

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4392294号
(P4392294)

(45) 発行日 平成21年12月24日 (2009. 12. 24)

(24) 登録日 平成21年10月16日 (2009. 10. 16)

(51) Int. Cl.

H04L 12/56 (2006.01)

F I

H04L 12/56 400Z

請求項の数 9 (全 36 頁)

(21) 出願番号	特願2004-176535 (P2004-176535)	(73) 特許権者	000005108
(22) 出願日	平成16年6月15日 (2004. 6. 15)		株式会社日立製作所
(65) 公開番号	特開2006-5402 (P2006-5402A)		東京都千代田区丸の内一丁目6番6号
(43) 公開日	平成18年1月5日 (2006. 1. 5)	(74) 代理人	110000350
審査請求日	平成19年3月13日 (2007. 3. 13)		ポレール特許業務法人
		(74) 代理人	100068504
			弁理士 小川 勝男
		(74) 代理人	100086656
			弁理士 田中 恭助
		(74) 代理人	100094352
			弁理士 佐々木 孝
		(72) 発明者	赤羽 真一
			東京都国分寺市東恋ヶ窪一丁目280番地
			株式会社日立製作所 中央研究所内

最終頁に続く

(54) 【発明の名称】 通信統計収集装置

(57) 【特許請求の範囲】

【請求項 1】

パケットフローを識別するためのフロー識別条件を定義した複数のフローエントリからなるフローテーブルと、ネットワーク受信パケットのヘッダから抽出された複数のヘッダ情報項目の組合せをフロー検索キーとして、上記フローテーブルからフロー検索キーに該当するフロー識別条件をもつフローエントリを検索する検索処理部を有し、上記フローテーブルの検索結果を利用して、パケットフロー別の統計情報を収集する通信統計情報収集装置において、

フロー識別条件と対応して、統計対象とすべきパケットを限定するための統計制御情報を定義した少なくとも1つの統計制御エントリを含む統計機能制御テーブルを有し、

上記検索処理部が、各受信パケットのヘッダ情報から生成したフロー検索キーに従って上記フローテーブルを検索し、フロー検索キーに該当するフローエントリがなかった場合に上記統計機能制御テーブルを検索し、上記フロー検索キーに該当する統計制御エントリが検索された時、該統計制御エントリが示す統計制御情報に従って、該統計制御エントリのフロー識別条件に該当するパケットフローの統計情報の収集処理を実行することを特徴とする通信統計情報収集装置。

【請求項 2】

前記統計機能制御テーブルが、フロー識別条件として、フロー検索キーとなる複数のヘッダ情報項目のうちの少なくとも1つについて統計対象となるパケットが備えるべきヘッダ情報値を指定した第1、第2の統計制御エントリを含み、

10

20

上記第1の統計制御エントリの統計制御情報が、フロー識別条件に該当するパケットフローについて、フロー検索キーで識別されるパケットフロー別に統計情報を収集すべきことを指定し、上記第2の統計制御エントリの統計制御情報が、フロー識別条件に該当するパケットフローについて、所定のサンプリングレートで受信パケットのコピーを生成すべきことを指定しており、

前記検索処理部が、フロー検索キーに該当するエントリとして上記第1の統計制御エントリが検索された時、前記フローテーブルに上記フロー検索キーをフロー識別条件とする新たなフローエントリを追加するための手段と、フロー検索キーに該当するエントリとして上記第2の統計制御エントリが検索された時、フロー識別条件に該当する受信パケットのコピーを所定のサンプリングレートで生成し、特定の統計情報処理装置に転送するための制御動作を開始する手段とを備えたことを特徴とする請求項1に記載の通信統計情報収集装置。

10

【請求項3】

前記統計機能制御テーブルが、フロー識別条件として、フロー検索キーとなる複数のヘッダ情報項目のうちの少なくとも1つについて統計対象となるパケットが備えるべきヘッダ情報値を指定し、統計制御情報の一部として、新たなフローエントリを登録すべきことを示す登録フラグを含む第1の統計制御エントリを含み、

前記検索処理部が、上記統計機能制御テーブルから、フロー検索キーに該当する統計制御エントリとして上記第1の統計制御エントリが検索された時、受信パケットのヘッダから抽出された複数のヘッダ情報項目の組合せをフロー識別条件とする新たなフローエントリを前記フローテーブルに追加するエントリ管理部を有することを特徴とする請求項1または請求項2に記載の通信統計情報収集装置。

20

【請求項4】

前記第1の統計制御エントリが、統計制御情報の一部として、統計処理の開始条件を含み、

前記エントリ管理部が、上記統計機能制御テーブルから上記第1の統計制御エントリが検索された時、上記統計処理の開始条件と該第1の統計制御エントリに対応した統計情報エントリが示す統計情報とを照合し、統計処理の開始条件が満たされた時点で、前記新たなフローエントリを前記フローテーブルに追加することを特徴とする請求項3に記載の通信統計情報収集装置。

30

【請求項5】

パケットフローを識別するためのフロー識別条件を定義した複数のフローエントリからなるフローテーブルと、ネットワーク受信パケットのヘッダから抽出された複数のヘッダ情報項目の組合せをフロー検索キーとして、上記フローテーブルからフロー検索キーに該当するフロー識別条件をもつフローエントリを検索する検索処理部を有し、上記フローテーブルの検索結果を利用して、パケットフロー別の統計情報を収集する通信統計情報収集装置において、

上記フローテーブルが、フロー識別条件と対応して、統計対象とすべきパケットを限定するための統計制御情報を定義した通常の統計制御エントリと、上記フロー識別条件として、検索キーとなる複数のヘッダ情報項目のうちの少なくとも1つについて統計対象となるパケットが備えるべきヘッダ情報値を指定し、統計制御情報の一部として、新たなフローエントリを登録すべきことを示す登録フラグを含む第1の統計制御エントリとを含み、

40

上記検索処理部が、各受信パケットのヘッダ情報から生成したフロー検索キーに該当するエントリとして、上記フローテーブルから上記通常の統計制御エントリが検索された時、該統計制御エントリが示す統計制御情報に従って、該統計制御エントリのフロー識別条件に該当するパケットフローの統計情報の収集処理を実行し、上記フローテーブルから上記第1の統計制御エントリが検索された時、受信パケットのヘッダから抽出された複数のヘッダ情報項目の組合せをフロー識別条件とする新たなフローエントリを前記フローテーブルに追加することを特徴とする通信統計情報収集装置。

【請求項6】

50

前記フローテーブルが、統計制御情報の一部として、所定のサンプリングレートで生成した受信パケットのコピーを予め指定された統計情報処理装置に転送するサンプル処理の開始条件と、サンプル処理の実行可否を示すサンプル処理フラグとを含む第2の統計制御エントリを含み、

前記検索処理部が、

上記フローテーブルから上記第2の統計制御エントリが検索された時、サンプル処理フラグがオフ状態であれば、上記サンプル処理の開始条件と該第2の統計制御エントリに対応した統計情報エントリが示す統計情報とからサンプル処理の開始可否を判定し、サンプル処理の開始条件が満たされた時点で上記サンプル処理フラグをオン状態に変更するサンプル判定部と、

10

サンプル処理フラグがオン状態の時、所定のサンプリングレートで受信パケットのコピーを生成するための制御信号を発生するサンプル処理部を備えたことを特徴とする請求項5に記載の通信統計情報収集装置。

【請求項7】

前記第2の統計制御エントリが、統計制御情報の一部として、サンプル処理の終了条件を含み、

前記サンプル判定部が、前記第2の統計制御エントリが検索された時、サンプル処理フラグがオン状態であれば、上記サンプル処理の終了条件と該統計制御エントリに対応した統計情報エントリが示す統計情報とからサンプル処理の終了可否を判定し、サンプル処理の終了条件が満たされた時点で上記サンプル処理フラグをオフ状態に戻すことを特徴とする請求項6に記載の通信統計情報収集装置。

20

【請求項8】

ネットワークに接続された通信統計情報収集装置であって、

パケットフローを識別するためのフロー識別条件と対応して、統計制御情報を定義した複数のフローエントリからなるフローテーブルと、

上記フローテーブルの各エントリと対応して統計情報を蓄積するための複数の統計情報エントリからなる統計情報テーブルと、

上記ネットワークから受信したパケットのヘッダから抽出された複数のヘッダ情報項目の組合せをフロー検索キーとして、上記フローテーブルからフロー検索キーに該当するフロー識別条件をもつフローエントリを検索するフローテーブル検索部と、

30

上記フローテーブル検索部によって検索されたフローエントリと対応する統計情報エントリに、パケットフロー別の統計情報を収集する統計収集処理部と、

上記統計情報テーブルに蓄積された統計情報を予め指定された他の統計情報処理装置に通知するためのパケットを生成する統計情報通知パケット生成部と、

上記フローテーブル検索部によって検索された特定のフローエントリが示す統計制御情報に従って、上記他の統計情報処理装置に転送すべき受信パケットのコピーを所定のサンプリングレートで生成するコピー生成部とを有することを特徴とする通信統計情報収集装置。

【請求項9】

前記フローテーブルが、フロー検索キーとなる複数のヘッダ情報項目のうちの少なくとも1つについて統計対象となるパケットが備えるべきヘッダ情報値を指定したフロー識別条件と対応して、統計対象とすべきパケットを限定するための統計制御情報を定義した少なくとも1つの統計制御エントリを含み、

40

前記フローテーブル検索部によって、フロー検索キーに該当するエントリとして上記統計制御エントリが検索された時、該エントリが示す統計制御情報に従って、上記フロー検索キーの内容をフロー識別条件とする新たなフローエントリを上記フローテーブルに追加するためのエントリ管理部を有することを特徴とする請求項8に記載の通信統計情報収集装置。

【発明の詳細な説明】

【技術分野】

50

【0001】

本発明は、通信統計収集装置に関し、更に詳しくは、通信ネットワークにノード装置として接続され、パケットフロー別にパケット数、バイト数などの統計情報を収集する通信統計収集装置に関する。

【背景技術】

【0002】

インターネットは、重要な社会インフラストラクチャとして定着し、従来のBest-Effort型データ通信だけでなく、音声、動画などのリアルタイムデータや、基幹業務のトランザクションデータなど、通信品質の保証を必要とするデータ通信にも応用され始めている。また、ADSL (Asymmetric Digital Subscriber Line) や、FTTH (Fiber To The Home) 技術によるアクセス回線のブロードバンド化に伴い、通信されるデータ量も増大化傾向にある。

10

【0003】

このような背景から、キャリアやISP (Internet Service Provider) などの通信サービス事業者は、ネットワーク上での通信状態を把握するために、通信データ量などの統計情報の収集と分析を行うネットワーク監視機能を必要としている。特に、データの送信元や宛先、アプリケーション、品質レベルなどによって分類される通信データ群（以下、フローと呼ぶ）毎に統計情報を収集、分析する機能の高度化要求が高い。

【0004】

キャリアやISPは、このようなフロー毎の統計情報を利用することによって、品質保証した通信サービスの提供時に、通信品質の保証状況を確認することが可能となる。また、限られたネットワーク資源を有効に活用して、データ量の増大に対応するトラフィック・エンジニアリング（以下、TEと略す）が可能となる。更には、顧客の需要を予測してネットワーク資源を計画的に準備し、通信帯域やサービスなどのユーザ要求に対して迅速にネットワーク資源を提供するプロビジョニングや、ネットワーク資源に対する不正ユーザからの攻撃の検出および分析、課金などを行うことが可能となる。統計情報収集機能は、一般に、ネットワーク上でパケットの転送制御を行うルータ、スイッチ等のノード装置に装備される。

20

【0005】

フロー統計情報の収集方式として、例えば、http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/nflov_pg.pptに記述されたキャッシュ型のフロー統計技術（非特許文献1）が知られている。上記従来技術を適用した統計情報収集システムは、ネットワーク上に分散して配置された複数の統計情報収集装置と、これらの統計情報収集装置から定期的に通知される統計情報に基づいて、ネットワーク全体のトラフィックを分析するコレクタ装置から構成される。

30

【0006】

キャッシュ型の統計情報収集機能をもつルータは、受信パケットの所属フローを識別するためのフローテーブルを備え、パケット受信の都度、受信パケットのヘッダ情報項目やパケットの入力回線インターフェース番号等を組合せからなる検索キーに従って、フローテーブルを検索する。フローテーブルは、フロー毎に用意された複数のフローエントリからなり、各フローエントリは、例えば、送信元IPアドレス、宛先IPアドレス、プロトコル種別、TOS (Type of Service) 値、送信元TCP (Transmission Control Protocol) /UDP (User Datagram Protocol) ポート番号、宛先TCP/UDPポート番号、入力回線インターフェース番号等の組合せによってフロー識別条件を定義している。

40

【0007】

受信パケットがフローテーブルに登録された何れかのフロー識別条件に一致した場合、このフロー識別条件と対応して用意された統計情報エントリにおいて、パケット数やバイト数等の統計データが更新される。上記フローテーブル検索の結果、受信パケットがフローテーブル上のどのフロー識別条件にも一致しなかった場合は、検索キーとなったヘッダ情報項目と入力インターフェース番号等の組合せをフロー識別条件とする新たなフローエ

50

ントリがフローテーブルに追加される。統計情報エントリの内容は、定期的に監視され、例えば、一定時間以上、統計データに変化がない統計情報エントリの内容が、統計情報データとしてコレクタ装置に送信される。また、コレクタ装置に通知済みとなった統計情報エントリと、これに対応するフローエントリは、エージング処理によってテーブルから削除される。

【0008】

フロー統計情報の他の収集方式として、例えば、Internet Engineering Task Force (IETF) のRFC3176 (非特許文献2) に記載されたサンプリング型のフロー統計技術が知られている。サンプリング型の統計情報収集システムでは、各ルータが、受信パケットのコピーを選択的にコレクタ装置に転送し、コレクタ装置側で、これらのコピーパケットからフローを識別し、統計情報の収集と分析を行う。

10

【0009】

サンプリング型の統計情報収集システムを構成する各ルータは、予めネットワーク管理者によって設定されたサンプリングレートに従って、受信パケットをサンプリングし、サンプリングされた受信パケットのコピー (コピーパケット) を予め規定されたカプセル化フォーマットでコレクタ装置に転送する。各カプセル化パケットには、例えば、受信パケットの入力回線インターフェース番号や、受信パケットのヘッダ情報から特定される出力回線インターフェース番号、次転送先ルータのIPアドレス (Next Hop IPアドレス) など、フロー識別用の情報が追加される場合もある。コレクタ装置は、ルータから転送されたカプセル化パケットからコピーパケットを抽出し、コピーパケットのヘッダ情報と、必要に応じて追加されたフロー識別用情報に基づいてフローを識別し、フロー別の統計情報を更新する。

20

【0010】

【非特許文献1】 <http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/nflov-pg.ppt>

【0011】

【非特許文献2】 Internet Engineering Task Force (IETF) のRFC3176

【発明の開示】

【発明が解決しようとする課題】

【0012】

上述したキャッシュ型の従来の統計情報収集システムでは、フロー識別条件と検索キーに適用される情報要素の組合せが固定的であり、統計情報を収集する各ルータが、全ての受信パケットについて一律にフロー別の統計情報を収集している。従って、フローテーブルに登録されるフローエントリ数、および統計情報エントリ数が増加するという問題がある。

30

【0013】

一般に、フロー識別に必要となるフロー識別条件情報は、200~600ビット程度となる。このような多数ビット情報を検索キーとして高速にテーブル検索する方式として、CAM (Content Addressable Memory) 用いた検索方式がある。CAM方式は、メモリに登録されたフロー識別条件を示すビットパターンと、検索キーとして与えられたビットパターンとを高速にマッチングすることが可能となる。しかしながら、CAMは、通常の半導体メモリに比較してビット単価が高いため、キャッシュ型の従来の統計情報収集システムのように、各ルータにおけるフローエントリ数が増加すると、フローテーブルの構成に多数のCAMチップを要し、ルータ価格が高価になるという問題がある。

40

【0014】

また、キャッシュ型の従来の統計情報収集システムでは、フロー識別条件として、固定的なヘッダ情報項目の組合せしか適用できないため、前述した情報項目以外の他の情報要素、例えば、TCPコネクションの制御パケット種類を識別するためのTCPフラグや、イーサネット (Ethernet: 登録商標) ヘッダ内の宛先MAC (Media Access Control) アドレス、送信元MACアドレス、仮想LANを識別するためのVLAN (Virtual LAN)

50

識別子などをフロー識別に利用することが困難となる。

【0015】

一方、サンプリング型の統計情報収集システムでは、コレクタ装置側でフロー識別しているため、ルータ側でフロー識別するキャッシュ型では不可能な高プロトコルレイヤのヘッダ情報を用いたフロー分類と、パケットデータの内容分析に基づく統計情報の収集が可能となる。また、サンプリング型では、受信パケットの入力回線インターフェース毎にコピーパケット生成のためのサンプリング可否を指定できるため、例えば、統計対象パケットを特定入力回線からの受信パケットに限定することによって、フロー統計精度を高めることが可能となる。

【0016】

しかしながら、サンプリング型の従来の統計情報収集システムでは、入力回線インターフェース以外の単位、例えば、プロトコル種別によるサンプリングの可否指定ができないため、コレクタ装置におけるフロー統計精度の向上に制約がある。また、従来技術では、サンプリングの可否は、ネットワーク管理者が予め設定しておく必要があり、サンプリング可否の設定をトラフィックの状況に応じてダイナミックに変えることができないという問題がある。

【0017】

本発明の目的は、統計対象パケットを動的に選択して、パケットフロー別の統計情報を収集可能にした通信統計情報収集装置を提供することにある。

本発明の他の目的は、予め指定された属性をもつパケットフローについて、フローテーブルにフロー識別エントリを柔軟に登録可能な通信統計情報収集装置を提供することにある。

本発明の更に他の目的は、パケットフローによってキャッシュ型とサンプリング型の統計情報収集機能を選択的に適用可能な通信統計情報収集装置を提供することにある。

【課題を解決するための手段】

【0018】

上記目的を達成するために、本発明の統計情報収集装置は、パケットフローを識別するためのフロー識別条件を定義した複数のフローエントリからなるフローテーブルと、フロー識別条件と対応して、統計対象とすべきパケットを限定するための統計制御情報を定義した少なくとも1つの統計制御エントリを含む統計機能制御テーブルと、ネットワーク受信パケットのヘッダから抽出された複数のヘッダ情報項目の組合せをフロー検索キーとして、上記フローテーブルと統計機能制御テーブルからフロー検索キーに該当するフロー識別条件をもつエントリを検索する検索処理部を有し、

上記検索処理部が、各受信パケットのヘッダ情報から生成したフロー検索キーに従ってフローテーブルを検索し、フロー検索キーに該当するフローエントリがなかった場合に統計機能制御テーブルを検索し、上記フロー検索キーに該当する統計制御エントリが検索された時、該統計制御エントリが示す統計制御情報に従って、該統計制御エントリの識別条件に該当するパケットフローの統計情報収集処理を実行することを特徴とする。

【0019】

本発明の特徴の1つは、上記検索処理部が、フロー検索キーに該当するエントリとして統計制御エントリが検索された時、該統計制御エントリが示す統計制御情報に従って、上記フローテーブルまたは上記統計機能制御テーブルの内容を変更することにある。

上記統計制御エントリは、通常のフローエントリとは異なり、フロー識別条件として、フロー検索キーとなる複数のヘッダ情報項目のうちの少なくとも1つについて、統計対象となるパケットが備えるべきヘッダ情報値を指定している。本発明の好ましい実施形態では、テーブル検索を高速化するため、上述した統計機能制御テーブルをフローテーブルに統合しておき、フロー検索キーに該当するフローエントリが見つからなかった時、フローテーブルからフロー検索キーに該当する統計制御情報エントリを検索できるようにしている。

【0020】

更に詳述すると、本発明の統計情報収集装置は、フローエントリおよび統計制御エントリのそれぞれと対応して統計情報を蓄積するための複数の統計情報エントリからなる統計情報テーブルを有し、上記検索処理部が、フロー検索キーによって検索されたフローエントリまたは統計制御エントリと対応する統計情報エントリにおいて、パケット受信に伴った統計情報の更新処理を行う統計収集処理部を備える。

【0021】

本発明の1つの特徴は、上記統計機能制御テーブル（またはフローテーブル）が、統計制御情報の一部として新たなフローエントリを登録すべきことを示す登録フラグを含む第1の統計制御エントリを含み、上記検索処理部によって、フロー検索キーに該当するエントリとして上記第1の統計制御エントリが検索された時、フロー検索キーで特定されるパケットフロー別の統計情報を収集するために、受信パケットのヘッダから抽出された複数のヘッダ情報項目の組合せをフロー識別条件とする新たなフローエントリを上記フローテーブルに追加するためのエントリ管理部を有することにある。

10

【0022】

本発明のもう1つの特徴は、上記統計機能制御テーブル（またはフローテーブル）が、統計制御情報で、フロー識別条件に該当するパケットフローについて、所定のサンプリングレート受信パケットのコピーを生成すべきことを指定した第2の統計制御エントリを含み、上記検索処理部が、フロー検索キーに該当するエントリとして上記第2の統計制御エントリが検索された時、フロー識別条件に該当する受信パケットのコピーを所定のサンプリングレートで生成し、コピーパケットを特定の統計情報処理装置に転送するための制御動作を開始することにある。

20

【0023】

本発明の1実施例では、上記第2の統計制御エントリが、統計制御情報の一部として、所定のサンプリングレートで生成した受信パケットのコピーを予め指定された統計情報処理装置に転送するサンプル処理の開始条件と、サンプル処理の実行可否を示すサンプル処理フラグとを含み、上記検索処理部が、フロー検索キーに該当するエントリとして上記第2の統計制御エントリが検索された時、サンプル処理フラグがオフ状態であれば、上記サンプル処理の開始条件と該第2の統計制御エントリに対応した統計情報エントリが示す統計情報とを照合し、サンプル処理の開始条件が満たされた時点で上記サンプル処理フラグをオン状態に変更するためのサンプル判定部と、サンプル処理フラグがオン状態の時、所定のサンプリングレートで受信パケットのコピーを生成するための制御信号を発生するためのサンプル処理部とを備える。

30

【0024】

本発明の1実施例では、上記第2の制御エントリが、統計制御情報の一部として、サンプル処理の終了条件を含む。この場合、サンプル判定部は、統計機能制御テーブルから第2の制御エントリが検索された時、サンプル処理フラグがオン状態であれば、上記サンプル処理の終了条件と該第2の制御エントリに対応した統計情報エントリが示す統計情報とを照合し、サンプル処理の終了条件が満たされた時点で上記サンプル処理フラグをオフ状態に戻す。サンプル処理の開始条件と終了条件は、例えば、パケットフローの帯域値で指定される。

40

【0025】

別の観点で見ると、本発明による通信統計情報収集装置は、

ネットワークから受信したパケットのヘッダから抽出された複数のヘッダ情報項目の組合せをフロー検索キーとして、フローテーブルからフロー検索キーに該当するフロー識別条件をもつフローエントリまたは統計制御エントリを検索するフローテーブル検索部と、

上記フローテーブル検索部によって検索されたエントリと対応する統計情報エントリに、パケットフロー別の統計情報を収集する統計収集処理部と、

統計情報テーブルに蓄積された統計情報を予め指定された他の統計情報処理装置に通知するためのパケットを生成する統計情報通知パケット生成部と、

上記フローテーブル検索部によって検索された特定のフローエントリが示す統計制御情

50

報に従って、上記他の統計情報処理装置に転送すべき受信パケットのコピーを所定のサンプリングレートで生成するコピー生成部とからなることを特徴とする。

【0026】

本発明による通信統計情報収集装置の1つの特徴は、上記フローテーブル検索部によって、フロー検索キーに該当するエントリとして上記統計制御エントリが検索された時、該エントリが示す統計制御情報に従って、上記フロー検索キーの内容をフロー識別条件とする新たなフローエントリを上記フローテーブルに追加するためのエントリ管理部を有することにある。

【0027】

統計情報通知パケット生成部への統計情報の供給は、上記エントリ管理部によって行うことができる。本発明の1実施例では、上記エントリ管理部が、上記統計情報テーブルの状態変化を監視し、所定時間を超えて統計情報に変化がない統計情報エントリを検出し、該統計情報エントリが示す統計情報と該エントリに対応するフロー識別条件を上記統計情報テーブルとフローテーブルから読み出して、上記統計情報通知パケット生成部に供給する。また、フローテーブルに新たなフローエントリを追加する時、上記エントリ管理部が、必要に応じてフローテーブルから削除すべきフローエントリを選択し、該フローエントリが示すフロー識別条件と、該フローエントリに対応する統計情報エントリが示す統計情報を上記フローテーブルと前記統計情報テーブルから読み出して、上記統計情報通知パケット生成部に供給する。

【0028】

本発明において、各フローエントリで定義するフロー識別条件は、例えば、受信パケットのIPヘッダから抽出されるヘッダ情報項目の他に、TCPあるいはUDPなどのレイヤ4ヘッダや、Ethernetなどのレイヤ2ヘッダから抽出されるヘッダ情報項目、受信パケットの入力回線番号および出力回線番号の組合せとすることができる。

【発明の効果】

【0029】

本発明によれば、統計制御エントリが示す統計制御情報で、統計対象となるパケットフローの種類を限定できるため、フローテーブルに登録されるフローエントリ数の増加を抑制できる。従って、フローテーブルに必要な高速メモリの容量が少なくて済み、装置価格を低減することが可能になる。

【0030】

また、本発明の構成によれば、統計制御エントリの統計制御情報によって、キャッシュ型とサンプリング型の統計情報収集を選択的に実行でき、サンプリング型の統計情報収集のためにコレクタ装置に転送すべきコピーパケットの生成条件を指定することも可能となる。例えば、監視対象となる特定パケットフローの属性をフロー識別条件とする統計制御エントリにおいて、統計制御情報の一部として、サンプリングの開始条件を示す帯域値を指定しておくことにより、上記特定パケットフローの帯域が開始条件に達した時点で、受信パケットのサンプリングを開始し、コピーパケットのコレクタ装置への転送を開始することが可能となる。

【0031】

この場合、コレクタ装置に送信されるサンプルの母集団を限定できるため、コレクタ装置における統計情報の蓄積を容易にし、分析精度を向上することが可能になる。また、これによって、例えば、特定サーバへのアタックデータ、ウィルスデータ等、トラフィックパターンに特徴があるパケットフローを自動的に検出し、解析することが容易になる。また、これによって、ネットワークやコレクタ装置のリソースの有効利用が可能になる。

【発明を実施するための最良の形態】

【0032】

以下、本発明の通信統計情報収集装置の実施例について図面を参照して説明する。

図1は、本発明の通信統計情報収集装置を適用したネットワーク構成の1例を示す。

ここに示したネットワークNWは、端末T1、T2、T3、T4を収容したルータR1

10

20

30

40

50

と、サーバS1を収容したルータR2と、サーバS2を収容したルータR3と、ルータR1に接続された統計情報のコレクタ装置C1から構成され、ルータR1が、本発明の通信統計情報収集装置としての機能を備えている。端末T1、T2、T3、T4は、それぞれ回線C-T1、C-T2、C-T3、C-T4を介してルータR1に接続され、ルータR1は、回線C-R2、C-R3を介してルータR2、R3に接続されている。

【0033】

上記ネットワークNWにおいて、端末T1、T3がサーバS1と、端末T2、T4がサーバS2と通信中で、サーバS1から端末T1、T3に送信されるIP (Internet Protocol) パケットのフローをそれぞれ「フロー1」、「フロー2」と呼び、サーバS2から端末T2、T4へのIPパケットフローをそれぞれ「フロー3」、「フロー4」と呼ぶことにする。

10

【0034】

ここで、フロー1は、IPの上位プロトコルがTCPで、IPヘッダ内のTOS (Type of Service) がTOS1、TCPヘッダ内の送信元ポート番号と宛先ポート番号が、それぞれSPRT1、DPRT1のパケット列からなり、フロー2は、IPの上位プロトコルがTCP、TOSがTOS1、送信元ポート番号と宛先ポート番号がそれぞれSPRT1、DPRT3のパケット列からなるものとする。また、フロー3は、IPの上位プロトコルがUDPで、TOSがTOS2、UDPヘッダ内の送信元ポート番号と宛先ポート番号がそれぞれSPRT2、DPRT2のパケット列からなり、フロー4は、IPの上位プロトコルがUDPで、TOSがTOS2、送信元ポート番号と宛先ポート番号が、それぞれSPRT2、DPRT4のパケット列からなるものとする。

20

【0035】

図2は、上記ネットワーク上で通信されるIPパケット10の構造を示す。

IPパケット10は、OSI (Open System Interconnection) 参照モデルのプロトコルレイヤに対応した複数レイヤのヘッダ、具体的には、レイヤ2ヘッダ11、レイヤ3ヘッダ12およびレイヤ4ヘッダ13と、データ14とから構成される。

【0036】

レイヤ2のプロトコルとしては、例えば、Ethernet (登録商標)、ATM (Asynchronous Transfer Mode)、MPLS (Multi-Protocol Label Switching) 等のプロトコルが適用でき、レイヤ3のプロトコルとしては、IP version 4 (IPv4)、IP version 6 (IPv6) 等のプロトコルを適用できる。また、レイヤ4のプロトコルとしては、TCP、UDP等のプロトコルを用いることができる。

30

【0037】

図3は、レイヤ2ヘッダ11の1例として、Ethernet V2フレームのヘッダ構造を示す。

Ethernet V2フレームヘッダには、フレームの開始を示すプリアンブル/SFD111と、レイヤ2における宛先端末アドレス (宛先MACアドレス) 112および送信元アドレス (送信元MACアドレス) 113と、レイヤ3のプロトコルを示すタイプ118が設定される。

【0038】

40

図4は、レイヤ2ヘッダ11の他の例として、Tag VLAN対応Ethernet V2フレームのヘッダ構造を示す。Tag VLAN対応のEthernet V2フレームヘッダには、フレームの開始を示すプリアンブル/SFD111、レイヤ2における宛先端末アドレス (宛先MACアドレス) 112および送信元アドレス (送信元MACアドレス) 113、Tag VLAN対応であることを示すTAGプロトコルID114、フレームの転送優先度を示す優先度115、レイヤ2のルーティング情報が格納されていることを示すCFI (Canonical Field Indicator) 116、VLAN識別子 (VLAN ID) 117と、レイヤ3のプロトコルを示すタイプ118が設定される。

【0039】

図5は、レイヤ3ヘッダ12の1例として、IPv4のヘッダ構造を示す。

50

I P v 4 ヘッダには、パケットの転送品質を示す T o S 1 2 1、レイヤ 4 のプロトコルを示すプロトコル 1 2 2、送信元 I P アドレス 1 2 6 A、宛先 I P アドレス 1 2 7 A、その他の情報が含まれる。T o S とプロトコルはそれぞれ 8 ビット、送信元 I P アドレスと宛先 I P アドレスはそれぞれ 3 2 ビットからなる。

【0040】

図 6 は、レイヤ 3 ヘッダ 1 2 の他の例として、I P v 6 のヘッダ構造を示す。

I P v 6 ヘッダには、パケットの転送品質を示すクラス 1 2 3、この I P v 6 ヘッダ部に続く次のヘッダの種別を示す次ヘッダ番号 1 2 5、送信元 I P アドレス 1 2 6 B、宛先 I P アドレス 1 2 7 B、その他の情報が含まれる。次ヘッダが、例えば、T C P や U D P の場合、次ヘッダ番号 1 2 5 として、レイヤ 4 のプロトコルを示す値が設定される。クラス 1 2 3 と次ヘッダ番号はそれぞれ 8 ビット、送信元 I P アドレスと宛先 I P アドレスは、それぞれ 1 2 8 ビットからなる。

10

【0041】

図 7 は、レイヤ 4 ヘッダ 1 3 の 1 例として、T C P のヘッダ構造を示す。

T C P ヘッダには、上位レイヤがアプリケーションを識別するための論理的なポート番号として、それぞれ 1 6 ビット長の送信元ポート番号 1 3 1 A および宛先ポート番号 1 3 2 A を含む。また、T C P コネクションにおけるパケット種別を示す T C P フラグ 1 3 3、その他の情報が含まれる。

【0042】

T C P フラグ 1 3 3 は、図 8 に示ように、受信端末に受信データを緊急にアプリケーションに渡すことを指示する緊急フラグ (U R G) 1 3 3 1、受信端末がデータを受信したことを送信端末に通知する A C K 1 3 3 2、送信端末と受信端末で遅延なくデータを渡すことを指示する P U S H 1 3 3 3、T C P コネクションのリセットを指示する R S T 1 3 3 4、コネクションの終了を指示する F I N 1 3 3 5、コネクションの確立を指示する S Y N 1 3 3 6 の 6 つのフラグから構成されている。

20

【0043】

図 9 は、レイヤ 4 ヘッダ 1 3 の他の例として、U D P のヘッダ構造を示す。

U D P ヘッダには、T C P ヘッダと同様、それぞれ 1 6 ビット長の送信元ポート番号 1 3 1 B と宛先ポート番号 1 3 2 B が含まれている。

【0044】

30

図 1 0 は、図 1 のルータ R 1 において統計情報の収集対象となるフロー識別条件を定義したフローテーブルの一部を示す。ここでは、統計情報の収集対象フローが、レイヤ 4 のプロトコルが T C P のフローに限定された場合を示している。

フローテーブルの各エントリは、フローエントリ番号 6 1 と対応して、フロー識別条件 6 2 と、図示しない統計制御情報とを示している。フロー識別条件 6 2 は、I P ヘッダが示す送信元 I P アドレス 6 2 1、宛先 I P アドレス 6 2 2、上位プロトコル 6 2 3 および T O S 6 2 4 と、T C P あるいは U D P ヘッダに含まれる送信元ポート番号 6 2 5 および宛先ポート番号 6 2 6 の値によって定義されている。尚、ここで示したヘッダ情報の組合せは、フロー識別条件の一例に過ぎず、フロー識別条件は、図 1 0 とは異なったヘッダ情報の組合せであってもよい。

40

【0045】

本発明の統計情報収集装置 (ルータ R 1) では、後述する検索処理部 4 0 によって、上記フローテーブルへのエントリの登録と削除、エントリ内容の部分的な訂正が動的に行われる。フローテーブルへの登録エントリをプロトコル種別が T C P のものに限定した場合、ルータ R 1 は、回線 C - R 2、C R - 3 から受信するパケットフローのうち、上位プロトコルが T C P となっているフロー 1 とフロー 2 のみをフローテーブルに登録することになる。

【0046】

図 1 1 は、ルータ R 1 の統計情報テーブルに収集される統計情報の一例を示す。

統計情報テーブルは、フローテーブルのフローエントリ番号 6 1 と対応した複数の統計

50

情報エントリからなる。

ここに示した例では、統計情報 7 2 として、フロー別の受信パケット数（以下、パケット数と言う） 7 2 1 と、受信パケットの累計バイト数（以下、バイト数と言う） 7 2 2 と、受信パケットの入力回線番号 7 2 3 と、受信パケットの転送先となる出力回線番号 7 2 4 と、その他の情報 7 2 9 とが収集されている。

【0047】

図 1 2 は、本発明の統計情報収集機能を備えたルータ R 1 の 1 実施例を示すブロック図である。

ルータ R 1 は、入力回線 I C n（n = 1 ~ N）に接続された受信パケット処理部 2 0 と、出力回線 O C n（n = 1 ~ N）に接続された送信パケット処理部 3 0 と、受信パケット処理部 2 0 に接続された検索処理部 4 0 と、検索処理部 4 0 に付随するフローテーブル 6 0、統計情報テーブル 7 0 およびルーティングテーブル 8 0 と、制御部 9 0 とから構成される。フローテーブル 6 0 は、後述するように、統計制御エントリを記憶した統計機能制御テーブルを兼用している。制御部 9 0 は、管理端末 1 3 0 0 に接続され、管理端末 1 3 0 0 からの指示に従って、受信パケット処理部 2 0、検索処理部 4 0、送信パケット処理部 3 0 に各種パラメータ情報の設定を行う。

【0048】

ルータ R 1 は、上述した受信パケット処理部 2 0、送信パケット処理部 3 0、検索処理部 4 0 および制御部 9 0 をそれぞれ専用の L S I で構成し、これらの専用 L S I を相互に接続した構成でもよいし、L S I 間の配線を少なくするために、複数の処理部を 1 つの専用 L S I で実現し、少数の専用 L S I を相互接続した構成としてもよい。また、専用 L S I を使用する代わりに、ルータ機能の一部を汎用の M P U（Micro Processing Unit）や N P（Network Processor）で実現してもよい。

【0049】

図 1 2 では、受信パケット処理部 2 0 と送信パケット処理部 3 0 とを信号線 L 1 で接続した構成を示しているが、受信パケット処理部 2 0 と送信パケット処理部 3 0 の個数をそれぞれ複数にし、受信パケット処理部と送信パケット処理部との間をクロスバースイッチで接続した装置構成とすることも可能である。また、検索処理部 4 0 が参照するフローテーブル 6 0 用のメモリとしては、高速の検索処理性能が要求される場合は、例えば、C A M または S S R A M を適用し、比較的低速の検索処理性能で十分な場合は、ビット当りの価格が安く、ビット当りのチップ面積も少なく済む D R A M を適用できる。

【0050】

図 1 3 は、ルータ R 1 の制御部 9 0 に接続される管理端末 1 3 0 0 の 1 例を示す。

管理端末 1 3 0 0 は、ルータ R 1 内の各種テーブルの内容を表示するための表示画面 1 3 0 1 と、表示画面に表示されたテーブル内容の任意箇所を選択、編集するためのマウス 1 3 0 2、キーボード 1 3 0 3 などの入力手段とからなる。管理端末 1 3 0 0 は、図 1 4 に示すように、ネットワーク N W を介してルータ R 1 に接続してもよい。また、管理端末 1 3 3 0 の機能をコレクタ装置 C 1 に持たせておき、コレクタ装置からルータのテーブル情報を更新するようにしてもよい。

【0051】

図 1 5 は、ルータ R 1 の内部で転送される内部パケットのフォーマットの 1 例を示す。

内部パケットは、図 2 に示したネットワークからの受信パケットの先頭に内部ヘッダ 1 5 を付加した構成となっている。内部ヘッダ 1 5 は、パケットの受信回線を示す入力回線番号 1 5 1 と、それぞれ検索処理部 4 0 によって決定されるパケットの出力回線番号 1 5 2、カプセル化指示フラグ 1 5 3、カプセルヘッダ情報 1 5 4 を含む。

【0052】

カプセル化指示フラグ 1 5 3 には、所定のレートでサンプリングした受信パケットのコピーをコレクタ装置 C 1 に転送する必要がある時、検索処理部 4 0 から送信パケット処理部 3 0 に、受信パケットのカプセル化を指示するためのフラグ情報が設定される。また、カプセルヘッダ情報 1 5 4 には、サンプリングされた受信パケットをコレクタ装置 C 1

10

20

30

40

50

に転送する際に必要となるカプセル化ヘッダの内容（レイヤ２ヘッダ、レイヤ３ヘッダ、レイヤ４ヘッダ）が設定される。カプセルヘッダ情報１５４の内容は、カプセル化指示フラグ１５３がオン状態の時に有効となる。

【００５３】

図１６は、受信パケット処理部２０の１実施例を示す。

受信パケット処理部２０は、それぞれ入力回線ＩＣｉに接続された複数の回線終端処理部２１－ｉ（ $i = 1 \sim N$ ）と、回線終端処理部２１－ｉから出力された受信パケットを一時的に蓄積するバッファメモリ２２－ｉ（ $i = 1 \sim N$ ）と、検索処理部４０から供給される統計情報通知パケットを一時的に蓄積するバッファメモリ２２－（ $N + 1$ ）と、これらのバッファメモリに接続されたパケット蓄積制御部２３と、パケットデータ蓄積メモリ２４、入力パケットヘッダ蓄積メモリ２５Ａ、出力パケットヘッダ蓄積メモリ２５Ｂと、メモリ状態管理部２６と、ヘッダ送信制御部２７と、コピー管理部２８と、パケット転送制御部２９とから構成される。

【００５４】

各回線終端処理部２１－ｉは、入力回線ＩＣｉからパケットを受信すると、パケットデータの誤り検出等のパケット終端処理を行う。各回線終端処理部２１－ｉは、データ誤りが検出された受信パケットは廃棄し、正常に受信したパケットは、バッファメモリ２２－ｉに蓄積して、パケット蓄積制御部２３にパケット受信を通知する。パケット蓄積制御部２３は、バッファメモリ２２－（ $N + 1$ ）についても、統計情報通知パケットが蓄積された時、検索処理部４０から信号線Ｌ５３０を介してパケット受信通知を受ける。

【００５５】

パケット蓄積制御部２３は、パケット受信通知があったバッファメモリから、予め決められた選択ルールに従って受信パケットを読み出し、受信パケットに付すべき内部ヘッダ１５を生成する。この時点では、内部ヘッダ１５は、入力回線番号１５１のフィールドのみが有効データを含み、その他のフィールド１５２～１５４は空状態となっている。入力回線番号１５１の値 k は、受信パケットが読み出されたバッファメモリ２２－ k （ $k = 1 \sim N + 1$ ）から一義的に決まる。

【００５６】

パケット蓄積制御部２３は、生成した内部ヘッダ１５と、受信パケットから抽出したレイヤ２ヘッダ１１～レイヤ４ヘッダ１３とを含む固定長ヘッダ部分を、図１７で説明するパケットデータ管理情報ブロック２００の一部として、入力パケットヘッダ蓄積メモリ２５Ａに格納する。受信パケットの残り部分である可変長のデータ部１４は、パケットデータ蓄積メモリ２４に格納される。

【００５７】

本実施例では、パケットデータ蓄積メモリ２４を固定長の複数のメモリブロックに分割しておき、各メモリブロックの空き状態（使用状態）をメモリ状態管理部２６で管理している。パケット蓄積制御部２３は、バッファメモリから１つの受信パケットを読み出すと、メモリ状態管理部２６に対して、受信パケットのデータ長に応じた個数の空きメモリブロックの割り当てを要求し、受信パケットのデータ部１４をこれらのメモリブロックに分割して格納する。

【００５８】

図１７は、パケットデータ管理情報ブロック２００の１例を示す。

パケットデータ管理情報ブロック２００は、データ部蓄積用として同一パケットに割り当てられた複数個のメモリブロックを順次を読み出すためのものであり、ブロック種別フラグ２０１と、同一パケットに対して割り当てられたメモリブロックの数２０２と、各メモリブロックに格納された有効データの長さを示す有効データ長２０３と、メモリアドレス２０４と、ヘッダ情報フィールド２０５とからなっている。

メモリアドレス２０４は、パケットデータ蓄積メモリ２４における各メモリブロックの先頭アドレスを示す。また、ヘッダ情報フィールド２０５には、図１５に示した内部パケットのヘッダ１５、１１～１３が設定される。

【0059】

本実施例では、図18に示すように、1つの受信パケットに複数の空きメモリブロック、例えば、ブロック k 、ブロック $k+2$ 、ブロック $k+3$ が割り当てられた場合、パケット蓄積制御部23が、割り当てメモリブロック数と同数のパケットデータ管理情報ブロック200-1~200-3を生成し、これらの管理情報ブロックを入力パケットヘッダ蓄積メモリ25AにFIFO形式で格納する。ブロック種別フラグ201は、その管理情報ブロック200が、同一パケットに付随する複数のパケットデータ管理情報ブロックのうち、先頭のものか否かを示している。

【0060】

図18では、各メモリブロックのサイズを L 、バッファメモリ22-iから読み出された受信パケットのデータ部14の長さを $2L+\Delta L$ と仮定して、ブロック k 、ブロック $k+2$ 、ブロック $k+3$ の3つのメモリブロックが割り当てられた場合を示している。この場合、先頭メモリブロック k と対応する第1のパケットデータ管理情報ブロック200-1は、ブロック種別フラグ201に先頭ブロックを示す値が設定され、メモリブロック数202には「3」、有効データ長203には「 L 」、メモリアドレス204には、矢印P1で示すように、メモリブロック k の先頭を示すポインタアドレス値が設定される。

【0061】

上記第1のパケットデータ管理情報ブロック200-1のヘッダ情報フィールド205には、内部ヘッダ15と、レイヤ2ヘッダ11~レイヤ4ヘッダ13の値が設定される。但し、内部ヘッダ15は、入力回線番号151のみが有効であり、出力回線番号152~カプセル化ヘッダ情報154の値は未定となっている。これらの未定のヘッダ情報要素は、後述するように、検索処理部40からの検索結果に従って補充される。

【0062】

第2、第3のメモリブロック $k+2$ 、 $k+3$ と対応する第2、第3のパケットデータ管理情報ブロック200-2、200-3は、ブロック種別フラグ201に、そのブロックが後続ブロックであることを示す値が設定され、メモリブロック数202とヘッダ情報フィールド205は未使用となる。第2のパケットデータ管理情報ブロック200-2の有効データ長203には「 L 」が設定され、メモリアドレス204には、矢印P2で示すように、メモリブロック $k+2$ の先頭を示すポインタアドレス値が設定される。また、第3のパケットデータ管理情報ブロック200-3の有効データ長203には「 ΔL 」が設定され、メモリアドレス204には、矢印P3で示すように、メモリブロック $k+3$ の先頭を示すポインタアドレス値が設定される。

【0063】

このように、入力パケットヘッダ蓄積メモリ25Aに、パケットデータ管理情報ブロック200-1~200-3をFIFO形式で格納し、第1の管理情報ブロック200-1で、組をなすメモリブロックの個数204と、データ部14に付すべきヘッダ情報205を指定しておく、これら1組のパケットデータ管理情報ブロック200-1~200-3を順次を読み出し、各管理情報ブロックが示すメモリアドレス204に従って、パケットデータ蓄積メモリ24から、複数ブロックに分割して蓄積された1パケット分のデータを次々と読み出すことが可能となる。また、必要に応じて第1の管理情報ブロック200-1が示すヘッダ情報205を利用することにより、受信パケットをカプセル化してコレクタ装置C1に転送することが可能となる。パケット受信処理部20の詳細動作については後で説明する。

【0064】

図19は、送信パケット処理部30の1実施例を示す。

送信パケット処理部30は、それぞれ出力回線OCiに接続された複数の回線終端処理部31-i ($i=1\sim N$)と、パケット出力制御部32と、パケットデータ蓄積メモリ33と、出力パケットヘッダ蓄積メモリ34と、メモリ状態管理部35と、パケット受信部36とから構成される。送信パケット処理部30の動作については、後で詳述する。

【0065】

図20は、検索処理部40の1実施例を示す。

検索処理部40は、信号線L27を介して受信パケット処理部のヘッダ送信制御部27に接続されたヘッダ情報蓄積部41と、それぞれヘッダ情報蓄積部41に接続されたフローテーブル検索部42、ルーティングテーブル検索部43およびフローエントリ管理部44と、サンプル処理部45と、サンプル判定部46と、統計収集処理部47と、信号線L48を介してヘッダ送信制御部27に接続された検索結果出力部48と、フローエントリ管理部44に付随するフロー管理テーブル49と、統計情報通知パケットヘッダ情報蓄積部50と、サンプルパケットヘッダ情報蓄積部51と、フロー情報蓄積部52と、統計情報通知パケット生成部53とから構成される。

【0066】

フローテーブル検索部42は、ヘッダ情報蓄積部41から出力されるヘッダ情報に基づいてフローテーブル60の検索キーを生成し、フローテーブル60から検索された統計制御情報をフローエントリ管理部44とサンプル判定部46に出力する。また、フローエントリ管理部44からの指示に従って、フローテーブルエントリの追加／削除を行い、削除対象となったフローエントリの内容をフロー情報蓄積部52に出力する。

【0067】

ルーティングテーブル検索部43は、ヘッダ情報蓄積部41が示すヘッダ情報から抽出した受信パケットの宛先IPアドレスに基づいて、ルーティングテーブル80にアクセスし、ルーティングテーブル80から検索されたルーティング情報をフローテーブル検索部42、サンプル処理部45、統計収集処理部47、検索結果出力部48に通知する。

【0068】

統計収集処理部47は、フローテーブル検索部42とルーティングテーブル検索部43による検索結果に応じて、統計情報テーブルの統計データを更新する。また、統計収集処理部47は、フローエントリ管理部44からの指令に応じて、統計情報テーブル70の特定エントリに蓄積された統計情報を読み出し、これをフロー情報蓄積部52に出力する。

【0069】

検索結果出力部48は、ルーティングテーブル検索部43からルーティングテーブル80の検索結果を受信すると、図23で詳述する検索結果通知480を生成し、これを信号線L48を介して受信パケット処理部20のヘッダ送信制御部27に送信する。

【0070】

本実施例で示す検索処理部40は、統計収集処理部47が統計情報テーブル70に蓄積した統計データを所定のタイミングでコレクタ装置C1に送信するキャッシュ型の統計収集機能と、特定フローの受信パケットについて、フローテーブル60で指定されたサンプリングレートでサンプル（コピーパケット）を生成し、これをコレクタ装置C1に送信するサンプリング型の統計収集機能とを備えている。

【0071】

サンプル処理部45は、フローテーブル（統計機能制御テーブル）から検索された統計制御エントリの統計制御情報がサンプル処理（コピーパケットのコレクタ装置への転送）を指示していた場合に、受信パケット処理部20に対して、サンプルの生成を指示するためのものである。サンプルの生成指示情報は、検索結果出力部48が信号線L48に出力する検索結果通知に含めた形で、受信パケット処理部20に通知される。また、サンプルをコレクタ装置C1に送信する際に必要となる宛先IPアドレス等のカプセル化ヘッダ情報は、サンプルパケットヘッダ情報蓄積部51から読み出され、検索結果通知の一部として受信パケット処理部20に通知される。

【0072】

サンプル判定部46は、後述するように、フローテーブル60の検索結果に応じて、受信パケット所属フローの統計情報をチェックし、サンプル処理を開始すべきフロー状態となった時、統計制御情報の一部であるサンプル処理フラグの書替えを行う。

【0073】

統計情報通知パケット生成部53は、フロー情報蓄積部52に蓄積されたフロー条件お

10

20

30

40

50

よび統計情報と、統計情報通知パケットヘッダ情報蓄積部50が示すカプセル化ヘッダ情報に基づいて、統計情報通知パケットを生成し、信号線L53を介して受信パケット処理部20のバッファメモリ22-Cに出力する。尚、統計データの通知先とサンプルパケットの転送先とが同一のコレクタ装置の場合、統計情報通知パケットヘッダ情報蓄積部50とサンプルパケットヘッダ情報蓄積部51を同一メモリで兼用することができる。

【0074】

統計情報通知パケットヘッダ情報蓄積部50とサンプルパケットヘッダ情報蓄積部51へのカプセルヘッダ情報の設定と、フローテーブル60、ルーティングテーブル80へのエントリ情報の設定は、信号線L90と制御部90を介してネットワーク管理者が行うことが可能である。

10

【0075】

図21と図22は、ルータR1が備えるフローテーブル60と統計情報テーブル70の具体的な内容の1例を示す。

フローテーブル60は、図21に示すように、フローエントリ番号61と対応して、フロー識別条件62と統計制御情報63とを示す複数のエントリからなり、統計情報テーブル70は、図22に示すように、フローエントリ番号61と対応して、統計情報72を示す複数のエントリからなる。

【0076】

尚、フローエントリ番号61は、フロー識別条件62、統計制御情報63、統計情報72を互いに関連付けるための情報として示してあり、テーブルの構成によっては、フローエントリ番号61を必要としない場合もあり得る。また、フローエントリ番号61をポインタとして用いることによって、フローテーブル60に定義された1群の複数のフロー識別条件を1つの統計制御情報エントリと1つの統計情報エントリに関連付けることも可能である。

20

【0077】

ここでは、フロー識別条件62として、図10に示した情報要素621～626にその他の情報629を加えた例を示している。その他の情報629としては、例えば、パケットの入、出力回線番号、図3に示した宛先/送信元MACアドレスとタイプ、図4に示したTAGプロトコルID、優先度、VLAN-ID、図8に示したTCPフラグの少なくとも一部を適用できる。

30

【0078】

フローテーブル60からは、検索結果として、統計制御情報63が示すように、登録処理フラグ631、登録処理レート632、統計収集フラグ633、帯域計算フラグ634、サンプル処理フラグ635、サンプリングレート636、サンプル判定フラグ637、サンプル開始帯域638、サンプル終了帯域639、その他の情報640が得られる。ここに示した例では、統計情報テーブル70には、統計情報72として、図11で示した情報項目721～724、729の外に、帯域725が追加されている。

【0079】

図21に示したフローテーブル60において、フローエントリ番号f1、f2をもつエントリEN-1、EN-2は、図10に示した上位プロトコルがTCPのフロー1、フロー2のフロー識別条件62と統計制御情報63を定義している。受信パケットのヘッダ情報がエントリEN-1、EN-2のフロー識別条件に合致した場合、検索処理部40は、統計情報テーブルのエントリSE-1、SE-2が示す情報項目について、統計情報を収集する。

40

【0080】

エントリ番号F12をもつエントリEN-x12は、統計制御エントリの1つであり、他のエントリEN-1、EN-2とは異なって、フロー識別条件62が、上位プロトコル623がTCPであれば、フロー識別条件62の他の情報要素621、622、624～629については任意（「*」）でよいことを示している。

【0081】

50

統計制御エントリ E N - x 1 2 は、統計制御情報 6 3 の登録処理フラグ 6 3 1 が「1」、登録処理レートが「1 / 1」となっており、フローテーブル 6 0 の検索結果としてエントリ E N - x 1 2 の統計制御情報が出力された場合、上記登録処理フラグ 6 3 1 に従って、検索処理部 4 0 は、フローテーブル 6 0 への新たなフローエントリの登録動作を実行する。すなわち、上記統計制御エントリ E N - x 1 2 は、フロー識別条件 6 2 に合致した新たなフローエントリをフローテーブル 6 0 に自動的に追加するためのフロー登録用のエントリとして機能する。

【0082】

例えば、フローテーブル 6 0 にエントリ E N - 1、E N - 2 が未登録の状態、ルータ R 1 がフロー 1 に属したパケットを受信した場合、フローテーブル検索部 4 2 は、該パケットのヘッダ情報に基づくフローテーブル 6 0 の検索結果として、エントリ E N - x 1 2 の統計制御情報 6 3 を出力する。後述するように、検索処理部 4 0 のフローエントリ管理部 4 4 は、フローテーブル検索部 4 2 が出力する統計制御情報 6 3 の登録処理フラグ 6 3 1 に着目しており、登録処理フラグ 6 3 1 が「1」である時、フローテーブル検索部 4 2 に対して、ヘッダ情報蓄積部 4 1 が示すヘッダ情報に基づく新たなフローエントリ E N - 1 の登録を指示する。

【0083】

従って、フローテーブル 6 0 に初期状態でフロー登録用の統計制御エントリ E N - x 1 2 を設定しておくことによって、該エントリのフロー識別条件を満たす受信パケットの処理時に、フローテーブル 6 0 に統計収集用の新たなフローエントリを自動的に追加することができる。エントリ E N - 1、E N - 2 は、上記統計制御エントリ E N - X 1 2 によって、フローテーブル 6 0 に自動的に追加されたものである。図 2 1 の状態にある時、ルータ R 1 が、エントリ E N - 1、E N - 2 のフロー識別条件に該当しない新たな T C P フローのパケットを受信した場合、フローテーブル 6 0 には、該受信パケットと対応して、統計収集用の別のフローエントリが追加されることになる。

【0084】

尚、フローテーブル 6 0 のエントリ配列を、統計収集用のフローエントリ E N - 1、E N - 2 が統計制御エントリ E N - x 1 2 に優先して検索されるようにしておくことによって、同一内容の統計収集用フローエントリが重複してフローテーブル 6 0 に登録されるのを回避することが可能となる。また、統計制御エントリ E N - x 1 2 をフローテーブル 6 0 とは別の統計機能制御テーブルに登録しておき、フローテーブル 6 0 に検索キーに該当するエントリが無かった場合に、統計機能制御テーブルを検索するようにしてもよい。

【0085】

本発明の実施例では、上述したように統計収集用のフローエントリをフローエントリ管理部 4 4 で自動的に生成するようにしているが、統計機能制御エントリ以外の統計収集用のフローエントリ群は、その一部を管理者が管理端末 1 3 0 0 からマニュアルで設定することも可能である。

【0086】

図 2 1 に示した統計制御情報 6 3 において、登録処理レート 6 3 2 は、フロー登録用の統計制御エントリ E N - x 1 2 にヒットした際の登録処理の実行レートを示し、登録処理レートの設定値は、登録処理フラグ 6 3 1 の設定値が「1」の場合に有効となる。登録処理レートの設定値「1 / 1」は、統計制御エントリ E N - x 1 2 がヒットした場合、必ずフロー登録処理を行うことを意味している。

【0087】

統計収集フラグ 6 3 3 は、設定値が「1」の場合に、該当フローの統計情報を更新することを意味している。帯域計算処理フラグ 6 3 4 は、設定値が「1」の場合、該当フローの帯域 7 2 5 を算出することを意味している。図 2 1 に示した例では、統計収集用のエントリ E N - 1、E N - 2 と、統計制御エントリ E N - x 1 2 は、統計収集フラグが「1」、帯域計算処理フラグ 6 2 4 が「0」に設定されている。従って、図 2 2 に示した統計情報 7 2 において、帯域 7 2 5 は統計の対象外の項目となっている。

【0088】

サンプル処理フラグ635は、設定値が「1」の時、サンプリングレート636に従って受信パケットのコピーを生成し、これをコレクタ装置C1に転送することを意味している。サンプリングレート636の設定値は、サンプル処理フラグ635の設定値が「1」の場合に有効となる。サンプリングレート636の設定値は、例えば、「1/1000」の場合、該当フローの1000パケットに1個の割合でコピーを生成すること意味する。図21の例では、フローエントリEN-1、EN-2、EN-x12は、サンプル処理フラグ635が「0」となっているため、サンプリングレート636の値は無意味となる。

【0089】

サンプル判定フラグ637は、その設定値が「1」の時、サンプル判定部46に対して、当該フローのサンプリングの開始、終了の判定処理の実行を指示する。設定値が「0」であれば、サンプル判定処理は実行されない。サンプル開始帯域638は、当該フローのサンプル開始条件となるフロー帯域値を示し、サンプル終了帯域639は、サンプル終了条件となるフロー帯域値を示す。

【0090】

サンプル判定部46は、サンプル判定フラグ637が「1」の場合、サンプル開始帯域638と、対応する統計情報エントリが示す現在の帯域725とを比較し、現在の帯域がサンプル開始帯域よりも大きくなった時点で、サンプル処理フラグ635を「1」に変更する。また、サンプル処理フラグ635が「1」状態にある時、現在の帯域725とサンプル終了帯域639とを比較し、現在帯域がサンプル終了帯域よりも小さくなった時点で、サンプル処理フラグ635を「0」に戻す。図21では、エントリEN-1、EN-2、EN-x12は、サンプル判定フラグが「0」に設定されているため、受信パケットのサンプリングによるコピーの生成は行われない。

【0091】

次に、図16、図19、図20を参照して、本発明によるルータの動作について詳細に説明する。最初に、フローテーブル60にフロー登録用エントリEN-x12のみが存在し、統計収集用のエントリEN-1、EN-2が未登録の状態において、パケット蓄積制御部23が、フロー1に属する受信パケットを処理する場合のルータ動作について説明する。

【0092】

パケット蓄積制御部23は、バッファメモリ22-1~22-(N+1)の1つから受信パケットを読み出すと、内部ヘッダ15を生成した後、受信パケットのデータ部の蓄積に必要なメモリブロックの個数を指定して、メモリ状態管理部26にメモリブロックの割り当てを要求する。メモリ状態管理部26は、パケットデータ蓄積メモリ24に用意された複数のメモリブロック（メモリアドレス）について、それぞれの使用状態を管理しており、空き状態にあるメモリブロックの中から、必要個数のメモリブロック（メモリアドレス）をパケット蓄積制御部23に割り当てる。

【0093】

パケット蓄積制御部23は、メモリ状態管理部26から割り当てられたメモリアドレスに従って、図18で説明したように、入力パケットヘッダ蓄積メモリ25Aへのパケットデータ管理情報ブロックの書き込みと、パケットデータ蓄積メモリ24への受信パケットデータ部の書き込みを実行する。尚、パケットデータ蓄積メモリ24に必要な個数の空きメモリブロックが無かった場合、パケット蓄積制御部23は、受信パケットを廃棄する。

【0094】

本実施例では、メモリ25Aへのパケットデータ管理情報ブロックの書き込みは、FIFO（Fast-In Fast-Out）形式で行うものとして説明するが、入力パケットヘッダ蓄積メモリ25Aを固定長の複数のメモリブロックに分割しておき、各パケットデータ管理情報ブロックに次ブロックのポインタアドレスを持たせることによって、1組のパケットデータ管理情報ブロックをメモリ25A内の任意の空きメモリブロックに分散して格納するようにしてもよい。

【0095】

パケット蓄積制御部23は、入力パケットヘッダ蓄積メモリ25Aへのパケットデータ管理情報ブロックの書き込み完了時、または、パケットデータ蓄積メモリ24へのパケットデータの書き込み完了時に、信号線L23を介して、ヘッダ送信制御部27にパケットの受信通知を送信する。

【0096】

上記パケット受信通知を受信したヘッダ送信制御部27は、入力パケットヘッダ蓄積メモリ25Aから、先頭のパケットデータ管理情報ブロック200-1を読み出し、該パケットデータ管理情報ブロックが示すヘッダ情報（内部ヘッダ15、レイヤ2ヘッダ11～レイヤ4ヘッダ13）を信号線L27を介して検索処理部40のヘッダ情報蓄積部41に転送する。また、ヘッダ送信制御部27は、先頭のパケットデータ管理情報ブロック200-1が示すメモリブロック数（M）に基づいて、後続するM-1個のパケットデータ管理情報ブロック200-2、200-3、…を順次を読み出し、これらの内容を一時的に保持する。

10

【0097】

図20において、検索処理部40のヘッダ情報蓄積部41は、ヘッダ送信制御部27から信号線L27を介して受信したヘッダ情報を一時的に蓄積した後、フローテーブル検索部42、ルーティングテーブル検索処理部43、フローエントリ管理部44、統計情報処理部47に分配する。

【0098】

20

フローエントリ管理部44は、上記ヘッダ情報を保持して、フローテーブル検索部42からの統計制御情報の受信を待つ。ルーティングテーブル検索処理部43は、上記ヘッダ情報からルーティングテーブル80の検索に必要な検索キーを生成し、ルーティングテーブル80から出力回線番号を含むルーティング情報を検索する。検索結果は、フローテーブル検索部42、サンプル処理部45、検索結果出力部48に分配される。

【0099】

フローテーブル検索部42は、ヘッダ情報と、必要に応じてルーティングテーブル検索処理部43が出力したルーティング情報とから、フロー識別条件62となる情報項目、すなわち、送信元IPアドレス、宛先IPアドレス、上位プロトコル、TOS、送信元ポート番号、宛先ポート番号、その他の情報を抽出し、これらの情報項目の組み合わせを検索キーとして、フローテーブル60を検索する。

30

【0100】

ここでは、上記ヘッダ情報がフロー1に属するパケットのもので、且つ、フローテーブルにはフローエントリEN-x12のみが登録されている状態を想定しているため、フローテーブル60の検索結果として、フローエントリEN-x12のフローエントリ番号（またはエントリアドレス）f12と、登録処理フラグが「1」、登録処理レートが「1/1」、統計収集フラグが「1」、サンプル処理フラグが「0」を示す統計制御情報が得られる。

【0101】

フローテーブル検索部42は、上記検索結果をフローエントリ管理部44、サンプル処理部45、サンプル判定部46、統計収集処理部47に分配する。この場合、サンプル処理フラグが「0」となっているため、サンプル処理部45とサンプル判定部46におけるサンプル生成のための特別な動作は発生しない。

40

【0102】

ヘッダ情報蓄積部41からヘッダ情報を受信した統計収集処理部47は、フローテーブル検索部42からの統計制御情報の受信を待っている。この例では、統計制御情報が示す統計収集処理フラグが「1」となっているのため、統計収集処理部47は、ルーティングテーブル検索部43から受信したルーティング情報とヘッダ情報蓄積部41から受信したヘッダ情報に基づいて、統計情報テーブル70におけるフローエントリ番号f12をもつテーブルエントリSE-x12の統計情報72を更新する。具体的には、テーブルエント

50

リSE-x12のパケット数721に1を加算し、バイト数722に上記ヘッダ情報が示す受信パケット長を加算し、入力回線番号723に上記ヘッダ情報が示す入力回線番号151の値を記録し、出力回線番号724に上記ルーティング情報が示す出力回線番号を記録する。

【0103】

一方、フローエントリ管理部44は、フローテーブル検索部42から受信した統計制御情報で、登録処理フラグが「1」で、登録処理レートが「1/1」となっているため、ヘッダ情報蓄積部41から受信したヘッダ情報をもつフローに関して、フローテーブル60に新たなフローエントリを登録すべきものと判断する。登録処理レートが「1/k」（kは1より大きい値）の場合は、登録処理レートに従って、フロー登録すべきか否かを判定する。

10

【0104】

フローエントリ管理部44は、フローテーブル60のエントリアドレスの使用状況を管理している。この場合、フローエントリ管理部44は、上記ヘッダ情報からフロー識別条件となる情報項目を抽出してエントリ番号f1をもつ新たなフロー識別条件を生成し、このフロー識別条件と、一部訂正した統計制御情報と、空きエントリアドレスとを含むフロー登録指示をフローテーブル検索部42に与える。フローテーブル60に新規フローエントリに必要な空きアドレスが無かった場合は、フローエントリ管理部44は、後述するフローエントリ削除処理を行った後、上述したフロー登録指示を発行する。

【0105】

20

フローエントリ管理部44からフロー登録指示を受けたフローテーブル検索部42は、指定されたエントリアドレス、フロー識別条件、統計制御情報に従って、フローテーブル60に新たなフローエントリを追加する。ここでは、フロー1に属するパケットを受信した場合を想定しているので、上記フロー登録指示に応答して、フローテーブル60に統計収集用のエントリEN-1が追加される。フロー2に属するパケットを受信した場合は、これと同様の動作によって、フローテーブル60に統計収集用のエントリEN-2が追加されることになる。

【0106】

検索結果出力部48は、ルーティングテーブル検索部43からルーティング情報を受信すると、検索結果通知480を生成し、信号線L48を介して受信パケット処理部20のヘッダ送信制御部27に送信する。検索結果通知480は、図23に示すように、出力回線番号481、コピー指示フラグ482、カプセル化指示フラグ483、カプセル化ヘッダ情報484、その他の情報485から構成される。

30

【0107】

ここで、コピー指示フラグ482は、受信パケット処理部20に受信パケットをコピーする必要があることを示すフラグであり、カプセル化指示フラグ483は、カプセルヘッダ情報484を適用して上記コピーパケットをカプセル化すべきことを示すフラグである。コピー指示フラグ482は、サンプル処理部45が信号線L45にコピー指示信号を出力した時点で生成される検索結果通知において、「1」に設定される。カプセル化指示フラグ483は、後述するように、コピー指示フラグが「1」に設定された検索結果通知の次に生成されるコピーパケット送信用の検索結果通知において、「1」に設定される。カプセル化ヘッダ情報484には、サンプルパケットヘッダ情報蓄積部51から読み出されたヘッダ情報が設定され、カプセル化指示フラグ483が「1」の場合にのみ有効となる。

40

【0108】

出力回線番号481とその他の情報485には、通常の実験結果通知の場合、ルーティングテーブル検索部43から受信したルーティング情報から抽出された出力回線番号と、その他の情報が設定される。但し、コピーパケット送信用の実験結果通知においては、コピーパケットをコレクタ装置に送信するために必要となる所定の出力回線番号とその他の情報が設定される。

50

本例の場合、サンプル処理部 45 からのコピー指示がないため、検索結果出力部 48 は、コピー指示フラグ 482 が「0」、カプセル化指示フラグ 483 が「0」、カプセルヘッダ情報 484 が無効データ、出力回線番号 491 とその他の情報 485 が有効データを含む検索結果通知 480 を生成して、信号線 L 48 に送出する。

【0109】

図 16 に戻って、ヘッダ送信制御部 27 は、信号線 L 48 を介して検索結果通知 480 を受信すると、既にメモリ 25A から読み出してある最初の packets データ管理情報ブロック 200-1 に、出力回線番号 152、カプセル化指示フラグ 153、カプセルヘッダ情報 154 として、上記検索結果通知 480 が示す出力回線番号 481、カプセル化指示フラグ 483、カプセルヘッダ情報 484 の内容を追加する。更新された packets データ管理情報ブロック 200-1 は、出力 packets ヘッダ蓄積メモリ 25B に書き込まれる。尚、必要に応じて、検索結果通知 480 が示すその他の情報 485 を packets データ管理情報ブロック 200-1 の内部ヘッダ 15 の一部として追加してもよい。

10

【0110】

図 18 で説明したように、後続の packets データ管理情報ブロック 200-2、200-3、…にはヘッダ情報を追加する必要がない。従って、ヘッダ送信制御部 27 は、これらの後続 packets データ管理情報ブロックについては、メモリ 25A から読み出したものをそのまま出力 packets ヘッダ蓄積メモリ 25B に書き込む。

【0111】

この後、ヘッダ送信制御部 27 は、コピー管理部 28 に対して、上記出力 packets ヘッダ蓄積メモリ 25B に書き込まれた各 packets データ管理情報ブロックが示すメモリアドレス 204 の値と、検索結果通知 480 から判明するコピー数を通知し、packets 転送制御部 29 に対して packets 転送開始を要求する。本例の場合、検索制御部 40 から受信した検索結果通知 480 でコピーフラグ 482 が「0」となっているため、ヘッダ送信制御部 27 は、コピー管理部 28 にコピー数「0」を通知する。

20

【0112】

コピー管理部 28 は、packets データ蓄積メモリ 24 の各メモリブロックの解放を制御するためのものであり、例えば、図 24 に示すように、packets データ蓄積メモリ 24 の各メモリブロック（メモリアドレス）281 と対応して、蓄積データの送信待ち回数 282 を記憶したメモリアドレス解放制御テーブル 280 を備えている。

30

【0113】

コピー管理部 28 は、ヘッダ送信制御部 27 から packets データ蓄積メモリ 24 のメモリアドレス 204 とコピー数を受信すると、通知されたコピー数に応じて、上記メモリアドレス解放制御テーブル 280 における上記メモリアドレス 204 と対応するメモリブロックの送信待ち回数 282 を変更する。送信待ち回数は、ヘッダ送信制御部 27 から通知されたコピー数が「0」の時は“1”、コピー数が「1」の時は“2”に設定される。

【0114】

図 24 のテーブル状態は、図 18 と対応しており、受信 packets のデータ部がブロック k、k+2、k+3 に分割して格納されている状態を示している。この場合、ヘッダ送信制御部 27 から通知されたコピー数が「0」であったため、これらのメモリブロック k、k+2、k+3 と対応する送信待ち回数として、“1”が設定されている。

40

【0115】

packets 転送制御部 29 は、ヘッダ送信制御部 27 から packets 転送開始要求を受信すると、出力 packets ヘッダ蓄積メモリ 25B から、先頭の packets データ管理情報ブロック 200-1 を読み出し、該ブロックが示すメモリアドレス 204 と有効データ長 203 に従って、packets データ蓄積メモリ 24 のメモリブロック k から最初のデータブロックを読み出す。packets 転送制御部 29 は、先頭の packets データ管理情報ブロック 200-1 が示すメモリブロック数 202 に従って、出力 packets ヘッダ蓄積メモリ 25B から FIFO 形式で第 2、第 3 の packets データ管理情報ブロック 200-2、200-3 を読み出し、これらの情報ブロックが示すメモリアドレス 204 と有効データ長 203 に従って

50

、パケットデータ蓄積メモリ24のメモリブロック $k+2$ 、 $k+3$ から後続のデータブロックを次々と読み出す。

【0116】

パケット転送制御部29は、先頭パケットデータ管理情報ブロック200-1から抽出したヘッダ情報205に続いて、これらのデータブロックから再構成されたパケットデータ部14を信号線L1に送出することによって、送信パケット処理部30に図15のフォーマットをもつ内部パケットを転送する。パケット転送制御部29は、1つの内部パケットの転送が完了すると、コピー管理部28に対して、データ読み出しが完了したメモリブロックのアドレスを示すパケット転送完了通知を出力する。

【0117】

コピー管理部28は、上記パケット転送完了通知を受信すると、通知されたメモリブロックアドレスに従って、メモリアドレス解放制御テーブル280の送信待ち回数282を減算する。この例では、メモリブロック k 、 $k+2$ 、 $k+3$ の送信待ち回数がそれぞれ1ずつ減算され、結果的に、全ての送信待ち回数が「0」になる。コピー管理部28は、送信待ち回数の更新の都度、残り回数をチェックし、送信待ち回数が「0」となったメモリブロックについては、蓄積データの保存が不要になったものと判断し、メモリ状態管理部26に、メモリアドレスの解放を指示する。メモリ状態管理部26は、解放指示のあったメモリアドレス（メモリブロック）を空き状態として管理し、これらのメモリアドレスをその後のパケット蓄積制御部23への割り当てアドレスに適用する。

【0118】

図19に示した送信パケット処理部30において、パケット受信部36は、信号線L1から内部パケットを受信すると、ヘッダ情報部分（ヘッダ15、11~13）を出力パケットヘッダ蓄積メモリ34に蓄積し、パケットのデータ部分14をパケットデータ蓄積メモリ33に蓄積する。これらのメモリへのヘッダ情報とパケットデータの蓄積は、図18で説明したパケットデータ管理情報ブロックを適用して、受信パケット処理部20の入力パケットヘッダメモリ25Aおよびパケットデータ蓄積メモリ24と同様の形式で行われる。パケットデータの蓄積に必要なメモリブロックの割り当ては、メモリ状態管理部35によって行われる。

受信処理部36は、出力パケットヘッダ蓄積メモリ34へのパケットデータ管理情報ブロックの書き込みと、パケットデータ蓄積メモリ33へのパケットデータの書き込みが完了すると、パケット出力制御部32にパケット送信要求を出力する。

【0119】

上記パケット送信要求を受信すると、パケット出力制御部32は、受信パケット処理部20のパケット転送制御部29と同様、出力パケットヘッダ蓄積メモリ34から読み出した先頭のパケットデータ管理情報ブロックが示すメモリブロック数202によって、後続するパケットデータ管理情報ブロックを読み出し、各パケットデータ管理情報ブロックが示すメモリアドレス204と有効データ長203に従って、パケットデータ蓄積メモリ33からパケットのデータ部を次々と読み出す。

【0120】

パケット出力制御部32は、複数のメモリブロックから読み出されたデータブロックを元のパケットデータ14に再構成した後、先頭のパケットデータ管理情報ブロックが示すカプセル化指示フラグ153の値から、出力パケットのカプセル化の可否を判定する。本例の場合、上記カプセル化指示フラグの値が「0」となっているため、出力パケットをカプセル化する必要はない。そこで、パケット出力制御部32は、先頭のパケットデータ管理情報ブロックから抽出したレイヤ2ヘッダ11、レイヤ3ヘッダ12、レイヤ4ヘッダ13を上記再構成されたパケットデータ14に付与することによって、出力パケットを生成し、これを上記パケットデータ管理情報ブロックが示す出力回線番号152で特定される回線終端処理部31-kに出力する。

回線終端処理部31-kは、パケット出力制御部32から受信した出力パケットに冗長符号等の付加情報を付与した後、出力回線OCkに送信する。

10

20

30

40

50

【0121】

次に、フローテーブル60に統計収集用のフローエントリEN-1が既に登録された状態で、パケット蓄積制御部23が、フロー1に属する受信パケットを処理した場合のルータR1の動作について説明する。

【0122】

ヘッダ送信制御部27が、受信パケットのヘッダ情報を検索処理部40に転送してから、検索処理部40で、フローテーブル検索部42がフローテーブル60を検索するまでの動作は、フローエントリEN-1が未登録の場合と同様である。今回は、フローテーブル60にフローエントリEN-1が既に登録済みの状態となっているので、フローテーブル検索部42は、フローテーブル60の検索結果として、フローエントリEN-1が示す統計制御情報を出力する。フローエントリEN-1の統計制御情報63は、図21に示すように、登録処理フラグ631が「0」、統計収集フラグ633が「1」、サンプル処理フラグ635とサンプル判定フラグ637が「0」となっている。

10

【0123】

登録処理フラグが「0」となっているため、フローエントリ管理部44によるフロー登録処理は行われない。また、サンプル処理フラグ、サンプル判定フラグが「0」となっているため、サンプル処理部45とサンプル判定部46による特別な動作は発生しない。

一方、統計収集処理フラグが「1」となっているため、統計収集処理部47は、フローエントリ番号f1の統計情報エントリSE-1において統計情報を更新する。

20

【0124】

具体的には、パケット数721に1を加算し、バイト数722にヘッダ情報蓄積部41から受信したヘッダ情報が示す受信パケットのバイト数を加算し、入力回線番号723に上記ヘッダ情報が示す入力回線番号を記録し、出力回線番号724にルーティングテーブル検索部43から受信したルーティング情報が示す出力回線番号を記録する。検索結果出力部48の動作と、受信パケット処理部20のその後の動作は、前述したフローエントリEN-1が未登録の場合と同様である。

【0125】

次に、フローエントリ管理部44が行うフローテーブルからのエントリの削除動作について説明する。

フローエントリ管理部44は、統計収集フラグが「1」、登録処理フラグ、サンプル処理フラグ、サンプル判定フラグが「0」のフローエントリを削除対象として、パケットの受信状況を監視し、パケット受信が所定時間以上途絶えたフローエントリをフローテーブル60から削除する。フローエントリ管理部44は、空きエントリ領域がない状態で、フローテーブル60に新たなフローエントリを登録する必要がある時も、上記削除対象エントリの中から特定のエントリを選択して、フローテーブル60から削除する。

30

【0126】

削除対象となるフロー情報は、フロー管理テーブル49に登録され、パケットの受信状況が定期的に監視される。フロー管理テーブル49は、例えば、図25に示すように、削除対象となる各エントリについて、フローエントリ番号49と、フローテーブル60におけるエントリアドレス492と、パケット数493、更新時刻494、非更新回数495を示している。ここで、パケット数493は、削除対象フローの通信状態を監視するために選ばれた代表的な統計情報であり、パケット数に代りにバイト数を監視対象にしてもよい。

40

【0127】

フローエントリ管理部44は、フロー管理テーブル49に登録されたフローエントリ番号をもつ各パケットフローについて、統計収集処理部47を介して、一定時間間隔で統計情報テーブル70からパケット数721の最新値を読み出し、フロー管理テーブル49が示す前回監視時のパケット数493と比較する。最新パケット数が前回値と異なる場合は、パケット数493を最新値に置き換えると共に、更新時刻494を現在時刻に書き換える。最新パケット数が前回値と同一の場合は、更新時刻494を変更することなく、非更

50

新回数 495 の値をインクリメントする。非更新回数 495 は、パケット数 493 の更新の都度、初期値に戻すようにしてもよい。

【0128】

フローエントリ管理部 44 は、上記インクリメントによって非更新回数が所定の閾値に達したフローエントリを不要エントリと判断し、フローテーブル検索部 42 に対して、エントリアドレス 492 を指定して不要フローエントリの削除を指示し、統計情報処理部 47 に対して、フローエントリ番号を指定して統計情報エントリの削除を指示する。

【0129】

フローエントリ管理部 44 は、フローテーブル検索部 42 からのフローエントリ ENx12 の統計制御情報の受信によって、フローテーブル 60 に新たなフローエントリを追加する必要が生じた時、もし、フローテーブルに空き領域がなかった場合は、フロー管理テーブル 49 から更新時刻 494 が最も古いエントリを不要フローエントリとして選択し、フローテーブル検索部 42 と統計情報処理部 47 に対して、上記と同様のエントリ削除を指示する。

【0130】

フローテーブル検索部 42 は、フローエントリ管理部 44 から不要フローエントリの削除指示を受信すると、フローテーブル 60 の指定エントリアドレスからフロー識別条件 62 を読み出す。フローテーブル検索部 42 は、読み出したフロー識別条件をフロー情報蓄積部 52 に転送した後、該フローエントリを削除し、フローエントリ管理部 44 に削除エントリのアドレスの解放を通知する。同様に、統計情報処理部 47 も、フローエントリ管理部 44 から不要フローエントリの削除指示を受信すると、統計情報テーブル 70 から指定エントリ番号をもつ統計情報エントリの内容を読み出し、これをフロー情報蓄積部 52 に転送した後、該統計情報エントリを削除する。

【0131】

フロー情報蓄積部 52 は、フローエントリの削除に伴ってフローテーブル検索部 42 から受信したフロー識別条件と、情報収集処理部 47 から受信した統計情報（以下、これら 2 種類の情報を併せてフロー情報と呼ぶ）をメモリに保持する。フロー情報蓄積部 52 に予め指定されたフロー数分のフロー情報が蓄積された時点で、統計情報通知パケット生成部 53 が、フロー情報蓄積部 52 から蓄積フロー情報を読み出し、統計情報通知パケットヘッダ情報蓄積部 50 が示すカプセルヘッダ情報を利用して、統計情報通知パケット 300 を生成する。統計情報通知パケット生成部 53 は、生成した統計情報通知パケット 300 を信号線 L53 に出力すると共に、信号線 L530 にパケットの受信通知を出力する。

【0132】

統計情報通知パケット 300 は、例えば、図 26 に示すように、ヘッダ 301 と、複数のフローレコード 302（302-1～302-N）とからなる。ヘッダ 301 は、ヘッダ情報蓄積部 50 から読み出されたカプセル化ヘッダ情報に基づいて生成され、宛先 IP アドレスとしてコレクタ装置 C1 の IP アドレスを含む。統計情報通知パケット 300 には、例えば、http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/nfc/nfc_3_0/nfc_ug/nfcform.htmに記載されたフォーマットを適用できる。

【0133】

ここに示した例では、各フローレコード 302 は、フロー識別子 303、サンプリングレート 304、フロー識別ヘッダ情報 305 と、パケット数 306A、バイト数 306B、出力回線番号 306C、入力回線番号 306D、その他の情報 306E を含む。情報項目 306A～306E には、情報収集処理部 47 から出力された統計情報が設定される。また、フロー識別子 303 にはフローエントリ番号 61、サンプリングレート 304 には、統計制御情報に適用される所定のサンプリングレート、フロー識別ヘッダ情報 305 には、フロー識別条件 62 が適用される。コレクタ装置は、上記統計情報通知パケットを受信した時、各フローレコードが示すサンプリングレート 304 から、ネットワーク上で実際に通信されているパケット数を推定できる。

【0134】

統計情報通知パケット生成部 53 から信号線 L 53 に出力された統計情報通知パケット 300 は、受信パケット処理部 20 のバッファメモリ 22 - (N + 1) に一時的に蓄積され、信号線 L 53 0 に出力されたパケット受信通知は、パケット蓄積制御部 23 に入力される。従って、パケット蓄積制御部 23 は、バッファメモリ 22 - (N + 1) に蓄積された統計情報通知パケット 300 を他のバッファメモリ 22 - 1 ~ 22 - N に蓄積された通常の受信パケットと同様に扱うことができる。

【0135】

パケット蓄積制御部 23 は、バッファメモリ 22 - (N + 1) から統計情報通知パケット 300 を読み出すと、ネットワークからの受信パケットの処理時と同様、内部ヘッダ 15 を生成し、メモリ状態管理部 26 に必要個数のメモリブロックアドレスを要求し、図 18 で説明したように、内部ヘッダ 15 とヘッダ 301 をパケットデータ管理情報ブロック形式で入力パケットヘッダ蓄積メモリ 25 A に蓄積し、統計情報通知パケット 300 のデータ部（フローレコード 302 - 1 ~ 302 - N）を固定長の複数のブロックに分割して、パケットデータ蓄積メモリ 24 に蓄積し、ヘッダ送信制御部 27 にパケット受信通知を出力する。

【0136】

ヘッダ送信制御部 27 と検索処理部 40 の動作は、通常の受信パケット処理時と同様であり、通知パケット 300 のヘッダ情報は、ネットワーク受信パケットのヘッダ情報と同様に処理される。その結果、統計情報通知パケット 300 は、ルーティングテーブルの検索結果が示す出力回線番号 152 を含む内部ヘッダを付した形で、送信パケット処理部 30 に転送され、送信パケット処理部 30 からコレクタ装置との接続回線に送出される。

【0137】

次に、パケット蓄積制御部 23 が、フロー登録用エントリ E N - x 12 が示すフロー識別条件に合致しないパケット、例えば、図 1 で説明した上位プロトコルが UDP のフロー 3 またはフロー 4 に属したパケットを処理した場合の検索処理部 40 の動作について説明する。

【0138】

ルーティングテーブル検索部 43 は、フロー識別条件とは無関係に、ヘッダ情報蓄積部 41 から受信したヘッダ情報に従ってルーティングテーブル 80 を検索し、検索結果を出力する。一方、フローテーブル検索部 42 は、ヘッダ情報と、必要に応じてルーティングテーブル 80 から検索されたルーティング情報とからフロー検索キーを生成し、フローテーブル 60 を検索する。

【0139】

本例では、受信パケットの上位プロトコルが UDP となっているため、フローテーブル 60 には、上記検索キーに該当するエントリ（統計制御エントリとフローエントリ）が全く存在していない。従って、フローテーブル検索部 42 は、該当する統計制御情報が無かったことを示す検索結果をフローエントリ管理部 44、サンプル処理部 45、サンプル判定部 46、統計収集処理部 47 に出力する。

【0140】

統計制御情報がなかった場合、フローエントリ管理部 44 は、フロー登録処理を行わない。サンプル処理部 45、サンプル判定部 46、統計収集処理部 47 も、それぞれに固有の動作を行わない。従って、検索結果出力部 48 は、コピーフラグ 482 とカプセル化指示フラグ 483 が「0」、カプセルヘッダ情報 484 が無効で、出力回線番号 481 とその他の情報 485 にのみ有効情報を含む検索結果通知 480 を生成し、これを信号線 L 48 に出力する。上記検索結果通知 480 に応答して実行される受信パケット処理部 20 の動作は、フロー 1 に属する受信パケットの場合と同様である。

【0141】

次に、本実施例のルータ R 1 が備えるサンプリング型の統計情報収集機能について説明する。ここでは、サンプル処理部 45 とサンプル判定部 46 が、フローテーブル 60 に登録された統計制御情報と統計情報テーブル 70 に蓄積された統計情報を利用して、特殊な

通信状況にあるパケットフローを検出し、サンプリングレートで指定されたタイミングで、受信パケット処理部20に受信パケットのコピー生成を指令する。

【0142】

例えば、図1に示したネットワークにおいて、端末T2または端末T4が、TCP (Transmission Control Protocol) におけるSYNパケットをサーバS2に送信することによって、サーバS2から他の端末への通信サービスを妨害 (SYN攻撃) する場合を想定する。SYN攻撃パケットは、TCPヘッダに定義されたコードビットのうちのSYNフラグが「1」に設定されている。

【0143】

以下の説明では、端末T2からサーバS2へ送信される一連のSYNパケットフローをフローFs2、端末T4からサーバS2へ送信される一連のSYNパケットフローをフローFs4と呼ぶ。また、端末T2、端末T4から送信されるSYNパケットの合計帯域が、時間経過と共に増加するものと仮定し、本実施例では、検索処理部40が、TCPのSYNパケットの合計帯域が50Mbps以上となった時点で、サンプリングレート1/10で受信パケットのサンプル (コピーパケット) 生成を開始し、合計帯域が40Mbps以下となった時点で、サンプル生成を停止する場合について説明する。

10

【0144】

図27は、SYN攻撃を検出するためのフローテーブル60の1例を示す。

フローテーブル60には、TCPのSYNパケットを監視してサンプリングの対象とするために、フローエントリ番号f24をもつエントリEN-x24が登録されている。エントリEN-x24も、統計制御エントリの一つであり、フロー識別条件62として、上位プロトコル623が「TCP」、SYNフラグ627が「1」、それ以外の項目621、622、624～626、629は任意値 (“*”) を指定している。

20

【0145】

上記エントリEN-x24は、検索結果として出力される統計制御情報63において、登録処理フラグ「0」、統計収集フラグ「1」、サンプル処理フラグ「0」、サンプリングレート「1/10」、サンプル判定フラグ「1」、サンプル開始帯域「50Mbps」、サンプル終了帯域「40Mbps」を指定している。

【0146】

図28は、統計情報テーブル70に用意されたフローエントリ番号f24をもつ統計情報エントリSE-x24の内容の1例を示す。現在時点での統計情報として、例えば、パケット数721が「P24」、バイト数722が「B24」、帯域735が「10Mbps」となっている。

30

【0147】

受信パケット処理部20のパケット蓄積部23が、何れかのバッファメモリから受信パケット (SYNパケット) を読み出し、ヘッダ送信制御部27が、受信パケットのヘッダ情報を検索処理部40に転送し、検索処理部40のルーティングテーブル検索部43とフローテーブル検索部42が、それぞれのテーブル検索を実行するまでの動作は、前述したフロー1の受信パケットの処理時と同様である。

【0148】

受信パケットがフローFs2に属するSYNパケットの場合、フローテーブル検索部42がヘッダ情報から生成した検索キーは、図27に示したエントリEN-x24のフロー識別条件に一致する。従って、フローテーブル検索部42は、検索結果として、エントリEN-x24が示す統計制御情報をフローエントリ管理部44、サンプル処理部45、サンプル判定部46、統計収集処理部47に分配する。

40

【0149】

今回は、検索された統計制御情報の登録処理フラグ631とサンプル処理フラグ635が「0」となっているため、フローエントリ管理部44とサンプル処理部45は、特別な応答動作は実行しない。統計収集処理部47は、統計制御情報の統計収集フラグ633が「1」となっているため、フローエントリ番号f24をもつエントリSE-x24の統計

50

情報 7 2 を更新する。従って、パケット数 7 2 1、バイト数 7 2 2、帯域 7 2 5 の値は、図 2 8 に示した値よりも増加する。

【0150】

一方、サンプル判定部 4 6 は、統計制御情報のサンプル判定フラグ 6 3 5 が「1」、サンプル処理フラグ 6 3 5 が「0」となっているため、受信パケットのサンプル処理を開始すべきか否かの判定（サンプル開始判定）を行う。サンプル開始判定は、統計収集処理部 4 7 に対して、フローエントリ番号 f 2 4 の統計情報を要求し、現在の帯域 7 3 5 と、統計制御情報が示すサンプル開始帯域 6 3 8 とを比較することを意味している。ここでは、帯域 7 3 5 の現在値「10 Mbps」が、サンプル開始帯域 6 3 8 の指定値「50 Mbps」よりも小さいため、サンプル判定部 4 6 は、サンプル処理不要と判断し、特別な動作は実行しない。従って、この時点では、検索結果出力部 4 8 は、コピーフラグ 4 8 2 とカプセル化指示フラグ 4 8 3 が「0」で、出力回線番号 4 8 1 とその他の情報 4 8 5 に有効情報を含む検索結果通知 4 8 0 を出力し、受信パケット処理部 2 0 でのサンプルパケットの生成はない。

10

【0151】

上述した動作が繰り返され、フローエントリ E N - 2 4 の帯域 7 3 5 の値が漸増して「51 Mbps」となったと仮定する。この状態で、パケット蓄積制御部 2 3 が、フロー F s 2 に属する S Y N パケットを処理し、ヘッダ送信制御部 2 7 が、ヘッダ情報を検索処理部 4 0 に転送すると、サンプル判定部 4 6 が、フローエントリ番号 f 2 4 のフローについてサンプル開始判定を実行し、現在帯域 7 3 5 が統計制御情報で指定されたサンプル開始帯域 6 3 8 を超えたことを検出する。サンプル判定部 4 6 は、今回は、サンプル処理開始と判断し、フローテーブル検索部 4 2 に対して、フローエントリ番号 f 2 4 のフローエントリ E N - x 2 4 におけるサンプル処理フラグ 6 3 5 の「1」への書き換えを指示する。フローテーブル検索部 4 2 は、上記書き換え指示に応答して、フローエントリ E N - x 2 4 の統計制御情報に含まれるサンプル処理フラグ 6 3 5 の値を「1」に書き換える。

20

【0152】

この時点では、統計情報テーブル 7 0 のエントリ S E - 2 4 の統計情報 7 2 と、フローテーブルのフローエントリ E N - 2 4 の統計制御情報が更新されただけであり、サンプル処理部 4 5 の動作には変化がない。従って、検索結果出力部 4 8 は、それまでと同様の検索結果通知 4 8 0 を信号線 L 4 8 に出力し、受信パケット処理部 2 0 でのサンプルパケットの生成はない。

30

【0153】

しかしながら、サンプル処理フラグ 6 3 5 の値が「1」に書き換えられた後で、フロー F s 2 に属する次に S Y N パケットが受信処理されると、検索処理部 4 0 の動作が変化する。サンプル判定部 4 6 は、フローテーブル検索部 4 2 から通知された統計制御情報において、サンプル判定フラグ 6 3 7 とサンプル処理フラグ 6 3 5 が両方とも「1」となっているため、フローエントリ番号 f 2 4 のフローについて、受信パケットのサンプル処理を終了すべきか否かの判定（サンプル終了判定）を実行する。サンプル終了判定は、統計収集処理部 4 7 に対して、フローエントリ番号 f 2 4 の統計情報を要求し、現在の帯域 7 3 5 と、サンプル終了帯域 6 3 9 とを比較することを意味している。ここでは、現在の帯域 7 3 5 が、サンプル終了帯域 6 3 9 を超えているため、サンプル判定部 4 6 は、サンプル処理フラグの書き換えは不要と判断し、次の統計制御情報を待つ。

40

【0154】

一方、サンプル処理部 4 5 は、フローテーブル検索部 4 2 から通知された統計制御情報において、サンプル処理フラグ 6 3 5 が「1」となっているため、例えば、パケットカウンタを使用して、サンプリングレート 6 3 6 に従った頻度で、サンプルパケット生成指示（コピー指示）を発生する。この例では、サンプル処理部 4 5 は、10 個の S Y N パケットに 1 個の割合でコピー指示を発生し、これを信号線 L 4 5 を介して検索結果出力部 4 8 に与る。コピー指示を発生しないサイクルでの検索結果出力部 4 8 の動作は、前述したサンプル処理フラグ 6 3 5 が「0」の場合と同様である。

50

【0155】

検索結果出力部48は、信号線L45からコピー指示を受信した場合、受信パケット処理部20にパケットコピーの生成が必要となったことを知らせる第1の検索結果通知を生成し、これを信号線L48に出力した後、受信パケット処理部20にカプセルヘッダ情報を適用したカプセル化コピーパケットをコレクタ装置に送信すべきことを知らせる第2の検索結果通知を生成し、これを信号線L48に出力する。

【0156】

第1の検索結果通知は、通常の実験結果通知480と同様に生成され、コピー指示フラグ482が「1」に設定される。すなわち、カプセル化指示フラグ483に「0」、出力回線番号481とその他の情報485に、ルーティングテーブルの実験結果から抽出された出力回線番号とその他の情報が設定され、カプセルヘッダ情報484は無効となっている。

10

【0157】

第2の実験結果通知は、コピー指示フラグ482に「0」、カプセル化指示フラグ483に「1」が設定され、カプセルヘッダ情報484に、サンプル（受信パケットのコピー）をコレクタ装置に送信するためのカプセルヘッダ情報が設定される。このカプセルヘッダ情報は、サンプルパケットヘッダ情報蓄積部51から読み出される。第2の実験結果通知の出力回線番号481とその他の情報485には、サンプルパケットヘッダ情報蓄積部1511内に予め用意された出力回線番号とその他の情報が設定される。

20

【0158】

図16において、受信パケット処理部20のヘッダ送信制御部27は、上記第1の実験結果通知480を受信すると、通常パケットの実験時と同様、該実験結果通知が示す出力回線番号481～カプセル化ヘッダ情報484を先頭のパケットデータ管理情報ブロック200-1の内部ヘッダ15に設定し、パケットデータ管理情報ブロック200-1を出力パケットヘッダ蓄積メモリ25Bに書き込む。今回受信した実験結果通知は、コピー指示フラグ482が「1」となっているため、ヘッダ送信制御部27は、出力パケットヘッダ蓄積メモリ25Bに書き込み済みとなったパケットデータ管理情報ブロック200-1を廃棄せずに保持しておく。後続のパケットデータ管理情報ブロック200-2、200-3、…が存在した場合は、これらをそのまま出力パケットヘッダ蓄積メモリ25Bに書き込み、パケットデータ管理情報ブロック200-1と同様、廃棄することなく保持しておく。

30

【0159】

この後、ヘッダ送信制御部27は、コピー管理部28に対して、コピー数と、上記各パケットデータ管理情報が示すメモリアドレス204の値とを通知し、パケット転送制御部29に対して、パケット転送開始を要求する。今回は、実験結果通知のコピー指示フラグ482が「1」となっているため、コピー管理部28にはコピー数「1」が通知される。従って、コピー管理部28は、図24に示したアドレス解放制御テーブル280において、ヘッダ送信制御部27から通知されたメモリアドレスと対応するメモリブロック281の送信待ち回数282を“2”に設定する。

【0160】

40

パケットの転送制御部29は、上記パケット転送開始要求に応答して、出力パケットヘッダ蓄積メモリ25Bからパケットデータ管理情報ブロック200-1、200-2、…を読み出し、これらのパケットデータ管理情報ブロックに基づいて、パケットデータ蓄積メモリ24からパケットデータ部分を読み出して、再編成された内部パケット（SYNパケット）を信号線L1に出力する。

【0161】

パケットの転送制御部29が内部パケットの転送が完了した時、コピー管理部28は、アドレス解放制御テーブル280において、データ送信を終えたメモリブロックの送信待ち回数を1ずつ減算する。今回は、データ送信を終えたメモリブロックの送信待ち回数の初期値が“2”に設定されているため、減算後の送信待ち回数がそれぞれ“1”として残

50

る。従って、これらのメモリブロックについては、メモリ状態管理部 26 へのアドレス解放通知の発行が抑制され、パケットデータ蓄積メモリ 24 に蓄積されたパケットデータがそのまま保存される。

【0162】

ヘッダ送信制御部 27 は、上記第 1 の検索結果通知に続いて、検索結果出力部 48 から第 2 の検索結果通知を受信する。第 2 の検索結果通知を受信したヘッダ送信制御部 27 は、第 1 の検索結果通知の受信時と同様、該検索結果通知が示す出力回線番号 481 ~ カプセル化ヘッダ情報 484 を先頭のパケットデータ管理情報ブロック 200-1 の内部ヘッダ 15 に設定し、パケットデータ管理情報ブロック 200-1 を出力パケットヘッダ蓄積メモリ 25B に書き込み、後続のパケットデータ管理情報ブロック 200-2、200-3、…が存在した場合は、これらをそのまま出力パケットヘッダ蓄積メモリ 25B に書き込む。今回は、第 2 の検索結果通知のコピー指示フラグ 482 が「0」となっているため、出力パケットヘッダ蓄積メモリ 25B に書き込み済みとなったパケットデータ管理情報ブロック 200-1、200-2、…は廃棄される。

10

【0163】

この後、ヘッダ送信制御部 27 は、コピー管理部 28 に対して、コピー数と、上記各パケットデータ管理情報が示すメモリアドレス 204 の値とを通知し、パケット転送制御部 29 に対して、パケット転送開始を要求する。今回は、コピー指示フラグ 482 が「0」となっているため、コピー管理部 28 は、アドレス解放制御テーブル 280 において、ヘッダ送信制御部 27 から通知されたメモリアドレスと対応するメモリブロック 281 の送信待ち回数 282 を「1」に設定する。従って、パケットの転送制御部 29 による内部パケットの転送が完了した時、データ送信を終えたメモリブロックについては、減算後の送信待ち回数がそれぞれ「0」となり、メモリ状態管理部 26 にアドレス解放通知の発行される。

20

【0164】

上記第 2 の検索結果通知に応答して、パケット転送制御部 29 から送信パケット処理部 30 に転送された内部パケット (SYN パケットのコピー) は、内部ヘッダ 15 のカプセル化指示フラグ 153 が「1」に設定されている。送信パケット処理部 30 のパケット出力制御部 32 は、出力パケットヘッダ蓄積メモリ 34 から読み出された先頭のパケットデータ管理情報ブロック 200-1 にヘッダ情報 205 の一部として含まれる内部ヘッダ 15 を抽出し、カプセル化指示フラグ 153 をチェックする。今回は、カプセル化指示フラグ 153 が「1」となっているため、内部ヘッダ情報 15 に含まれるコレクタ装置宛のカプセル化ヘッダ情報 154 (レイヤ 2 ヘッダ ~ レイヤ 4 ヘッダ) をコピーパケットの先頭に付与し、出力回線番号 152 によって特定される回線終端処理部 30-k に送信する。

30

【0165】

上述したコピーパケットの生成と、コレクタ装置へのカプセル化パケットの送信は、監視対象となっている SYN パケットの帯域 725 が、フローエントリ EN-24 で指定するサンプル終了帯域 639 より低下する迄、サンプリングレート 636 に従った頻度で、繰り返して実行される。フローエントリ EN-24 のサンプル処理フラグ 635 が「1」に設定された状態で、フロー識別条件 62 に該当する SYN パケットの送出量が次第に減少し、統計情報テーブル 70 における帯域 775 の値が、サンプル終了帯域 639 で指定された「40 Mbps」よりも低下した場合、検索処理部 40 は次のように動作する。

40

【0166】

受信パケット処理部 20 のパケット蓄積制御部 23 が、新たな SYN パケットの蓄積処理を終え、上記 SYN パケットのヘッダ情報がヘッダ送信制御部 27 から検索処理部 40 のヘッダ情報蓄積部 41 に転送されると、フローテーブル検索部 42 は、フローテーブル 60 から検索したフローエントリ EN-24 の統計制御情報 63 をフローエントリ管理部 44、サンプル処理部 45、サンプル判定部 46、統計収集処理部 47 に分配する。

【0167】

フローエントリ管理部 44 は、統計制御情報 63 の登録処理フラグが「0」となってい

50

るため、特別な応答動作はしない。統計収集処理部47は、統計制御情報63の統計収集フラグが「1」となっているため、ヘッダ情報蓄積部41から受信したヘッダ情報に従って、統計情報エン트리SE-x24の統計情報72を更新する。サンプル処理部45は、統計制御情報63のサンプル処理フラグ635が「1」となっているため、これまでと同様に、サンプリングレート636に従ったコピー指示動作を繰り返す。

【0168】

一方、サンプル判定部46は、統計制御情報63のサンプル判定フラグ637とサンプル処理フラグ635が両方とも「1」となっているため、フローエン트리番号f24のフローについて、サンプル終了判定を実行する。今回は、現在の帯域735がサンプル終了帯域639より低下しているため、サンプル判定部46が、フローテーブル検索部42に、フローエン트리番号f24のエン트리EN-24におけるサンプル処理フラグ635の「0」への書き換えを指示し、フローテーブル検索部42が、エン트리EN-24の統計制御情報63を初期状態に戻す。従って、SYNパケットフローの帯域が再びサンプル開始帯域を超え、サンプル処理フラグ635が「1」に設定されるまでの間は、SYNパケット処理時のサンプル処理部45からのコピー指示の発生はなくなり、コレクタ装置へのカプセル化パケットの送信は休止状態となる。

【0169】

本発明では、フロー識別条件におけるその他の情報629として、例えば、TCPフラグや、Ethernetヘッダの宛先/送信元MACアドレス、VLAN IDの値を指定することによって、TCPコネクションの特定の制御パケットを用いたサーバへのDenial of Serviceアタック(DOSアタック)の検出や、VLAN-ID、MACアドレス別の統計情報収集が可能になる。

【0170】

実施例では、パケット蓄積制御部23が、各受信パケットに付すべき内部ヘッダ15を生成し、これをパケットデータ管理情報ブロック200に設定して、入力パケットヘッダ蓄積部25Aに蓄積したが、内部ヘッダを各回線終端処理部21-1~21-Nで生成し、パケット蓄積制御部23が、バッファメモリ22-1~22-Nから内部パケット形式で受信パケットを読み出すようにしてもよい。この場合、バッファメモリ22-(N+1)に蓄積される統計情報通知パケット300にも内部ヘッダ15を付与する必要があるため、統計情報通知パケットヘッダ情報蓄積部50に、予め内部ヘッダ15を用意しておけばよい。

【0171】

また、実施例では、フロー登録用の統計制御エン트리EN-x12が検索された時、フローテーブル60に無条件で新たなフローエントリが追加される例について説明したが、統計制御エン트리EN-x12の統計制御情報63で、新たなフローエントリの登録条件を指定しておき、この条件が満足された時、フローテーブル60に新たなフローエントリが追加されるようにすることもできる。

【0172】

例えば、エン트리EN-x12において、サンプル開始帯域638は、サンプル判定フラグ637が「1」の場合は、サンプル処理の開始条件を示し、サンプル判定フラグ637が「0」で登録処理フラグ631が「1」の場合は、新エントリの登録開始条件を示すものと約束しておけば、統計制御エン트리EN-x12の統計制御情報で、登録処理フラグ631、統計収集フラグ633、帯域計算フラグ634をそれぞれ「1」に設定し、サンプル判定フラグ637を「0」にして、サンプル開始帯域638に登録開始帯域を設定しておくことにより、フローエントリ管理部44に、TCPフローで登録開始帯域が満たされた時、フローテーブル60への新エントリの追加動作をスタートさせることが可能となる。

【図面の簡単な説明】

【0173】

【図1】本発明の統計収集装置が適用される通信ネットワークの1例を示す図。

【図 2】図 1 の通信ネットワークで通信されるパケットのフォーマットを示す図。

【図 3】Ethernet V2 のフレームのヘッダフォーマットを示す図。

【図 4】Tag VLAN 対応の Ethernet V2 フレームのヘッダフォーマットを示す図。

【図 5】IPv4 パケットのヘッダフォーマットを示す図。

【図 6】IPv6 パケットのヘッダフォーマットを示す図。

【図 7】TCP のヘッダフォーマットを示す図。

【図 8】図 7 における TCP フラグ 133 の詳細を示す図。

【図 9】UDP ヘッダのフォーマットを示す図。

【図 10】図 1 のルータ R1 で収集されるフロー識別条件の 1 例を示す図。

10

【図 11】図 1 のルータ R1 で収集される統計情報の 1 例を示す図。

【図 12】本発明の統計収集機能を備えるルータ R1 の 1 実施例を示す構成図。

【図 13】本発明のルータ R1 と管理端末 1300 との接続関係の 1 例を示す図。

【図 14】本発明のルータ R1 と管理端末 1300 との接続関係の他の例を示す図。

【図 15】本発明のルータの内部で扱われる内部パケットのフォーマットの 1 例を示す図。

。

【図 16】図 12 の受信パケット処理部 20 の 1 実施例を示すブロック図。

【図 17】図 16 のメモリ 25A、25B に蓄積されるパケットデータ管理情報ブロック 200 の 1 例を示す図。

【図 18】図 16 のメモリ 25A（または 25B）に蓄積されるパケットデータ管理情報ブロックと、メモリ 24 に蓄積されるデータブロックとの関係を示す図。

20

【図 19】図 16 の送信パケット処理部 30 の 1 実施例を示すブロック図。

【図 20】図 16 の検索処理部 40 の 1 実施例を示すブロック図。

【図 21】図 16 のフローテーブル 60 の 1 例を示す図。

【図 22】図 16 の統計情報テーブル 70 の 1 例を示す図。

【図 23】図 20 の検索結果出力部 48 が出力する検索結果通知 480 の 1 例を示す図。

【図 24】図 16 のコピー管理部 28 が備えるアドレス解放制御テーブル 280 の 1 例を示す図。

【図 25】図 20 のフロー管理テーブル 49 の 1 例を示す図。

【図 26】図 20 の統計情報通知パケット生成部 53 が出力する統計情報通知パケット 300 のフォーマットの 1 例を示す図。

30

【図 27】図 12 に示したフローテーブル 60 の他の実施例を説明するための図。

【図 28】図 12 に示した統計情報テーブル 70 の他の実施例を説明するための図。

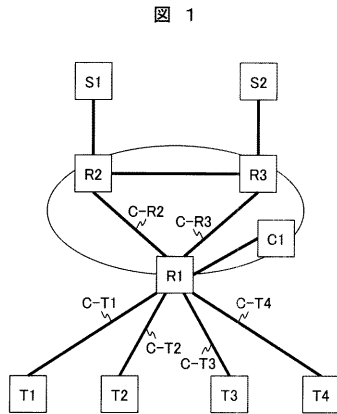
【符号の説明】

【0174】

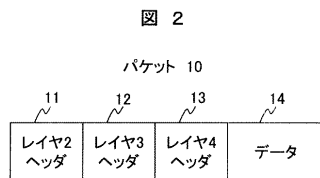
S1、S2：サーバ、R1～R3：ルータ、T1～T4：端末、C1：コレクタ装置、
20：受信パケット処理部、30：送信パケット処理部、40：検索処理部、
60：フローテーブル、70：統計情報テーブル、80：ルーティングテーブル、
42：フローテーブル検索処理部、43：ルーティングテーブル検索部、
44：フローエントリ管理部、45：サンプル処理部、46：サンプル判定部、
47：統計収集処理部、48：検索結果出力部、53：統計情報通知パケット生成部。

40

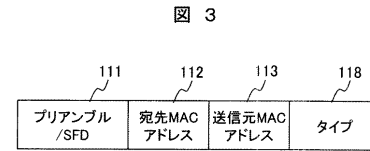
【図 1】



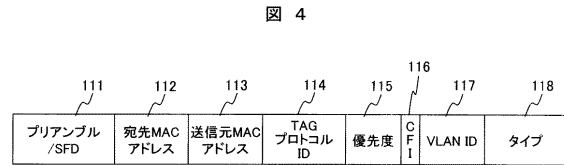
【図 2】



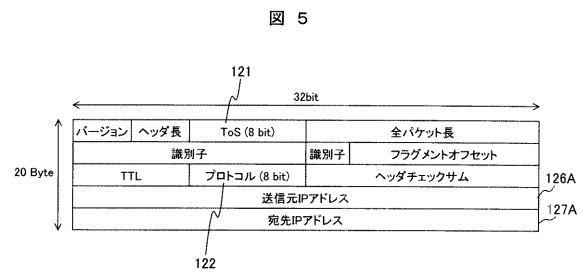
【図 3】



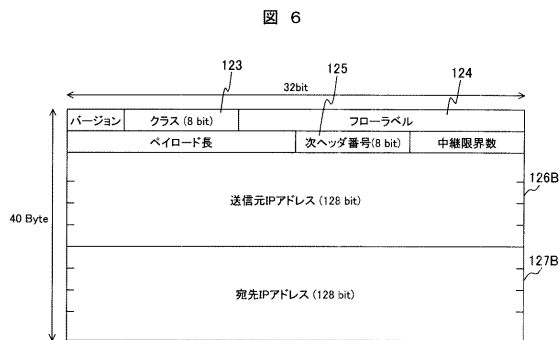
【図 4】



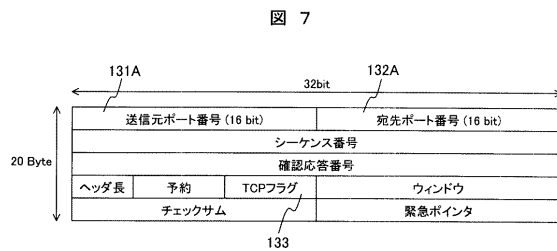
【図 5】



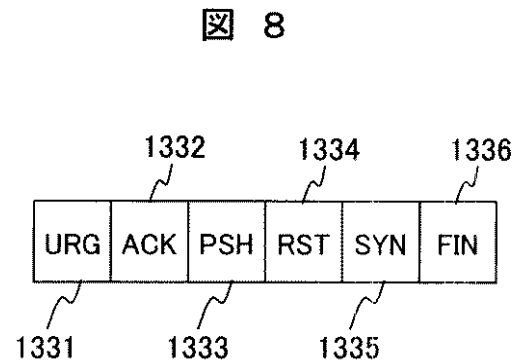
【図 6】



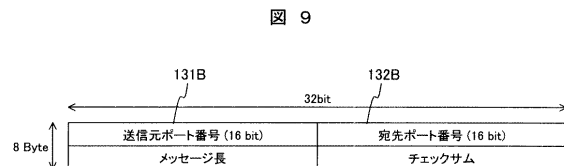
【図 7】



【図 8】



【図 9】



【図 10】

図 10

フロー エントリ 番号	フロー識別条件					
	送信元IP アドレス	宛先IP アドレス	上位 プロトコル	TOS	送信元 ポート番号	宛先 ポート番号
f1	IP-S1	IP-T1	TCP	TOS1	SPRT1	DPRT1
f2	IP-S1	IP-T3	TCP	TOS1	SPRT1	DPRT3

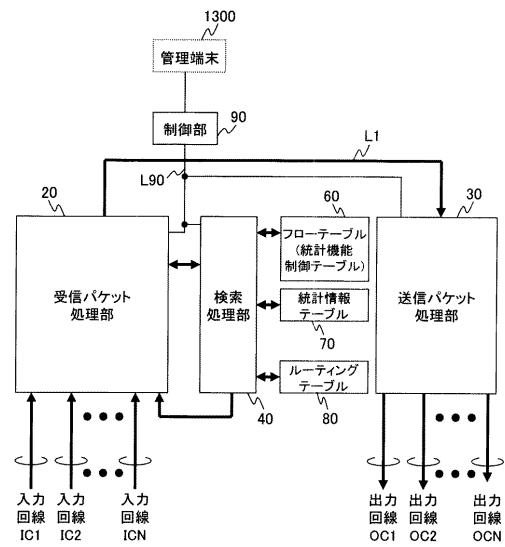
【図 11】

図 11

フロー エントリ 番号	統計情報				
	パケット 数	バイト数	入力回線 番号	出力回線 番号	その他 の情報
f1	10	2000	C-R2	C-T1	...
f2	20	2000	C-R2	C-T3	...

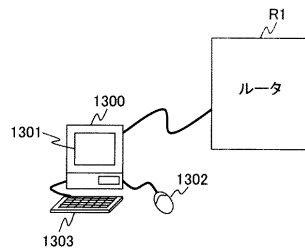
【図 12】

図 12



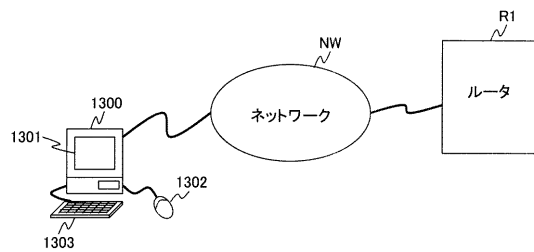
【図 13】

図 13



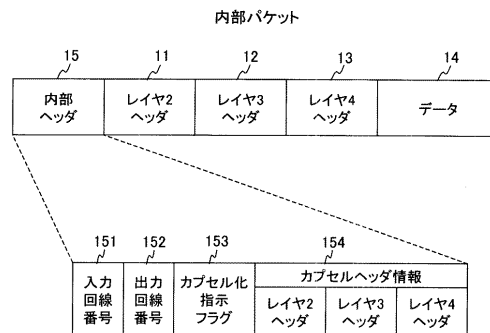
【図 14】

図 14

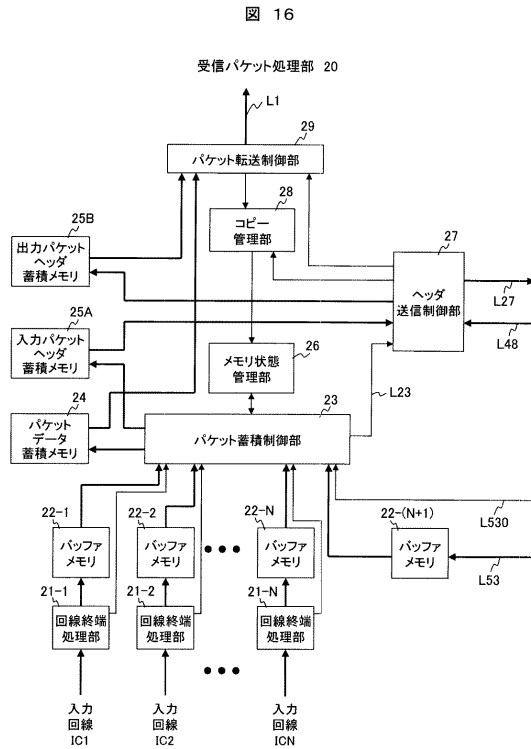


【図 15】

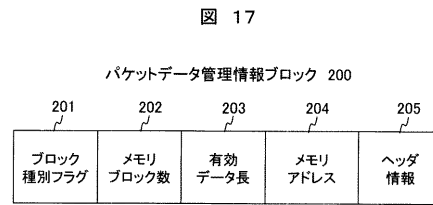
図 15



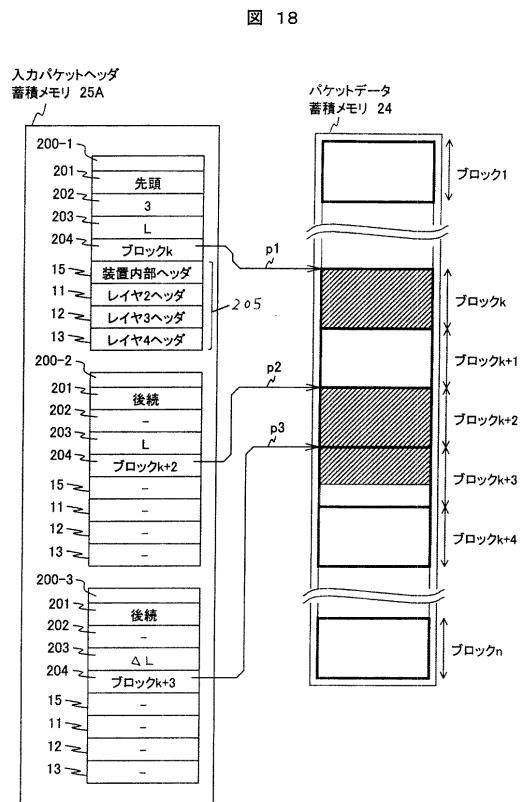
【図 16】



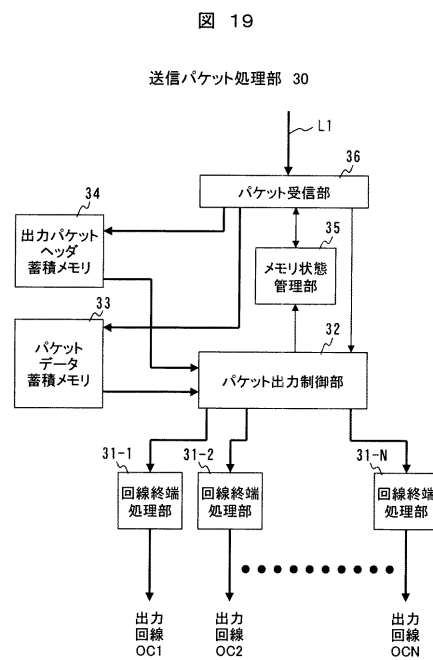
【図 17】



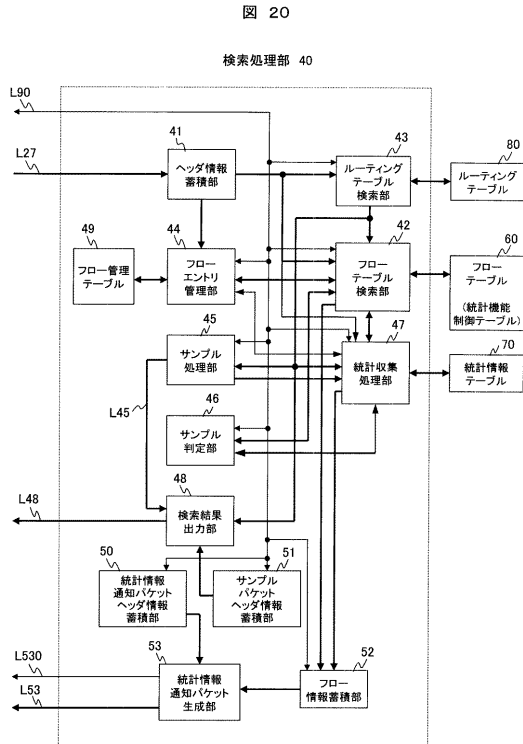
【図 18】



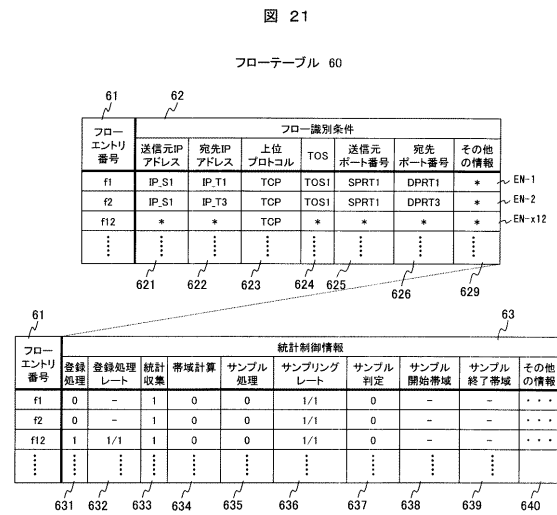
【図 19】



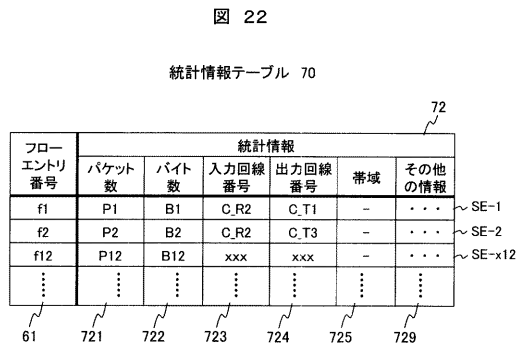
【図 20】



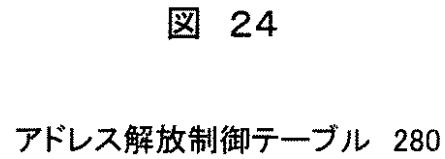
【図 21】



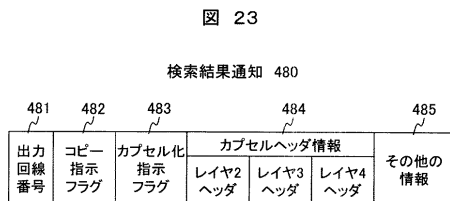
【図 22】



【図 24】



【図 23】



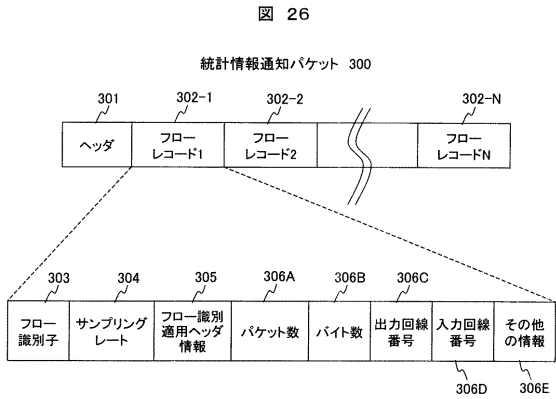
【図 2 5】

図 25

フロー管理テーブル 49

491 フロー エントリ 番号	492 フローテーブル エントリ アドレス	493 パケット数	494 更新時刻	495 非更新 回数
f1	1	P1'	100	0
f2	2	P2'	200	1
⋮	⋮	⋮	⋮	⋮

【図 2 6】



【図 2 8】

図 28

統計情報テーブル 70

フロー エントリ 番号	統計情報					
	パケット 数	バイト 数	入力回線 番号	出力回線 番号	帯域	その他 の情報
f24	P24	B24	xxx	xxx	10Mbps	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮

61 721 722 723 724 725 729

【図 2 7】

図 27

フローテーブル 60

フロー エントリ 番号	フロー識別条件							
	送信元IP アドレス	宛先IP アドレス	上位 プロトコル	TOS	送信元 ポート番号	宛先 ポート番号	SYN フラグ	その他 の情報
f24	*	*	TCP	*	*	*	1	*
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

61 621 622 623 624 625 626 627 629 EN-x24

フロー エントリ 番号	統計制御情報									
	登録 処理	登録 処理 レート	統計 収集	帯域 計算	サンブル 処理	サンプリング レート	サンブル 判定	サンブル 開始帯域	サンブル 終了帯域	その他 の情報
f24	0	-	1	1	0	1/10	1	50Mbps	40Mbps	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

61 631 632 633 634 635 636 637 638 639 640 63

フロントページの続き

(72)発明者 長坂 充

神奈川県秦野市堀山下1番地 株式会社日立製作所 IPネットワーク事業部内

(72)発明者 須貝 和雄

神奈川県秦野市堀山下1番地 株式会社日立製作所 IPネットワーク事業部内

(72)発明者 石川 有一

東京都国分寺市東恋ヶ窪一丁目280番地 株式会社日立製作所 中央研究所内

審査官 矢頭 尚之

(56)参考文献 特開2001-257722 (JP, A)

特開2002-016599 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/56