(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5673805号
(P5673805)
(45)発行日　平成27年2月18日(2015.2.18)　(24)登録日　平成27年1月9日(2015.1.9)

(51)Int.Cl.　F I
H04L 12/813 (2013.01)　H04L 12/813
H04L 12/70 (2013.01)　H04L 12/70　100Z

請求項の数 7　(全 10 頁)

(21)出願番号　特願2013-512461(P2013-512461)
(86)(22)出願日　平成24年4月27日(2012.4.27)
(86)国際出願番号　PCT/JP2012/061338
(87)国際公開番号　WO2012/147909
(87)国際公開日　平成24年11月1日(2012.11.1)
審査請求日　平成25年10月21日(2013.10.21)
(31)優先権主張番号　特願2011-99223(P2011-99223)
(32)優先日　平成23年4月27日(2011.4.27)
(33)優先権主張国　日本国(JP)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100080816
弁理士　加藤　朝道
(72)発明者　田淵　公士
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　永井　啓司

最終頁に続く

(54)【発明の名称】ネットワーク装置、通信システム、異常トラヒックの検出方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
所定の制限レートを超えたトラヒックに対してマーキングを行うマーキング部と、
前記マーキングしたトラヒック量を計測する計測部と、
検出対象の異常トラヒックの想定継続時間に応じて定められた期間における前記計測したトラヒック量を出力する監視部と、
を備えるネットワーク装置。
【請求項２】
前記計測部は、前記マーキング部によりパケットに書き込まれた情報を検出するフィルタを用いて、トラヒック量を計測する請求項１のネットワーク装置。
【請求項３】
前記マーキング部は、パケットヘッダの既知の値が設定されている領域の値を書き換えることで、マーキングを行い、
前記計測部は、前記マーキング部により書き換えられた情報を、前記既知の値に復元する処理を行う請求項１または２のネットワーク装置。
【請求項４】
前記監視部は、任意の時点におけるトラヒック量と、前記任意の時点より前の時点におけるトラヒック量との差が、所定のしきい値を超えていた場合、異常トラヒックが発生したものとして通知を行う請求項１から３いずれか一のネットワーク装置。
【請求項５】

前記検出対象の異常トラヒックは、マイクロバーストである請求項１から４いずれか一のネットワーク装置。
【請求項６】
前記マーキング部は、ポリシングを行うポリシング処理部によって構成されている請求項１から５いずれか一のネットワーク装置。
【請求項７】
所定の制限レートを超えたトラヒックに対してマーキングを行う処理と、
前記マーキングしたトラヒック量を定期的に計測する処理と、
検出対象の異常トラヒックの想定継続時間に応じて定められた期間における前記計測したトラヒック量を出力する処理と、
をネットワーク装置に搭載されたコンピュータに実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
［関連出願についての記載］
本発明は、日本国特許出願：特願２０１１－０９９２２３号（２０１１年　４月２７日出願）の優先権主張に基づくものであり、同出願の全記載内容は引用をもって本書に組み込み記載されているものとする。
本発明は、ネットワーク装置、通信システム、異常トラヒックの検出方法およびプログラムに関し、特に、比較的短い期間において発生する異常トラヒックを検出できるネットワーク装置、通信システム、異常トラヒックの検出方法およびプログラムに関する。
【背景技術】
【０００２】
本発明に直接関連はないが、出願前の調査により特許文献１、２が検出されている。特許文献１は、複数のデバイス間におけるデータ伝送に関する輻輳状態を監視する輻輳監視システムにおいて、少なくとも一つのデバイスに備えられ、未処理のデータの滞留量と所定の閾値との比較結果に応じて前段のデバイスにデータ送信の停止あるいは継続を指示するバックプレッシャ情報を生成するバックプレッシャ情報生成手段と、前記バックプレッシャ情報生成手段を備えたデバイスの前段のデバイスに備えられ、前記バックプレッシャ情報の内容に応じてデータの送信を停止させるデータ送信停止手段と、対応する前記バックプレッシャ情報生成手段から前記データ送信停止手段に送られるバックプレッシャ情報の変動を時間の経過に対応して監視する監視手段と、対応する前記監視手段による監視によって得られた情報に基づいて、バックプレッシャの発生頻度を示す指標を算出する指標算出手段とを備え、輻輳状態に対する切迫度を示す指標をリアルタイムで求めることが可能な輻輳監視システムというものである。
【０００３】
特許文献２は、複数のユーザの各メータＩＤのトークン値を加算したトークン値を保持する外部ＲＡＭのトークンカウンタを設け、各パケットデータのメータＩＤ及びレングス情報を抽出し所定数のパケットのメータＩＤ及びレングスと所定数のメータＩＤの相互の同一性を表す一致フラグとからなるパケット情報を格納する第１と第２の情報キャッシュを設け、第１と第２の情報キャッシュの一方をパケット情報の入力動作を行うよう駆動し、他方を各メータＩＤについてトークン演算部によるトークン演算を行うようタイミング生成部で切替え、演算結果としてパケットデータの通過・廃棄を表すフラグが設定される第１の情報バッファと第２の情報バッファを備えるよう構成する、というものである。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００５－１１７３９２号公報
【特許文献２】特開２００９－２０６８９６号公報
【発明の概要】

【発明が解決しようとする課題】
【０００５】
以下の分析は、本発明によって与えられたものである。近年、コンピュータ利用において仮想サーバ環境の利用が増え、仮想サーバ環境を用いたホスティングサービスも多く存在している。このとき複数の異なる加入者の仮想サーバを一つの物理サーバ上で動作させることも多く行なわれているが、ある加入者の仮想サーバのトラフィックが、マイクロバーストを発生させることで、別の加入者のサーバ上の業務に影響を与え、仮想サーバのホスティングサービスの障害として取り扱われる可能性がある。
【０００６】
図６は、ｎ台の物理サーバを用意し、各物理サーバ上で仮想サーバを構成し、ｋ個の端末からアクセス可能な構成を示す図である。図６のような構成においては、ネットワーク装置１００に搭載されたＩｎｇｒｅｓｓ処理部（図３の１０参照）、Ｅｇｒｅｓｓ処理部（図３の５０参照）に実装されたパケット個数またはパケット長を計数する機能（パケットカウンタ）を用いて監視を行うことが考えられる。
【０００７】
より具体的には、この種のネットワーク装置１００は、インタフェースポートの帯域の上限に達した場合、廃棄したパケット個数、またはパケット長の合計をカウンタ値として保持する機能を備えている。このカウンタ値を定期的に参照し、その値の差分から、トラヒック量が予め設定された水準よりも高い状態が検出された場合、これを輻輳として検知することができる。また、この場合、監視の周期としては、数秒～数分が一般的である。
【０００８】
しかしながら、上記した定期的な監視方法は、全トラヒックを監視対象としており、監視処理の負荷の観点から監視周期を短くすることができない。このため、上記数秒～数分といった監視期間内のトラヒック量が観測される。この結果、当該期間のトラヒック量が所定の通知水準に達せず、マイクロバーストに代表されるように、数ｍｓ～数十ｍｓという短期間に発生し、収束する輻輳を輻輳状態として検知することができないという問題点がある。
【０００９】
本発明は、負荷を増大させることなく、検出対象の異常トラヒックを捉えることのできるネットワーク装置、通信システム、異常トラヒックの検出方法およびプログラムを提供することを目的とする。
【課題を解決するための手段】
【００１０】
本発明の第１の視点によれば、所定の制限レートを超えたトラヒックに対してマーキングを行うマーキング部と、前記マーキングしたトラヒック量を計測する計測部と、検出対象の異常トラヒックの想定継続時間に応じて定められた期間における前記計測したトラヒック量を出力する監視部と、を備えるネットワーク装置が提供される。
【００１１】
本発明の第２の視点によれば、所定の制限レートを超えたトラヒックに対してマーキングを行うマーキング部を備えた第１のネットワーク装置と、前記マーキングしたトラヒック量を計測する計測部と、検出対象の異常トラヒックの想定継続時間に応じて定められた期間における前記計測したトラヒック量を出力する監視部と、を備える第２のネットワーク装置と、を含む通信システムが提供される。
【００１２】
本発明の第３の視点によれば、所定の制限レートを超えたトラヒックに対してマーキングを行うステップと、前記マーキングしたトラヒック量を定期的に計測するステップと、検出対象の異常トラヒックの想定継続時間に応じて定められた期間における前記計測したトラヒック量を出力するステップと、を含む異常トラヒック検出方法が提供される。本方法は、上記マーキング、計測を行うネットワーク装置と監視装置という特定の機械に結びつけられている。

【００１３】
本発明の第４の視点によれば、所定の制限レートを超えたトラヒックに対してマーキングを行う処理と、前記マーキングしたトラヒック量を定期的に計測する処理と、検出対象の異常トラヒックの想定継続時間に応じて定められた期間における前記計測したトラヒック量を出力する処理と、をネットワーク装置に搭載されたコンピュータに実行させるプログラムが提供される。なお、このプログラムは、コンピュータが読み取り可能な記憶媒体に記録することができる。即ち、本発明は、コンピュータプログラム製品として具現することも可能である。
【発明の効果】
【００１４】
本発明によれば、負荷を増大させることなく、検出対象の異常トラヒックを捉えることが可能となる。
【図面の簡単な説明】
【００１５】
【図１】本発明の概要を説明するための図である。
【図２】本発明の概要を説明するための図である。
【図３】本発明の第１の実施形態のネットワーク装置の構成を示すブロック図である。
【図４】本発明の第１の実施形態のネットワーク装置のフィルタ処理部の詳細構成を示すブロック図である。
【図５】本発明の第２の実施形態のネットワーク装置の構成を示すブロック図である。
【図６】本発明のネットワーク装置の接続例を示す図である。
【発明を実施するための形態】
【００１６】
始めに、本発明の一実施形態の概要について説明する。以下、この概要に付記した図面参照符号は、理解を助けるための一例として各要素に便宜上付記したものであり、本発明を図示の態様に限定することを意図するものではない。
【００１７】
本発明は、その一実施形態において、図１に示すように、受信部１０Ａ、送信部５０Ａのほかに、所定の制限レートを超えたトラヒックに対してマーキングを行うマーキング部２０Ａと、前記マーキングされたトラヒック量を定期的に計測する計測部３０Ａと、前記計測したトラヒック量の監視機能を提供する監視部４０Ａと、を備えるネットワーク装置にて実現できる。
【００１８】
より具体的には、マーキング部２０Ａは、図２の左側のグラフの網掛け領域に示すように、所定の制限レートを超えたトラヒックに対してマーキングを行う。そして、前記計測部３０Ａは、前記マーキングされたトラヒック量を定期的に計測する。監視部４０Ａは、図２の右側のグラフに示すように、検出対象の異常トラヒックの想定継続時間に応じて定められた期間におけるトラヒック量を所定の監視装置２に出力する。
【００１９】
例えば、検出対象の異常トラヒックがマイクロバーストである場合、例えば、数十ｍｓといった想定継続時間に応じて定められた期間におけるトラヒック量を、マーキングし、可視化することで、マイクロバーストの発生やその予兆を検出することが可能となる。なお、マイクロバーストとは、数秒～数分の監視周期では補足できない、短期間に発生し、収束するトラヒックのことをいう。
【００２０】
［第１の実施形態］
続いて、本発明の第１の実施形態について図面を参照して詳細に説明する。図３は、本発明の第１の実施形態のネットワーク装置の構成を示すブロック図である。図３を参照すると、入力ポート６１と、Ｉｎｇｒｅｓｓ処理部１０と、ポリシング処理部２０と、フィルタ処理部３０と、監視部４０と、Ｅｇｒｅｓｓ処理部５０と、出力ポート６２と、を備

えたネットワーク装置１が示されている。

【００２１】

入力ポート６１は、外部のノードからパケットを受信する。ここで「外部のノード」とは、パケットを送信しているサーバなどの端末、他の通信装置などが挙げられる。

【００２２】

Ｉｎｇｒｅｓｓ処理部１０は、入力ポート６１経由で受信したパケットについて、所定の入力処理を行った後、ポリシング処理部２０に出力する。前記所定の入力処理は、通常のネットワーク装置が搭載しているＩｎｇｒｅｓｓ処理部において行われている内容と同等である。例えば、ネットワーク装置１が、イーサネット（登録商標）スイッチである場合、ＭＡＣアドレス学習、パケット送信、受信、破棄に伴う、パケット計数処理などが行われる。

【００２３】

ポリシング処理部２０は、Ｉｎｇｒｅｓｓ処理部１０から入力されたパケット毎にマーキング（カラーリング）処理を施した後、フィルタ処理部３０に出力する。本実施形態のポリシング処理部２０は、リーキーバケット（Ｌｅａｋｙ　Ｂｕｃｋｅｔ）のアルゴリズムによりパケットの処理レート監視を行ない、所定の制限レートを超えた場合にそのタイミングで処理していたパケットに対しマーキングを行なう。前記所定の制限レートは、任意に設定可能であり、例えば、データレートが１Ｇｂｐｓの回線において５００Ｍｂｐｓを制限レートとした場合に、受信のタイミングで５００Ｍｂｐｓを越えたパケットに対してマーキングを行なうことになる。

【００２４】

なお、このマーキング処理は、ＶＬＡＮタグ（ＩＥＥＥ８０２．１ｑ）内の優先度指定用のＣｏＳ（Ｃｌａｓｓ　ｏｆ　Ｓｅｒｖｉｃｅ）値を、ある任意の特定の値に設定することで実現できる。

【００２５】

例えば、図６に示したような仮想サーバ環境では、仮想サーバを識別するためにＶＬＡＮタグを用いるため、外部より受信したパケットにはＶＬＡＮタグ（ＩＥＥＥ８０２．１ｑ）が設定されている。ＶＬＡＮタグではパケットの優先度を表すＣｏＳ値を設定することが可能であるが、外部のノードにおいて、任意の固定値、例えば“０”が設定されているものとする。この場合、マーキング処理は、前記ＣｏＳ値を先の固定値以外の任意の値、例えば“１”に設定する処理が行われる。

【００２６】

フィルタ処理部３０は、前記ポリシング処理部２０によりマーキング処理が行われたパケット個数またはパケット長の合計を計数する。また、フィルタ処理部３０は、計数後、マーキングしたパケットを元に戻す処理を行うことが望ましい。例えば、前述のＣｏＳ値を“０”から“１”に変えるマーキングが行われている場合、ＣｏＳ値を元の固定値である“０”に戻す処理が行われる。

【００２７】

さらに、フィルタ処理部３０は、前記マーキングされたパケットおよびマーキングしていないパケットをＥｇｒｅｓｓ処理部５０に転送する。

【００２８】

Ｅｇｒｅｓｓ処理部５０は、所定の出力処理を行った後、出力ポート６２から、受信したパケットを送出する。前記所定の出力処理は、通常のネットワーク装置が搭載しているＥｇｒｅｓｓ処理部において行われている内容と同等である。例えば、ネットワーク装置１が、イーサネット（登録商標）スイッチである場合、ＭＡＣアドレスの学習テーブルを参照して、出力先の出力ポートを特定し、その出力ポートにパケットを出力する処理が行われる。

【００２９】

監視部４０は、マイクロバーストを検出できるよう定められた周期で、フィルタ処理部３０のカウンタの値を読み出す。監視部４０は、前回読み出したカウンタ値を記憶してお

り、前回の値との差分が、所定のしきい値を超えていた場合（図２の右図参照）、マイクロバーストが発生したものと見做し、本ネットワーク装置１を含むネットワーク全体を監視している監視装置２や運用者に対して、その旨の通知を行なう。

【００３０】

所定のしきい値については、ネットワークの運用目標に併せて、任意に設定することができる。例えば、所定のしきい値を１とした場合、フィルタ処理部３０のカウンタの前回値との差分が１以上あった場合に通知が行なわれる。この場合、厳密にマイクロバースト発生の検出し、通知できることとなる。前記所定のしきい値は、１以外のその他の値とすることも可能である。

【００３１】

ここで、上記ネットワーク装置１のフィルタ処理部３０の詳細構成について説明する。図４は、本発明の第１の実施形態のネットワーク装置のフィルタ処理部の詳細構成を示すブロック図である。

【００３２】

図４を参照すると、フィルタ条件検索部３０１と、カウンタ処理部３１１と、パケット処理部３１２と、カウンタ値記憶部３２０とを備えた構成が示されている。

【００３３】

フィルタ条件検索部３０１は、マーキングされたパケットに適合する条件が定められた第１フィルタ３０２と、マーキングされたパケットを含むすべてのパケットに適合する条件が定められた第２フィルタ３０３とが設定されている。フィルタ条件検索部３０１は、入力されたパケットが第１フィルタ３０２に適合すると、カウンタ処理部３１１にカウンタ値記憶部３２０に記憶されたカウンタ値を、パケットに応じた値だけ増加するように通知する。例えば、マーキングとして、ＶＬＡＮタグのＣｏＳ値が書き換えられている場合、第１フィルタ３０２には、前記ＣｏＳ値が書き換え後の値（前述の例では、“１”）となっているパケットを抽出するマッチング条件が設定される。

【００３４】

カウンタ処理部３１１としては、パケット個数を計数する機能またはパケット長を累計していく機能、またはその両方を備えるカウンタを採用できる。

【００３５】

パケット処理部３１２は、第１フィルタ３０２に対してマッチングしたパケットの前記マーキングされた箇所を復元した後、Ｅｇｒｅｓｓ処理部５０に出力する。また、パケット処理部３１２は、第２フィルタ３０３に対してマッチングしたパケットも、同様にＥｇｒｅｓｓ処理部５０に出力する。

【００３６】

なお、図３に示したネットワーク装置１の各部（処理手段）は、ネットワーク装置１に搭載されたコンピュータに、そのハードウェアを用いて、上記した各処理を実行させるコンピュータプログラムにより実現することもできる。

【００３７】

以上のように、本実施形態のネットワーク装置１によれば、所定の制限レートを超えたパケットについてマーキングを行い（図２の左側図の網掛け部分参照。）、これをフィルタ処理部３０にて計数し、監視部４０にて可視化する処理が行われる（図２の右側図参照。）。

【００３８】

特に本実施形態では、ポリシング処理部によるマーキング（カラーリング）を使用しているので、周期の短い監視でも、負荷を増大させずに、マイクロバーストに代表されるごく短い期間に現れる異常トラヒックを観測ができる。また、本実施形態では、一般的に広く用いられているポリシング処理部およびフィルタ処理部を応用して構成することが可能であるので、実装も容易である。

【００３９】

なお、上記実施形態では、ＶＬＡＮタグのＣｏＳ値を書き換えるマーキング（カラーリ

ング）処理を用いるものとして説明したが、その他のＩＰヘッダフィールドを用いることも可能である。例えば、ＩＰヘッダ内のＴＯＳ値を使用し、フィルタ処理部においてＴＯＳ値が書き換えられたパケットを計数することとしてもよい。ＩＰヘッダ内のＴＯＳ値を用いた場合、ＶＬＡＮヘッダは不要である。

【００４０】

また、上記した実施形態では、フィルタ処理部３０内のパケット処理部３１２にてマーキング（カラーリング）を元に戻すものとして説明したが、マーキング（カラーリング）を戻さない構成としてもよい。この場合、Ｅｇｒｅｓｓ処理部５０またはネットワーク装置１の外部でマーキング（カラーリング）に基づいた優先度制御が可能になる。

【００４１】

また、上記した実施形態では、ポリシング処理部２０におけるレート監視のアルゴリズムとしてリーキーバケットを用いるものとして説明したが、その他アルゴリズムを用いることも可能である。

【００４２】

［第２の実施形態］

続いて、複数のネットワーク装置に機能を分散させた本発明の第２の実施形態について図面を参照して詳細に説明する。以下、上記した第１の実施形態との相違点を中心に説明する。

【００４３】

図５は、本発明の第２の実施形態のネットワーク装置の構成を示すブロック図である。図５を参照すると、ネットワーク装置１ａと、ネットワーク装置１ｂとが直列に接続された構成が示されている。

【００４４】

ネットワーク装置１ａ、１ｂは、ネットワーク装置１と略同様の構成であるが、ポリシング処理部２０の前段にフィルタ処理部３０が設けられている点で装置している。

【００４５】

前段に配置されたネットワーク装置１ａのフィルタ処理部３０は、入力ポート６１から入ってきたパケットに対しては何も行わず、パケットの転送のみ行う。一方、後段に配置されたネットワーク装置１ｂのポリシング処理部２０は、マーキング（カラーリング）処理を行なわずにパケットをＥｇｒｅｓｓ処理部５０に転送する。

【００４６】

前段のネットワーク装置１ａのＥｇｒｅｓｓ処理部５０と、出力ポート６２および後段のネットワーク装置１ｂの入力ポート６１、ｉｎｇｒｅｓｓ処理部１０は、ネットワーク装置１ａのポリシング処理部２０から出力されたパケットを、ネットワーク装置１ｂのフィルタ処理部３０に中継する。

【００４７】

上記した第１の実施形態の監視部４０と同様に、ネットワーク装置１ｂの監視部４０がマイクロバーストを検出できるよう定められた周期で、フィルタ処理部３０のカウンタの値を読み出す。これにより、監視部４０に接続された監視装置２にてマイクロバーストの発生を検知できる。

【００４８】

以上のように、本発明は、複数のネットワーク装置を用いて実現することができる。また、上記した説明では省略したが、ネットワーク装置１ｂからネットワーク装置１ａに送信されたパケットについても、同様の処理順序で監視を行うことができる。

【００４９】

以上、本発明の好適な実施形態を説明したが、本発明は、上記した実施形態に限定されるものではなく、本発明の基本的技術的思想を逸脱しない範囲で、更なる変形・置換・調整を加えることができる。例えば、図５では、本発明の理解を助けるために２台のネットワーク装置を直列に接続した構成を示したが、ネットワーク装置１の数は、３台以上であってもよく、また、ネットワーク装置１ａ、１ｂの間に、他のネットワーク装置が存在し

ていてもよい。

【００５０】

また、上記した第２の実施形態の構成に限らず、フィルタ処理部３０の後にポリシング処理部２０を配設した構成でも、本発明を実現することが可能である。この場合、前段側のネットワーク装置のフィルタ処理部３０でのパケット計数動作と、後段側のネットワーク装置のフィルタ処理部３０でのマーキング（カラーリング）処理を省略することができる。

なお、前述の特許文献の開示を、本書に引用をもって繰り込むものとする。

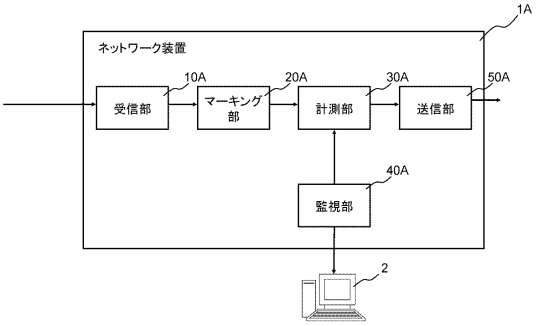
本発明の全開示（請求の範囲および図面を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態ないし実施例の変更・調整が可能である。また、本発明の請求の範囲および図面の枠内において種々の開示要素（各請求項の各要素、各実施例の各要素、各図面の各要素等を含む）の多様な組み合わせないし選択が可能である。すなわち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。

【符号の説明】

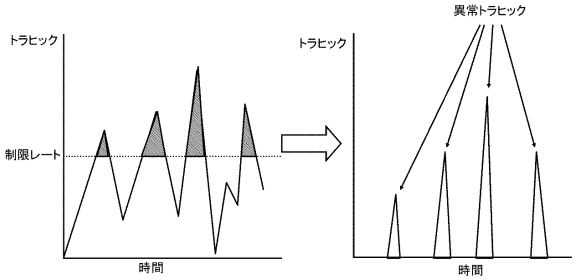
【００５１】

１、１Ａ、１ａ、１ｂ、１００　ネットワーク装置
２　監視装置
１０　Ｉｎｇｒｅｓｓ処理部
１０Ａ　受信部
２０　ポリシング処理部
２０Ａ　マーキング部
３０　フィルタ処理部
３０Ａ　計測部
４０、４０Ａ　監視部
５０　Ｅｇｒｅｓｓ処理部
５０Ａ　送信部
６１　入力ポート
６２　出力ポート
１１０　上位ネットワーク装置
１２０　端末
３０１　フィルタ条件検索部
３０２　第１フィルタ
３０３　第２フィルタ
３１１　カウンタ処理部
３１２　パケット処理部
３２０　カウンタ値記憶部

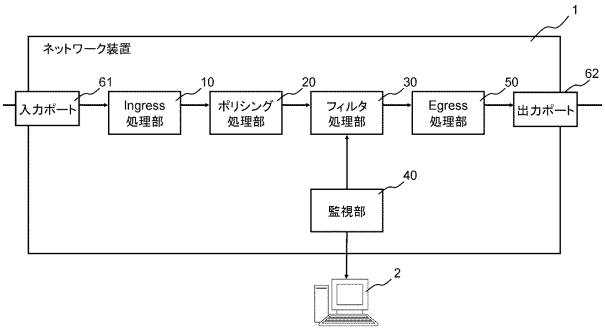
【図１】



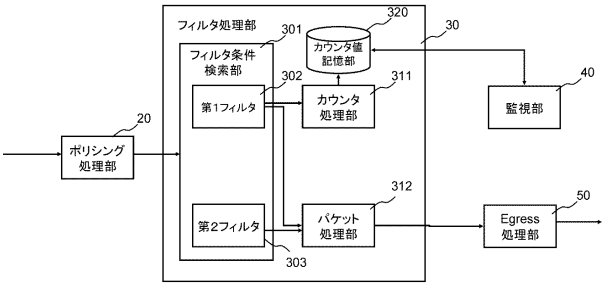
【図２】



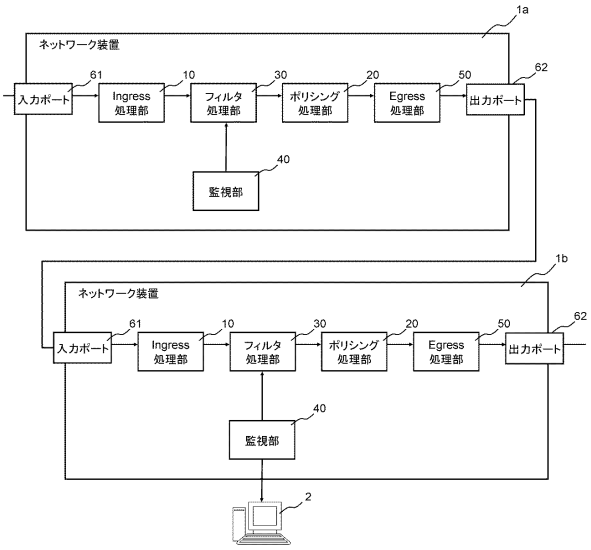
【図３】



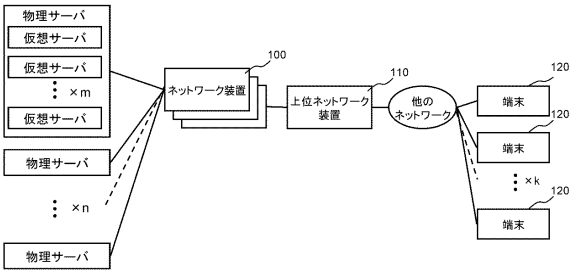
【図４】



【図５】



【図６】



フロントページの続き

(56)参考文献 特開平０８－１８６５７２（ＪＰ，Ａ）
G. Karagiannis, Requirements for Signaling of (Pre-) Congestion Information in a DiffServ Domain, draft-ietf-pcn-signaling-requirements-00, ２０１０年 7月 5日, ＵＲＬ, http://tools.ietf.org/id/draft-ietf-pcn-signaling-requirements-00.txt

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ １２／００－１２／２６、１２／５０－１２／９５５