(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4823156号
(P4823156)
(45)発行日　平成23年11月24日(2011.11.24)　(24)登録日　平成23年9月16日(2011.9.16)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　400Z

請求項の数 6　(全 12 頁)

(21)出願番号　特願2007-173850(P2007-173850)
(22)出願日　平成19年7月2日(2007.7.2)
(65)公開番号　特開2009-16987(P2009-16987A)
(43)公開日　平成21年1月22日(2009.1.22)
審査請求日　平成21年12月15日(2009.12.15)

(73)特許権者　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　110000028
特許業務法人明成国際特許事務所
(72)発明者　加賀野井　晴大
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　汲田　直也
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

審査官　安藤　一道

最終頁に続く

(54)【発明の名称】リモートトラフィック監視方法

(57)【特許請求の範囲】
【請求項１】
ネットワークのトラフィックを監視するトラフィック監視システムであって、
サンプリング装置と転送処理部とを有する転送装置と、
オフロード処理装置と、
トラフィック解析装置と、
を備え、
前記サンプリング装置は、
前記トラフィックから予め設定された基準に基づいて転送データを抽出し、前記抽出された転送データを複製してサンプリングデータを生成する抽出部と、
前記サンプリングデータに対して、前記オフロード処理装置を宛先とするヘッダを付加するカプセル化処理を実行してカプセル化データを生成するカプセル化処理部と、
を備え、
前記転送処理部は、前記転送データと前記カプセル化データとを転送し、
前記オフロード処理装置は、前記転送されたカプセル化データに応じて前記トラフィックを解析するためのフローデータを生成し、前記フローデータを前記トラフィック解析装置に転送し、
前記トラフィック解析装置は、前記転送されたフローデータに基づいて前記トラフィックを解析するトラフィック監視システム。
【請求項２】

請求項１記載のトラフィック監視システムであって、
前記カプセル化処理は、前記カプセル化データを転送した転送装置を特定するための情報を前記カプセル化データに格納する処理を含むトラフィック監視システム。
【請求項３】
請求項１または２に記載のトラフィック監視システムであって、
前記ネットワークは、複数の転送装置を有し、
前記トラフィック監視システムは、複数のオフロード処理装置を備え、
前記複数の転送装置の各々は、前記複数のオフロード処理装置のいずれかに前記カプセル化データを転送するように割り当てられているトラフィック監視システム。
【請求項４】
ネットワークのトラフィックを監視するために前記トラフィックから転送データを抽出してオフロード処理装置に転送するサンプリング装置であって、
前記トラフィックから予め設定された基準に基づいて転送データを抽出し、前記抽出された転送データを複製してサンプリングデータを生成する抽出部と、
前記サンプリングデータに対して、前記オフロード処理装置を宛先とするヘッダを付加するカプセル化処理を実行してカプセル化データを生成するカプセル化処理部と、
前記転送されたカプセル化データに応じて、前記オフロード処理装置に前記トラフィックを解析するためのフローデータを生成させるために、前記オフロード処理装置に対して前記カプセル化データを送信する出力部と、
を備えるサンプリング装置。
【請求項５】
ネットワークにおいてデータの転送を行うための転送装置であって、
請求項４記載のサンプリング装置と、
前記転送データと前記カプセル化データとを転送する転送処理部と、
を備える転送装置。
【請求項６】
ネットワークのトラフィックを監視するトラフィック監視方法であって、
サンプリング装置と転送処理部とを有する転送装置と、
オフロード処理装置と、
トラフィック解析装置と、
を準備する工程と、
前記サンプリング装置が前記トラフィックから予め設定された基準に基づいて転送データを抽出し、前記抽出された転送データを複製してサンプリングデータを生成する抽出工程と、
前記サンプリング装置が前記サンプリングデータに対して、前記オフロード処理装置を宛先とするヘッダを付加するカプセル化処理を実行してカプセル化データを生成するカプセル化処理工程と、
前記転送処理部が前記転送データと前記カプセル化データとを転送する工程と、
前記オフロード処理装置が前記転送されたカプセル化データに応じて前記トラフィックを解析するためのフローデータを生成し、前記フローデータを前記トラフィック解析装置に転送する工程と、
前記トラフィック解析装置が前記転送されたフローデータに基づいて前記トラフィックを解析する工程と、
を備えるトラフィック監視方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークシステムに関し、特に、ネットワーク上を流れるトラフィックの計測に係る技術に関する。
【背景技術】

【０００２】
従来から安定したネットワークを実現するためにネットワーク内のフロー統計を使用したネットワーク管理技術が提案されている。このようなネットワーク管理技術には、たとえばＮｅｔＦｌｏｗ統計やｓＦｌｏｗ統計といった技術が一般的に普及している。これらの技術では、ネットワーク内のルータやスイッチといったネットワークデバイスが備えるエージェントが監視対象となるトラフィックからパケットを抽出するとともに、抽出されたパケットを加工してコレクタに送信している。一方、特許文献１に開示されるように予め設定された対象のパケットのコピーを監視装置にミラーリングする技術も提案されている。
【０００３】
【特許文献１】特開２００６－０５０４３３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかし、単純なミラーリングではなく、ネットワークデバイスが備えるエージェントがパケットの加工を行う方法では、ルータやスイッチといったネットワークデバイスの負担の増大あるいは抽出可能なフロー数や精度（粒度）の制限といった問題が生じていた。
【０００５】
本発明は、上述の課題を解決するためになされたものであり、ネットワークシステムにおいて、ルータやスイッチといったネットワークデバイスの負担を軽減する技術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】
【０００６】
本発明は、ネットワークのトラフィックを監視するトラフィック監視システムを提供する。このトラフィック監視システムは、
サンプリング装置と転送処理部とを有する転送装置と、
オフロード処理装置と、
トラフィック解析装置と、
を備え、
前記サンプリング装置は、
前記トラフィックから予め設定された基準に基づいて転送データを抽出し、前記抽出された転送データを複製してサンプリングデータを生成する抽出部と、
前記サンプリングデータに対して、前記オフロード処理装置を宛先とするヘッダを付加するカプセル化処理を実行してカプセル化データを生成するカプセル化処理部と、
を備え、
前記転送処理部は、前記転送データと前記カプセル化データとを転送し、
前記オフロード処理装置は、前記転送されたカプセル化データに応じて前記トラフィックを解析するためのフローデータを生成し、前記フローデータを前記トラフィック解析装置に転送し、
前記トラフィック解析装置は、前記転送されたフローデータに基づいて前記トラフィックを解析する。
【０００７】
本発明のトラフィック監視システムでは、処理負担の大きなフローデータの生成処理が転送装置とは別個のオフロード処理装置で処理され、転送装置が担当する処理が抽出・複製・カプセル化と本来の機能である転送だけとなるので負担が顕著に軽減される。さらに、本願発明者は、ネットワークの監視内容がネットワーク毎に相違し、詳細な解析から簡易な解析まで用途によって様々であり、さらに監視内容も時間とともに変動する場合もあるというスケーラビリティの要請にも着目した。このような要請に対し、本願発明者は、処理負担の大きなフローデータの生成処理をオフロードすれば、オフロード処理装置の選択や交換のみ柔軟に対応でき、高いスケーラビリティを実現することができる点に想到し

た。
【０００８】
ここで、抽出・複製・カプセル化の処理を担当するサンプリング装置は、転送装置の内部にＡＳＩＣその他の態様でハードウェア的に実装することも可能であるし、あるいはソフトウェア的に実装することも可能である。本願発明は、処理負担が小さいのでソフトウェア的に実装してもＣＰＵの負担が小さいという利点がある。加えて、転送装置が担当する抽出・複製・カプセル化の各処理のうち複製・カプセル化は、転送装置が転送処理で実行する処理なので、その機能をそのまま利用可能である。さらに、抽出処理も転送処理で行われる振り分け処理の拡張として対処可能である。このため、サンプリング処理のソフトウェア的な実装は、リソースの消費も少ないという特徴をも有している。
【０００９】
このように、本願発明者は、処理負担が大きくボトルネックとなる可能性があるとともに、転送装置の本来の処理とは本質的に相違する処理をオフロードするとともに、転送装置の本来の機能の流用や拡張で対処可能な処理であって、かつ、転送装置でのみ可能な抽出・複製・カプセル化といった処理を転送装置で実行させるという極めて合理的なシステムの創作に成功した。さらに、本願発明は、転送装置へのソフトウェア的な実装も実用的なので、極めて実装性が高く広汎な用途に適用可能なシステムとして実現されている。
【００１０】
上記トラフィック監視システムにおいて、
前記カプセル化処理は、前記カプセル化データを転送した転送装置を特定するための情報を前記カプセル化データに格納する処理を含むようにしても良い。
【００１１】
こうすれば、オフロード処理装置は、どの転送装置のフローから抽出されたデータかを識別した上で統計・解析処理を行うことができる。
【００１２】
上記トラフィック監視システムにおいて、
前記ネットワークは、複数の転送装置を有し、
前記トラフィック監視システムは、複数のオフロード処理装置を備え、
前記複数の転送装置の各々は、前記複数のオフロード処理装置のいずれかに前記カプセル化データを転送するように割り当てられていても良い。
【００１３】
こうすれば、オフロード処理装置の追加や削減によって監視内容や監視対象（たとえば転送装置の数）の変化に起因する負荷の変動に柔軟に対応することができる。さらに、たとえば、監視対象のスイッチやルータの数の増加に応じて、オフロード処理装置を増やしていくことができるので、最初からオフロード処理負担に十分に対応できるシステムよりも消費電力を軽減し、かつ初期投資を小さくすることができるという利点もある。
【００１４】
本発明は、さらに、トラフィック解析装置によるネットワークのトラフィックの解析のために使用されるフローデータを生成するオフロード処理装置を提供する。
このオフロード処理装置は、
前記トラフィックから予め設定された基準に基づいて抽出され、複製された後にカプセル化処理によって前記オフロード処理装置を宛先とするヘッダが付加されたカプセル化データを受信するカプセル化データ受信部と、
前記受信したカプセル化データに応じて、前記トラフィックを解析するためのフローデータを生成するフローデータ生成部と、
前記フローデータに応じて、前記トラフィック解析装置に前記トラフィックを解析させるために、前記トラフィック解析装置に前記フローデータを送信する出力部と、
を備える。
【００１５】
本発明は、さらに、ネットワークのトラフィックを監視するために前記トラフィックか

ら転送データを抽出してオフロード処理装置に転送するサンプリング装置を提供する。
このサンプリング装置は、
前記トラフィックから予め設定された基準に基づいて転送データを抽出し、前記抽出された転送データを複製してサンプリングデータを生成する抽出部と、
前記サンプリングデータに対して、前記オフロード処理装置を宛先とするヘッダを付加するカプセル化処理を実行してカプセル化データを生成するカプセル化処理部と、
前記転送されたカプセル化データに応じて、前記オフロード処理装置に前記トラフィックを解析するためのフローデータを生成させるために、前記オフロード処理装置に対して前記カプセル化データを送信する出力部と、
を備える。
【００１６】
本発明は、さらに、ネットワークにおいてデータの転送を行うための転送装置を提供する。
この転送装置は、
上記サンプリング装置と、
前記転送データと前記カプセル化データとを転送する転送処理部と、
を備える。
【００１７】
本発明は、さらに、ネットワークのトラフィックを監視するトラフィック監視方法を提供する。
このトラフィック監視方法は、
サンプリング装置と転送処理部とを有する転送装置と、
オフロード処理装置と、
トラフィック解析装置と、
を準備する工程と、
前記サンプリング装置が前記トラフィックから予め設定された基準に基づいて転送データを抽出し、前記抽出された転送データを複製してサンプリングデータを生成する抽出工程と、
前記サンプリング装置が前記サンプリングデータに対して、前記オフロード処理装置を宛先とするヘッダを付加するカプセル化処理を実行してカプセル化データを生成するカプセル化処理工程と、
前記転送処理部が前記転送データと前記カプセル化データとを転送する工程と、
前記オフロード処理装置が前記転送されたカプセル化データに応じて前記トラフィックを解析するためのフローデータを生成し、前記フローデータを前記トラフィック解析装置に転送する工程と、
前記トラフィック解析装置が前記転送されたフローデータに基づいて前記トラフィックを解析する工程と、
を備える。
【００１８】
なお、本発明は、上記の態様に限ることなく、ネットワーク監視制御方法としての態様で実現することも可能である。さらには、それら方法や装置を構築するためのコンピュータプログラムとしての態様や、そのようなコンピュータプログラムを記録した記録媒体としての態様など、種々の態様で実現することも可能である。
【発明を実施するための最良の形態】
【００１９】
以下、本発明の実施の形態について、実施例に基づき以下の順序で説明する。
Ａ．本発明の第１実施例におけるトラフィック監視システム：
Ｂ．本発明の第２実施例におけるトラフィック監視システム：
Ｃ．変形例：
【００２０】

Ａ．本発明の第１実施例におけるトラフィック監視システム：

図１は、本発明の第１実施例におけるトラフィック監視システム１０の概要を示すブロック図である。トラフィック監視システムは、本実施例では、説明を分かりやすくするために２台のクライアントシステムＴ１、Ｔ２と５個のスイッチＳＷ１～ＳＷ５と、各スイッチを含む機器間を接続する回線Ｃｔ＿１、Ｃ１＿２、Ｃ２＿３、Ｃ３＿４、Ｃ４＿ｔ、Ｃ２＿５、Ｃ３＿５、Ｃ３＿ａ、Ｃ５＿ｏを備えたネットワーク１０のトラフィックを監視するものとする。ネットワーク１０は、本実施例では、レイヤ２のローカルエリアネットワークとして構成されているものとする。

【００２１】

トラフィック監視システムは、本実施例では、一例としてｓＦｌｏｗ統計を使用してトラフィックを監視するものとする。ｓＦｌｏｗ統計は、端末間のトラフィック（フロー）特性や隣接するネットワーク単位のトラフィック特性の分析を行うためにネットワークの上を流れるトラフィックを中継装置（ルータやスイッチ）で監視する機能である。ｓＦｌｏｗ統計は、公開されたフロー統計プロトコル（ＲＦＣ３１７６）でレイヤ２からレイヤ３までの統計情報がサポートされている。

【００２２】

トラフィック監視システムは、ｓＦｌｏｗ統計を使用してトラフィックを監視するために、スイッチＳＷ２に備えられたｓＦｌｏｗエージェント３１０（拡大図ＥＶ１）と、オフロード処理部１００と、解析処理部２００とを備えている。ＳＦｌｏｗエージェント３１０は、抽出部３１１と、カプセル化処理部３１２と、を備えている。ｓＦｌｏｗエージェント３１０は、たとえばＡＳＩＣとしてハードウェア的に構成しても良いし、あるいはソフトウェア的に構成しても良い。スイッチＳＷ２は、さらに、他のスイッチＳＷ１、ＳＷ３～ＳＷ５と同様にデータ（パケット）を転送するための転送処理部３５０を備えている。監視対象のトラフィックは、この例では、２台のクライアントシステムＴ１、Ｔ２の間の転送トラフィックＴＲｔ１＿ｔ２（図１）とする。ただし、監視対象のトラフィックは、この例に限られず後述するように任意に設定することができる。

【００２３】

図１には、さらに、従来技術におけるｓＦｌｏｗエージェント３１０ａを備えるスイッチＳＷ２ａが示されている（拡大図ＥＶ２）。ｓＦｌｏｗエージェント３１０ａは、サンプル生成部３１３を備える点で、これを備えない第１実施例のｓＦｌｏｗエージェント３１０と相違する。第１実施例では、サンプル生成部３１３の処理は、スイッチＳＷ２の外部に存在するオフロード処理部１００にオフロードされている。

【００２４】

図２は、第１実施例のトラフィック監視処理の内容を示すフローチャートである。ステップＳ１００では、ｓＦｌｏｗエージェント３１０が備える抽出部３１１は、転送トラフィックＴＲｔ１＿ｔ２（図１）から予め設定された抽出基準に基づいてパケットを抽出する。抽出基準として、たとえばアクセス制御リスト（ＡＣＬ）や特定の入出力ポートの指定、一定の割合でのサンプリング、あるいはこれらの組合せとして実現することができる。

【００２５】

ステップＳ２００では、ｓＦｌｏｗエージェント３１０が備えるカプセル化処理部３１２は、抽出されたパケットに対してカプセル化処理を行う。カプセル化処理とは、本実施例では、抽出されたパケットの複製を生成し、この複製されたパケットをペイロードとして特定のヘッダーと付加情報とを付加する処理である。

【００２６】

図３は、レイヤ２のローカルエリアネットワークとして構成された第１実施例のカプセル化処理の内容を示す説明図である。図３には、抽出されたパケットＤ１（イーサネットフレーム）にヘッダと付加情報を付加してカプセル化されたカプセル化パケットＤ１ｃ（イーサネットフレーム）とが示されている。カプセル化パケットＤ１ｃのヘッダには、宛先ＭＡＣアドレスＤＭＡＣとしてのオフロード処理部１００のＭＡＣアドレスと、送信元

ＭＡＣアドレスＳＭＡＣとしてのスイッチＳＷ２のＭＡＣアドレスと、プロトコルの種類を表すイーサタイプＴＹＰＥとを含んでいる。カプセル化パケットＤ１ｃの付加情報としては、スイッチＳＷ２の装置ＩＤや送受信インターフェース情報、Ｎｅｘｔｈｏｐ情報やＱｏＳ情報といったパケット処理に関する情報が含まれる。

【００２７】

このように、カプセル化処理は、イーサネットフレームとしてのパケットＤ１を複製してペイロードの一部とし、付加情報もペイロードに加えて、宛先ＭＡＣアドレスＤＭＡＣをクライアントシステムＴ１からオフロード処理部１００に変更する処理である。このような処理は、レイヤ２のローカルエリアネットワークだけでなく、たとえば後述するレイヤ３のインターネット層といった他の層の通信やＭＰＬＳ通信といった他種の通信でも実現することができる。

【００２８】

図４は、変形例としてのレイヤ３のインターネット層に構成されたネットワークのカプセル化処理の内容を示す説明図である。図４には、抽出されたパケットＤ２（ＩＰパケット）にＩＰヘッダと付加情報とを付加してカプセル化されたカプセル化パケットＤ２ｃ（ＩＰパケット）とが示されている。カプセル化パケットＤ２ｃのＩＰヘッダには、宛先ＩＰアドレスＤＩＰとしてのオフロード処理部１００のＩＰアドレスと、送信元ＩＰアドレスＳＩＰとしてのスイッチＳＷ２のＩＰアドレスと、サービスタイプその他の他情報を含んでいる。カプセル化パケットＤ２ｃの付加情報は、カプセル化パケットＤ１ｃの付加情報と同様とすることができる。このようにしてカプセル化処理が完了すると、処理がステップＳ３００（図２）に進められる。

【００２９】

ステップＳ３００では、スイッチＳＷ２が備える転送処理部３５０（図１）は、パケットＤ１（図３）の転送に引き続き、カプセル化処理部３１２から受け取ったカプセル化パケットＤ１ｃを転送する。ただし、転送先は相互に相違する。すなわち、パケットＤ１は、クライアントシステムＴ１の宛先ＭＡＣアドレスＤＭＡＣがヘッダに含まれているので、回線Ｃ２＿３の接続されたポート（図示せず）に出力されてスイッチＳＷ３に転送されることになる。一方、カプセル化パケットＤ１ｃは、オフロード処理部１００の宛先ＭＡＣアドレスＤＭＡＣがヘッダに含まれているので、回線Ｃ３＿５の接続されたポート（図示せず）に出力されてスイッチＳＷ５に転送されることになる。

【００３０】

このようにして、スイッチＳＷ１における処理が完了し、スイッチＳＷ５を介してカプセル化パケットＤ１ｃがオフロード処理部１００に到達すると、処理がステップＳ４００に進められる。

【００３１】

ステップＳ４００では、オフロード処理部１００は、サンプル生成処理を実行する。サンプル生成処理とは、解析処理部２００におけるトラフィック解析に使用するためのサンプルデータを生成するための処理である。サンプルデータには、トラフィックの流れを表すフローサンプル（フロー統計）と、送受信カウンタエラーその他のインターフェースで発生するイベントを表すカウンタサンプル（インターフェース統計）とが含まれている。

【００３２】

図５は、オフロード処理部１００が生成するｓＦｌｏｗパケットＦ１の内容を示す説明図である。ｓＦｌｏｗパケットＦ１は、ｎ個のフローサンプルとｍ個のカウンタサンプルとにｓＦｌｏｗヘッダを付加したパケットとして構成されている。ｓＦｌｏｗヘッダには、ｓＦｌｏｗパケットＦ１に含まれるサンプル数やｓＦｌｏｗパケットＦ１の生成時刻、ＳＦｌｏｗエージェント３１０のＩＰアドレスやｓＦｌｏｗパケットのシーケンス番号といったデータが格納されるとともに、解析処理部２００の宛先ＭＡＣアドレスＤＭＡＣが含まれている。

【００３３】

ｎ個のフローサンプルの各々は、基本データ形式と拡張データ形式のデータにフローサ

ンプルヘッダが付加された構成とされている。フローサンプルヘッダは、フローサンプルのサンプリング間隔やインタフェースに到着したパケットの総数といた情報を格納している。基本データ形式のデータは、オリジナルのパケット長やサンプルしたパケットの内容といったトラフィックの流れを表すフローサンプルを格納している。拡張データ形式のデータは、スイッチ情報（ＶＬＡＮ情報など）やルータ情報（Ｌ３のＮｅｘｔＨｏｐなど）、ゲートウェイ情報（Ｌ３のＡＳ番号など）、ユーザ情報（ＴＡＣＡＣＳ／ＲＡＤＩＵＳ情報など）、ＵＲＬ情報といった情報を格納している。

【００３４】

ｍ個のカウンタサンプルの各々には、カウンタサンプル種別とカウンタサンプル情報とにカウンタサンプルヘッダが付加された構成とされている。カウンタサンプルヘッダは、カウンタサンプル発生源（特定のポート）を表すＳＮＭＰやカウンタサンプルの送信間隔といった情報を表すデータを格納している。カウンタサンプル種別のデータは、イーサネット統計やトークンリング統計といった種別を表すデータを格納している。カウンタサンプル情報は、種別毎の統計情報を表すデータが格納されている。

【００３５】

ステップＳ５００では、オフロード処理部１００は、このようにして生成されたｓＦｌｏｗパケットＦ１を回線Ｃ５＿ｏを介してスイッチＳＷ５に転送する。スイッチＳＷ５に転送されたｓＦｌｏｗパケットＦ１は、解析処理部２００の宛先ＭＡＣアドレスＤＭＡＣが含まれているので、スイッチＳＷ３を介して解析処理部２００に転送されることになる。

【００３６】

ステップＳ６００では、解析処理部２００は、ｓＦｌｏｗパケットを収集するとともに、収集されたｓＦｌｏｗパケットに基づいてトラフィック解析を実行し、たとえば解析結果をクライアントシステムＴ１に送信する。解析処理部２００は、図示しないディスプレイにトラフィック状況をグラフィカルに表示するように構成されていても良い。

【００３７】

このように、第１実施例では、負荷の大きなｓＦｌｏｗパケットの生成処理をスイッチＳＷ２からオフロードしているので、スイッチＳＷ２が担当する処理が抽出・複製・カプセル化と本来の機能である転送だけとなるので負担が顕著に軽減される。さらに、ネットワークの監視内容がネットワーク毎に相違し、詳細な解析から簡易な解析まで用途によって様々であり、さらに監視内容も時間とともに変動する場合もあるというスケーラビリティの要請に対して十分に応えるものとして構成されている。

【００３８】

Ｂ．本発明の第２実施例におけるトラフィック監視システム：

図６は、本発明の第２実施例におけるトラフィック監視システム１０ａの概要を示すブロック図である。第２実施例のトラフィック監視システム１０ａは、２台のオフロード処理部１００、１００ａを備えている点で第１実施例のトラフィック監視システムと相違する。

【００３９】

第２実施例のトラフィック監視システム１０ａでは、オフロード処理部１００が３つのスイッチＳＷ１、ＳＷ２、ＳＷ５からのカプセル化データの受信を担当し、オフロード処理部１００ａが２つのスイッチＳＷ３、ＳＷ４からのカプセル化データの受信を担当するように設定されている。

【００４０】

このように、第２実施例では、５つのスイッチＳＷ１～ＳＷ５の各々は、予め設定された２つのオフロード処理部１００、１００ａのいずれかにカプセル化データを転送するように割り当てられているので、オフロード処理の負担の変動に応じてオフロード処理装置の追加や削減を行うことによって柔軟に対応することができる。こうすれば、監視対象のスイッチやルータの数の増加に応じて、オフロード処理装置を増やしていくことができるので、最初からオフロード処理負担に十分に対応できるシステムよりも消費電力を軽減し

、かつ初期投資を小さくすることができるという利点もある。

【００４１】

Ｃ．変形例：

以上、本発明のいくつかの実施の形態について説明したが、本発明はこのような実施の形態になんら限定されるものではなく、その要旨を逸脱しない範囲内において種々なる態様での実施が可能である。たとえば、以下のような変形例が可能である。

【００４２】

Ｃ－１．上述の各実施例では、解析処理部２００がコレクタとアナライザの双方の処理を行っているが、たとえば別個の装置として構成するようにしても良い。

【００４３】

Ｃ－２．上述の各実施例では、サンプリング装置が転送装置の内部にＡＳＩＣその他の態様でハードウェア的に実装されているが、ソフトウェア的に実装することも可能である。ソフトウェア的な実装は、本願発明では、サンプリング処理の処理負担が小さいのでソフトウェア的に実装してもＣＰＵの負担が小さいという利点がある。加えて、転送装置が担当する抽出・複製・カプセル化の各処理のうち複製・カプセル化は、転送装置が転送処理で実行する処理なので、その機能を利用可能である。さらに、抽出処理も転送処理で行われる振り分け処理の拡張として対処可能である。このように、サンプリング処理のソフトウェア的な実装は、リソースの消費も少ないという特徴を有している。

【００４４】

このように、本願発明は、処理負担が大きくボトルネックとなる可能性があるとともに、転送装置の本来の処理とは本質的に相違する処理をオフロードするとともに、転送装置の本来の機能の流用や拡張で対処可能な処理であって、かつ、転送装置でのみ可能な抽出・複製・カプセル化といった処理を転送装置で実行させるという極めて合理的なシステムとして構成されている。さらに、本願発明は、転送装置へのソフトウェア的な実装も実用的なので、極めて実装性が高く広汎な用途に適用可能なシステムとして実現されている。

【００４５】

Ｃ－３．上述の各実施例では、トラフィック解析にｓＦｌｏｗ統計が使用されているが、たとえばｎｅｔＦｌｏｗ統計を使用するトラフィック解析にも適用することができる。本発明は、広く転送データ（パケット）を収集してトラフィック解析を行うトラフィック監視システムに適用することができる。

【図面の簡単な説明】

【００４６】

【図１】本発明の第１実施例におけるトラフィック監視システムの概要を示すブロック図。

【図２】第１実施例のトラフィック監視処理の内容を示すフローチャート。

【図３】レイヤ２のローカルエリアネットワークとして構成された第１実施例のカプセル化処理の内容を示す説明図。

【図４】変形例としてのレイヤ３のインターネット層に構成されたネットワークのカプセル化処理の内容を示す説明図。

【図５】オフロード処理部１００が生成するｓＦｌｏｗパケットＦ１の内容を示す説明図。

【図６】本発明の第２実施例におけるトラフィック監視システムの概要を示すブロック図。

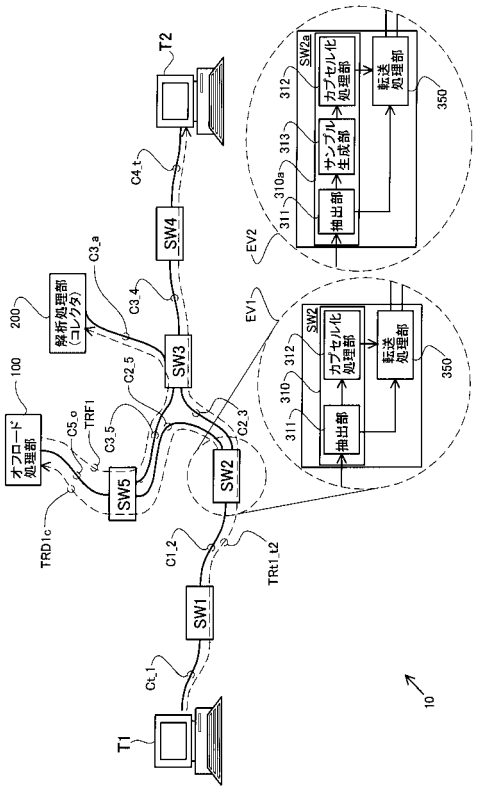
【符号の説明】

【００４７】

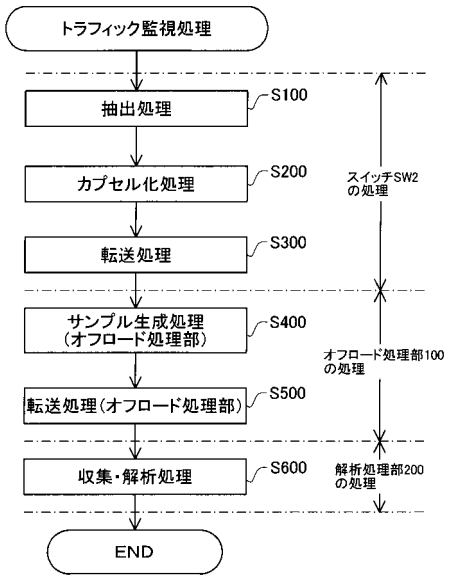
１０…ネットワーク
１００、１００ａ…オフロード処理部
２００…解析処理部
３１１…抽出部
３１２…カプセル化処理部

３１３…サンプル生成部
３５０…転送処理部
Ｔ１、Ｔ２…クライアントシステム

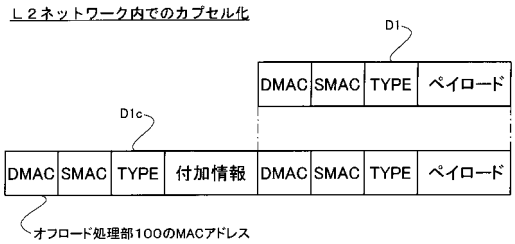
【図１】



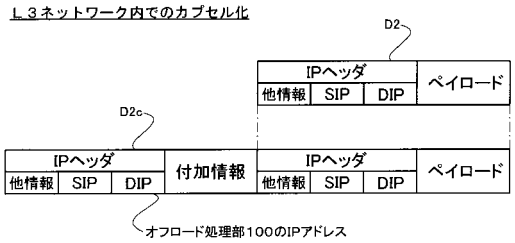
【図２】



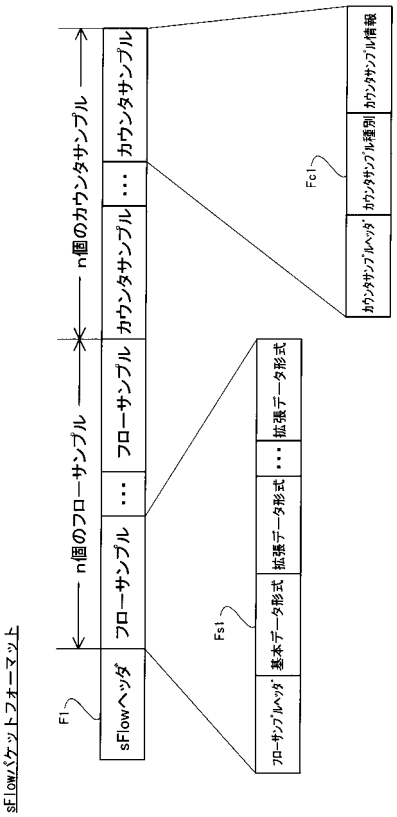
【図３】



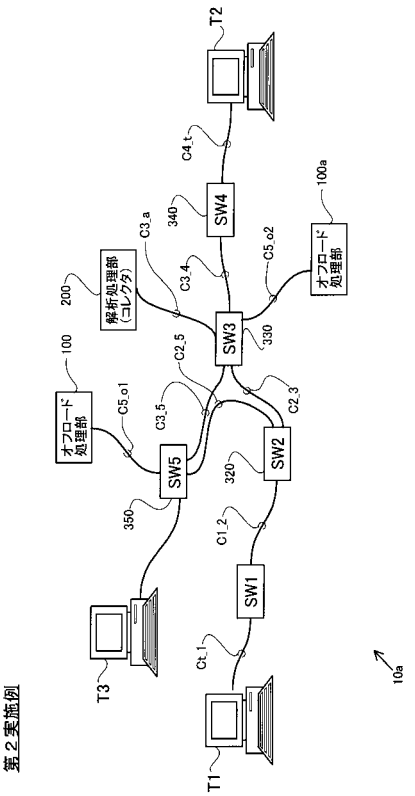
【図４】


L３ネットワーク内でのカプセル化
D2
IPヘッダ
他情報
SIP
DIP
ペイロード
D2c
付加情報
オフロード処理部100のIPアドレス

【図５】


sFlowパケットフォーマット上
n個のフローサンプル
n個のカウンタサンプル
sFlowヘッダ
フローサンプル
カウンタサンプル
F1
Fs1
Fc1
フローサンプルヘッダ
基本データ形式
拡張データ形式
カウンタサンプルヘッダ
カウンタサンプル種別
カウンタサンプル情報

【図６】


第２実施例
T1
T2
T3
SW1
SW2
SW3
SW4
SW5
オフロード処理部
解析処理部（コレクタ）
100
100a
200
320
330
340
350
C1_2
C2_3
C2_5
C3_4
C3_5
C3_a
C4_t
C5_o1
C5_o2
Ct_1
10a

フロントページの続き

(56)参考文献 特開２００７－０１３５９０（ＪＰ，Ａ）
特開２００６－００５４０２（ＪＰ，Ａ）
特開２００６－３５２８３１（ＪＰ，Ａ）
小林 淳史 Atsushi KOBAYASHI, フロー・メディエータを用いた大容量トラフィック・コレクタの設計 The Designing for Large-Scale Traffic Collector using Flow Mediator, 電子情報通信学会技術研究報告 Ｖｏｌ．１０７ Ｎｏ．３０ IEICE Technical Report, 日本, 社団法人電子情報通信学会 The Institute of Electronics,Information and Communication Engineers, ２００７年 5月 3日, 第107巻, pp.77-82

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ １２／５６