(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2010-34708
(P2010-34708A)
(43)公開日　平成22年2月12日(2010.2.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	(2006.01)	H04L	12/56	200B	5K030
		H04L	12/56	400B	

審査請求 未請求　請求項の数 10　ＯＬ　（全 18 頁）

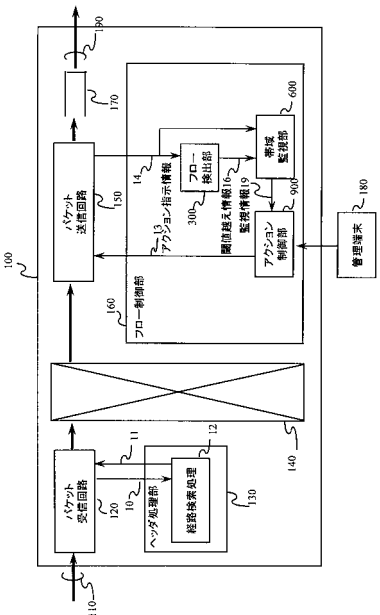
(21)出願番号　特願2008-192768 (P2008-192768)
(22)出願日　平成20年7月25日 (2008.7.25)

(71)出願人　504411166
アラクサラネットワークス株式会社
神奈川県川崎市幸区鹿島田８９０
(74)代理人　100107010
弁理士　橘爪　健
(74)代理人　100134061
弁理士　菊地　公一
(72)発明者　矢野　大機
神奈川県川崎市幸区鹿島田８９０　アラクサラネットワークス株式会社内
(72)発明者　秋元　剛之
神奈川県横浜市西区みなとみらい二丁目３番３号　日立情報通信エンジニアリング株式会社内

最終頁に続く

(54)【発明の名称】中継装置

(57)【要約】
【課題】　多量のトラフィックが流れる高速なネットワークにおいても、過大トラフィックのような不適切なトラフィックを検出し、また、該トラフィックの特性に合った遮断や帯域制御などの制御を自律的に行う。
【解決手段】　通信ネットワーク上に配置されたノードであるルータ１００に対して、フローを自動的に検出するフロー検出部３００と、検出したフローがポリシに違反しているかどうかを判定する帯域監視部６００と、ポリシ違反したフローに対して複数の制御を順番に適用するアクション制御部９００を備える。
【選択図】　図１



【特許請求の範囲】
【請求項１】
パケットの送信処理を行うパケット送信部と、
受信または送信するパケットからフローを検出するフロー検出部と、
前記フロー検出部が検出したフローがあらかじめ設定されたポリシに違反するか遵守するかを判定する帯域監視部と、
前記帯域監視部が判定したポリシに違反したフローに対して、あらかじめ設定された複数のアクション制御動作を順番に実行するアクション制御部と、
を備え、
パケット送信部は、受信したパケットのヘッダ情報を前記フロー検出部に送信し、
前記フロー検出部は、前記パケット送信部から受信したパケットのヘッダ情報を用いてフローを特定し、特定したフローのフロー情報毎にパケット数をカウントし、該パケット数が設定された閾値を超えたフローのフロー情報を含む閾値越え情報を前記帯域監視部へ送信し、
前記帯域監視部は閾値越え情報で特定されたフローの帯域を監視し、フロー情報と、違反又は遵守に関する情報を含む監視情報を生成し、監視情報を前記アクション制御部に送信し、
前記アクション制御部は、監視情報に基づき、実行するアクション制御を決定し、フロー情報とアクション内容を含むアクション指示情報を前記パケット送信部へ送信する。
前記パケット送信部では、前記アクション制御部から送られてきたアクション指示情報を元に、該当フローに対して制御を行い、一方、アクションが指示されていなければ、該当フローに相当するパケットをそのまま送信する
ようにしたパケットを中継する中継装置。

【請求項２】
前記フロー検出部は、テーブル番号とフロー情報とパケット数カウンタとを含むエントリを記憶するフローテーブルを備え、
前記フロー検出部は、
受信したヘッダ情報に含まれる、フロー情報を抽出し、
抽出された項目の組み合わせより、パケット数を積算するための前記フローテーブルのテーブル番号を複数生成し、
複数のテーブル番号を生成したら、複数の全てのテーブル番号に相当する前記フローテーブルの内容を確認し、該当するエントリ内のパケット数カウンタに１を加え、
パケット数カウンタが、予め定められた閾値を超えているかどうかを確認し、
閾値を越えていた場合、前記フロー情報を含む閾値越え情報を生成し、前記帯域監視部に送信し、
閾値を越えていなかった場合は、閾値越え情報を送信しないこと
を特徴とする請求項１に記載の中継装置。

【請求項３】
前記テーブル番号を生成するとき、フロー情報のうち予め定められた選択項目に対してハッシュ関数を複数使用し、得られた複数のハッシュ値をテーブル番号とすることを特徴とする請求項２に記載の中継装置。

【請求項４】
前記帯域監視部は、フロー情報と帯域と初回違反時間と前回違反時間と使用中又は未使用のフラグとを含むエントリを記憶する帯域監視テーブルを備え、
前記帯域監視部は、
受信したパケットヘッダ情報に含まれるフロー情報と、帯域監視テーブルに格納されているフロー情報とを、フラグが使用中の全てのエントリについて比較し、

ａ．　一致するエントリが存在しなかった場合、エントリ無しの情報及びフロー情報を含む監視情報を前記アクション制御部へ送信し、

ｂ．　一致するエントリが存在した場合、帯域を測定し、予め定められた閾値を超えているか確認し、
ｉ）　帯域が閾値を超えていない場合、帯域遵守であると判定し、現在時刻と該当するエントリの前回違反時間との差分の時間が、時刻閾値を超えているかを確認し、
　時刻閾値を超えている場合、監視対象から除外するために、帯域監視テーブルから該当エントリをフラグを未使用にすることで削除し、一方、時刻閾値を超えていない場合、監視対象のままとし、
　該当フローの、エントリ有りの情報とフロー情報と帯域遵守情報と一定時間以上帯域を遵守していたかどうかの情報を含む監視情報を前記アクション制御部へ送信し、

ｉｉ）　帯域が閾値以上の場合、帯域違反が発生したと判定し、初回違反時間に基づき違反回数を確認し、
　該当フローのエントリの初回違反時間と前回違反時間を更新し、
　該フローの、エントリ有の情報とフロー情報と帯域違反情報と違反が１回目又は２回目以降であるという情報とを含む監視情報を前記アクション制御部へ送信する
ことを特徴とする請求項１乃至３のいずれかに記載の中継装置。

【請求項５】
　前記帯域監視部は、
　前記フロー検出部より送られてきた閾値越え情報をもとに、既に存在する全ての帯域監視テーブルのフロー情報と、前記フロー検出部より送られてきた閾値越え情報に含まれるフロー情報とを比較し、
　一致するテーブルが存在しなかった場合には、前記フロー情報と、帯域及び初回違反時間及び前回違反時間の予め定められた設定値と、フラグの使用中設定値とにより、帯域監視テーブルに新規エントリを作成すること
を特徴とする請求項４に記載の中継装置。

【請求項６】
　前記アクション制御部は、
　フロー情報と、該当エントリが登録された時刻を格納するアクション開始時刻と、アクションが実行されていた時間の長さを格納するアクション実行時間を含むエントリを記憶するフローデータベースと、
　一連又は一組のアクションについて、アクションの開始時刻とアクションの終了時刻とアクション内容とを含むエントリをアクションの順序に従い記憶されているアクションデータベースと
を備え、
　前記アクション制御部は、
　前記帯域監視部から送られてきた監視情報に基づき、前記帯域監視部の帯域監視テーブルにエントリが有ったか無かったかのチェックを行い、

ａ．　エントリが無かったと判定された場合、パケット送信回路に対し、該当フローに対するアクションは何も実行せず送信可能であるというアクション指示情報を送信し、

ｂ．　エントリが有りと判定された場合、帯域を遵守していたか違反していたかの帯域遵守／違反チェックを行い、
　前記帯域遵守／違反チェックにより、帯域を違反していたと判定された場合、前記帯域

制御部から送られてきた監視情報を元に、違反が１回目か２回目以降なのかの回数判定を行い、
ｉ）　前記回数判定で１回目であると判定された場合、前記フローデータベースより、監視情報に含まれるフロー情報とフロー情報が一致するエントリが存在するかどうかを検索し、
　エントリが存在した場合、該当のエントリのアクション開始時刻に‘０’を書き込み、アクション実行時間を読み込み、前記アクションデータベースより、アクション実行時間の時間が開始時刻と終了時刻の間に入っているアクションを検索し決定し、
　一方、エントリが存在しなかった場合、フロー情報に書き込み、アクション開始時刻に現在時刻を書き込み、アクション実行時間に‘０’を書き込むことにより、新規にエントリを登録し、
　アクション開始時刻と現在時刻の差にアクション実行時間を加算した値が、開始時刻と終了時刻の間に入っているアクションを、前記アクションデータベースより検索しアクションを決定し、

ｉｉ）　前記回数判定で２回目以降であると判定された場合、前記フローデータベースより、監視情報に含まれるフロー情報とフロー情報が一致するエントリのアクション開始時刻とアクション実行時間を読み込み、
　アクション開始時刻と現在時刻より差を求め、その値とアクション実行時間の値を加算し、その加算した値が開始時刻と終了時刻の間に入っているアクションを前記アクションデータベースより検索し、決定し、

　パケット送信回路に対して、決定されたアクションを実行するように、フロー情報とアクション内容を含むアクション指示情報を送信すること
を特徴とする請求項１乃至５のいずれかに記載の中継装置。

【請求項７】
　前記帯域遵守／違反チェックにより、帯域を遵守していたと判定された場合、
　帯域制御部から送られてきた監視情報をもとに、一定時間以上帯域を遵守していたか判定し、
　一定時間以上帯域を遵守していたと判定された場合、前記フローデータベースより、フロー情報が一致するエントリが存在するかどうかを検索し、
ｉ）　前記フローデータベースに該当エントリが存在した場合、該当エントリのアクション実行時間に、現在時刻からアクション開始時刻の差を求め、その差からさらに遵守していた時間である時間閾値情報に設定された値を減算した時間を書き込み、パケット送信回路に対し、該当フローに対するアクションは何も実行せず送信可能であるというアクション指示情報を送信し、
　一方、一定時間以上帯域を遵守していないと判定された場合、パケット送信回路に対し、該当フローに対するアクションは何も実行せず、送信可能であるという情報を送信し、

ｉｉ）　一方、前記フローデータベースに該当エントリが存在しなかった場合、特にアクションは行わず、パケット送信回路に対し、該当フローに対するアクションは何も実行せず、送信可能であるという情報を送信すること
を特徴とする請求項６に記載の中継装置。

【請求項８】
　前記アクションデータベースを複数備え、
　前記アクションデータベースのうちどの一つ又は複数選択するかを、宛先、送信元、プロトコル番号、又は、時間等のフローの特長毎に割り当てることを特徴とする請求項６又は７のいずれかに記載の中継装置。

【請求項９】
前記フロー情報は、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョンの情報を含むことを特徴とする請求項１乃至８のいずれかに記載の中継装置。

【請求項１０】
前記帯域監視部は、監視を実行するにあたり、帯域の代わりに、該当フローが消費している電力、又は、単位時間あたりのセッション開始数を監視することで遵守、違反を判定することを特徴とする請求項１乃至９に記載の中継装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、中継装置に係り、特に、ネットワーク上に配置され、フロー制御を実行することができる中継装置に関する。
【背景技術】
【０００２】
インターネットなどの広域ネットワークはオープンな環境であり、誰もが自由に接続することが可能である。また、近年のＦＴＴＨ（Ｆｉｂｅｒ ｔｏ ｔｈｅ Ｈｏｍｅ）等の普及により回線の高速化が進んでいる。また、さまざまなアプリケーションの登場により、ネットワーク上を流れるフローの種類が増え挙動が複雑になってきている。キャリアやＩＳＰ（Ｉｎｔｅｒｎｅｔ Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ）のネットワーク上では、ユーザ間の公平性を確保したり、ＤｏＳ（Ｄｅｎｉａｌ ｏｆ Ｓｅｒｖｉｃｅ）攻撃等から装置を守るために、フィルタ等の技術を使用している。現状のフィルタ技術は、予想されるフロー条件をあらかじめ設定し、そのフロー条件に合致したフローに対してどのような制裁を実行するかといった条件もあらかじめ設定しておく。フィルタが設定された装置は、自装置内を流れるフローと設定されている複数個の条件を常に比較し、条件に合致したフローを発見した場合、その条件に設定されている制裁を実行する。
また、特許文献１～３には、トラフィック情報を統計的に処理しながら不正なトラフィックを検出し、トラフィックの遮断や帯域制限を行う技術が開示されている。
【０００３】
【特許文献１】特開２００６－３１４０７７号公報
【特許文献２】特開２００４－３５６９０６号公報
【特許文献３】特開２００５－２７７８０４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
従来の技術では、装置内を流れるフロー条件を予測し、かつ、そのフローに対して有効に動作する制御条件を事前に設定しておく必要があった。しかし、回線を流れるフローの増加により、事前にフロー条件を設定しておくことが困難になりつつある。さらにさまざまなアプリケーションやプロトコルの出現により、該当フローに有効な制御を一意に決定し事前に設定しておくことも困難になりつつある。
本発明は、以上の点に鑑み、複数の装置が接続される通信ネットワーク上に配置され、設定されたポリシ違反であるフローを自動的に検出し、そのようなフローに対し複数の制裁条件を実行することを目的とする。

【課題を解決するための手段】
【０００５】
本発明の解決手段によると、
パケットの送信処理を行うパケット送信部と、

受信または送信するパケットからフローを検出するフロー検出部と、
前記フロー検出部が検出したフローがあらかじめ設定されたポリシに違反するか遵守するかを判定する帯域監視部と、
前記帯域監視部が判定したポリシに違反したフローに対して、あらかじめ設定された複数のアクション制御動作を順番に実行するアクション制御部と、
を備え、
パケット送信部は、受信したパケットのヘッダ情報を前記フロー検出部に送信し、
前記フロー検出部は、前記パケット送信部から受信したパケットのヘッダ情報を用いてフローを特定し、特定したフローのフロー情報毎にパケット数をカウントし、該パケット数が設定された閾値を超えたフローのフロー情報を含む閾値越え情報を前記帯域監視部へ送信し、
前記帯域監視部は閾値越え情報で特定されたフローの帯域を監視し、フロー情報と、違反又は遵守に関する情報を含む監視情報を生成し、監視情報を前記アクション制御部に送信し、
前記アクション制御部は、監視情報に基づき、実行するアクション制御を決定し、フロー情報とアクション内容を含むアクション指示情報を前記パケット送信部へ送信する。
前記パケット送信部では、前記アクション制御部から送られてきたアクション指示情報を元に、該当フローに対して制御を行い、一方、アクションが指示されていなければ、該当フローに相当するパケットをそのまま送信する
ようにしたパケットを中継する中継装置が提供される。

【発明の効果】
【０００６】
本発明によると、事前にフロー条件を設定せずにすみ、該当フローに有効な制裁を自動的に発動することが可能となる。
また、本発明によると、中継装置でフロー条件をあらかじめ設定しておくのではなく、ポリシのみを設定しておくだけで、ポリシに違反する自律的フローを特定し、そのフローの特性にあった帯域制御などの制御を実行することができる。

【発明を実施するための最良の形態】
【０００７】
図１は、本実施の形態のルータ１００を示す。以下に、本実施の形態のフロー制御機構を所持するルータ（中継装置）１００の構成を図１を用いて説明する。
ルータ１００は、パケットが入力する入力回線１１０とパケットの受信処理を行うパケット受信回路１２０と、パケットを出力する出力回線１９０の識別子である出力回線番号の判定等を実行するヘッダ処理部１３０と、パケットを前記出力回線番号に基づきスイッチングするパケット中継処理手段１４０と、送信側バッファ１７０へパケットを書き出してパケットの送信処理を行うパケット送信回路１５０と、受信したパケットのフロー情報を抽出し、事前に定義された複数のアクションから一つを決定し実行するフロー制御部１６０と、パケットを出力する出力回線１９０を備える。管理端末１８０は、ルータ１００の管理と各種設定を行なう。ヘッダ処理部１３０は、経路検索処理部１２を有する。フロー制御部１６０は、フロー検出部３００と帯域監視部６００とアクション制御部９００を有する。図１には入力回線１１０と出力回線１９０がそれぞれ１回線ずつ記載されているが、実際には、ルータ１００は、通常、複数の入力回線１１０と出力回線１９０から構成される。
【０００８】
図２に、ネットワーク上を流れるパケットのフォーマットの一例を示す。
図２には一例としてＥｔｈｒｅｎｅｔ回線の場合を示した。パケットはＬ２ヘッダ部２２０とＬ３ヘッダ部２２１とＬ４ヘッダ部２２２とデータ部２２３を含む。Ｌ２ヘッダ部２２０は、Ｌ２のアドレス情報などパケットの入力回線の種類によって異なる情報から構

成される。この例ではＬ２ヘッダ部２２０は、送信元ＭＡＣアドレス２１０と、宛先ＭＡＣアドレス２１１を含む。Ｌ３ヘッダ部２２１は、ＩＰのバージョンを示すＩＰバージョン２１２と上位層（Ｌ４層）の種別を示すプロトコル番号２１３と送信元アドレスである送信元ＩＰアドレス２１４と、宛先アドレスである宛先ＩＰアドレス２１５、Ｌ３ヘッダ部２２１とＬ４ヘッダ部２２２とデータ部２２３を足したバイト長であるＬ３パケット長２１６を含む。Ｌ４ヘッダ部２２２は、送信元ポート２１７と宛先ポートを表す宛先ポート２１８を含む。また、データ部２２３は任意のユーザデータである、データ２１９を含む。

【０００９】

次に、本発明のルータ１００の動作概要を図１を用いて説明する。

パケットはまず入力回線１１０よりパケット受信回路１２０に入力する。パケットがパケット受信回路１２０に入力すると、パケット受信回路１２０は、受信したパケットのＬ２ヘッダ部２２０、Ｌ３ヘッダ部２２１、Ｌ４ヘッダ部２２２を含むパケットヘッダ情報１０をヘッダ処理部１３０に送信する。ヘッダ処理部１３０は、パケット受信回路１２０より受信したパケットヘッダ情報１０を用いて経路検索処理１２を実行し、出力回線番号を検索し、その検索結果をパケット受信回路１２０へ送信する。

パケット中継処理手段１４０は、パケット受信回路１２０がヘッダ処理部１３０から受信した出力回線番号１１に従いパケットをスイッチングし、出力回線１９０毎のパケット送信回路１５０へパケットを送信する。

パケット送信回路１５０は、パケット中継処理手段１４０より受信したパケットのＬ３ヘッダ部２２１とＬ４ヘッダ部２２２をフロー制御部１６０に送信する。フロー検出部３００は、Ｌ３ヘッダ情報２２１とＬ４ヘッダ情報２２２を用いてフローを特定する。フロー検出部３００では、例えば、ＩＰバージョン２１２、プロトコル番号２１３、送信元ＩＰアドレス２１４、宛先ＩＰアドレス２１５、送信元ポート２１７、宛先ポート２１８の全フィールドが同じ値のものを同一のフローとして定義する。フロー検出部３００では、フロー毎にパケット数をカウントし、パケット数が設定された閾値を超えたフローの情報（閾値越え情報１６）を帯域監視部６００へ送信する。帯域監視部６００は、閾値越え情報１６に含まれるフロー情報で指定されたフローの監視を行い、帯域の監視を行った結果と違反回数と遵守時間を含む監視情報１９を生成し、監視情報１９をアクション制御部９００に送信する。アクション制御部９００は、監視情報１９を基に実行する制御を決定し、アクション指示情報１３をパケット送信回路１５０へ送信する。なお、フロー検出部３００、帯域監視部６００、アクション制御部９００による処理の詳細は、後述する。パケット送信回路１５０は、アクション指示情報１３の指示に従い、該当パケットのパケット送信バッファ１９０への送信、もしくは該当パケットの廃棄もしくは、パケットヘッダの書き換え等を実行する。

パケット送信バッファ１７０に送信されたパケットは、出力回線１９０に送信される。

【００１０】

図３に、本実施の形態のフロー検出部を示すブロック図を示す。フロー検出部３００は、閾値情報３０、フロー解析部３１、フローテーブル３２を備える。

図５に、本実施の形態のフロー検出部のフローチャートを示す。

次に、フロー検出部３００の詳細動作について図５を用いて説明する。フロー検出部３００のフロー解析部３１は、受信したＬ３ヘッダ情報２２１とＬ４ヘッダ情報２２２に含まれる、フロー情報を抽出する（ステップ５０１）。フロー情報としては、例えば、ＩＰバージョン、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号が含まれる。フロー情報の要素はこれらに限定されるわけではなく、これらの要素のうち所望のいずれか複数のみとしてもよいし、必要に応じて他の要素を加えてもよい。また、ステップ５０１におけるパケットからのフロー情報の取り出しは、受信パケット全てではなく、適当なサンプリング処理により選択されたパケットに対してのみ行うようにしてもよい。これにより、膨大なトラフィックが流れる高速ネットワークにおいても処理可能となる。

次に、フロー解析部３１は、ステップ５０１で選択された項目の組み合わせより、パケット数を積算するためのフローテーブル３２のテーブル番号を生成する（ステップ５０２）。

【００１１】

図４に、フローテーブル３２の一例を示す。

１フロー分のフローテーブル３２は、テーブル番号４０１、フロー情報（送信元ＩＰアドレス４０２、宛先ＩＰアドレス４０３、送信元ポート番号４０４、宛先ポート番号４０５、プロトコル番号４０６、ＩＰバージョン４０７）、パケット数カウンタ４０８を含み、これらの組みが複数格納された構造となっている。全てのフローが格納できるような広大なフローテーブル３２空間を割り当てることは難しい場合もあるため、テーブル番号決定方法としては、選択された項目の組み合わせに対して適当なハッシュ関数を適用し、得られたハッシュ値をテーブル番号とする方法をとることができる。また、異なるフローが同一のハッシュ値となり、フローテーブル３２の利用が偏ってしまうことが考えられるため、ハッシュ関数を複数使用するとよい。ここでは、一例として、ハッシュ関数を４つ用意し、一つのフローに対して、４つのハッシュ値を生成する。このハッシュ値そのものをフローテーブル３２のテーブル番号として使用する。フローテーブル３２は、テーブル番号１のテーブルには、テーブル番号を“１”を書き込み、それ以外のフィールドには“０”を書き込んでおく。同様にテーブル番号Ｎのテーブルには、テーブル番号“Ｎ”を書き込み、それ以外のフィールドには“０”を書き込んでおく。フロー解析部３１は、このようにしてＮ個のフローテーブル３２を予め用意しておく。

フロー解析部３１は、ステップ５０２で、例えば４つのハッシュ関数に対する４つのテーブル番号を生成したら、４つ全てのテーブル番号に相当するフローテーブル３２の内容を確認する（ステップ５０３）。ここでは、まず、フロー解析部３１は、フローテーブル３２の送信元ＩＰアドレス４０２、宛先ＩＰアドレス４０３、送信元ポート番号４０４、宛先ポート番号４０５、プロトコル番号４０６、ＩＰバージョン４０７の各値と、ステップ５０１で抽出されたフロー情報の各値がすべて一致するテーブルが存在するか確認する。フロー情報中の全てのフィールドが一致するテーブルが存在した場合、同一テーブル有と判定する。フロー解析部３１は、フロー情報中の全てのフィールドが一致するテーブルが存在しなかった場合、未使用のテーブルが存在するか確認する。未使用かどうかは、パケット数カウンタが“０”であるかどうかで判断する。フロー解析部３１は、パケット数カウンタが“０”の場合、未使用であると判断し、空きテーブル有と判定する。全てのテーブルのパケット数カウンタが“０”以外であった場合、空きテーブル無と判定する。

また、フロー解析部３１は、ステップ５０３の結果、空きテーブル有と判定された場合は、フロー解析部３１は、該当するテーブル番号のフローテーブル３２にステップ５０１で抽出されたフロー情報を書き込む（ステップ５０５）。テーブル番号ｎのテーブルが空きテーブル有りと判定されたとすると、送信ＩＰアドレスフィールド４０２－ｎ、宛先ＩＰアドレスフィールド４０３－ｎ、送信元ポート番号４０４－ｎ、宛先ポート番号４０５－ｎ、プロトコル番号４０６－ｎ、ＩＰバージョン４０７－ｎにステップ５０１で抽出されたフロー情報を書き込み、パケット数カウンタ４０８－ｎには“０”を書き込む。複数個のエントリが未使用であった場合、テーブル番号が予め定められた順番で、例えば、最も小さい（又は最も大きい）エントリを使用する。次に、フロー解析部３１は、前記エントリ内のパケット数カウンタ値４０８－ｎに１を加える（ステップ５０６）。

【００１２】

また、ステップ５０３の結果、同一テーブル有と判定された場合は、フロー解析部３１は、同一テーブル内のパケット数カウンタ値に１を加える（ステップ５０６）。ここではテーブル番号ｙのテーブルが同一テーブルであると判定されたとする。パケット数カウンタフィールド４０８－ｙに“１”を加え、それ以外のフィールドには何も実行しない。

さらに、ステップ５０３の結果、空きテーブル無と判定された場合は、フロー解析部３１は、４つのテーブル中のどれか一つのテーブルを上書きする。４つのテーブル中どのテーブルを上書きするかは、例えば、４つのテーブルのパケット数カウンタフィールドを比

較し、一番小さいパケット数のテーブルを上書き可能テーブルとして決定する（ステップ５０４）。ここではテーブル番号ｚのテーブルが上書き可能テーブルとして決定されたとする。決定されたテーブルに対し、送信ＩＰアドレスフィールド４０２－ｚ、宛先ＩＰアドレスフィールド４０３－ｚ、送信元ポート番号４０４－ｚ、宛先ポート番号４０５－ｚ、プロトコル番号４０６－ｚ、ＩＰバージョン４０７－ｚの各フィールドに該当パケットから抽出された情報を書き込み、パケット数カウンタ値フィールド４０８－ｚに“０”を書き込む（ステップ５０５）。次に、フロー解析部３１は、パケット数カウンタフィールド４０８－ｚに“１”を加える（ステップ５０６）。

次に、フロー解析部３１は、上述のようにステップ５０６でパケット数カウンタフィールドに“１”を加えた結果、パケット数カウンタが規定の閾値を超えているかどうかを確認する（ステップ５０７）。前記閾値は、閾値情報３０に格納されているので、フロー解析部３１はこれを参照する。閾値情報３０の内容は、例えば、管理端末１８０を用いて事前に設定しておくことができる。フロー解析部３１は、ステップ５０７において、前記パケット数フィールドの値が閾値情報３０の閾値フィールドに定義されている値と一致した場合又はそれ以上の場合、閾値越えが発生したと判断し、閾値越え情報１６を生成し、帯域監視部６００に送信する（ステップ５０８）。閾値越え情報１６の内容は、例えば、前記エントリ内に格納されている、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等のフロー情報を含む。閾値を超えていなかった場合は、何もしない。

【００１３】

図６に、本実施の形態の帯域監視部を示すブロック図を示す。

次に帯域監視部６００の構成を図６を用いて説明する。帯域監視部６００は、帯域監視処理部６１と、監視対象を格納しておく帯域監視テーブル６２と、監視帯域閾値を格納しておく帯域閾値情報６０と、監視時間情報を格納しておく時刻閾値情報６３と、現在時刻を示す時刻情報６４を備える。帯域閾値情報６０と時刻閾値情報は、例えば、管理端末１８０より設定される。

以下に、帯域監視部６００の詳細動作を図７を用いて説明する。帯域監視部６００の帯域監視処理部６１はフロー検出部３００から情報をもらう場合と、パケット送信回路１５０より情報をもらう場合、の二つの場合が存在する。フロー検出部３００から情報をもらった場合はステップ７０１を実行し、パケット送信回路から情報をもらった場合はステップ７０２以降を実行する。

ステップ７０１で、帯域監視処理部６１は、フロー検出部３００より送られてきた閾値越え情報１６をもとに帯域監視テーブル６２のエントリを作成する。

【００１４】

図８に、帯域監視テーブルの一例を示す。帯域監視テーブル８００は、フロー情報８０１と帯域８０２と初回違反時間８０３と前回違反時間８０４とフラグ８０５を含む。フロー情報８０１には送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等の情報が格納され、帯域８０２にはフロー情報８０１で指示されるフローの現在の帯域情報が格納され、初回違反時間８０３には、初めて帯域違反と判定された時刻が格納され、前回違反時間には、直前に帯域違反と判定された時刻が格納されて、フラグ８０５には、当該テーブルが使用中のテーブルであれば“１”が、未使用のテーブルであれば“０”が格納される。初期状態では全てのテーブルのフラグが“０”に設定されている。

【００１５】

ステップＳ７０１では、まず、帯域監視処理部６１は、既に存在する全ての帯域監視テーブル６２のフロー情報８０１と、フロー検出部３００より送られてきた閾値越え情報１６とを比較する。フロー情報８０１と閾値越え情報１６にはともに、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等の情報が格納されている。帯域監視処理部６１は、この比較では、フラグが“１”のテーブルのフロー情報８０１と閾値越え情報１６の全てのフィールドが一致するテーブ

ルがあるかどうかをチェックする。
帯域監視処理部６１は、一致するテーブルが存在しなかった場合には、新規エントリを作成する。フロー情報８０１には閾値越え情報１６として送られてきた、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン、が格納され、帯域８０２、初回違反時間８０３、前回違反時間８０４のフィールドには０が格納され、フラグ８０５が“１”に設定される。新規テーブルを作成する場合は、予め定められた順番により、例えば、フラグが“０”で一番アドレスが小さいテーブルを選択する。
一方、一致するエントリが存在した場合には、帯域監視処理部６１は、該等閾値越え情報１６を無視する。
【００１６】
ステップ７０２として、帯域監視処理部６１は、受信したパケットヘッダ情報２２１に含まれる、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョンから生成したフロー情報と、帯域監視テーブル８００に格納されているフロー情報８０１の、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等とを比較する。帯域監視処理部６１は、帯域監視テーブル８００に格納されているフラグが“１”の全てのエントリと比較を行い、一致するエントリを検索する。
一致するエントリが存在しなかった場合、該当フロー情報を含む監視情報１９をアクション制御部９００へ送信する（ステップ７１３）。送信する監視情報１９は、帯域監視テーブル８００に“エントリ無”の情報と、フロー情報（送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等）と、を送信する。
帯域監視処理部６１は、ステップ７０２で、一致するエントリが存在した場合、帯域を測定する（ステップ７０３）。帯域とは、例えば、単位時間（１秒）あたりの受信バイト数とすることができる。受信バイト数とは、受信したパケットのパケットヘッダ情報２２１に含まれるＬ３パケット長２１６を単位時間に受信した数だけ加算した値とすることができる。また、これ以外の方法で帯域を測定してもよく、そのために、帯域監視テーブル８００に帯域を監視するための受信バイト数を格納しておくフィールド等の帯域計算に必要なフィールドを加えても良い。
次に、帯域監視処理部６１は、ステップ７０３で計測された帯域の値が、閾値を超えているか確認する（ステップ７０４）。前記閾値は帯域閾値情報６０に設定されているので、帯域監視処理部６１はこれを参照する。閾値を超えるかもしくは等しい場合、帯域監視処理部６１は、帯域違反が発生したと判定する。一方、閾値を超えていない場合、帯域監視処理部６１は、帯域遵守であると判定する。
【００１７】
ステップ７０４で帯域遵守と判定された場合、帯域監視処理部６１は、現在時刻情報６４及び時刻閾値情報６３を参照し、ステップ７０２で一致するエントリとして検索されたフローが書き込まれている帯域監視テーブル８００のエントリの前回違反時間８０４と現在時刻の差分の時間が、時刻閾値情報６３を超えているかを確認する（ステップ７０５）。閾値を超えている場合、帯域監視処理部６１は、一定時間以上該当フローは帯域を遵守していると判断し、監視対象から除外する。帯域監視処理部６１は、この該当フローを監視対象から除外するために、帯域監視テーブル８００から該当エントリを削除する（ステップ７０７）。エントリの削除とは該当エントリのフラグ８０５を“０”にすることである。ステップ７０４で時刻閾値情報６３を超えていない場合、帯域監視処理部６１は、一定時間以上該当フローが帯域を遵守していないと判断し、監視対象のままとする。
次に、帯域監視処理部６１は、該当フローのエントリ情報を含む監視情報１９をアクション制御部９００へ送信する（ステップ７１２）。送信する監視情報１９は、帯域監視テーブルに“エントリ有”の情報と、フロー情報（送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等）と、帯域を

遵守したことを表す帯域遵守情報と、ステップ７０５で確認した一定時間以上帯域を遵守していたかどうかの情報である。

【００１８】

ステップ７０４で帯域違反と判定された場合、帯域監視処理部６１は、違反回数を確認する（ステップ７０６）。該当フローのエントリの初回違反時間８０３が０である場合、１回目であると判定される。

１回目と判断された場合、帯域監視処理部６１は、該当フローのエントリの初回違反時間８０３と前回違反時間８０４に、現在時刻を書き込む（ステップ７０８）。次に、帯域監視処理部６１は、該フローのエントリ情報を含む監視情報１９をアクション制御部９００へ送信する（ステップ７１０）。送信する監視情報１９は、帯域監視テーブルに“エントリ有”の情報と、フロー情報（送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等）と、帯域を違反したことを表す帯域違反情報と、違反が１回目であるという情報である。

ステップ７０６で２回目以降であると判断された場合、帯域監視処理部６１は、該当フローのエントリの前回違反時間８０４に現在時刻を格納する（ステップ７０９）。次に該当フローのエントリ情報を含む監視情報１９をアクション制御部９００へ送信する（ステップ７１１）。送信する監視情報１９は、帯域監視テーブルに“エントリ有”の情報と、フロー情報（送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等）と、帯域違反情報と、違反が２回目以降であるという情報である。

【００１９】

図９に、本実施の形態のアクション実行部を示すブロック図を示す。

アクション制御部９００を図９を用いて説明する。アクション制御部９００は、フロー情報を格納しておくフローデータベース９０と、アクションを決定するアクション決定部９１と、実行すべきアクションの内容と順序が格納されているアクションデータベース９２と、時間閾値情報９３と、現在時刻情報９４とを含む。

図１０に、フローデータベースの例を示す。

フローデータベース１０００は、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等の情報を格納するフロー情報フィールド１００１と、該当エントリが登録された時刻を格納するアクション開始時刻フィールド１００２と、アクションが実行されていた時間の長さを格納するアクション実行時間フィールド１００３を含む。

図１２に、アクションデータベースの例を示す。

アクションデータベース１２００は、アクションの開始時刻を表すフィールド１２０１と、アクションの終了時刻を表すフィールド１２０２と、アクション内容１２０３を含む。例えば、開始時刻０秒から終了時刻１０秒まではアクション内容としてアクションＴＯＳ値を“５”にマーキングの処理を実行、開始時刻１０秒から終了時刻３０秒まではアクション内容としてＷＲＥＤを実行、開始時刻３０秒から終了時刻６０秒まではアクション内容としてＵＰＣを実行、といったように、一連又は一組等のアクション処理を構成する各々のアクション内容とアクションの順序が設定される。開始時刻と終了時刻の間の時間が複数のテーブルで重複して設定された場合は、予め定められた順番により、例えば、テーブルアドレスが小さいものが優先して選択されるものとする。アクションデータベース９２と時間閾値情報９３は、例えば、管理端末１８０を用いて事前に設定することができる。

【００２０】

図１１に、本実施の形態のアクション実行部のフローチャートを示す。

次にアクション制御部９００の詳細動作を図１１を用いて説明する。

アクション制御部９００のアクション決定部９１は、帯域監視部６００から送られてきた監視情報１９を元に、帯域監視テーブル６２にエントリが有ったかどうかのチェックを行う（ステップ１１００）。

ステップ１１００でエントリが無かったと判定された場合、アクション決定部９１は、パケット送信回路１５０に対し該当フローに対するアクションは何も実行せず、送信可能であるという情報を送信する（ステップ１１０５）。

ステップ１１００でエントリ有と判定された場合、アクション決定部９１は、次に帯域を遵守していたか違反していたかのチェックを行う（ステップ１１０１）。

ステップ１１０１で遵守していたと判定された場合、アクション決定部９１は、さらに帯域制御部６００から送られてきた監視情報１９をもとに、一定時間以上帯域を遵守していたか判定する（ステップ１１０２）。

【００２１】

ステップ１１０２で一定時間以上帯域を遵守していたと判定された場合、アクション決定部９１は、フローデータベース９０より、フロー情報フィールドに格納されている送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等のフロー情報が一致するエントリが存在するかどうかを検索する（ステップ１１０３）。

ステップ１１０３の検索の結果、該当エントリが存在した場合、アクション決定部９１は、現在時刻情報９４及び時間閾値情報９３を参照し、現在時刻からアクション開始時刻１００２の差を求め、その差からさらに遵守していた時間である時間閾値情報９３に設定された値を減算した時間を求め、その時間を該当エントリのアクション実行時間フィールド１００３に書き込む（ステップ１１０４）。このフィールドを使用することで、次回同一のフローが帯域違反をした場合に、最も有効であったアクションを違反した直後から実行できるようにする。例えば、アクション開始時刻と現在時刻との差が３０秒であったならば（時間閾値情報９３に0が設定されている場合）、アクション実行時間フィールド１００３に３０という値が書き込まれる。次に、アクション決定部９１は、パケット送信回路１５０に対し、該当フローに対するアクションは何も実行せず、送信可能であるという情報を送信する（ステップ１１０５）。

【００２２】

ステップ１１０２で一定時間以上帯域を遵守していないと判定された場合、アクション決定部９１は、エントリ削除対象では無いと判断し、エントリの削除は行わず、パケット送信回路１５０に対し、該当フローに対するアクションは何も実行せず、送信可能であるという情報を送信する（ステップ１１０５）。

ステップ１１０３での検索の結果、該当エントリが存在しなかった場合、アクション決定部９１は、特にアクションは行わず、パケット送信回路１５０に対し、該当フローに対するアクションは何も実行せず、送信可能であるという情報を送信する（ステップ１１０５）。

【００２３】

一方、ステップ１１０１で違反していたと判定された場合、アクション決定部９１は、さらに帯域制御部６００から送られてきた監視情報１９を元に、違反が１回目か２回目以降なのかの判定を行う（ステップ１１０６）。

ステップ１１０６で１回目であると判定された場合、アクション決定部９１は、フローデータベース９０を参照し、フロー情報フィールドに格納されている送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等のフロー情報が一致するエントリが存在するかどうかを検索する（ステップ１１０７）。

【００２４】

ステップ１１０７でエントリが存在した場合、アクション決定部９１は、該当のエントリのアクション開始時刻１００２に“０”を書き込み、アクション実行時間１００３を読み込む。アクション決定部９１は、アクション実行時間１００３の情報より、次のように実行すべきアクションを決定する。すなわち、アクション決定部９１は、アクションデータベース９２より、アクション実行時間１００３の時間が開始時刻と終了時刻の間に入っているアクションを検索し決定する（ステップ１１０８）。次にアクション決定部９１は

、パケット送信回路１５０に対して決定されたアクションを実行するようにアクション指示情報１３を送信する（ステップ１１０９）。送信するアクション指示情報１３は、フロー情報（送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等）と、アクション内容である。

【００２５】

ステップ１１０７でエントリが存在していなかった場合、アクション決定部９１は、フローデータベース９０に新規にエントリを登録する。新しく、フロー情報フィールド１００１に送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョンを書き込み、アクション開始時刻１００２に現在時刻９４より現在時刻情報を読み込み値を書き込み、アクション実行時間に“０”を書き込む（ステップ１１１０）。次に、アクション決定部９１は、アクション開始時刻１００２と現在時刻９４の差にアクション実行時間を加算した値（ここでは“０”秒）が開始時刻１２０１と終了時刻１２０２の間に入っているアクションを、アクションデータベースより検索しアクション内容１２０３を決定する（ステップ１１１１）。この場合、開始時刻が０秒に設定されているアクションを検索することになる。次に、アクション決定部９１は、パケット送信回路１５０に対して決定されたアクションを実行するようにアクション指示情報１３を送信する（ステップ１１０９）。送信するアクション指示情報１３は、フロー情報（送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等）と、アクション内容である。

【００２６】

ステップ１１０６で２回目以降であると判定された場合、アクション決定部９１は、フローデータベース９０を参照し、フロー情報フィールドに格納されている送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等のフロー情報が一致するエントリが存在するかどうかを検索する。２回目以降の場合は必ずエントリが存在するので、アクション決定部９１は、該当エントリのアクション開始時刻１００２とアクション実行時間１００３を読み込む。アクション決定部９１は、現在時刻情報９４を参照し、アクション開始時刻と現在時刻との差を求め、その値とアクション実行時間の値を加算する。アクション決定部９１は、その加算した値が開始時刻１２０１と終了時刻１２０２の間に入っているアクションをアクションデータベース９２より検索し、アクション内容１２０３を決定する。例えば、アクション開始時刻と現在時刻との差が１０秒であり、アクション実行時間の値が３０秒であれば、合計４０秒となる。この４０秒の値を元に、アクションデータベース９２より開始時刻１２０１と終了時刻１２０２の間に４０秒を含むアクション内容１２０３を検索することになる。例えば、開始時刻１０秒、終了時刻６０秒のアクションがあれば、そのアクションが選択される。次にアクション決定部９１は、パケット送信回路１５０に対して決定されたアクションを実行するように情報を送信する（ステップ１１０９）。送信するアクション指示情報１３は、フロー情報（送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号、宛先ポート番号、プロトコル番号、ＩＰバージョン等）と、アクション内容である。

【００２７】

パケット送信回路１５０では、アクション制御部９００から送られてきたアクション指示情報１３を元に、該当フローに対して制御を行う。例えば、アクション内容としての実行情報がＴＯＳ値の書き換えといったパケットヘッダの書き換え指示であったならば、パケット送信回路１５０は、パケットの該当フィールドの値を書き換える。例えば、アクション内容としての実行情報がパケットの廃棄であったならば、パケット送信回路１５０は、該当パケットの廃棄処理を行う。特にアクションが指示されていなければ、パケット送信回路１５０は、該当フローに相当するパケットをそのまま送信する。

【００２８】

本実施の形態ではアクションデータベースを一組だけ持つ例を示したが、複数組みのアクションデータベースをもっても良い。どの組みのアクションデータベースを選択するかは、フローの特長毎に割り当てれば良い。例えば、受信パケットの宛先ポート番号の範囲

でアクションデータベースの組みを決定しても良い。例えば、宛先ポートが０～１０２４まではアクションデータベースの１組目からアクションを決定、１０２５～２０４８まではアクションデータベースの２組目からアクションを決定、それ以外はアクションデータベースの３組目から決定、等としてもよい。また同様に、プロトコル番号の範囲でアクションデータベースの範囲を決定しても良い。さらには、時刻によりアクションデータベースを決定してもよい。０時～１２時まではアクションデータベースの１組目からアクションを決定。１２時～２４時まではアクションデータベースの２組目からアクションを決定としてもよい。

以上のように、複数の制御動作を順番に実行するアクション制御部９００において、あらかじめ設定された制御順番を最適なものに自律的に変更することができる。また、アクション制御部９００は、フローがポリシ違反している時間の長さにより、制御動作の切替を行うことができる。さらに、アクション制御部９００は、制御の順番と制御内容を記載した組みを複数組み持つことができる。

【産業上の利用可能性】

【００２９】

以上、本発明の実施の形態について説明したが、本システムは上述の図示例にのみ限定されるものではない。上述の説明では帯域監視部６００で監視を実行するにあたり、帯域を用いたが、これを帯域ではなく、該当フローが消費している電力を算出し、電力を監視することで遵守、違反を判定しても良い。また、単位時間あたりのセッション開始数を監視対象としても良い。

【図面の簡単な説明】

【００３０】

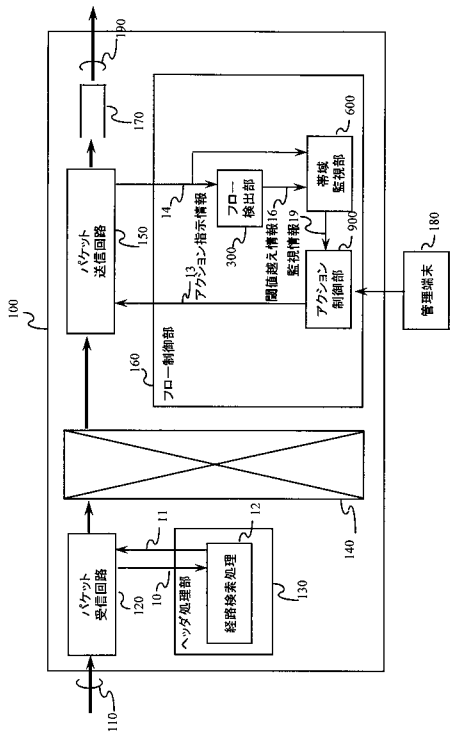
【図１】本実施の形態を適用したルータ１００を説明するブロック図。
【図２】パケットのフォーマットを表す図。
【図３】本実施の形態のフロー検出部を示すブロック図。
【図４】本実施の形態のフローテーブルのフォーマットを表す図。
【図５】本実施の形態のフロー検出部のフローチャートを表す図。
【図６】本実施の形態の帯域監視部を示すブロック図。
【図７】本実施の形態の帯域監視部のフローチャートを表す図。
【図８】本実施の形態の帯域監視テーブルのフォーマットを表す図。
【図９】本実施の形態のアクション実行部を示すブロック図。
【図１０】本実施の形態のフローデータベースのフォーマットを表す図。
【図１１】本実施の形態のアクション実行部のフローチャートを表す図。
【図１２】本実施の形態のアクションデータベースのフォーマットを表す図。

【符号の説明】

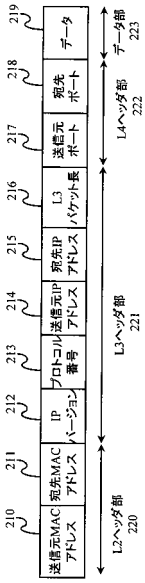
【００３１】

１６０…フロー制御部
３００…フロー検出部
６００…帯域監視部
９００…アクション制御部
１０…パケットヘッダ情報
１１…出力回線番号
１３…アクション指示情報
１４…パケットヘッダ情報
１６…閾値越え情報
１９…監視情報

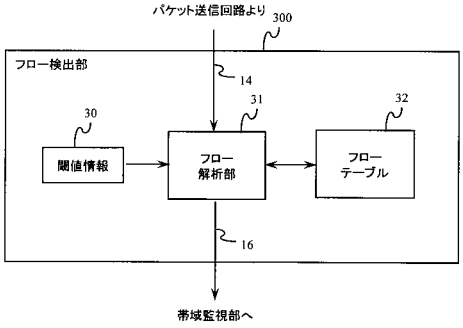
【図１】


100
110
120
130
140
150
160
170
180
190
300
600
900
パケット送信回路
パケット受信回路
フロー制御部
フロー検出部
帯域監視部
アクション制御部
管理端末
ヘッダ処理部
経路検索処理
L3アクション指示情報
閾値越え情報
監視情報

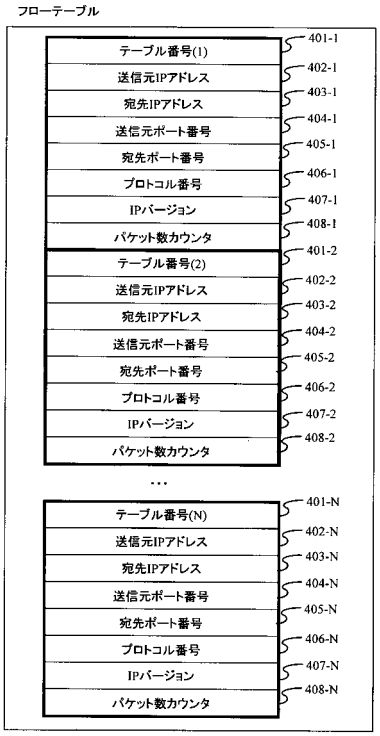
【図２】


219 データ
218 宛先ポート
217 送信元ポート
216 L3パケット長
215 宛先IPアドレス
214 送信元IPアドレス
213 プロトコル番号
212 IPバージョン
211 宛先MACアドレス
210 送信元MACアドレス
データ部 223
L4ヘッダ部 222
L3ヘッダ部 221
L2ヘッダ部 220

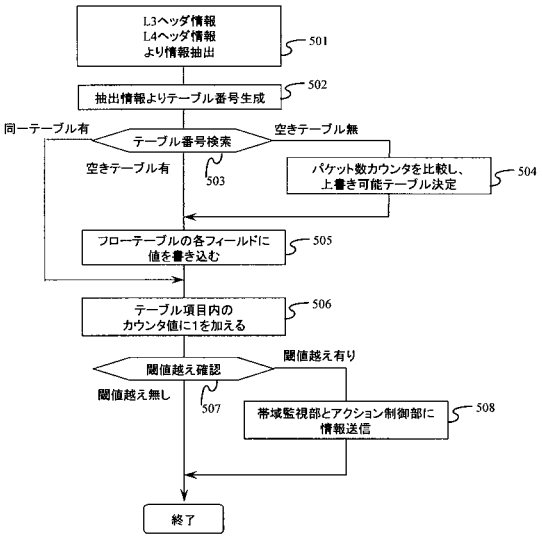
【図３】


パケット送信回路より
300
フロー検出部
14
30
閾値情報
31
フロー解析部
32
フローテーブル
16
帯域監視部へ

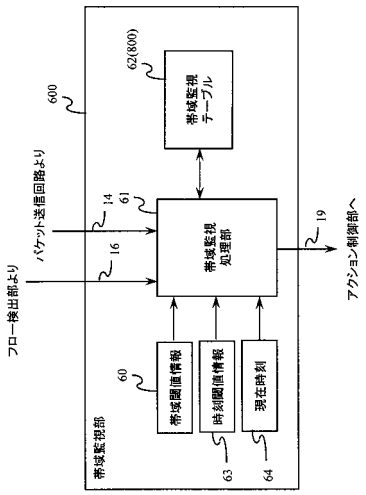
【図４】


フローテーブル
テーブル番号(1) 401-1
送信元IPアドレス 402-1
宛先IPアドレス 403-1
送信元ポート番号 404-1
宛先ポート番号 405-1
プロトコル番号 406-1
IPバージョン 407-1
パケット数カウンタ 408-1
テーブル番号(2) 401-2
送信元IPアドレス 402-2
宛先IPアドレス 403-2
送信元ポート番号 404-2
宛先ポート番号 405-2
プロトコル番号 406-2
IPバージョン 407-2
パケット数カウンタ 408-2
…
テーブル番号(N) 401-N
送信元IPアドレス 402-N
宛先IPアドレス 403-N
送信元ポート番号 404-N
宛先ポート番号 405-N
プロトコル番号 406-N
IPバージョン 407-N
パケット数カウンタ 408-N

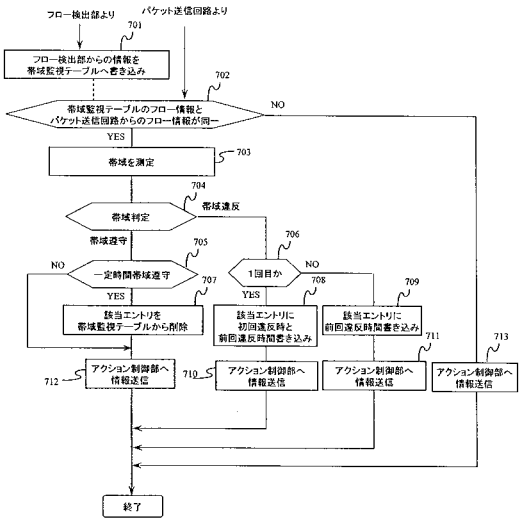
【図５】


L3ヘッダ情報
L4ヘッダ情報
より情報抽出
501
抽出情報よりテーブル番号生成
502
同一テーブル有
テーブル番号検索
空きテーブル無
空きテーブル有
503
パケット数カウンタを比較し、
上書き可能テーブル決定
504
フローテーブルの各フィールドに
値を書き込む
505
テーブル項目内の
カウンタ値に1を加える
506
閾値越え確認
閾値越え有り
閾値越え無し
507
帯域監視部とアクション制御部に
情報送信
508
終了

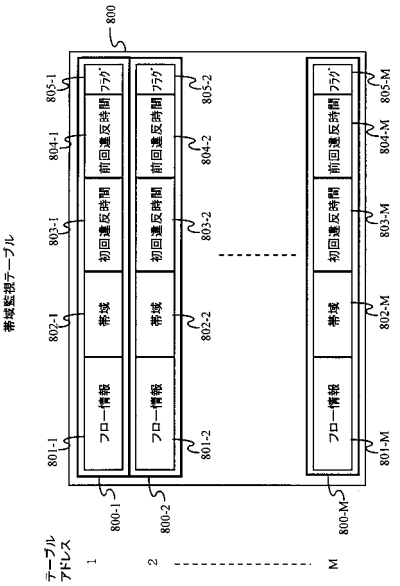
【図６】


600
62(800)
帯域監視
テーブル
パケット送信回路より
14
61
16
帯域監視
処理部
19
アクション制御部へ
フロー検出部より
60
帯域閾値情報
時刻閾値情報
現在時刻
帯域監視部
63
64

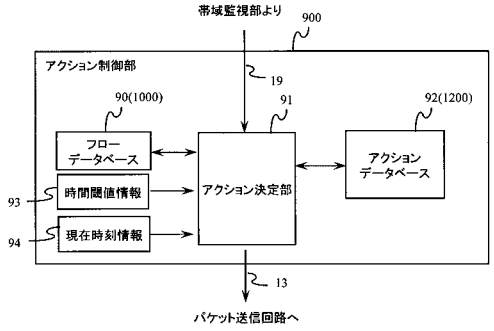
【図７】


フロー検出部より
パケット送信回路より
701
フロー検出部からの情報を
帯域監視テーブルへ書き込み
702
帯域監視テーブルのフロー情報と
パケット送信回路からのフロー情報が同一
NO
YES
帯域を測定
703
704
帯域判定
帯域違反
帯域遵守
705
706
NO
一定時間帯域遵守
1回目か
NO
YES
707
708
709
該当エントリを
帯域監視テーブルから削除
該当エントリに
初回違反時と
前回違反時間書き込み
該当エントリに
前回違反時間書き込み
711
713
712
710
アクション制御部へ
情報送信
アクション制御部へ
情報送信
アクション制御部へ
情報送信
アクション制御部へ
情報送信
終了

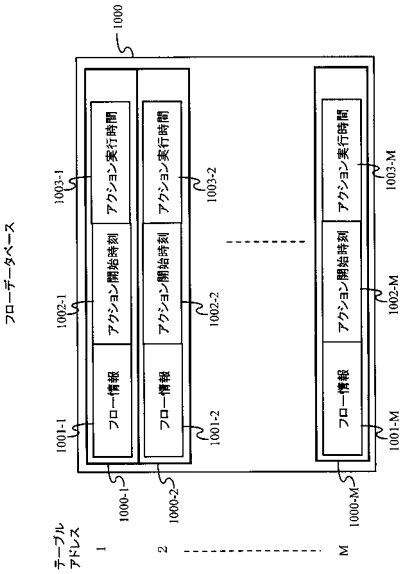
【図８】


800
帯域監視テーブル
805-1
804-1
803-1
802-1
801-1
フラグ
前回違反時間
初回違反時間
帯域
フロー情報
805-2
804-2
803-2
802-2
801-2
805-M
804-M
803-M
802-M
801-M
800-1
800-2
800-M
テーブル
アドレス
1
2
M

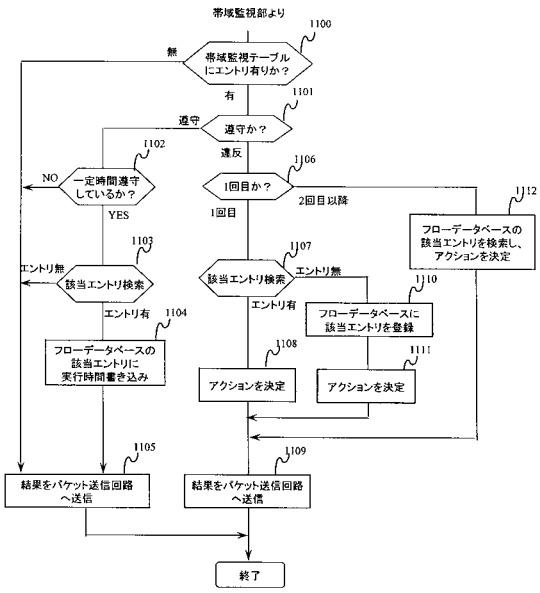
【図９】



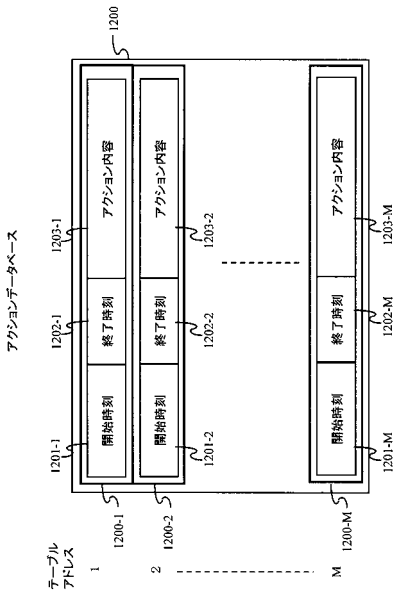
【図１０】



【図１１】



【図１２】



フロントページの続き

Ｆターム(参考) 5K030 GA13 HA08 HB11 HC01 HD03 JA10 KA04 KA05 LC01 LC14
MA04 MB18 MC08 MD08