(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2013-179678
(P2013-179678A)
(43)公開日　平成25年9月9日(2013.9.9)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	***12/859***	***(2013.01)***	H04L	12/859		5K030
H04L	***12/46***	***(2006.01)***	H04L	12/46	B	5K033

審査請求 有　請求項の数 11　ＯＬ　（全 12 頁）

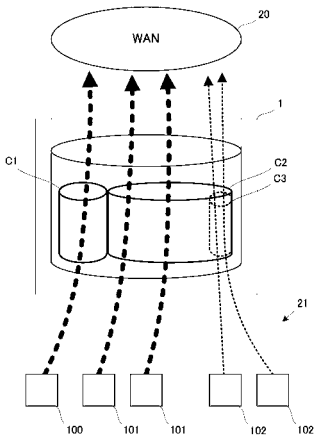
(21)出願番号　特願2013-101673 (P2013-101673)
(22)出願日　平成25年5月13日 (2013.5.13)
(62)分割の表示　特願2006-261832 (P2006-261832)の分割
原出願日　平成18年9月27日 (2006.9.27)

(71)出願人　000004075
ヤマハ株式会社
静岡県浜松市中区中沢町１０番１号
(74)代理人　100123940
弁理士　村上　辰一
(72)発明者　加藤　裕昭
静岡県浜松市中区中沢町１０番１号　ヤマハ株式会社内

Ｆターム(参考)　5K030 GA03 GA13 HD03 HD06 LC01 LC11 MA04 MB09
5K033 AA01 CB06 CB08 DA06 EA02 EA06

(54)【発明の名称】ルータ装置

(57)【要約】
【課題】複数のサービスが同じクラスに分類されている場合でも、そのクラスのトラフィックの逼迫を抑制することができるルータ装置を提供する。
【解決手段】２つのネットワーク間を転送されるパケットを、そのパケットの属性に基づいて、それぞれ優先度または帯域幅が異なる複数のクラスに分類し、各クラスに応じた優先度または帯域幅でそのパケットを転送するＱｏＳ転送制御手段と、一方のネットワークに接続された複数のクライアントによる他方のネットワークとの通信量を、少なくとも１つのクラスにおいて各クライアントのフロー別に監視する監視手段と、監視しているいずれかのクラスにおいていずれかのクライアントの通信量が所定値を超えたとき、この通信量が超過したクライアントのフローのパケットを優先度の低いクラスまたは帯域幅が狭いクラスへ分類を変更することにより、このクライアントの通信を制限する通信制限手段とを備える。
【選択図】　図４



【特許請求の範囲】
【請求項１】
２つのネットワーク間で通信パケットを転送するルータ装置であって、
前記２つのネットワーク間を転送されるパケットを、そのパケットの属性に基づいて、それぞれ優先度または帯域幅が異なる複数のクラスに分類し、各クラスに応じた優先度または帯域幅でそのパケットを転送するＱｏＳ転送制御手段と、
一方のネットワークに接続された複数のクライアントによる他方のネットワークとの通信量を、少なくとも１つのクラスにおいて各クライアントのフロー別に監視する監視手段と、
監視しているいずれかのクラスにおいていずれかのクライアントの通信量が所定値を超えたとき、該通信量が超過したクライアントの前記フローのパケットを優先度の低いクラスまたは帯域幅が狭いクラスへ分類を変更することにより、該クライアントの通信を制限する通信制限手段と、
を備えたルータ装置。
【請求項２】
前記帯域幅が狭いクラスは、前記監視されているクラスとの間で、動的トラフィック制御により可変帯域幅に設定されている請求項１に記載のルータ装置。
【請求項３】
２つのネットワーク間で通信パケットを１または複数のクラスで転送するルータ装置であって、
一方のネットワークに接続された複数のクライアントによる他方のネットワークとの通信量を、少なくとも１つのクラスにおいて各クライアントのフロー別に監視する監視手段と、
監視しているいずれかのクラスにおいていずれかのクライアントの通信量が所定値を超えたとき、該通信量が超過したクライアントの前記フローのパケットの通信を遮断することにより、該クライアントの通信を制限する通信制限手段と、
を備えたルータ装置。
【請求項４】
前記通信制限手段は、特定のクライアントを除外クライアントとして設定し、該除外クライアントの前記監視しているいずれかのクラスにおける通信量が前記所定値を超えても前記通信の制限を行わない請求項１乃至請求項３のいずれかに記載のルータ装置。
【請求項５】
前記通信制限手段は、送信元または宛先ＩＰアドレス、および、送信元または宛先ポート番号のうち少なくとも１つの項目について設定可能である請求項１乃至請求項４に記載のルータ装置。
【請求項６】
前記監視手段は、各クライアントが、前記他方のネットワークに送信する送信パケット、前記他方のネットワークから受信する受信パケットの一方または両方について、その通信量を監視し、
前記通信制限手段は、いずれかのクライアントの送信パケットまたは受信パケットの通信量が所定値を超えたとき、前記送信パケット、受信パケットのうち、前記通信量が所定値を超えた側のパケットについて、前記通信の制限を行う請求項１乃至請求項５のいずれかに記載のルータ装置。
【請求項７】
前記監視手段は、各クライアントが、前記他方のネットワークに送信する送信パケット、前記他方のネットワークから受信する受信パケットの一方または両方について、その通信量を監視し、
前記通信制限手段は、いずれかのクライアントの送信パケットまたは受信パケットの通信量が所定値を超えたとき、前記送信パケット、受信パケットの両方について、前記通信の制限を行う請求項１乃至請求項５のいずれかに記載のルータ装置。

【請求項８】
前記通信制限手段は、送信パケットおよび受信パケットのうち、監視するパケットまたは制限するパケットを設定可能である請求項が自由に設定できる請求項６または請求項７に記載のルータ装置。
【請求項９】
前記２つのネットワークは、有線ローカル・エリア・ネットワークおよび広域ネットワークであり、
前記ＱｏＳ転送制御手段、前記監視手段、および、前記通信制限手段は、前記有線ローカル・エリア・ネットワークから前記広域ネットワーク（以下、ＷＡＮと呼ぶ）に転送されるパケットについて上記処理を行う請求項１乃至請求項５のいずれかに記載のルータ装置。
【請求項１０】
前記通信制限手段は、前記通信の制限を、制限の開始から一定時間が経過したのち解除する請求項１乃至請求項８のいずれかに記載のルータ装置。
【請求項１１】
２つのネットワーク間で通信パケットを転送するルータ装置であって、
前記２つのネットワーク間を転送するパケットを、そのパケットの属性に基づいて、それぞれ優先度または帯域幅が異なる複数のクラスに分類し、各クラスに応じた優先度または帯域幅でそのパケットを転送するＱｏＳ転送制御手段と、
一方のネットワークに接続された複数のクライアントの、他方のネットワークとの通信量を、少なくとも１つのクラスにおいて各クライアント別に監視する監視手段と、
監視しているいずれかのクラスにおいていずれかのクライアントの通信量が所定値を超えたとき、該通信量が超過したクライアントが少なくとも該クラスにおいて送信または受信するパケットを優先度の低いクラスまたは帯域幅が狭い制限クラスへ分類を変更することにより、該クライアントの通信を制限する通信制限手段と、
前記制限クラスの数、および、その優先度または帯域幅を設定する設定手段と、
を備えたルータ装置。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、帯域幅の異なるネットワーク間を接続するルータ装置に関する。
【背景技術】
【０００２】
ルータ装置は、異なるネットワーク間を接続するレイヤ３の装置であるが、ＬＡＮからインターネットなどのＷＡＮ回線に接続する場合、限られたＷＡＮ帯域をＬＡＮの同一セグメントに存在する複数のクライアントＰＣで分け合いながら通信をすることになる。一般的にＬＡＮ回線よりＷＡＮ回線の帯域の方が狭いため、各クライアントＰＣ間でＷＡＮ帯域の奪い合いが発生し、あるクライアントが帯域を占有してしまうと他のクライアントは満足に通信ができないという状況が起こり得る。
【０００３】
ルータは、ＬＡＮ側の各クライアントから送られてきたパケットをキューに蓄積し、これを所定の順序でＷＡＮに送出してゆくが、ＬＡＮの帯域幅に比べてＷＡＮの帯域幅が狭い場合、一定時間以内に送信できなかったパケットは破棄される。
【０００４】
しかし、パケットが破棄されるとレスポンスが極端に遅くなる等の問題が発生するため、音声信号を伝送するＶｏＩＰ等の特定種類のネットワークサービスは、正常なサービスを維持するためには、パケットが破棄されないようなトラフィックを確保することが必要となる。
【０００５】
そこで、ＷＡＮの帯域幅が限られていても特定のサービスの通信パケットを優先的に処

理して、サービスの品質を確保するＱｏＳ（Quality of Service)という技術が実用化されている（たとえば非特許文献１）。ＱｏＳの代表的なパケット制御方式として帯域制御方式および優先制御方式がある。

【０００６】

帯域制御方式は、ネットワークを用いる複数のサービスをクラス分けし、各クラス毎に使用できる上限帯域を割り当てる方法である。そして、ネットワーク上に流れているパケットについて送出元ＩＰアドレス、宛先ＩＰアドレス、アプリケーション毎のポート番号等により、そのパケットがどのサービスのものかを識別し、そのクラスに割り当てられた帯域の範囲内でそのパケットを処理する。この方式によれば、各サービスは、自己が属するクラスに割り当てられた帯域までしか使用できないため、複数のサービスを同時に使用しても他のクラスのサービスに影響をあたえない。

【０００７】

この方式を用いて、ＶｏＩＰ等のパケット破棄が許容されないサービスを特定のクラス（クラス１）に分類して他のサービスのクラス（クラス２）とクラスを分けることにより、クラス２でトラフィックの逼迫が生じていても、クラス１で通信するＶｏＩＰに影響を及ぼさない。

【先行技術文献】

【非特許文献】

【０００８】

【非特許文献１】「ＱｏＳとは？：ＱｏＳ機能を利用するヤマハルーター」、［online］、ヤマハ株式会社、［平成18年9月4日検索］、インターネット〈URL：http://netvolante.jp/solution/advanced/qos/about.html〉

【発明の開示】

【発明が解決しようとする課題】

【０００９】

このように、特定サービスを別クラスに分類することによって、異なるクラスのトラフィックの逼迫からは解放されるが、同じクラスに複数のサービスが分類されている場合には、同じクラスの他のサービスが帯域を占有してしまうと、やはりトラフィックの逼迫が生じてしまうという問題点があった。

【００１０】

すなわち、図５に示すように、クラス１のＶｏＩＰは常時安定した通信を行うことができるが、多数のサービスが分類されているクラス２において、ファイル交換ソフトが動作しているクライアントＰＣやウィルスに感染し膨大なスパムメールが送信されているクライアントＰＣ等の異常なクライアント１０２がクラス２に割り当てられている通信帯域を占有してしまった場合、他の一般のクライアント１０１が正常な通信を行えなくなってしまうという問題点があった。

【００１１】

また、このトラフィックの逼迫は、上記例において、クラス１にＶｏＩＰ以外に他のサービスが分類された場合にも起こり得る問題である。

【００１２】

一方、他のサービスによってトラフィックの逼迫が生じないように、各サービスをそれぞれ別々のクラスに分類しておくことも考えられるが、ネットワークを介して通信するサービスは非常に多数にのぼるため、それぞれに固定的に帯域を割り当ててしまうことは、却って帯域を無駄にし、通信効率を低下させてしまうことになる。

【００１３】

この発明は、複数のサービスが同じクラスに分類されている場合でも、そのクラスのトラフィックの逼迫を抑制することができるルータ装置を提供することを目的とする。

【課題を解決するための手段】

【００１４】

この発明の第１の側面によるルータ装置は、２つのネットワーク間で通信パケットを転

送するルータ装置であって、ＱｏＳ転送制御手段、監視手段、および、通信制限手段を備える。ＱｏＳ転送制御手段は、２つのネットワーク間を転送されるパケットを、そのパケットの属性に基づいて、それぞれ優先度または帯域幅が異なる複数のクラスに分類し、各クラスに応じた優先度または帯域幅でそのパケットを転送する。監視手段は、一方のネットワークに接続された複数のクライアントによる他方のネットワークとの通信量を、少なくとも１つのクラスにおいて各クライアントのフロー別に監視する。通信制限手段は、監視しているいずれかのクラスにおいていずれかのクライアントの通信量が所定値を超えたとき、この通信量が超過したクライアントのフローのパケットを優先度の低いクラスまたは帯域幅が狭いクラスへ分類を変更することにより、このクライアントの通信を制限する。

【００１５】

帯域幅が狭いクラスが、前記監視されているクラスとの間で、動的トラフィック制御により可変帯域幅に設定されていてもよい。

【００１６】

この発明の第２の側面によるルータ装置は、２つのネットワーク間で通信パケットを転送するルータ装置であって、ＱｏＳ転送制御手段、監視手段、および、通信制限手段を備える。ＱｏＳ転送制御手段は、２つのネットワーク間を転送されるパケットを、そのパケットの属性に基づいて、それぞれ優先度または帯域幅が異なる複数のクラスに分類し、各クラスに応じた優先度または帯域幅でそのパケットを転送する。監視手段は、一方のネットワークに接続された複数のクライアントによる他方のネットワークとの通信量を、少なくとも１つのクラスにおいて各クライアントのフロー別に監視する。通信制限手段は、監視しているいずれかのクラスにおいていずれかのクライアントの通信量が所定値を超えたとき、この通信量が超過したクライアントのフローのパケットの通信を遮断することにより、このクライアントの通信を制限する。

【００１７】

通信制限手段が、特定のクライアントを除外クライアントとして設定し、監視しているいずれかのクラスにおける除外クライアントの通信量が所定値を超えても通信の制限を行わないようにしてもよい。

【００１８】

通信制限手段が、送信元または宛先ＩＰアドレス、および、送信元または宛先ポート番号のうち少なくとも１つの項目について設定可能としてもよい。

【００１９】

監視手段が、各クライアントが他方のネットワークに送信する送信パケット、各クライアントが他方のネットワークから受信する受信パケットの一方または両方についてその通信量を監視し、通信制限手段が、いずれかのクライアントの送信パケットまたは受信パケットの通信量が所定値を超えたとき、送信パケット／受信パケットのうち通信量が所定値を超えた側のパケットについて通信の制限を行うようにしてもよい。

【００２０】

監視手段が、各クライアントが他方のネットワークに送信する送信パケット、各クライアントが他方のネットワークから受信する受信パケットの一方または両方についてその通信量を監視し、通信制限手段が、いずれかのクライアントの送信パケットまたは受信パケットの通信量が所定値を超えたとき、送信パケット／受信パケットの両方について通信の制限を行うようにしてもよい。

【００２１】

通信制限手段が、送信パケットおよび受信パケットのうち、監視するパケットまたは制限するパケットを設定可能であってもよい。

【００２２】

２つのネットワークが、有線ローカル・エリア・ネットワークおよび広域ネットワークであり、ＱｏＳ転送制御手段、前記監視手段、および、前記通信制限手段が、有線ローカル・エリア・ネットワークから広域ネットワークに転送されるパケットについて上記の処

理を行うものであってもよい。
【００２３】
通信制限手段は、通信の制限を、制限の開始から一定時間が経過したのち解除してもよい。
【００２４】
この発明の第３の側面によるルータ装置は、ＱｏＳ転送制御手段、監視手段、通信制限手段、および、設定手段を備える。ＱｏＳ転送制御手段は、２つのネットワーク間を転送するパケットを、そのパケットの属性に基づいて、それぞれ優先度または帯域幅が異なる複数のクラスに分類し、各クラスに応じた優先度または帯域幅でそのパケットを転送する。監視手段は、一方のネットワークに接続された複数のクライアントの、他方のネットワークとの通信量を、少なくとも１つのクラスにおいて各クライアント別に監視する。通信制限手段は、監視しているいずれかのクラスにおいていずれかのクライアントの通信量が所定値を超えたとき、この通信量が超過したクライアントが少なくともこのクラスにおいて送信または受信するパケットを優先度の低いクラスまたは帯域幅が狭い制限クラスへ分類を変更することにより、このクライアントの通信を制限する。設定手段は、制限クラスの数、および、その優先度または帯域幅を設定する。
【発明の効果】
【００２５】
この発明によれば、特定のフローの通信量があるしきい値を超えたとき、そのフローが特定のサービス機能に占有されていると予想して、トラフィックの逼迫を防止するために、そのフローの通信を制限する。これにより、帯域を有効に活用しつつ、逼迫を効果的に抑制することができる。
【図面の簡単な説明】
【００２６】
【図１】この発明の実施形態であるルータ装置のブロック図
【図２】同ルータ装置のフラッシュメモリに記憶されるＱｏＳおよびＤＣＣのルール設定テーブルを示す図
【図３】同ルータ装置の動作を示すフローチャート
【図４】前記ＱｏＳおよびＤＣＣが適用された場合のトラフィック状況を説明する図
【図５】前記ＱｏＳのみが適用された場合のトラフィック状況を説明する図
【発明を実施するための形態】
【００２７】
図面を参照してこの発明の実施形態について説明する。図１は、この発明の実施形態であるルータ装置のブロック図である。
【００２８】
ルータ装置は、２つのネットワークをつなぐ機器である。この実施形態では、一般的なルータ装置であるブロードバンドルータについて説明する。ブロードバンドルータは、インターネット等のＷＡＮとＬＡＮとを常時接続する機器として機能する。
【００２９】
図１において、ルータ装置１は、４つのＬＡＮ側ポート１４および１つのＷＡＮ側ポート１６を備えている。ＷＡＮ側ポート１６は、インターネットサービスを提供するＩＳＰ等に接続される。ＷＡＮ側ポート１６は、ＰＨＹチップ１５を介してＣＰＵ１０に接続される。
【００３０】
４つのＬＡＮ側ポート１４には、それぞれクライアント装置（不図示）が接続される。これらＬＡＮ側ポート１４は、レイヤ２スイッチチップ１３に接続されている。レイヤ２スイッチチップ１３は、ＬＡＮ側ポート１４に接続される複数のクライアント装置間の通信を制御する。また、このレイヤ２スイッチチップ１３には前記ＣＰＵ１０も接続されている。ＣＰＵ１０は、ＷＡＮ側ポート１６とＬＡＮ側ポート１４との通信を制御する。
【００３１】

なお、この実施形態では、ＷＡＮ－ＬＡＮ間の通信を制御する制御部としてＣＰＵ１０を用いているが、ネットワークプロセッサという専用ＬＳＩを用いてもよい。

【００３２】

ＣＰＵ１０には、フラッシュメモリ１１およびＲＡＭ１２が接続されている。フラッシュメモリ１１は、ルータ装置の機能を実現するのための動作プログラム、各種設定テーブルを記憶しているとともに、図２に示すような、ＱｏＳ機能実現のためのクラス設定テーブル、ＤＣＣ（後述）機能実現のためのルール設定テーブル等を記憶している。ＲＡＭ１２は、通信状況等を記憶する。

【００３３】

ＣＰＵ１０は、入力したパケットに対してルーティングやアドレス／ポート変換等を行う。ルーティングは、ＬＡＮ側ポート１４から入力したパケットのうち、送信先ＩＰアドレスがＬＡＮ側に存在するサブネットを指していれば再びＬＡＮ側へ戻し、そうでなければＷＡＮ側ポート１６へ転送するというように、あらかじめ決められた経路制御規則に基づいて、パケットを適切なインタフェースへと送信する機能である。アドレス／ポート変換とは、ＮＡＴやＩＰマスカレードの実現のため、パケットに含まれるＩＰアドレスやポート番号フィールドなどを書き換えてから配送する機能である。

【００３４】

また、このルータ装置１は、ＱｏＳ(Quality of Service)機能を備えている。ＱｏＳ機能は、通信パケットを複数のクラス（クラス１、クラス２）に分類して処理することにより、通信帯域が十分でない通信回線においても特定の通信パケットが破棄されないようにする技術である。このＱｏＳ機能は、帯域の広いネットワーク（ＬＡＮ）から帯域の狭いネットワーク（ＷＡＮ）への通信において特に有効である。なお、設定するクラスの数は２つに限定されず、３以上であってもよい。

【００３５】

ＱｏＳ機能を用いたクラス別のパケット転送は、一般的には次のような手順で行う。

（１）受信したパケットを、送信元/宛先ＩＰアドレス、送信元／宛先ポート番号（アプリケーション）、入力インタフェース等の属性に基づいて分類する。

（２）分類されたパケットに対し、予め設定されているクラス分け条件に基づいて、所属クラスを識別するためのマーキングを行う。

（３）マーキングを参照して、各パケットをその所属クラスのキューに登録する。

（４）各クラスのキューに登録されたパケットを、定められた帯域制御方式または優先制御方式に基づいて転送する。

【００３６】

帯域制御方式は、各クラス毎に予め帯域を割り当て（予約）しておく方式である。各クラスの通信は、予め割り当てられた帯域までしか使用できないためクラス２のトラフィックが逼迫しても、クラス１の通信には影響を及ぼさない。

【００３７】

優先制御方式は、クラス１の通信パケットをクラス２の通信パケットに対して優先的に処理するようにルールづけておき、クラス２のキューに送信パケットが溜まっていても、後からクラス１のキューに登録されたパケットを優先的に処理する方式である。この方式では、ネットワークのトラフィックが逼迫している状況でもクラス１のパケットが滞留することがない。

【００３８】

なお、以下の実施形態では、説明を簡略化するため、通信パケットを、図２（Ａ）に示すような２クラスに分類した例について説明する。

【００３９】

図２（Ａ）のクラス設定テーブルに設定されているクラス分けルールは、以下のとおりである。アプリケーション（アプリケーション層のプロトコル）を条件としてクラス分けし、ＶｏＩＰをクラス１に分類し、その他の全アプリケーション（ｈｔｔｐ，ｆｔｐ，ｓｍｔｐ等）をクラス２に分類するというものである。図２（Ａ）のクラス設定テーブルは

、フラッシュメモリ１１に登録される。この登録は、このルータ装置１にネットワークを介してログインしたＰＣまたはＵＳＢ等で接続されたＰＣから行われる。

【００４０】

またさらに、このルータ装置１は、各クラス内での通信の逼迫に対応するために、ＤＣＣ(Dynamic Class Control) の機能を備えている。ＤＣＣとは、あるクラス内で特定のクライアントのＷＡＮ－ＬＡＮ間通信の帯域占有率が一定値を超えた場合、このクライアントの通信を制限することにより、各クラスにおける安定したトラフィックを維持する技術である。クライアントの通信を制限する方式として、このクライアントの通信を一定時間遮断する方式のほか、このクライアントが送信および／または受信するパケット（このクライアントのＩＰアドレスが送信元/宛先ＩＰアドレスとなっているパケット）を優先度の低いクラスまたは帯域幅の狭いクラスに一定期間または無期限（係員が解除操作を行うまで解除しない）移動させる方式がある。このようにクライアントの通信帯域占有率に基づいてダイナミックに、そのクライアントが送受信するパケットのクラスを移動させることから、ＤＣＣ(Dynamic Class Control) と呼ばれる。

【００４１】

各クライアントに対してこのＤＣＣ機能を適用するためのルールが、図２（Ｂ）に示すようなものである。

ＤＣＣ適用ルールは、以下のような事項からなる。なお、ルールは１つであってもよく複数あってもよい。

【００４２】

「クラス」監視対象のクラスを指定する。実施形態の例ではクラス２を指定する。

【００４３】

「クライアント」監視対象のクライアントを指定する。一般的にはこのクラスの通信を行う全クライアントを指定すればよいが、たとえばサーバ装置は、帯域占有率が高くなることが許容されるため適用を除外するようにしてもよい。また、不特定人が使用するクライアントＰＣのみに適用する等、一部のクライアントにのみ適用されるルールとしてもよい。

【００４４】

「送信／受信」監視対象のパケットを指定する。送信パケット（送信元ＩＰアドレス）または受信パケット（宛先ＩＰアドレス）のいずれか一方または両方を指定する。

「帯域占有率」帯域占有率のしきい値を指定する。たとえば８０％で６０秒等の数値で設定する。監視対象のクライアントの帯域占有率が定められた時間以上定められた数値を超えたとき、このルールに規定している通信の制限を適用する。

【００４５】

「動作」通信制限の方式を規定する。

【００４６】

「期間」上記通信制限の適用時間を指定する。適用時間は、無期限としてもよい。無期限の場合には、係員（ネットワーク管理者）が、このルータ１に対して通信制限の解除操作を行うまで、ルータ１は通信制限を継続する。

【００４７】

上記「動作」で設定する通信制限には、たとえば以下のような方式がある。

【００４８】

（１）該当のクライアントのＷＡＮ－ＬＡＮ間の通信を遮断する。

【００４９】

（２）該当のクライアントが送受信するパケットをより優先度の低いクラスまたは帯域幅の狭いクラスへ移動させる。

【００５０】

ここで、図２（Ａ）に示すクラス設定では、クラス２よりも優先度の低いクラスや帯域幅の狭いクラスは存在しないが、ＤＣＣ技術を適用する場合には、通信制限のための専用の優先度の低いクラスまたは帯域幅の狭いクラス（クラス３）を予め設定しておく。通常

使用しないクラスに予め帯域幅を割り当てておくことは帯域の無駄になるが、ＤＴＣ(Dynamic Traffic Control) 技術を適用して、クラス２とクラス３で帯域幅を共有させることにより、通信制限が行われるクライアントがないときは、クラス３の割当帯域を０として帯域の無駄を無くすことができる。

【００５１】

また、送信パケット（送信元ＩＰアドレスがそのクライアントのＩＰアドレスであるパケット）の帯域占有率がしきい値を超えた場合、送信パケットのみに通信制限を適用するか、送信パケットのみならず受信パケット（宛先ＩＰアドレスがそのクライアントのＩＰアドレスであるパケット）に対しても通信制限を適用するかは、ルール上で設定可能であるものとする。また、受信パケットの帯域占有率がしきい値を超えた場合も同様である。

【００５２】

このようにＤＣＣでは、クライアント単位でトラフィックを細分化して帯域占有率を監視している。クライアントＰＣの帯域占有率を監視することにより、通信帯域を占有してトラフィックを逼迫させるファイル交換ソフトやウィルスソフト等の特定のプログラムを、その通信内容を解析することなく、監視し抑制することが可能になる。

【００５３】

図３は、同ルータ装置の動作を説明するフローチャートである。同図（Ａ）はパケット処理のメインルーチンを示している。パケットを受信すると（Ｓ１）、この受信したパケットを、その属性に基づいてクラス分けし（Ｓ２）、そのクラスのキューに登録する。そして、そのクラスに対して定義されている帯域幅または優先順位でこのパケットを伝送する（Ｓ３）。以上が、ＱｏＳを実行するルータ装置の通常処理である。

【００５４】

この処理を行いつつ、ＤＣＣで監視するクラス（クラス２）における各クライアント単位のトラフィック（フロー）を監視する（Ｓ４）。いずれかクライアントのフローの帯域占有率がＤＣＣのルールに定められた帯域占有率（図２（Ｂ）参照）を超えた場合（Ｓ５）、このクライアントに対してＤＣＣに定めた通信制限を適用する（Ｓ６）。

【００５５】

同図（Ｂ）は、通信制限が適用されたクライアントが発生した場合の通信制限管理処理を示すフローチャートである。図２（Ｂ）に示すＤＣＣルールには、通信制限を適用する期間が定められている。この期間が無制限の場合にはこの処理は不要であるが、有限時間が適用されている場合は、この通信制限管理処理で通信制限を行っている時間を計測し、適用期間の経過後、通信制限を解除して、該当のクライアントの通信状態を元に戻す。Ｓ１０では通信制限を行っている時間を計測して適用期間が経過したかを判断する。適用期間が経過していない場合には何もしない。適用期間が経過した場合には、前記Ｓ６で適用した通信制限を解除してクライアントの通信状態を元の状態に戻す（Ｓ１１）。ここで元の状態に戻すとは、クライアントＰＣの通信を遮断している場合には、この遮断を解除する動作、クライアントＰＣ（の通信パケット）を優先度の低いクラスまたは帯域幅の狭いクラスに移動させた場合には、このクライアントＰＣ（の通信パケット）を元のクラスに戻す動作である。

【００５６】

以上のようなＤＣＣ処理をすることにより、クラス内のトラフィックを各クライアントのフロー単位で監視し、異常に帯域を占有するクライアントが発生した場合には、そのクライアントの通信を制限することにより、クラス内のトラフィックの安定性を維持することができる。

【００５７】

すなわち、ＱｏＳを適用することにより、クラス１に分類されているＶｏＩＰ通信１００は常に正常に行われるが、ＱｏＳのみでは、図５のように、クラス２において異常に帯域を占有するクライアントＰＣ（ファイル交換ソフトが動作しているＰＣ、ウィルスに感染したＰＣなど）１０２によってクラス２の帯域が占有され、一般のクライアントＰＣ１０１の通信が正常に行えない状況になる。この場面で、ＤＣＣを適用したことにより、図

４に示すように、上記異常なクライアントＰＣ１０２の通信がクラス３に分類されて同図の細線矢印のように制限され、一般のクライアント１０１の通信はクラス２において同図の太線矢印のように正常に行われるようになる。

【００５８】

なお、このようにＱｏＳを用いてパケットをクラス分けする場合、クラス分けの基準として、上述したようにパケットの破棄が許容されないＶｏＩＰ等のサービスを別クラスに分類するほか、正当な理由で一時的に広い帯域幅を占有するサービスがＤＣＣによって抑制されないようにこの正当なサービスを別クラスに分類するようにすればよい。

【００５９】

上記実施形態は、ＱｏＳ技術を用いてパケットをクラス分けした場合において、特定のクラスに対してＤＣＣを適用する場合について説明したが、ＱｏＳ技術を適用せずクラス分けしない場合においても全パケットに対して適用してもよい。この場合の通信制限は通信の遮断のみとなる。

【００６０】

≪実施形態の効果≫

以上説明したように、この実施形態で説明したルータ装置によれば、以下のような効果を奏することができる。

【００６１】

クライアント単位でそのフローの帯域占有率に応じて動的に送信優先度／受信優先度や送信帯域／受信帯域を変更、あるいは、送信／受信の遮断等の通信の制限を行うことが可能になる。

【００６２】

通信制限を適用する時間を任意に設定可能である。

【００６３】

通信の制限を適用するトリガとなる送信／受信帯域しきい値を、送信元クライアント、送信先クライアントの両方の視点で任意に設定可能であり、上り帯域と下り帯域のいずれか片方、あるいは同時に両方でトラフィックの管理制御が可能である。

【００６４】

ＮＡＴやＶＰＮを使用している環境下においても、クライアント単位のフロー制御が可能である。

【００６５】

サーバ機器などのように送信／受信帯域の占有を許したい機器がある場合、それらの機器を送信／受信帯域の監視対象から除外することが可能である。

【００６６】

帯域を占有しているクライアントだけ制限をかけ、他のクライアントには全く影響が及ばない。

【００６７】

一般的なＰ２Ｐアプリケーションの通信遮断機構は、対象アプリケーションを特定して通信パケットを検出しなければならず、新種のＰ２Ｐアプリケーションが流行する度に個別の対応が必要である。ＤＣＣでは、汎用的な特性からＰ２Ｐアプリケーションの通信を異常なトラフィックと捉え通信を遮断することができるので、対象となるアプリケーションは問わない。このことは、ウィルスに感染したＰＣから発生する膨大なトラフィックについても同様に有効であり、セキュリティ被害の二次感染を防ぐことが可能である。

【００６８】

マンションの住民やインターネットカフェなどのようにユーザごとに差別化することができない環境では、予めユーザ毎に帯域を割り当てることは問題視されるため、本発明のようにユーザ毎のトラフィック流量に応じて動的に制御する機構が有効となる。

【００６９】

「特開２００２－２７１３５９号公報」のようなＤＨＣＰを使用しなければいけないという制約がなく、ネットワーク環境に縛られない。また、「特開２００２－２７１３５９

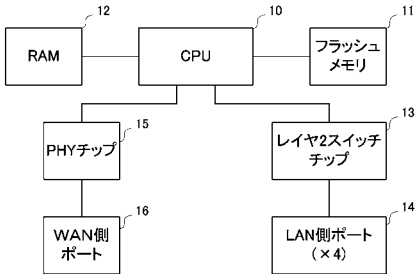
号公報」のようにアドレス資源を無駄に使用することがなく、実際に通信を行っているクライアントのみを対象として送信／受信帯域の監視をするので、「特開２００２－２７１３５９号公報」のように帯域が無駄に空いてしまうことはなく、帯域の有効活用ができる。

【符号の説明】

【００７０】

１　ルータ装置
１０　ＣＰＵ
１１　フラッシュメモリ
１２　ＲＡＭ
１３　レイヤ２スイッチチップ
１４　ＬＡＮ側ポート
１５　ＰＨＹチップ
１６　ＷＡＮ側ポート
２０　ＷＡＮ
２１　ＬＡＮ
Ｃ１　クラス１
Ｃ２　クラス２
Ｃ３　クラス３
１００　ＶｏＩＰ通信を行っているクライアント
１０１　一般のクライアント
１０２　異常なトラフィックのクライアント

【図１】



【図２】

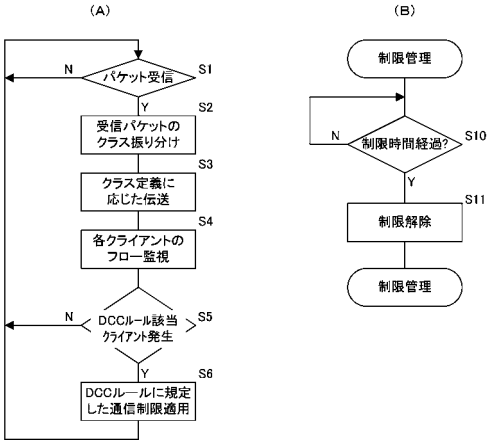
(A)

クラス	条件
1	アプリケーション：VoIP
2	その他のアプリケーション

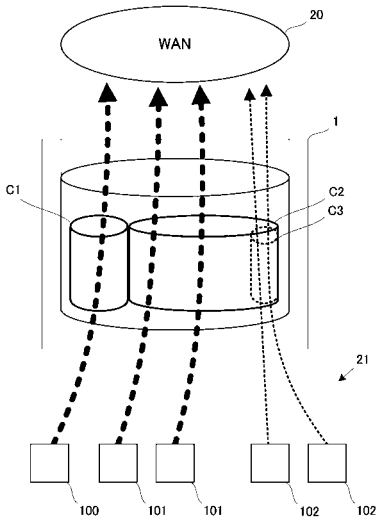
(B)

クラス	1 or 2
クライアント	全クライアント or 一部
送信 and/or 受信	送信 and/or 受信
帯域占有率	たとえば「80%超」
動作	遮断/クラスを下げる 等
期間	無期限/数秒～数分

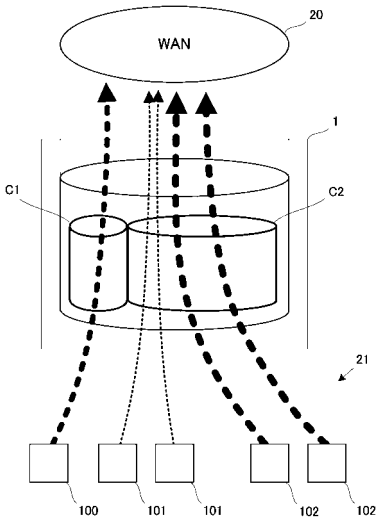
【図３】



【図４】


WAN
20
1
C1
C2
C3
21
100
101
101
102
102

【図５】


WAN
20
1
C1
C2
21
100
101
101
102
102