

(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2004-282697

(P2004-282697A)

(43) 公開日 平成16年10月7日(2004.10.7)

(51) Int.Cl.⁷

H04L 12/56

F I

H04L 12/56 200C

テーマコード (参考)

5K030

審査請求 未請求 請求項の数 14 O L 外国語出願 (全 25 頁)

(21) 出願番号 特願2003-361503 (P2003-361503)
 (22) 出願日 平成15年10月22日 (2003.10.22)
 (31) 優先権主張番号 02292681.0
 (32) 優先日 平成14年10月29日 (2002.10.29)
 (33) 優先権主張国 欧州特許庁 (EP)

(71) 出願人 391030332
 アルカテル
 フランス国、75008 パリ、リュ・ラ
 ・ボエティ 54
 (74) 代理人 100062007
 弁理士 川口 義雄
 (74) 代理人 100113332
 弁理士 一入 章夫
 (74) 代理人 100114188
 弁理士 小野 誠
 (74) 代理人 100103920
 弁理士 大崎 勝真
 (74) 代理人 100124855
 弁理士 坪倉 道明

最終頁に続く

(54) 【発明の名称】 トラフィックエンジニアリングの方法、および方法を実施するように構成された入口ルータ

(57) 【要約】

【課題】 パケットネットワーク内のトラフィックを管理する方法を提供すること。

【解決手段】 パケットネットワークの入口ルータと出口ルータの間のトラフィックを管理する方法であって、トラフィックが異なるサービスクラスに属するキューの入口ルータ内でスケジュールされ、トラフィック部分が入口ルータと出口ルータの間の専用のトンネルをたどる方法は、専用のトンネルに向かうトラフィック部分を別個に一時的に記憶すべく、専用のトンネルを流れてようとするトラフィック部分に専用のトンネルキューを準備するステップと、トラフィックトンネルに入る前に専用トンネルに向かうトラフィック部分をシェーピングする更なるステップとを含む。別の実施形態は、異なるサービスクラスに属する1組のキューを、1以上の専用トラフィックトンネルに対して準備すること、ならびに関連シェーパを準備することを含む。

【選択図】 図1

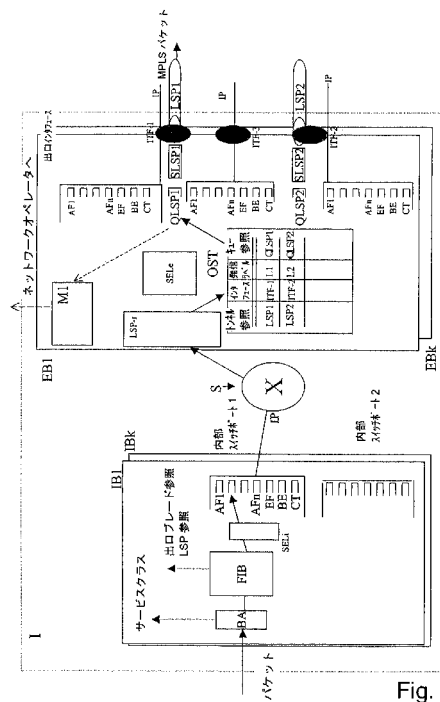


Fig. 1

【特許請求の範囲】**【請求項 1】**

異なるサービスクラスに属するキューにトラフィックが入口ルータ内でスケジュールされ、入口ルータと出口ルータの間の専用トンネルをたどるトラフィック部分を決定するステップを含む、パケットネットワークの入口ルータと出口ルータの間のトラフィックをエンジニアリングする方法であって、

前記専用トンネルに向かう前記トラフィック部分を別々にかつ一時的に記憶するために、前記専用トンネルを通して流れようとする前記トラフィック部分に対し専用のトンネルキューを準備するステップを含み、

トラフィックトンネルに入る前に前記専用トンネルに向かう前記トラフィック部分をシェーピングするステップを更に含むことを特徴とする方法。 10

【請求項 2】

前記専用トラフィックトンネルに関連づけられた 1 組のトンネルキューを準備するステップを含み、前記 1 組のトンネルキューのそれぞれが異なるサービスクラスに属することを特徴とする請求項 1 に記載の方法。

【請求項 3】

前記 1 組のトンネルキューのそれぞれに対し、前記 1 組のトンネルキューのうち前記それぞれのキューからのトラフィックをシェーピングするための別々のシェーパが設けられることを特徴とする請求項 2 に記載の方法。

【請求項 4】

前記 1 組のトンネルキューが、前記入口ルータの同じ出口インタフェースに属する複数の専用トラフィックトンネルに関連づけられることを特徴とする請求項 2 または 3 に記載の方法。 20

【請求項 5】

前記専用トンネルを通るトラフィックを監視するステップと、前記監視の結果を前記専用トンネルに対する予約された帯域幅と比較するステップと、前記比較の結果に応じて、ネットワーク管理者にメッセージを送ることにより、前記ネットワーク管理者に情報を知らせるステップとを含むことを特徴とする請求項 1 から 3 のいずれか一項に記載の方法。

【請求項 6】

前記出口インタフェースにある前記複数の専用トンネルを通るトラフィックを監視するステップと、前記監視の結果を前記複数の専用トンネルに対する予約された帯域幅と比較するステップと、前記比較の結果に応じて、ネットワーク管理者にメッセージを送ることにより、前記ネットワーク管理者に情報を知らせるステップとを含むことを特徴とする請求項 4 に記載の方法。 30

【請求項 7】

前記専用トンネル、または前記複数の専用トンネルを通るトラフィックが、所定の値より大きいことを示すメッセージを受信すると、前記ネットワーク管理者が前記予約された帯域幅を増大させるが、前記専用トンネル、または前記複数の専用トンネルについて、前記入口ルータと前記出口ルータの間の新しい 1 つまたは複数の経路が計算されることを特徴とする請求項 5 または 6 に記載の方法。 40

【請求項 8】

前記トンネルキューまたは前記 1 組のトンネルキューを前記準備するステップが、前記ネットワーク管理者による、前記方法を使用可能にするメッセージの送信に依存することを特徴とする請求項 1 から 7 のいずれか一項に記載の方法。

【請求項 9】

パケットネットワーク内で、出口ルータに至る少なくとも 1 つの専用トンネル (LSP 1、LSP 2) を通って前記パケットネットワークの前記出口ルータにパケットを経路指定するように構成され、異なるサービスクラスに属する少なくとも複数のキュー (AF 1、. . .、Afn、EF、BE、CT) を含み、着信パケットを、それらパケットのサービスクラスに基づいて、またそれらパケットの宛先に基づいて、これらのキューの 1 つに 50

一時的に記憶するように構成された、パケットネットワークの入口ルータ（I）であって、

前記少なくとも1つの専用トンネル（L S P 1、L S P 2）に専用であり且つ関連づけられる、少なくとも1つのトンネルキュー（Q L S P 1、Q L S P 2）を更に含み、

前記入口ルータ内の前記少なくとも1つのトンネルキュー（Q L S P 1、Q L S P 2）に前記着信パケットの一部を一時的に記憶するように更に構成され、

前記少なくとも1つの専用トンネル（L S P 1、L S P 2）に関連づけられ、前記少なくとも1つの専用トンネル（L S P 1、L S P 2）のトラフィックをシェーピングするように構成されている少なくとも1つのトンネルシェーパ（S L S P 1、S L S P 2）を更に含むことを特徴とする入口ルータ（I）。 10

【請求項10】

異なるサービスクラスに属し、前記少なくとも1つの専用トンネルに関連づけられる少なくとも1組のトンネルキューを更に含むことを特徴とする請求項9に記載の入口ルータ（I）。

【請求項11】

前記少なくとも1つの専用トンネルに関連づけられる少なくとも1組のトンネルシェーパを更に含むことを特徴とする請求項10に記載の入口ルータ（I）。

【請求項12】

異なるサービスクラスに属する前記少なくとも1組のトンネルキューが、前記入口ルータの同じ出口インタフェースに属する複数の専用トンネルに関連づけられることを特徴とする請求項10または11に記載の入口ルータ（I）。 20

【請求項13】

前記少なくとも1つの専用トンネルまたは前記複数の専用トンネルのトラフィックを監視し、前記トラフィックを、前記少なくとも1つの専用トンネルまたは前記複数の専用トンネルに対して予約された帯域幅に関係づけられる所定の閾値と比較し、前記比較の結果に応じて、ネットワーク管理者に向けてメッセージを生成するように構成された監視装置（M1）を含むことを特徴とする請求項9から12のいずれか一項に記載の入口ルータ（I）。

【請求項14】

前記少なくとも1つのトンネルキューまたは前記1組のトンネルキューを使用可能にすることに関係する所定のメッセージを前記ネットワーク管理者から受け取り、そのメッセージから前記少なくとも1つの専用トンネルを対象とするパケットを受け取るために前記少なくとも1つのトンネルキューを使用可能にするか否かを決定するように構成されていることを特徴とする請求項9から13のいずれか一項に記載の入口ルータ（I）。 30

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、請求項1の非特徴部分に記載のトラフィックエンジニアリングの方法に関し、また請求項9のプレアンブルに記載の入口ルータに関する。

【背景技術】

【0002】

当技術分野において、かかる方法は、例えばIETFワーキンググループの、インターネットのウェブページ<http://www.ietf.org/rfc/html>上に公開され、「Multi-Protocol Label Switching (MPLS) Support of Differentiated Services」という表題のRFC 3270によってすでに知られている。

【0003】

この文書には、インターネットなどのパケットネットワークの入口ルータ内で、この文書でBehavior Aggregate（動作集約）と呼ばれ、BAと略称される、そのサービスクラスに従ってパケットをキューに入れる基本原理が記載されている。この 50

記載は、同じウェブページで他のRFC、すなわちRFC 3290の記載で補足される。RFC 3290では、BA選別機構(classifier)および異なるキューが更に記載されている。このBA選別機構は、入口ソースルータ内の装置であり、パケットがどのキューに一時的に記憶されるかを決定する。同じウェブページのRFC 3031には、トラフィックが流れ得る専用トンネルを設けるという概念が更に記載されている。

【0004】

したがって、従来技術のインターネット入口ルータは、着信パケットを「標準の」IP経路をたどるものと、トンネル(インターネットの場合には主にMPLSトンネル)を通ろうとするものとに区別するように構成される。さらに、これらの従来技術のルータでは、かかる入口ルータの出口インタフェース当たり複数のキューが存在するように、パケットの異なるサービスクラス間で更に区別をすることができる。これらのキューは、例えばインターネットにおいてはDiffServキューからなり、サービスクラス当たり1つのキューであり、これらのキューの中で、そのインタフェース上を伝送されるはずのすべてのパケットは、それ自体のサービスクラスに従って分類される。この場合、「標準の」IPトラフィックと「トンネルによる」MPLSトラフィックとが区別されないこと、換言すれば、両方のトラフィック型のパケットが同じサービスカテゴリに属する場合には同じキューに記憶されることを理解することが大切である。

【0005】

しかしながら、従来技術の方法および入口ルータには、MPLSトンネルは、トラフィックで容易に過剰負荷となり得るという欠点がある。なぜなら、ネットワーク管理者により最初に通知される、特定のトンネルに対して予約されたこのトンネルの推定帯域幅は、単に予測なだけであり、あまり現実的でないと判明する場合もあり、そのため、通信渋滞問題が起こることもあるからである。したがって、この状態では、MPLSトンネルの対象となるトラフィックとして、トラフィックエンジニアリングの解決方法は利用できない。

【0006】

【非特許文献1】RFC 3270、「Multi-Protocol Label Switching (MPLS) Support of Differentiated Services」、IETFワーキンググループ、ウェブページ<http://ietf.org/rfc.html>

【非特許文献2】RFC 3290、IETFワーキンググループ、ウェブページ<http://ietf.org/rfc.html>

【非特許文献3】RFC 3031、IETFワーキンググループ、ウェブページ<http://ietf.org/rfc.html>

【発明の開示】

【発明が解決しようとする課題】

【0007】

したがって、本発明の一目的は、パケットネットワーク内のトラフィックエンジニアリング、特に特定のトンネルを対象とするトラフィック部のトラフィックエンジニアリングのためのかかる方法を提供することである。

【課題を解決するための手段】

【0008】

本発明によれば、この目的は、請求項1の特徴部分に記載のステップを更に含む方法、および請求項9の特徴部分に更に記載の上記のステップを実施するように構成された入口ルータにより達成される。

【0009】

このようにして、入口ルータ内にトンネルごとの専用トンネルキューを設けることにより、またトンネルキューごとまたはトンネルごとの専用シェーパによりトラフィックを更にシェーピング(shaping)することにより、そのトンネルの対象となるトラフィックをトラフィックエンジニアリングするための簡単な方法が実現される。

【0010】

請求項2および請求項10に、本発明の更なる特徴を記述している。

【0011】

トンネルごとに1組のキューをサービスクラスごとに1つのキューとなるように提供することにより、1つのトンネルに対するサービスクラス間の差別化が実現される。この場合、総トンネルトラフィックのシェーピングが行われ、一方、サービスクラスごとにキューが1つとなるような1組のキューが、そのトンネルに対して作成される。これによる利点は、総トンネルトラフィックはあるシェーパレートに制限されるが、異なる各サービスクラスは、依然としてそのトンネル内のdiffserv特性などのサービスクラスに従って別々に処理されることである。

10

【0012】

異なるサービスクラス間の区別は、請求項3および11に記載しているように、これらのキューのそれぞれに対して別々のシェーパを提供することにより更に精巧にすることができ、それによって、トラフィックエンジニアリングトンネルを更に使用して、複数のサービスクラスをエンジニアリングすることができる。この場合、トンネルのサービスクラスごとに1つのキューおよび関連シェーパを設けることにより、各サービスクラストラフィックを別々に監視し、シェーピングすることが可能になる。

【0013】

本発明の他の特徴を、請求項4および請求項12に記載している。

【0014】

したがって、各キューが異なるサービスクラスに属する1組のキューが、複数のトンネルに対するトラフィックに対して提供され、この複数のトンネルはすべて、この入口ルータの同じ出口インタフェースに属する。

20

【0015】

請求項5、6、および13に記載されているように、特にこの専用のトンネルまたは複数のトンネルを通る負荷またはトラフィックを制御するために、監視装置を設ける。これは、キューから送り出されたパケット数およびパケットサイズ、またはキューから送り出されたオクテット数を定期的に測定することにより実施される。この監視に基づいて、トンネルに対する所定の予約帯域幅との比較を行うことができる。これは、例えば、監視されたトラフィックをこの所定の予約帯域幅に関係づけられた所定の閾値と比較することによって実施することができる。この閾値より大きい場合、ネットワーク管理者への通知メッセージが生成される。次いで、かかるメッセージに基づいて、後者がそのトンネル、または複数のトンネルに対する予約帯域幅を増大させ、それによって、請求項7に記載されているようにこの新しい帯域幅を有する1つまたは複数のトンネル用の新しい経路を計算することができるようになる。さらに、その結果、ネットワーク管理者が専用のトンネルシェーパに新しいシェーピングパラメータを提供することもできるようになる。

30

【0016】

前述の特徴に加えて、本発明の方法は、請求項8および14に更に記載されているように、ネットワーク管理者が所定のメッセージを入口ルータに送ることによって使用可能になる。

40

【0017】

一実施形態についての以下の説明を本発明による入口ルータの詳細を概略的に示す添付図面と併せ参照することにより、本発明の以上およびその他の目的および特徴がより明らかになり、本発明自体を最も良く理解することができよう。

【発明を実施するための最良の形態】

【0018】

本発明は、各着信IPパケットのヘッダに基づく従来のIP転送またはルータごとのネクストホップ計算に加え、ラベルスイッチングされる所定の経路またはトンネルも存在する、パケットネットワーク、例えばインターネットの分野で使用される。図には、入口ルータIが示され、IPパケットにはこのルータのいくつかの入口ブレードIB1ないしI

50

Bkに到達することができる。同図には、入口ブレードIB1に到達するIPパケットが示されている。着信IPパケットが、この入口ルータIから出口ルータ（図示せず）に、従来のIP経路指定を使用して転送されるのか、それともMPLSトンネルを介して転送されるのかは、この入口ルータ内のFIBで示したFIBルックアップ装置内で決定される。このFIBルックアップ装置はさらに、そのパケットを転送するのに、この入口ルータIのどの出口ブレード、およびその出口ブレードのどの出口インタフェースを使用するかを決定するように構成されている。この図には、出口ブレードEB1およびその出口インタフェースITF-1が選択された状態を示す。図に示す実施形態では、入口ルータは、内部スイッチSを介して入口ブレードIB1ないしIBkに結合されたn個のかかる出口ブレードを含む。さらに、このFIB装置の他の機能は、LSP参照とも呼ばれるトンネル参照を決定することであり、それについては、その使用と共にこの明細書の以下の段落で説明する。

10

【0019】

宛先情報に加えて、各着信IPパケットは、例えばDSCPを介して所定のサービスクラスに帰属される。このDSCPは、各パケットのヘッダ中のDifferentiated Service Code Point（差別化サービスコードポイント）マーカの省略語である。これらの別々のクラスに対して予約される、異なる帯域幅に適切かつ十分に対処するために、クラスごとに別々のキューが入口ブレードごとに予測され、これらはAF1ないしAFn、EF、BE、およびCTで示される。これらは、それぞれIETFのDiffServワーキンググループによって標準化されたAssured Forwarding（確実な転送）、Expedited Forwarding（優先転送）、Best Effort（最大努力）、及びControl Traffic（制御トラフィック）の省略語である。これらの異なるクラスに属するトラフィックは、初期化されたまたは更新された帯域幅、およびウェイトや優先順位（実時間または非実時間の）制約などその他の制約に従って、異なるようにスケジューラされ、シェーピングされる。したがって、着信パケットは、まず入口ブレード内のサービスクラスごとに別々のキューに一時的に記憶される。各着信パケットを記憶すべき適切なキューの決定は、BAで示す装置BA-IP選別機構中で実施され、この選別機構が、着信パケットのDSCPマーカなど着信パケット内の情報に基づいて、適切なサービスクラスを決定する。

20

【0020】

図中、点線の矢印で示される、このBAおよびFIB装置内で取り出された情報は、その後、入口ブレードの例えば図中のスイッチポート1などの内部スイッチポートを決定するため、またこの内部スイッチポートに関連づけられる特定のキューを決定するために、SELiで示される入口セクタ内で使用される。パケットは、入口ブレード上で一時記憶するために、このキューに向けて送られる。

30

【0021】

図に示す入口ルータI中で、入口ブレードごとの着信パケットは、更に適切な出口ブレード上の適切な出口インタフェースに向けて転送される。これらの出口インタフェースのそれぞれに、また各出口ブレードごとに、同様な1組のサービスクラスキューが、着信パケットを一時的に記憶するために予測される。図で、出口ブレードEB1は、それぞれITF-1、ITF-2、およびITF-3で示され、また灰色の楕円で示される3つの出口インタフェースを有するものとして示されている。ITF-3というこれらの出口インタフェースの1つだけは、従来のIPトラフィックに属し、従来の1組のサービスクラスキューを有し、この場合にもAF1ないしAFn、EF、BE、およびCTで示される。ITF-1およびITF-2は、従来のIPトラフィックとは違って、MPLSトラフィックなどのトンネルトラフィックをも運ぶように構成されている。したがって、2つのトンネルLSP1およびLSP2は、それぞれITF-1およびITF-2を起点としている。LSP1では、L1は発信MPLSラベルであり、LSP2では、L2が発信ラベルである。これらは図中に、そういうものとしては示されていないが、パケットのさらなる経路指定にとって重要である。

40

50

【0022】

図面中、IPトラフィックを運ぶリンクはIPで示され、トンネルはそれらのトンネル参照によって示されている。

【0023】

この目的で、両方のインタフェースは前述したように従来の1組のキューに結合されるだけでなく、本発明の重要な特徴として、トンネルごとの少なくとも1つの専用キューにも結合される。これについては図から明らかであり、この図では、インタフェースITF-1は、例えばインタフェースITF-3のそれに類似の1組のキューに結合されるだけでなく、QLSP1で示される専用のトンネルキューにも結合される。同様に、従来の1組のキューと違って、専用のトンネルキューQSLP2は、ITF-2に結合される。

10

【0024】

各パケットが一時的に記憶される、出口ブレード上のキューの決定は複数のステップで実施される。まず、図上にLSP-rで示すLSP参照チェック装置は、出口ブレードEB-1上の着信パケットが従来のIP転送をたどる必要があるのか、それともMPLSトンネルをたどる必要があるのかをチェックするように構成されている。従来のIPの場合、入口ブレード上の入口セレクトASELiと同様な機能を有する、SELeで示す出口セレクトが、サービスクラスおよび出口インタフェース参照に基づいて適切な出口インタフェースおよびそのキューを決定する。この情報は、例えば、カプセル化装置（図示せず）の入口ブレード内でIPパケットの前に追加された特定のパケットヘッダから、SELe装置それ自体の内部で導き出される。この特定のヘッダは、入口ルータの入口ブレード内でBAやFIBなどの装置中で以前に決定された、サービスクラス、出口ブレード参照、出口インタフェース参照、LSP参照などのような内部パラメータを含む。

20

【0025】

LSP-r装置により、MPLSトンネルを通してパケットを送るべきであると判明した場合には、図中にOSTで示すアウトセグメントテーブルを使用して、特定のパケットヘッダから抽出可能なトンネル参照またはトンネルラベルに基づいて、適切な記憶キューを決定する。

【0026】

他の実施形態（図示せず）では、同じ出口インタフェースに属する1つまたは複数のトンネルに対して、各サービスクラスについてキューが1つとなる1組のキューさえも存在する。このことにより、1つのトンネルに対して1組のキューが存在する場合は同じトンネル内の、また、同じ出口インタフェースに属する1群のトンネルに対して1組のキューが存在する場合は1群のトンネル内の、異なるサービスクラスにまたがるMPLSトラフィックを更に差別化することが可能になる。

30

【0027】

図に示す実施形態では、各MPLSトンネルに対して1つのキューが予測されているが、1つの関連シェーパもその出口ブレードに存在している。これらのシェーパは、それぞれSLSP1およびSLSP2で示されており、よって、キュー用に構成されたピーク情報速度（Peak Information Rate）などの予約された帯域幅に従って、それぞれのMPLSトンネルLSP1およびLSP2に対してそのトラフィックを適

40

【0028】

さらに、図に示してはいないが、かかるシェーパも各IPキューごとに存在することができることに注意されたい。

【0029】

トンネルシェーパまたはMPLSシェーパについては、別々のシェーパのピーク情報速度をトンネルの予約済み帯域幅に設定した実施形態が可能である。しかしながら、他のシェーパ装置を設けることもでき、その場合にはネットワーク管理者により最初に決定されるその他のトラフィックパラメータが使用される。これらのシェーパは、当業者にはよく知られているので、かかるシェーパについてはさらに詳細には論じないことにする。

50

【0030】

どのキューにMPLSパケットを記憶するかを決定するため、OSTをキュー参照で拡張する。他の実施形態では、トンネル当たり複数のトンネルキューがある場合に、サービスクラスに従って、1つのキュー参照だけが追加されたOSTテーブルを考えることができるが、その場合、この追加参照は、トンネルキューブロックに対する参照となる。次いで、キューブロックの入口で、どの実際のキューをパケットの記憶用に用いるかをさらに決定することができる。ただし、アウトセグメントテーブルを実際のキュー参照で更新することもできる。

【0031】

図に示すように、OSTテーブルは、トンネル参照をこのテーブルへのインデックスとして使用しており、トンネルの発信ラベル(L1またはL2)、出口インタフェース(ITF-1またはITF-2)、キュー参照(QLSP1またはQLSP2)などのエントリを含む。 10

【0032】

図で、各出口ブレードは、さらに監視装置を含む。しかしながら、他の実施形態では、キューごとまたは出口インタフェースごとに監視装置を含むことができる。かかる監視装置の機能は、トンネルを通るトラフィックを監視することである。この機能は、出口ブレードの出口インタフェースのどれかに接続されたキューを監視することにより実施される。その目的で、この装置は、例えば各キューの占有状態をチェックすることにより、キューから送られるトラフィックの量を監視し、これをこのトンネルの最初に予約された帯域幅に関係づけられた所定の閾値と比較するように構成されている。さらに、かかる監視装置は、オーバーフロー状態の場合にネットワーク管理者にメッセージを生成するように構成されている。したがって、それぞれのトンネルキューの占有状態を監視し、オーバーフローの場合に、通信渋滞などのトラフィック問題を示すメッセージをネットワーク管理者向けに生成する。次いで、ネットワーク管理者(図示せず)は、トンネルを適合させることができるが、それは一般におそらく新しい出口ブレードおよび新しい出口インタフェースの選択を含めて、新しい「トンネル経路」を決定することを意味している。これは、この場合にもFIB選択機構にこの情報を提供しなければならないことを意味する。次に、トラフィックを異なるようにシェーピングする必要があるので、そのトンネルに帰属するシェーピング装置にも情報を知らせなければならない。 20 30

【0033】

本発明の方法のもう1つの特徴は、ネットワーク管理者がこの方法を有効にすることができる、したがってトンネルごとに別々のキューを有する特徴を有効にすることができることである。その目的で、例えばSNMPプロトコルと略称されるSimple Network Management Protocol(簡易型ネットワーク管理プロトコル)を用いて、ネットワーク管理者からメッセージが送られる(図示せず)。このプロトコルでは、新しいトンネル構成オブジェクトが、トンネル用のかかる専用キューを使用可能とするように入口ルータに指示または命令する。これは通常、いわゆるMIB(Management Information Base(管理情報ベース)の省略語)の追加管理オブジェクトを用いて実施される。ただし、他の通信手段、例えば、CLI、すなわちコマンドラインインタフェース(Command Line Interface)を使用することも可能である。そのとき、入口ルータは、かかるメッセージを受け取り、トンネルごとにかかる別々のトンネルキューを使用可能にするかどうかの指示をその内容から引き出し、要求された場合にはそのキューを使用可能にするようにも構成されている。別の実施形態では、トンネル当たり、様々なサービスクラスに属する複数のキューが可能であり、入口ルータへのネットワーク管理者からのこのメッセージに、トンネル当たり複数のキューを使用可能にするについての詳細を含めることもできる。同様にこれらの実施形態では、入口ルータはさらに、そのとき、キューを使用可能にするかどうかをこのメッセージ内容から引き出し、それに応じて実施するように構成されている。 40

【0034】

本発明の原理を特定の機器に関して説明してきたが、この説明は例として行ったものにと
すぎず、添付の特許請求の範囲に定義する、本発明の範囲を限定するものではないことが
明確に理解されよう。

【図面の簡単な説明】

【0035】

【図1】本発明による入口ルータの詳細を示す概略図である。

【符号の説明】

【0036】

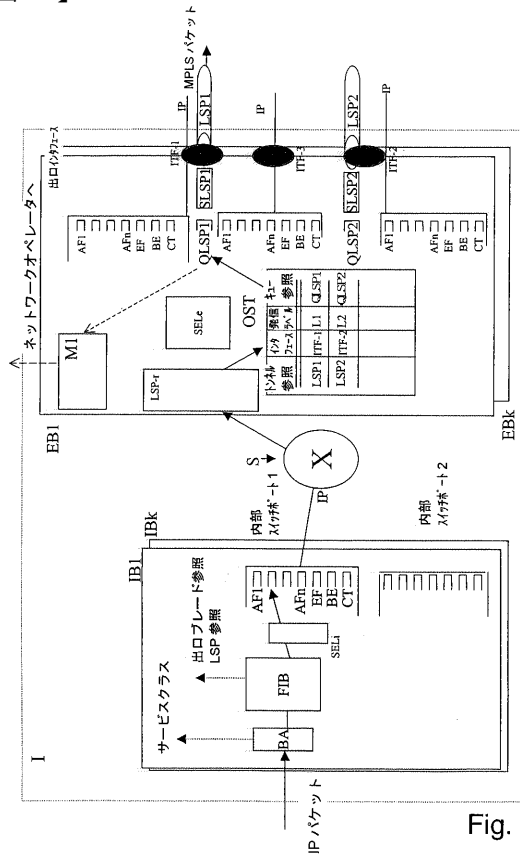
I B 1 ～ I B k 入口ブレード
F I B F I B ルックアップ装置
E B 1 ～ E B k 出口ブレード
I T F - 1、I T F - 2、I T F - 3 出口インタフェース
S 内部スイッチ
D S C P 差別化サービスコードポイント
A F 1 ～ A F n 確実な転送
E F 優先転送
B E 最大努力
C T 制御トラフィック
B A B A - I P 選別機構
S E L i 入口セクタ
S E L e 出口セクタ
L S P 1、L S P 2 トンネル
L 1、L 2 発信 M P L S ラベル
Q L S P 1、Q L S P 2 専用トンネルキュー
L S P - r L S P 参照チェック装置
O S T アウトセグメントテーブル
S L S P 1、S L S P 2 トンネルシェーパ
S N M P 簡易型ネットワーク管理プロトコル
M I B 管理情報ベース
C L I コマンド行インタフェース

10

20

30

Fig. 1



フロントページの続き

(72)発明者 フイフエン・セテイン

ベルギー国、2018・アントワープ、ランゲ・ロザンナストラート・153/11

(72)発明者 リザ・セテイン

ベルギー国、2018・アントワープ、ランゲ・ロザンナストラート・153/11

Fターム(参考) 5K030 HA08 HD03 KA03 LB05 LC02 MB09 MB11

【外国語明細書】

Specification

Title of Invention

METHOD FOR TRAFFIC ENGINEERING AND INGRESS ROUTER

ADAPTED TO PERFORM SUCH A METHOD

The present invention relates to a method for traffic engineering as is described in the non-characteristic part of claim 1, and to an ingress router as is described in the preamble of claim 9.

Such a method is already known in the art, e.g. from RFC 3270 of the IETF working group, which can be publicly found on the Internet on the web-page <http://IETF.org/rfc.html> and which is titled " Multi-Protocol Label Switching (MPLS) Support of Differentiated Services" .

Therein the basic principles for queuing packets according to their service class, in this document called a Behavior Aggregate and abbreviated with BA, within ingress routers of a packet network such as the Internet, is described. This is supplemented by what is described in another RFC at the same webpage, being RFC3290, in which a BA-classifier and the different queues are further described, the BA-classifier being the device within the ingress source router which determines in which queue a packet will be temporarily stored. Furthermore RFC 3031 from the same webpage describes the concept of having dedicated tunnels to which traffic can flow.

State of the art Internet ingress routers are thus adapted to discriminate incoming packets into those following the "normal" IP-route , and those intended to follow the tunnel, in the Internet case being mostly MPLS-tunnels. Moreover, these state of the art routers can further discriminate between the different service classes of the packets such that, per egress interface of such an ingress router, several queues are present. These queues can for instance consist of Diffserv queues in the Internet, and being one per service class, in which all packets intended to be transported over that interface are classified in accordance to their service class. It is important to recognize that in this case no distinction is made between the "normal" IP-traffic, and the "tunnel" MPLS-traffic,

in other words, both traffic type packets are stored in the same queue if these have the same service category.

This state of the art method and ingress router however has the drawback that the MPLS tunnel can be easily overloaded with traffic, since the estimated bandwidth for this tunnel, which is initially communicated by the network administrator and which is reserved for the specific tunnel, is just a prediction which may prove not be very realistic, and which may give rise to congestion problems. In the present situation no traffic engineering solution is thus available for the traffic intended for the MPLS-tunnels.

An object of the present invention is thus to provide such a method for traffic engineering within a packet network, especially for that part of the traffic intended to a specific tunnel .

According to the invention, this object is achieved by the method which further includes the steps as described in the characterising portion of claim 1, and by an ingress router which is adapted to perform these steps as is further described in the characterising portion of claim 9.

In this way, by providing a dedicated tunnel queue per tunnel within the ingress router, and by further shaping the traffic by a dedicated shaper per tunnel queue or per tunnel, a simple method for traffic engineering the traffic intended for the tunnel is provided.

A further characteristic features of the present invention is mentioned in claim 2 and claim 10.

By providing, per tunnel, a set of queues, one per service class, differentiation between the service classes for one tunnel is provided. In this case, total tunnel traffic , is shaped, while a set of queues, one per service class is created for the tunnel. The advantage of this is that the total tunnel traffic is limited at a certain shaper rate while each different service class is still treated separately according to their service class, such as the diffServ characteristics, in the tunnel.

The distinction between the different service classes can be even more further elaborated by providing a separate shaper for each of these queues , as described in claims 3 and 11, such that a traffic engineering tunnel can be further used to engineer multiple service classes. In this case, having one queue

and associated shaper per service class of the tunnel allows monitoring and shaping each service class traffic separately.

Another characteristic feature of the present invention is described in claim 4 and claim 12.

Thereby one set of queues, each queue of the set pertaining to a different service class, is provided for the traffic for a plurality of tunnels, all tunnels of this plurality pertaining to the same egress interface of this ingress router.

A monitoring device is provided, specifically to control the load or traffic via this dedicated tunnel or the plurality of tunnels, as is described in claims 5, 6 and 13. This may be performed by periodically measuring the number of packets and their size sent out from the queues, or the number of octets sent out from the queues. On the basis of this monitoring, a comparison can be made with the predetermined reserved bandwidth for the tunnel. This may for instance be performed by comparing the monitored traffic with a predetermined threshold related to this predetermined reserved bandwidth. If this threshold is exceeded, a notification message to the network administrator is generated. The latter can then, based on such a message, increase the reserved bandwidth for the tunnel or the plurality of tunnels, which may in its turn result in calculating a new path for the tunnel or tunnels with this new bandwidth as described in claim 7. Furthermore, this can also result in providing new shaping parameters by the network administrator to the dedicated tunnel shapers.

In addition to the aforementioned features, the present method is enabled by the network administrator through the sending of a predetermined message to the ingress router, as is further described in claims 8 and 14.

The above and other objects and features of the invention will become more apparent and the invention itself will be best understood by referring to the following description of an embodiment taken in conjunction with the accompanying drawing wherein the figure schematically shows details of an ingress router according to the present invention.

The present invention is used in the field of packet networks, for instance the Internet, wherein, apart from the conventional IP forwarding or next-hop calculation per router, based on the header of each incoming IP packet, also predetermined label switched paths or tunnels are present. In the drawing an ingress router I is depicted to which IP packets may arrive at a number of ingress blades IB1 to IBk. In the drawing an IP packet is depicted which arrives at ingress blade IB1. The determination of whether an incoming IP packet will be forwarded using the conventional IP routing, or will be transferred via the MPLS tunnel, from this ingress router I to an (not shown) egress router, is decided upon within the ingress router, within the FIB-look-up device, denoted FIB. This FIB-look-up device is further adapted to determine which egress blade, and which egress interface of this egress blade of the ingress router I, will be used for sending the packet to. In the figure a situation is depicted whereby egress blade EB1 is selected, and egress interface ITF-1 thereof. In the embodiment depicted in the figure, the ingress router includes n of such egress blades which are coupled, via an internal switch S, to ingress blades IB1 to IBk. Moreover, another function of this FIB-device is the determination of the tunnel reference, also called LSP-reference, which will be described as well as its use, within a further paragraph of this document.

In addition to the destination information, each incoming IP packet is attributed a predetermined service class, via for instance the DSCP which is the abbreviation of Differentiated Services Code Point marker in the header of each packet. For appropriately and adequately coping with the different bandwidth reserved for these separate classes, separate queues per class are foreseen per ingress blade, and which are denoted AF1 to AFn, EF, BE and CT. These are respectively the abbreviation of Assured Forwarding, Expedited Forwarding, Best Effort and Control Traffic as standardized by the DiffServ working group at IETF. Traffic pertaining to these different classes will be scheduled and shaped differently, according to initialized or updated bandwidth and other constraints such as weight, priority (real-time or non-real-time) constraints. Therefore the incoming packets will first be temporarily stored in separate queues, per service

class in the ingress blade. The determination of the appropriate queue wherein each incoming packet is to be stored, is performed in the device BA-IP Classifier, denoted with BA, which determines, based on information within the incoming packet such as the DSCP marker of the incoming packet, the appropriate service class.

The information extracted within the BA and FIB-devices, in the figure denoted with the arrows in dotted lines, is then used within an ingress selector, denoted SELi, in order to determine an internal switch port such as for instance switch port 1 in the figure, of the ingress blade, and to determine a specific queue associated to this internal switch port, towards which the packet will be sent for temporary storage on the ingress blade.

In the ingress router I depicted in the figure, the incoming packets per ingress blade will be further forwarded towards an appropriate egress interface on an appropriate egress blade. To each of these egress interfaces, and for each egress blade, a similar set of service class queues is foreseen for temporarily storing the incoming packets. In the figure egress blade EB1 is depicted as having three egress interfaces, respectively denoted ITF-1, ITF-2, and ITF-3, and indicated by means of the gray ellipse. One of these egress interfaces, being ITF-3 is only pertaining to classical IP-traffic and has the traditional set of service-class queues, again denoted AF1 to Afn, EF, BE and CT. ITF-1 and ITF-2 are, apart from the conventional IP-traffic, also adapted to carry tunnel traffic such as MPLS traffic. Two respective tunnels, LSP1 and LSP2, are therefore originating from respectively ITF-1 and ITF-2. For LSP1, L1 is the outgoing MPLS label, for LSP2, L2 is the outgoing label. These are not shown as such in the figure but are important for the further routing of the packet.

In the drawing, the links carrying the IP-traffic are indicated with IP, whereas the tunnels are indicated by means of their tunnel reference.

To this purpose, both interfaces are not only coupled to the classical set of queues as described before, but, as an important feature of the present invention, also to at least one dedicated queue per tunnel. This is clear from the figure, where interface ITF-1 is not only coupled to a set of queues similar to the

one of for instance interface ITF-3, but is also coupled to a dedicated tunnel queue denoted QLSP1. Similarly, to ITF-2 is coupled a dedicated tunnel queue QSLP2, apart from the conventional set of queues.

The determination of the queue on the egress blade, where each packet will be temporarily stored, is performed in several steps. Firstly a LSP-ref-check device, denoted LSP-r on the figure, is adapted to check whether the incoming packet on the egress blade EB-1 has to follow the classical IP forwarding, or an MPLS-tunnel. If classical IP, an egress selector, denoted SELe, having similar functionality as the ingress selector SELi on the ingress blade, determines the appropriate egress interface and queue thereof, on the basis of the service class and egress-interface reference. This information is for instance derived within the SELe device itself from a special packet header which was added in front of the IP-packet, within an encapsulating device (not shown on the figure) ingress blade. This special header contains internal parameters like service class, egress-blade reference, egress-interface reference, LSP reference etc., which were earlier determined within the ingress blade of the ingress router, within devices such as BA and FIB.

In case the LSP-r device finds out that the packet is to be sent via an MPLS-tunnel, an out-segment table, denoted OST in the figure, is used to determine the appropriate storage queue on the basis of the tunnel reference or tunnel label, extractable from the special packet header.

In another embodiment (not shown on the figure) even a set of queues, one for each service class, for one or more tunnels pertaining to the same egress interface, is present. This allows to further differentiate the MPLS traffic across the different service classes within the same tunnel, in case a set of queues exists for one tunnel, or within a group of tunnels, in case a set queues exists for a group of tunnels pertaining to the same egress interface.

In the shown embodiment, whereby for each MPLS tunnel, one queue was foreseen, also one associated shaper is present in the egress blade. These are respectively denoted SLSP1 and SLSP2, and will then adapt the traffic for the

respective MPLS tunnel LSP1 and LSP2, in accordance with the reserved bandwidth such as the Peak Information Rate configured for the queue.

It can be further remarked that such shapers may also be present, although not shown in the figure, for each IP queue.

For the tunnel or MPLS shapers, embodiments whereby the Peak Information Rate of the separate shapers is set to the reserved bandwidth of the tunnel, are possible. However other shaper devices may be provided, where other traffic parameters, determined initially by the network administrator, are used. Since these shapers are well known to a person skilled in the art, such shapers will not be further discussed into detail.

To determine in which queue an MPLS packet will be stored, the OST is extended with the queue-reference. In another embodiment, in case of several tunnel queues per tunnel, according to their service class, an OST-table with also only one queue reference added can be envisaged, whereby this extra reference will then be a reference to a tunnel-queue-block. At the entry of the queue-block it can then be further determined which actual queue will be taken for the storage of the packet. However, the out-segment table could as well be updated with the actual queue reference.

The OST-table, as depicted in the figure, uses the tunnel reference as index to this table, and includes entries such as the outgoing label of the tunnel (L1 or L2), the egress interface (ITF-1 or ITF-2) and the queue reference (QLSP1 or QLSP2).

In the figure each egress blade further includes a monitoring device. However other embodiments may include monitoring devices per queue, or per egress interface. The function of such a monitoring device is to monitor the traffic via the tunnels. This may be performed by monitoring the queues attached to any of the egress interfaces of an egress blade. To this purpose, this device is adapted to monitor the amount of the traffic sent from the queue, for instance by checking the occupation of each queue, and to compare this with a predetermined threshold related to an initial reserved bandwidth for this tunnel. Furthermore such a monitoring device is further adapted to generate a message

to the network administrator in case of overflow conditions. Thus the occupancy of the respective tunnel queues will be monitored, and in case of overflow, a message will be generated to the network administrator, indicative of traffic problems such as congestion. The network administrator (not shown on the drawing) can then adapt the tunnel, this generally implying determining a new "tunnel path", possibly including the selection of a new egress blade, and a new egress interface. This means that this information again has to be provided to the FIB classifier. Also the shaping device attributed to the tunnel has to be informed since traffic will now have to be differently shaped.

An additional feature of the method of the present invention is that the network administrator can enable this method, thus can enable the feature of having the separate queue per tunnel. To this purpose a message is sent (not shown in the drawing) from the network administrator, for instance by means of the Simple Network Management Protocol, abbreviated by SNMP-protocol, wherein a new tunnel configuration object indicates or orders the ingress router to enable such a dedicated queue for a tunnel. This is usually performed by means of an additional management object of a so-called MIB, being the abbreviation of Management Information Base . However, other means of communication are possible , for instance by using the CLI Command Line Interface. The ingress router is then also adapted to receive such a message, and to extract from its contents the indication whether or not to enable such a separate tunnel queue per tunnel, and to enable the queue in the requested case. In another embodiment, where several queues per tunnel, pertaining to different service classes, are possible, this message from the network administrator to the ingress router may as well contain details about the enabling of the plurality of queues per tunnel. Similarly, in these embodiments the ingress router is then further adapted to extract from the contents of this message whether to enable the queues or not, and accordingly perform so.

While the principles of the invention have been described above in connection with specific apparatus, it is to be clearly understood that this

description is made only by way of example and not as a limitation on the scope of the invention, as defined in the appended claims.

Brief Description of Drawings

Figure 1 schematically shows details of an ingress router according to the present invention.

Claims

1. Method for engineering traffic between an ingress router and an egress router of a packet network, said traffic being scheduled within said ingress router in queues pertaining to different service classes, said method further including a step of determining a part of the traffic which will follow a dedicated tunnel between said ingress and said egress router

characterized in that

said method includes the provisioning of a tunnel queue dedicated to said part of the traffic intended to flow via said dedicated tunnel, for separately and temporarily storing said part of the traffic towards said dedicated tunnel

said method further includes a step of shaping said part of the traffic towards said dedicated tunnel before entering in said traffic tunnel.

2. Method according to claim 1

characterised in that

said method includes the provisioning of a set of tunnel queues, associated to said dedicated traffic tunnel, each tunnel queue within said set pertaining to a different service class .

3. Method according to claim 2

characterised in that

to each tunnel queue of said set a separate shaper is provided for shaping the traffic from said each tunnel queue of said set.

4. Method according to claim 2 or 3

characterised in that

said set of tunnel queues is associated to a plurality of dedicated traffic tunnels, pertaining to the same egress interface of said ingress router.

5. Method according to claim 1, 2 or 3

characterised in that

said method includes a step of monitoring the traffic via said dedicated tunnel, a step of comparing the result of said monitoring with a reserved bandwidth for said dedicated tunnel, and, depending upon the result of said comparison, a step of informing a network administrator by sending a message to said network administrator.

6. Method according to claim 4

characterised in that

said method includes a step of monitoring the traffic via said plurality of dedicated tunnels at said egress interface, a step of comparing the result of said monitoring with a reserved bandwidth for said plurality of dedicated tunnels, and, depending upon the result of said comparison, a step of informing a network administrator by sending a message to said network administrator.

7. Method according to claims 5 or 6

characterised in that

upon receipt of a message indicating that the traffic through said dedicated tunnel, respectively said plurality of dedicated tunnels, exceeds a predetermined value, said network administrator increases the reserved bandwidth, whereas a new path or paths are calculated for said dedicated tunnel, respectively said plurality of dedicated tunnels, between said ingress router and said egress router.

8. Method according to any of the previous claims

characterised in that

said provisioning of said tunnel queue or of said set of tunnel queues is dependent upon the sending, by said network administrator, of a message enabling said method.

9. Ingress router (I) of a packet network, said ingress router being adapted to route packets within said packet network to an egress router of said packet

network via at least one dedicated tunnel (LSP1, LSP2) to said egress router, said ingress router (I) including at least one plurality of queues (AF1,...,Afn, EF, BE, CT) pertaining to different service classes, said ingress router being adapted to temporarily store incoming packets within one of these queues, on the basis of their service class and on the basis of their destination

characterised in that

said ingress router(I) further includes at least one tunnel queue (QLSP1, QLSP2) dedicated and associated to said at least one dedicated tunnel (LSP1, LSP2),

said ingress router (I) is further adapted to temporarily store part of the incoming packets within said at least one tunnel queue (QLSP1, QLSP2) within said ingress router,

whereby said ingress router further includes at least one tunnel shaper (SLSP1, SLSP2) associated to said at least one dedicated tunnel (LSP1, LSP2), and adapted to shape the traffic of said at least one dedicated tunnel (LSP1, LSP2).

10. Ingress router (I) according to claim 9

characterised in that

said ingress router further includes at least one set of tunnel queues, pertaining to different service classes, and associated to said at least one dedicated tunnel.

11. Ingress router (I) according to claim 10

characterised in that

said ingress router further includes at least one set of tunnel shapers associated to said at least one dedicated tunnel.

12. Ingress router (I) according to claim 10 or 11

characterised in that

said at least one set of tunnel queues pertaining to different service classes, is associated to a plurality of dedicated tunnels pertaining to the same egress interface of said ingress router.

13. Ingress router (I) according to claims 9, 10, 11 or 12
characterised in that

said ingress router (I) includes a monitoring device (M1) adapted to monitor the traffic of said at least one dedicated tunnel or of said plurality of dedicated tunnels, to compare said traffic with a predetermined threshold related to a reserved bandwidth for said at least one dedicated tunnel or said plurality of dedicated tunnels, and to generate a message to a network administrator depending on the result of said comparison.

14. Ingress router (I) according to any of the previous claims 9 to 13
characterised in that

said ingress router is further adapted to receive a predetermined message from said network administrator related to the enabling of said at least one tunnel queue or said set of tunnel queues, and to determine therefrom whether or not to enable said at least one tunnel queue for receiving packets intended to said at least one dedicated tunnel.

1. Abstract

A method for engineering traffic between an ingress router and an egress router of a packet network , whereby said traffic is scheduled within said ingress router in queues pertaining to different service classes, and whereby part of the traffic follows a dedicated tunnel between said ingress and said egress router, includes the step of provisioning of a tunnel queue dedicated to said part of the traffic intended to flow via said dedicated tunnel, for separately and temporarily storing said part of the traffic towards said dedicated tunnel, and a further step of shaping said part of the traffic towards said dedicated tunnel before entering in said traffic tunnel. Further embodiments comprise the provisioning of a set of queues, pertaining to the different service classes, to one or more of these dedicated traffic tunnels, as well as the provisioning of associated shapers.

2. Representative Drawing

Fig. 1

Fig. 1

