】

図 1 1 において、フレームフィルタ部 3 3 は、廃棄判定部 4 1 と、ハッシュ演算部 4 2 とを備えている。廃棄判定部 4 1 及びハッシュ演算部 4 2 には、M A C フォワーディング部 3 1 B からのフレームが入力される。ハッシュ演算部 4 2 は、所定のハッシュ関数を用いてフレームに対するハッシュ演算を行い、ハッシュ値を廃棄判定部 4 1 に送る。廃棄判定部 4 1 は、フラディング検出部 3 2 から制御線 4 0 を通じてフラディング検出信号(フラディング情報)を受け取るように構成されている。

40

【 0 1 0 2 】

廃棄判定部 4 1 は、フラディング検出信号を受け取っていない場合には、M A C フォワーディング部 3 1 B からのフレームを廃棄することなくアクセス回線(アクセス回線 2 5)へ送出する。これに対し、廃棄判定部 4 1 は、フラディング検出信号を受け取った場合には、M A C フォワーディング部 3 1 B からのフレームに関する廃棄判定を行う。

【 0 1 0 3 】

ここに、廃棄判定部 4 1 には、フィルタ制御部 3 7 によって、ハッシュ値に対する所定

50

の閾値、及び閾値判定結果に応じたフレームの廃棄条件が設定されるようになっている。フィルタ制御部 37 には、その外部から廃棄判定部 41 に通知すべき閾値 / 廃棄条件(フィルタ条件)が設定される。フィルタ条件として、例えば、ハッシュ値が閾値より大きい場合にフレームを廃棄するという第 1 の条件と、ハッシュ値が閾値以下の場合にフレームを廃棄するという第 2 の条件との一方を設定することができる。

【0104】

廃棄判定部 41 は、ハッシュ値と閾値との比較を行い、比較結果が廃棄判定部 41 に設定されている第 1 及び第 2 の条件の一方に合致する場合に、フレームを廃棄(フィルタリング)し、そうでなければ、フレームを廃棄することなくアクセス回線に送出する。例えば、廃棄判定部 41 に第 1 の条件が設定されている場合では、廃棄判定部 41 は、ハッシュ値が閾値より大きいフレームを廃棄し、閾値以下のフレームを通過させる。

10

【0105】

第 1 の条件が仮想 PE # 1 - 2 に設定される場合には、仮想 PE # 4 - 1 に第 2 の条件が設定される。逆に、第 2 の条件が仮想 PE # 1 - 2 に設定される場合には、仮想 PE # 4 - 1 に第 1 の条件が設定される。同一の廃棄条件が仮想 PE # 1 - 2 及び # 4 - 1 の双方に同時に設定されることはない。

【0106】

これによって、仮想 PE # 1 - 2 及び # 4 - 1 の双方に同一の E - フレームが到着した場合に、二つの廃棄判定部 41 の一方でフレームが廃棄され、廃棄判定部 41 の他方でフレームがアクセス回線に送出される。このようにして、冗長化収容された拠点(ヘッドオフィス 101)に同一のフレームが二重に到着することが防止される。また、閾値を調整することで、例えば、所望の分配率で仮想 PE # 1 - 2 及び # 4 - 1 の夫々からフレームがユーザ拠点(ヘッドオフィス 101)へ送出されるようにすることができる。

20

【0107】

フィルタ条件は、フィルタ制御部 37 によって変更(解除(撤廃)を含む)可能となっている。例えば、アクセス回線状態メッセージ受信部 36 は、仮想 PE # 4 - 1 で収容されるアクセス回線 26 の障害(異常)を示すアクセス回線状態メッセージを受信すると、アクセス回線 26 の障害をフィルタ制御部 37 に通知する。すると、フィルタ制御部 37 は、フィルタ条件の変更(例えば、フィルタ条件の解除)を廃棄判定部 41 に指示する。アクセス回線 26 に障害が生じると、仮想 PE # 4 - 1 からのヘッドオフィス 101 へフレームを転送できなくなる。この場合、仮想 PE # 1 - 2 のフィルタ条件が解除されることで、同一のフレームを仮想 PE # 1 - 2 から正常なアクセス回線 25 を通じてヘッドオフィス 101 に転送することができる。

30

【0108】

なお、図 11 に示す構成例において、アクセス回線 25 から受信されたフレームはフレームフィルタ部 33 を常に透過し、MAC フォワーディング部 31B に渡される。

【0109】

図 9 に戻って、アクセス回線異常検出部 34 は、Ethernet(登録商標)のリンクダウン(link down)を検出したり、IEEE802.3ah や IEEE802.1ag の中で規定された Ethernet(登録商標) OAM、あるいは ITU-T 勧告 Y.1731 の OAM などの機能を用いてアクセス回線の異常を検出する。

40

【0110】

アクセス回線状態メッセージ送信部 35 は、アクセス回線異常検出部 34 でアクセス回線(図 9 の例ではアクセス回線 25)の異常が検出された場合に、そのアクセス回線 25 とともに冗長化を実現しているアクセス回線(アクセス回線 26)を収容している他の PE 又は仮想 PE(図 9 の例では仮想 PE # 4 - 1)に対して異常検出を通知する。即ち、アクセス回線の異常を示すアクセス回線状態メッセージが送信される。

【0111】

また、冗長化アクセス回線の一つを収容する PE 又は仮想 PE の間で定期的にアクセス回線状態メッセージを交換することにより、PE 又は仮想 PE が正常に動作していること

50

の監視に利用することも考えられる。即ち、周期的又は定期的に受信すべきアクセス回線状態メッセージが受信されない場合に、そのアクセス回線状態メッセージを送信すべき P E 又は仮想 P E に障害が発生したと判断することができる。

【 0 1 1 2 】

図 1 2 は、アクセス回線状態メッセージのフォーマット例を示す図である。図 1 2 において、アクセス回線状態メッセージは、メッセージ送出元の P E 又は仮想 P E の識別子と、宛先 P E 又は仮想 P E の識別子と、アクセス回線異常検出情報とを含むことができる。

【 0 1 1 3 】

アクセス回線状態メッセージ受信部 3 6 は、他の P E 又は仮想 P E からのアクセス回線状態メッセージを受信する。冗長化されたアクセス回線を持つ拠点に関して、冗長化された複数のアクセス回線の一つに異常が検出されるか、或いはその拠点を収容している P E 又は仮想 P E の一つに障害が発生すると、その拠点へのフラッディングフレームの一部又は総てがその拠点で受信されなくなってしまう可能性がある。このため、冗長収容された拠点を収容している P E 又は仮想 P E は、相互にアクセス回線の状態、及び P E / 仮想 P E の状態を監視する。P E 又は仮想 P E の異常は、例えば周期的に送出されるアクセス回線状態メッセージが一定期間受信されなかった場合に検出される。

【 0 1 1 4 】

フィルタ制御部 3 7 は、アクセス回線状態メッセージ受信部 3 6 によって検出されたアクセス回線の異常又は他の P E 若しくは仮想 P E の異常に従って、フレームフィルタ部 3 3 に与えるフィルタ条件(閾値 / 廃棄条件)を変更する。異常が生じたアクセス回線、P E 及び仮想 P E と、フィルタ条件の変更内容との関係は、予め決められており、フィルタ制御部 3 7 に予めセットされる。フィルタ制御部 3 7 は、アクセス回線状態メッセージ受信部 3 6 でのアクセス回線状態メッセージの受信状況、或いはアクセス回線状態メッセージの内容に従って、フィルタ条件の変更指示を必要に応じてフレームフィルタ部 3 3 に与える。

【 0 1 1 5 】

図 8 に示す P E # 2 及び # 3 の夫々は、図 9 に示した仮想 P E # 1 - 1 とほぼ同様のブロック構成を有する。

【 0 1 1 6 】

なお、図 9 に示した例では、P E # 1 内の仮想 P E # 1 - 1 及び # 1 - 2 が、共通の(1 つの)フォワーディングテーブル 3 8 を使用する例について説明した。但し、仮想 P E 毎に、第 1 及び第 2 のフォワーディングテーブルの一方を個別に有する構成を適用することも可能である。例えば、仮想 P E # 1 - 1 が図 1 0 に示したエントリ群 3 8 A のみを有する第 1 のフォワーディングテーブルを有し、仮想 P E # 1 - 2 が図 1 0 に示したエントリ群 3 8 B のみを有する第 2 のフォワーディングテーブルを持つように変形可能である。

【 0 1 1 7 】

また、図 9 に示した例では、二つの M A C フォワーディング部 3 1 A 及び 3 1 B を有する例について説明したが、物理的に 1 つの M A C フォワーディング部が論理的に二つの M A C フォワーディング部 3 1 A 及び 3 1 B として機能し、二つの仮想 P E が実現されるようになっていても良い。

【 0 1 1 8 】

また、図 8 ~ 図 1 2 に示した具体例では、冗長化されたヘッドオフィス 1 0 1 のアクセス回線 2 5 及び 2 6 を収容する P E # 1 及び P E # 4 の夫々が仮想 P E を有する場合の V P L S システム(V P N システム)について説明した。但し、このような V P N システムの代わりに、冗長化された拠点が有する複数のアクセス回線の 1 つを収容する P E が、そのアクセス回線のみを収容する場合であっても、本発明は成立する。

【 0 1 1 9 】

例えば、図 1 3 に示すように、P E # 4 が、ヘッドオフィス 1 0 1 のアクセス回線 2 6 のみを収容し、他の拠点のアクセス回線を収容しない場合を想定する。この場合、P E # 4 は、二つの仮想 P E を有する必要はない。但し、この場合でも、仮想 P E # 1 - 2 と P

10

20

30

40

50

E # 4 とが擬似回線で接続されると、ループが発生する可能性があるので、両者間に擬似回線は設定されない。また、図 1 3 に示す P E # 4 は、図 9 の仮想 P E # 1 - 2 とほぼ同様の構成を有する。

【 0 1 2 0 】

以上説明した V P L S システム (V P N 装置) の実施形態によれば、冗長化された複数のアクセス回線 (アクセス回線 2 5 及び 2 6) を有するユーザ拠点 (顧客ヘッドオフィス) に關して、顧客ヘッドオフィスからアクセス回線 2 5 及び 2 6 の一方に送出された E - フレームが、 P E # 1 及び P E # 4 を経由し、アクセス回線 2 5 及び 2 6 の他方を通じて顧客ヘッドオフィスに戻ること (E - フレームのループ) を防止することができる。これによって、複数のアクセス回線の帯域を適正に利用することができる。

10

【 0 1 2 1 】

また、 V P L S システムの実施形態によれば、 V P L S 網内でフラディングされた E - フレームが、アクセス回線 2 5 及び 2 6 の双方を通じて顧客ヘッドオフィスに二重到着することを防止することができる。

【 0 1 2 2 】

その他

上述した実施形態は、以下の発明を開示する。以下の発明は、本発明の目的を逸脱しない範囲で、必要に応じて適宜組み合わせることができる。

(付記 1) 単一のアクセス回線 (21, 22) を夫々有する複数の第 1 の拠点 (102, 103, 104, 105) と、少なくとも二つのアクセス回線 (25, 26) を有する第 2 の拠点 (101) とを含む複数の拠点間 (101, 102, 103, 104, 105) を結ぶ仮想プライベート網 (V P N) サービスを提供するための複数の V P N 装置 (P E # 1, P E # 2, P E # 3, P E # 4) を備える V P N システム (100) において、前記複数の第 1 の拠点の 1 つ (105) が有する単一のアクセス回線 (24)、及び前記第 2 の拠点 (101) が有する少なくとも二つのアクセス回線の一方 (25) が接続される V P N 装置 (P E # 1) であって、

20

前記複数の第 1 の拠点の 1 つ (105) が有する単一のアクセス回線 (24) が接続され、前記第 1 の拠点 (105) を含む少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第 1 のフォワーディングテーブル (38A) に従ってフレーム転送処理を行う第 1 の仮想 V P N 装置 (P E # 1-1) と、

前記第 2 の拠点 (101) が有する少なくとも二つのアクセス回線の一方 (25) が接続され、前記第 2 の拠点 (101) を含む少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第 2 のフォワーディングテーブル (38B) に従ってフレーム転送処理を行う第 2 の仮想 V P N 装置 (P E # 1-2) であって、前記少なくとも二つのアクセス回線の他方 (26) が接続された他の V P N 装置 (P E # 4) へのフレーム転送を行わない設定を有する第 2 の仮想 V P N 装置 (P E # 1-2) と

30

を含む V P N 装置。 (1) (図 1 3、図 9、図 1 0)

(付記 2) 前記第 1 の仮想 V P N 装置 (P E # 1-1) は、他の V P N 装置の総て (P E # 2, P E # 3, P E # 4) と擬似回線を介してフルメッシュ状に接続されており、

前記第 2 の仮想 V P N 装置 (P E # 1-2) は、前記少なくとも二つのアクセス回線の他方 (26) が接続された他の V P N 装置 (P E # 4) を除く他の V P N 装置の総て (P E # 2, P E # 3) と擬似回線を介してフルメッシュ状に接続されており、

40

前記第 1 の仮想 V P N 装置 (P E # 1-1) と前記第 2 の仮想 V P N 装置 (P E # 1-2) とは擬似回線を介して接続されており、

前記第 1 及び第 2 の仮想 V P N 装置 (P E # 1-1, P E # 1-2) の夫々は、対応するアクセス回線 (24, 25) から受信されたフレームを他のアクセス回線及び擬似回線へ転送することを許容し、且つ擬似回線から受信されたフレームを他の擬似回線を除くアクセス回線 (25, 26) に転送する設定を有する

付記 1 に記載の V P N 装置。 (2) (図 1 3、図 9、図 1 0)

(付記 3) 前記少なくとも二つのアクセス回線の他方 (25) が接続された他の V P N 装置 (P E # 4) が、前記複数の第 1 の拠点の 1 つ (105) と異なる第 1 の拠点 (104) が有する単一のア

50

クセス回線(23)が接続され、前記第2の拠点(101)を含まない少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第1のフォワーディングテーブル(38A)に従ってフレーム転送処理を行う第3の仮想VPN装置(PE#4-2)、及び前記第2の拠点(101)が有する少なくとも二つのアクセス回線の他方(26)が接続され、前記第2の拠点(101)を含む少なくとも二つの拠点間で送受信すべきフレームの転送処理用の第2のフォワーディングテーブル(38B)に従ってフレーム転送処理を行う第4の仮想VPN装置(PE#4-1)を含む場合には、前記第2の仮想VPN装置(PE#1-2)は、前記第4の仮想VPN装置(PE#4-1)へのフレーム転送を行わず、且つ前記第4の仮想VPN装置(PE#4-1)からフレームを受信しないようになっている

付記1記載のVPN装置。(3)(図8,図9,図10)

(付記4) 前記第1の仮想VPN装置(PE#1-1)は、前記第3及び第4の仮想VPN装置(PE#4-2, PE#4-1)、及び前記他のVPN装置(PE#4)を除く残りの他のVPN装置(PE#2, PE#3)の総てと擬似回線を介してフルメッシュ状に接続されており、

前記第2の仮想VPN装置(PE#1-2)は、前記第4の仮想VPN装置(PE#4-1)、及び前記第4の仮想VPN装置(PE#4-1)を含む他のVPN装置(PE#4)を除く残りの他のVPN装置(PE#2, PE#3)の総てと擬似回線を介してフルメッシュ状に接続されており、

前記第1の仮想VPN装置(PE#1-1)と前記第2の仮想VPN装置(PE#1-2)とは擬似回線を介して接続されており、

前記第1の仮想VPN装置(PE#1-1)及び第2の仮想VPN装置(PE#1-2)の夫々は、対応するアクセス回線(24,25)から受信されたフレームを他のアクセス回線及び擬似回線へ転送することを許容されており、且つ擬似回線から受信されたフレームを他の擬似回線を除くアクセス回線に転送することを許容されている

付記3に記載のVPN装置。(4)(図8,図9,図10)

(付記5) 前記第2の仮想VPN装置(PE#1-2)は、

フレーム送信元からフレームを受信するための二つの擬似回線を収容し、二つの擬似回線でほぼ同時に同一のフレームが受信された場合に、このフレームが前記フレーム送信元でのフラッディングによって受信されたフラッディングフレームであることを検出する検出部(32)と、

フラッディングフレームの転送先を第2のフォワーディングテーブル(38B)に従って決定するフォワーディング部(31B)と、

決定されたフラッディングフレームの転送先が前記少なくとも二つのアクセス回線の一方(25)を含む場合に、該フラッディングフレームを所定のフィルタ条件に従って廃棄するフィルタ部(33)であって、当該フラッディングフレームと同一のフレームが前記他のVPN装置(PE#4)から前記第2の拠点(101)へ転送される場合に、当該フラッディングフレームを廃棄するフィルタ部(33)と

を含む付記1~4のいずれかに記載のVPN装置。(図7,図9,図11)

(付記6) 前記第2の仮想VPN装置(PE#1-2)は、

前記少なくとも二つのアクセス回線の他方(26)の状態を示すアクセス回線状態メッセージを受信する受信部(36)と、

前記受信部(36)で前記少なくとも二つのアクセス回線の他方(26)の異常を示すアクセス回線状態メッセージが受信された場合に、前記フィルタ部(33)に設定されているフィルタ条件を変更するフィルタ制御部(37)と

をさらに含む付記5記載のVPN装置。(図9,図11,図12)

(付記7) 前記第2の仮想VPN装置(PE#1-2)は、前記少なくとも二つのアクセス回線の一方(25)の状態を監視する監視部(34)と、

前記監視部(34)の監視結果に基づくアクセス回線状態を含むアクセス回線状態メッセージを前記他のVPN装置(PE#4)へ送信する送信部(35)と

をさらに含む付記6記載のVPN装置。

(付記8) 前記フィルタ制御部(37)は、周期的に受信すべきアクセス回線状態メッセージが所定時間前記受信部(36)で受信されなかった場合に、前記他のVPN装置(PE#4)に異

10

20

30

40

50

常が発生したと判断して、前記フィルタ条件の変更を行う
付記 6 又は 7 記載の V P N 装置。

(付記 9) 単一のアクセス回線を夫々有する複数の第 1 の拠点(102,103,104,105)と、少なくとも二つのアクセス回線(25,26)を有する第 2 の拠点(101)とを含む複数の拠点間を結ぶ仮想プライベート網(V P N)サービスを提供するための複数の V P N 装置(PE#1,PE#2,PE#3,PE#4)を備える V P N システムにおいて、前記第 2 の拠点(101)が有する少なくとも二つのアクセス回線の一方(25)が接続される V P N 装置(PE#1)であって、

フレーム送信元(PE#2)からフレームを受信するための二つの擬似回線を収容し、二つの擬似回線でほぼ同時に同一のフレームが受信された場合に、これらのフレームがフレーム送信元(PE#2)でのフラッディングによって到着したフラッディングフレームであることを検出する検出部(11,32)と、

前記第 2 の拠点(101)を含む拠点間で送受信すべきフレーム転送処理用のフォワーディングテーブル(38A)に従ってフラッディングフレームの転送先を決定するフォワーディング部(12,31B)と、

決定されたフラッディングフレームの転送先が前記少なくとも二つのアクセス回線の一方(25)を含む場合に、該フラッディングフレームを所定のフィルタ条件に従って廃棄するフィルタ部(13,33)であって、前記少なくとも二つのアクセス回線の他方(26)が接続された他の V P N 装置(PE#4)から前記第 2 の拠点(101)へ当該フラッディングフレームと同一のフレームが転送される場合に、当該フラッディングフレームを廃棄するフィルタ部(13,33)と

を含む V P N 装置。(5) (図 7 , 図 8 , 図 9 , 図 1 1)

(付記 1 0) 前記少なくとも二つのアクセス回線の他方(26)の状態を示すアクセス回線状態メッセージを受信する受信部(36)と、

前記受信部(36)で前記少なくとも二つのアクセス回線の他方(26)の異常を示すアクセス回線状態メッセージが受信された場合に、前記フィルタ部(33)に設定されているフィルタ条件を変更するフィルタ制御部(37)と

をさらに含む付記 9 記載の V P N 装置。(6) (図 8 , 図 9 , 図 1 1)

(付記 1 1) 前記少なくとも二つのアクセス回線の一方(25)の状態を監視する監視部(34)と、

前記監視部(34)の監視結果に基づくアクセス回線状態を含むアクセス回線状態メッセージを前記他の V P N 装置(PE#4)へ送信する送信部(35)と

をさらに含む付記 1 0 記載の V P N 装置。(図 8 , 図 9 , 図 1 1)

(付記 1 2)

前記フィルタ制御部は、周期的に受信すべきアクセス回線状態メッセージが所定時間前記受信部で受信されなかった場合に、前記他の V P N 装置に異常が発生したと判断して、前記フィルタ条件の変更を行う

付記 1 0 又は 1 1 記載の V P N 装置。(7) (図 8 , 図 9 , 図 1 1)

【図面の簡単な説明】

【 0 1 2 3 】

【図 1】図 1 は、E S R P (登録商標)の動作説明図である。

【図 2】図 2 は、E S R P (登録商標)の動作説明図であって、現用系(アクティブ側)の障害発生時の様子を示す。

【図 3】図 3 は、V P L S の動作説明図である。

【図 4】図 4 は、V P L S の動作説明図であって、V P L S 網と顧客拠点との間にループが発生した様子を示す。

【図 5】図 5 は、V P L S の動作説明図であって、V P L S 網からのフレームが顧客拠点に二重到着する様子を示す。

【図 6】図 6 は、本発明に係る V P L S システムにおいて、ループの発生を回避するための手段を説明する図である。

【図 7】図 7 は、本発明に係る V P L S システムにおいて、フレームの二重到着を回避す

10

20

30

40

50

るためのVPLS装置(PE)の構成例を示す図である。

【図8】図8は、本発明の具体例に係るVPLSシステム(VPLS網)の構成例を示す図である。

【図9】図9は、図8に示したPE#1(VPLS装置)のブロック構成例を示す図である。

【図10】図10は、図8及び図9に示したPE#1が保持するフォワーディングテーブルの例を示す図である。

【図11】図11は、図9に示したフレームフィルタ部の構成例を示す図である。

【図12】図12は、アクセス回線状態メッセージのフォーマット例を示す図である。

【図13】図13は、本発明に係るVPLSシステムにおいて、仮想PEを有するPEが一つの場合を示す図である。

10

【符号の説明】

【0124】

PE#1～PE#4・・・プロバイダエッジスイッチ(VPLS装置、VPN装置)

PE#1-1, PE#1-2, PE#4-1, PE#4-2・・・仮想PE

5・・・プロバイダMPLS網(プロバイダ網)

A1～A4, 21～26・・・アクセス回線

11, 32・・・MACフォワーディング部

12, 31・・・フラッディング検出部

13, 33・・・フレームフィルタ部

20

34・・・アクセス回線異常検出部

35・・・アクセス回線状態メッセージ受信部

36・・・アクセス回線状態メッセージ送信部

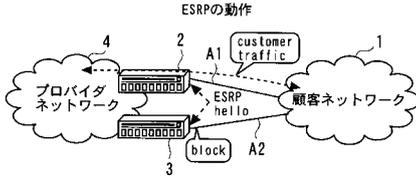
37・・・フィルタ制御部

38・・・フォワーディングテーブル

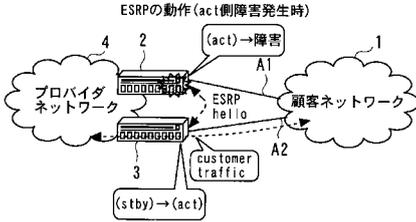
38A・・・エントリ群(第1のフォワーディングテーブル)

38B・・・エントリ群(第2のフォワーディングテーブル)

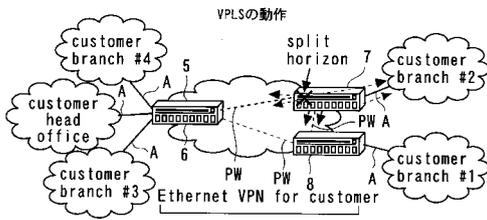
【 図 1 】



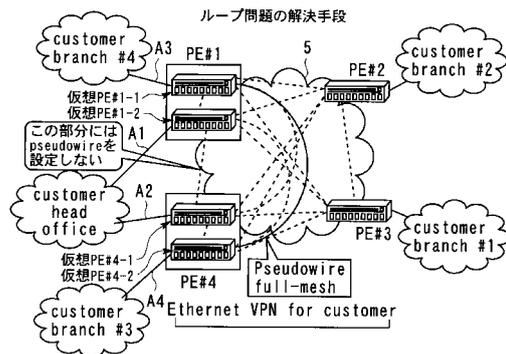
【 図 2 】



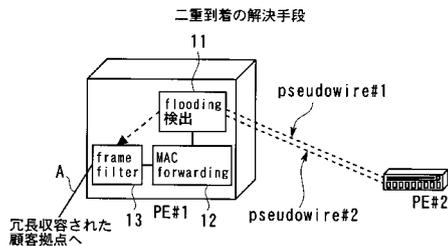
【 図 3 】



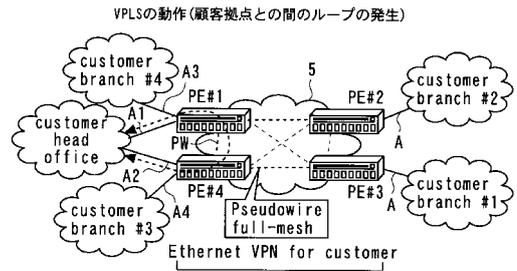
【 図 6 】



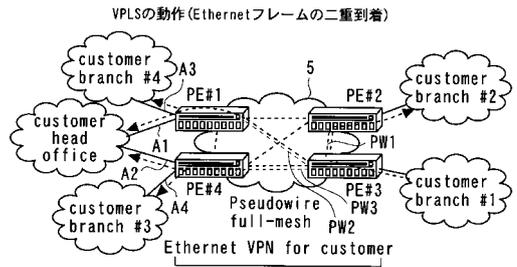
【 図 7 】



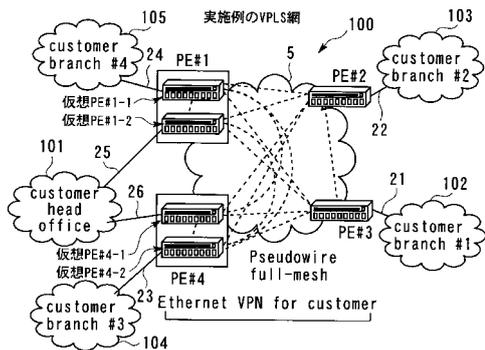
【 図 4 】



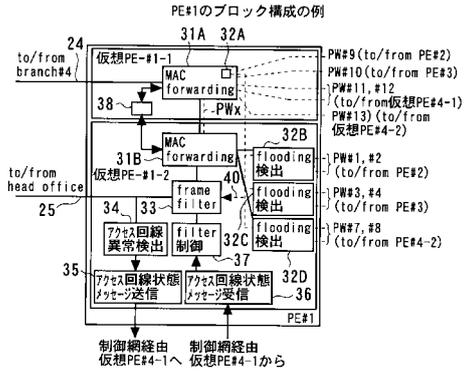
【 図 5 】



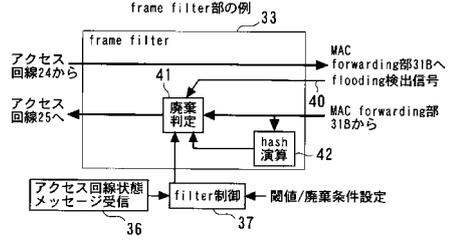
【 図 8 】



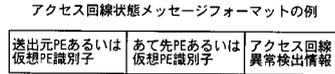
【 図 9 】



【 図 1 1 】



【 図 1 2 】



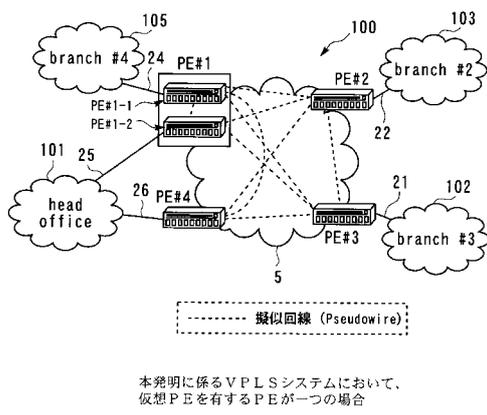
【 図 1 0 】

PE#1のフォーワーディングテーブルの例

VPN番号	仮想PE番号	宛先MAC address	送出先	
38A	#100	#1-1	branch #2の端末1	PW#9
	#100	#1-1	branch #2の端末2	PW#9
	#100	#1-1	branch #3の端末1	PW#13
	#100	#1-1	branch #4の端末1	アクセス回線24
	#100	#1-1	head officeの端末1	仮想PE#1-2
38B	#100	#1-2	branch #2の端末1	PW#1
	#100	#1-2	branch #2の端末2	PW#1
	#100	#1-2	branch #3の端末1	PW#3
	#100	#1-2	branch #4の端末1	仮想PE#1-1
	#100	#1-2	head officeの端末1	アクセス回線25

PW:Pseudowire

【 図 1 3 】



フロントページの続き

Fターム(参考) 5K030 GA11 HA08 HD03 HD06 KA05 LB05