

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4910488号
(P4910488)

(45) 発行日 平成24年4月4日(2012.4.4)

(24) 登録日 平成24年1月27日(2012.1.27)

(51) Int.Cl. F I
H O 4 L 12/56 (2006.01) H O 4 L 12/56 4 O O Z

請求項の数 8 (全 23 頁)

(21) 出願番号	特願2006-155724 (P2006-155724)	(73) 特許権者	000005223 富士通株式会社
(22) 出願日	平成18年6月5日(2006.6.5)		神奈川県川崎市中原区上小田中4丁目1番1号
(65) 公開番号	特開2007-325154 (P2007-325154A)	(74) 代理人	100094514 弁理士 林 恒徳
(43) 公開日	平成19年12月13日(2007.12.13)	(74) 代理人	100094525 弁理士 土井 健二
審査請求日	平成21年3月9日(2009.3.9)	(72) 発明者	菊地 俊介 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
		(72) 発明者	野村 祐士 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

最終頁に続く

(54) 【発明の名称】 網の経路状態を調査する管理装置及びその網システム

(57) 【特許請求の範囲】

【請求項1】

網の経路状態を調査する管理装置において、
前記網からのトラフィックを受信するパケット送受信部と、
受信した前記トラフィックから、アドレス情報を抽出するアドレス抽出部と、
抽出された前記アドレス情報を送信先とするプローブパケットを生成するプローブパケット生成部とを備え、

前記パケット送受信部は、生成された前記プローブパケットを前記網に送信するとともに、前記プローブパケットに対するプローブ応答パケットを受信し、

前記プローブパケット生成部は、抽出された前記アドレス情報を送信先とする前記プローブパケットに対して予め設定されたホップ数分の前記プローブパケットを生成し、更に、前記プローブパケットごとに異なる識別子を前記プローブパケットに付加することを特徴とする管理装置。

【請求項2】

更に、前記プローブ応答パケットから経路情報を作成し、前記経路情報を保存する結果保存部を備えることを特徴する請求項1記載の管理装置。

【請求項3】

前記結果保存部は、保存した第1の経路情報と、新たに受信した前記プローブ応答パケットから作成した第2の経路情報とを比較することで、前記網に転送される前記トラフィックの経路の変動を検出することを特徴とする請求項2記載の管理装置。

10

20

【請求項 4】

前記ユーザトラフィック抽出部は、抽出した前記アドレス情報を保存し、新たに受信した前記トラフィックから抽出した前記アドレス情報と同一のときは、前記プローブパケット生成部に対し前記プローブパケットを生成させないようにすることを特徴とする請求項 1 記載の管理装置。

【請求項 5】

前記ユーザトラフィック抽出部は、保存した前記アドレス情報を一定時間経過後消去することを特徴とする請求項 4 記載の管理装置。

【請求項 6】

網の経路状態を調査する管理方法において、
前記網からのトラフィックを受信し、
受信した前記トラフィックから、アドレス情報を抽出し、
抽出された前記アドレス情報を送信先とするプローブパケットを生成し、
生成された前記プローブパケットを前記網に送信するとともに、前記プローブパケットに対するプローブ応答パケットを受信し、
前記プローブパケットを生成するとき、抽出された前記アドレス情報を送信先とする前記プローブパケットに対して予め設定されたホップ数分の前記プローブパケットを生成し、更に、前記プローブパケットごとに異なる識別子を前記プローブパケットに付加することを特徴とする管理方法。

10

【請求項 7】

網の経路状態を調査する管理プログラムにおいて、
前記網からのトラフィックを受信する処理と、
受信した前記トラフィックから、アドレス情報を抽出する処理と、
抽出された前記アドレス情報を送信先とするプローブパケットを生成する処理と、
生成された前記プローブパケットを前記網に送信するとともに、前記プローブパケットに対するプローブ応答パケットを受信する処理と、
をコンピュータに実行させ、
前記プローブパケットを生成する処理において、抽出された前記アドレス情報を送信先とする前記プローブパケットに対して予め設定されたホップ数分の前記プローブパケットを生成し、更に、前記プローブパケットごとに異なる識別子を前記プローブパケットに付加する処理を前記コンピュータに実行させることを特徴とする管理プログラム。

20

30

【請求項 8】

端末とサーバとが網を介して接続されるとともに、網の経路状態を調査する管理装置が前記網に接続された網システムにおいて、
前記管理装置には、
前記端末から前記サーバに転送されるトラフィックを受信するパケット送受信部と、
受信した前記トラフィックから、アドレス情報を抽出するアドレス抽出部と、
抽出された前記アドレス情報を送信先とするプローブパケットを生成するプローブパケット生成部とを備え、
前記パケット送受信部は、生成された前記プローブパケットを前記網に送信するとともに、前記プローブパケットに対するプローブ応答パケットを受信し、
前記プローブパケット生成部は、抽出された前記アドレス情報を送信先とする前記プローブパケットに対して予め設定されたホップ数分の前記プローブパケットを生成し、更に、前記プローブパケットごとに異なる識別子を前記プローブパケットに付加することを特徴とする網システム。

40

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、網の経路状態を調査する管理装置、及びその網システムに関する。詳しくは、網の経路状態が即時取得可能で経路変動も検出可能な管理装置等に関する。

50

【背景技術】

【0002】

従来から、網（又はネットワーク、以下「網」と称す）の経路状態を把握するコマンドとして、`traceroute`コマンドがある。

【0003】

`traceroute`コマンドの起動により、TTL（Time to Live：パケットの有効期限）を「1」から順に大きくしたパケットが宛て先アドレスに送出される。TTLの値に従い、当該コマンドを発行した端末から数えて1ホップ目、2ホップ目、・・・のネットワークノードは、有効期限エラーを示すパケットを返信する。宛て先アドレスの端末がこのパケットを返信するまで、TTLを順に大きくすることで、その間の経路が明らかになる。

10

【0004】

また、他の従来技術として、コマンド発行端末から経路トレースを示すフラグを付したフォーマット信号が送信され、各ノードは受信ポートのアドレス及び送出ポートのアドレスを付加して次のノードに送信し、付加累積された受信ポート及び送出ポートのアドレスの繋がりから送信経路をトレースするようにしたものがある（例えば、以下の特許文献1）。

【0005】

更に、送信されたフィルタ設定パケットから、経路に沿った動的パケットフィルタを設定し、このフィルタによって検出されたデータの収集により、ネットワーク内の実パケットを追跡することで、経路情報を取得するようにしたものも開示される（例えば、以下の特許文献2）。

20

【特許文献1】特開2000-244563号公報

【特許文献2】特開2005-312033号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかしながら、`traceroute`コマンドは、網オペレータ又はユーザ（以下、「網オペレータ等」と称す）が自ら端末を操作して発行させる必要がある。元来、当該コマンドは、網オペレータ等が何らかの方法で網の障害を認識した後で発行されるコマンドである。従って、障害発生時点で当該コマンドを発行した場合でなければ、障害発生時点での経路状態を取得することは困難である。

30

【0007】

また、`traceroute`コマンドの発行をスクリプト等により、ある程度自動化（例えば、一定時間）することも考えられる。しかし、同様に、障害が発生した時点でコマンドが発行されなければ障害発生時点での経路状態を取得することは困難である。

【0008】

更に、`traceroute`コマンドはその場限りのコマンドであり、当該コマンドの起動により発行される各パケットにおいて、その前後の結果を比較して経路変動を把握することはできない。従って、当該コマンドでは、経路が変動した場合でも、網オペレータ等に通知することができない。

40

【0009】

一方、特許文献1及び2に関しても、フォーマット信号やフィルタ設定パケットを網オペレータ等が端末の操作により自ら発行させる必要があり、障害発生時点での経路状態を取得することが困難である。

【0010】

そこで、本発明は、上記問題点に鑑みてなされたもので、その目的は、ユーザトラフィックに応じて網の経路状態を即時取得できる管理装置、管理方法、プログラム、及びその網システムを提供することにある。

【0011】

50

また、本発明の他の目的は、網の経路変動を検出できる管理装置等を提供することにある。

【課題を解決するための手段】

【0012】

上記目的を達成するために、本発明の一実施態様によれば、網の経路状態を調査する管理装置において、前記網からのトラフィックを受信するパケット送受信部と、受信した前記トラフィックから、アドレス情報を抽出するアドレス抽出部と、抽出された前記アドレス情報を送信先とするプローブパケットを生成するプローブパケット生成部とを備え、前記パケット送受信部は、生成された前記プローブパケットを前記網に送信するとともに、前記トラフィックが転送される前記網の経路に沿って送信された前記プローブパケットに対するプローブ応答パケットを受信することを特徴とする。

10

【0013】

また、本発明の他の実施態様によれば、前記管理装置において、更に、前記プローブ応答パケットから経路情報を作成し、前記経路情報を保存する結果保存部を備えることを特徴とする。

【0014】

更に、本発明の他の実施態様によれば、前記管理装置において、前記結果保存部は、保存した第1の経路情報と、新たに受信した前記プローブ応答パケットから作成した第2の経路情報とを比較することで、前記網に転送される前記トラフィックの経路の変動を検出することを特徴とする。

20

【0015】

更に、本発明の他の実施態様によれば、前記管理装置において、前記ユーザトラフィック抽出部は、抽出した前記アドレス情報を保存し、新たに受信した前記トラフィックから抽出した前記アドレス情報と同一のときは、前記プローブパケット生成部に対し前記プローブパケットを生成させないようにすることを特徴とする。

【0016】

更に、本発明の他の実施態様によれば、前記管理装置において、前記ユーザトラフィック抽出部は、保存した前記アドレス情報を一定時間経過後消去することを特徴とする。

【0017】

更に、本発明の他の実施態様によれば、前記管理装置において、前記パケット送受信部は、前記プローブ応答パケットを受信するとともに、前記網に転送されずループバック機能により前記プローブパケットを受信し、前記結果保存部は、前記プローブ応答パケットと、前記ループバック機能により受信した前記プローブパケットとから前記経路情報を作成することを特徴とする。

30

【0018】

更に、本発明の他の実施態様によれば、前記管理装置において、前記プローブパケット生成部は抽出された前記アドレス情報に対して予め設定されたホップ数分の前記プローブパケットを生成することを特徴とする。

【0019】

更に、本発明の他の実施態様によれば、前記管理装置において、前記プローブパケット生成部は前記プローブパケットごとに異なる識別子を生成された前記プローブパケットに付加することを特徴とする。

40

【0020】

更に、本発明の他の実施態様によれば、前記管理装置において、前記識別子は前記プローブパケットの送信先であるターゲットごとにユニークなシーケンス番号と、送信される前記プローブパケットのホップ数を示す値とを含むことを特徴とする。

【0021】

更に、本発明の他の実施態様によれば、前記管理装置において、前記結果保存部は前記シーケンス番号が同一の前記プローブ応答パケットを同一エントリ内にまとめて保存することを特徴とする。

50

【 0 0 2 2 】

更に、本発明の他の実施態様によれば、前記管理装置において、前記プローブ応答パケットには前記プローブパケットの送信された前記ターゲットのアドレス情報が含まれ、前記結果保存部には前記アドレス情報が前記エントリ内に含まれることを特徴とする。

【 0 0 2 3 】

また、上記目的を達成するために本発明の他の実施態様によれば、網の経路状態を調査する管理方法において、前記網からのトラフィックを受信し、受信した前記トラフィックから、アドレス情報を抽出し、抽出された前記アドレス情報を送信先とするプローブパケットを生成し、生成された前記プローブパケットを前記網に送信するとともに、前記トラフィックが転送される前記網の経路に沿って送信された前記プローブパケットに対するプローブ応答パケットを受信することを特徴とする。

10

【 0 0 2 4 】

更に、上記目的を達成するために本発明の他の実施態様によれば、網の経路状態を調査する管理プログラムにおいて、前記網からのトラフィックを受信する処理と、受信した前記トラフィックから、アドレス情報を抽出する処理と、抽出された前記アドレス情報を送信先とするプローブパケットを生成する処理と、生成された前記プローブパケットを前記網に送信するとともに、前記トラフィックが転送される前記網の経路に沿って送信された前記プローブパケットに対するプローブ応答パケットを受信する処理と、をコンピュータに実行させることを特徴とする。

【 0 0 2 5 】

更に、上記目的を達成するために本発明の他の実施態様によれば、端末とサーバとが網を介して接続されるとともに、網の経路状態を調査する管理装置が前記網に接続された網システムにおいて、前記管理装置には、前記端末から前記サーバに転送されるトラフィックを受信するパケット送受信部と、受信した前記トラフィックから、アドレス情報を抽出するアドレス抽出部と、抽出された前記アドレス情報を送信先とするプローブパケットを生成するプローブパケット生成部とを備え、前記パケット送受信部は、生成された前記プローブパケットを前記網に送信するとともに、前記トラフィックが転送される前記網の経路に沿って送信された前記プローブパケットに対するプローブ応答パケットを受信することを特徴とする。

20

【 発明の効果 】

30

【 0 0 2 6 】

本発明によれば、ユーザトラフィックに応じて網の経路状態を即時取得できる管理装置、管理方法、プログラム、及びその網システムを提供することができる。また、本発明によれば、網の経路変動を検出できる管理装置等を提供することができる。

【 発明を実施するための最良の形態 】

【 0 0 2 7 】

以下、図面を参照して本発明を実施するための最良の形態を説明する。

【 実施例 1 】

【 0 0 2 8 】

まず、実施例 1 について説明する。本実施例 1 は、網に転送されるトラフィック（又はパケットデータ）をキャプチャし、そのパケットと同じアドレスを持つプローブパケットを、トラフィックの転送と略同時に網に転送させて、その応答パケット等を保存する等により、経路状態を即時に取得することができるようにした例である。

40

【 0 0 2 9 】

図 1 は、実施例 1 において適用されるネットワークシステム（網システム）100の構成例を示す図である。ネットワークシステム100は、キャプチャ/プローブ端末（以下、「キャプチャ端末」と称す）1と、端末200と、サーバ400とから構成される。キャプチャ端末1等はIP（Internet Protocol）ネットワーク300を介して互いに接続される。

【 0 0 3 0 】

50

また、IPネットワーク300は、複数のノード310～370を有し、図1に示す経路により互いに接続される。

【0031】

図2は、キャプチャ端末1の構成例を示す図である。キャプチャ端末1は、パケット送受信部10と、ユーザトラフィック抽出部20と、プローブパケット生成部30、及びプローブ受信部40を備える。このキャプチャ端末1が、網の経路状態を調査する管理装置としての役割を果たす。

【0032】

パケット送受信部10は、パケット受信部11と、振り分け部12、及びパケット送信部13を備える。

【0033】

パケット受信部11は、端末200や各ノード310～370、サーバ400から送信されたパケットデータを受信する。

【0034】

振り分け部12は、パケット受信部11で受信したパケットが、ユーザトラフィックのパケットか、後述するプローブ応答パケット(或いはプローブパケット)か、を判別する。そして、振り分け部12は、ユーザトラフィックのパケットをユーザトラフィック抽出部20に、プローブ応答パケット等はプローブ受信部40に振り分ける(又は、廃棄する)。振り分けは、受信したパケットデータのプロトコルフィールドやポート番号を利用する。詳細は後述する。

【0035】

パケット送信部13は、プローブパケット生成部30で生成されたプローブパケットを、IPネットワーク300を介して、端末200や各ノード310～370、サーバ400に送信する。前述のプローブ応答パケットは、プローブパケットを受信した各ノード310～370等がキャプチャ端末1に対して送信するパケットである。

【0036】

ユーザトラフィック抽出部20は、アドレス抽出部21を備える。アドレス抽出部21は、ユーザトラフィックのパケットから、送信元アドレス(Srcアドレス)と、宛て先アドレス(Dstアドレス)とを抽出する。アドレス抽出部21は、抽出した送信元アドレス等をプローブパケット生成部30に出力する。

【0037】

プローブパケット生成部30は、パケット生成部31と、ターゲット定義テーブル32と、シーケンス値カウンタ33とを備える。

【0038】

パケット生成部31は、送信元アドレスと宛て先アドレスとから、プローブパケットを生成する。パケット生成部31は、ターゲット定義テーブル32を参照して、合致した送信元アドレス及び宛て先アドレスの組がある場合にプローブパケットを生成する。また、パケット生成部31は、シーケンス値カウンタ33を参照し、プローブパケットのシーケンス番号を演算し、プローブパケットの所定フィールドに格納する。詳細は後述する。パケット生成部31は、生成したプローブパケットをパケット送信部13に出力する。

【0039】

ターゲット定義テーブル32は、プローブパケットの送信を行うターゲットを定義するテーブルである。具体的には、ターゲット定義テーブル32には、ターゲット(プローブパケットの送信先)のアドレスが記憶される。

【0040】

シーケンス値カウンタ33は、シーケンス番号のベースとなる値を保持するカウンタである。シーケンス番号は、どのターゲット宛てのプローブパケットか、ターゲットの重複を識別するために、或いは、ターゲットが同じになるようなプローブパケットを送信するときにターゲットの重複を区別するために、プローブパケットに付与される番号である。詳細は後述する。

10

20

30

40

50

【 0 0 4 1 】

プローブ受信部 4 0 は、結果保存部 4 1 と、結果保存データベース (D B) 4 2 とを備える。

【 0 0 4 2 】

結果保存部 4 1 は、振り分け部 1 2 からのプローブパケットとプローブ応答パケットとを分類して結果保存 D B 4 2 に格納する。結果保存 D B 4 2 には、後述するように各パケットに基づくエントリが記憶され、調査した経路状態を把握することができる。

【 0 0 4 3 】

次に、キャプチャ端末 1 の動作について説明するが、その前に、まずユーザトラフィックのパケットである、 I P パケットの例について説明する。

10

【 0 0 4 4 】

図 3 (A) は、パケット受信部 1 1 で受信する I P パケット 5 0 0 の構成例を示す図である。 I P パケット 5 0 0 は、プロトコルを識別するためのデータが格納されるプロトコルフィールド 5 1 0 と、送信元と宛て先の夫々の I P アドレスが格納される送信元 I P アドレスフィールド 5 1 1 及び宛て先 I P アドレスフィールド 5 1 2 と、送信元と宛て先の夫々のポート番号が格納される送信元ポート番号フィールド 5 1 3 及び宛て先ポート番号フィールド 5 1 4 と、種々のデータが格納されるペイロード 5 1 5 とから構成される。

【 0 0 4 5 】

パケット送受信部 1 0 の振り分け部 1 2 では、パケットを振り分けることになるが、例として H T T P パケットをユーザトラフィックのパケットとした場合は以下のようになる。即ち、振り分け部 1 2 は、送信元ポート番号と宛て先ポート番号とを、受信した I P パケット 5 0 0 の該当フィールド 5 1 3、 5 1 4 から取り出す。そして、そのいずれかの番号が「 8 0 」又は「 8 0 8 0 」のとき、振り分け部 1 2 は受信したパケットが H T T P パケットであるとしてユーザトラフィック抽出部 2 0 に出力する。

20

【 0 0 4 6 】

なお、振り分け部 1 2 は、ユーザトラフィックのパケットを振り分けた後、引き続いてプローブパケット、プローブ応答パケットの振り分け処理を行う。即ち、受信した I P パケット 5 0 0 のプロトコルフィールド 5 1 0 を取り出し、それがプローブパケット又はプローブ応答パケット (I C M P パケット) であることを示すものであったとき、振り分け部 1 2 は受信したパケットがプローブパケット又はプローブ応答パケットであるとして

30

【 0 0 4 7 】

図 4 は、ユーザトラフィック抽出部 2 0 で実行されるアドレス抽出処理のフローチャートの例である。

【 0 0 4 8 】

まず、ユーザトラフィック抽出部 2 0 は、アドレス抽出機能を実行するための処理を開始すると (S 1 0)、振り分け部 1 2 から出力された H T T P パケットから、送信元アドレス (S r c アドレス) と宛て先アドレス (D s t アドレス) とを抽出する (S 1 1)。そして、抽出した各アドレスをプローブパケット生成部 3 0 のパケット生成部 3 1 に出力する (S 1 2)。そして、アドレス抽出機能の処理が終了する。

40

【 0 0 4 9 】

その後、プローブパケット生成部 3 0 において、抽出したアドレスに基づいて、プローブパケットの生成機能が実行される。図 5 は、そのフローチャートの例である。

【 0 0 5 0 】

尚、本実施例では、この機能が実行される前に、以下の処理が行われる。まず、オペレータ等は、ターゲット定義テーブル 3 2 にターゲットを記憶しておく。図 3 (B) は、ターゲット定義テーブル 3 2 の例である。同図に示すように、プローブパケットのターゲットとなるべき、サーバ 4 0 0 等のアドレスが記憶される。

【 0 0 5 1 】

また、オペレータ等はプローブパケットを送信するホップ数も予め設定しておく。例え

50

ば、キャプチャ端末1のメモリ等に記憶する。調査したいホップ数を設定するもので、網の規模等によって数も変動する。

【0052】

更に、オペレータ等は、シーケンス値カウンタ33を任意の値で初期化する。

【0053】

本実施例では、ターゲット定義テーブル32を「*」（すべてのターゲット、即ち、ノード310を通る全てのHTTPパケットを対象にする）、ホップ数を「5」、シーケンス値カウンタ33の初期値を「1」とする。

【0054】

図5に戻り、プローブパケット生成機能を実行するための処理が開始されると（S20）、パケット生成部31は、TTLカウンタ値を「0」にして初期化する（S21）。 10

【0055】

TTLカウンタ値とは、送信するプローブパケットのホップ数をカウントするための値である。予め設定されたホップ数分のプローブパケットの生成が終了すると、プローブ生成処理が終了する。

【0056】

次いで、パケット生成部31は、ターゲット定義テーブル32に記憶されたエントリを参照して、ユーザトラフィック抽出部20で抽出されたアドレスがターゲット定義テーブル32に存在するか否かを判断する（S22）。ターゲット定義テーブル32に存在しないと（S22で「ない」）、プローブパケット生成機能は終了する。 20

【0057】

一方、ターゲット定義テーブル32に抽出したアドレスが存在すれば（S22で「あり」）、パケット生成部31は、TTLカウンタ値を「+1」加算する（S23）。上記設定では、ターゲット定義テーブル32は「*」のため、抽出したアドレスが存在し、TTLカウンタ値が「1」となる。

【0058】

次いで、パケット生成部31は、実際にプローブパケットの生成処理（S24、S25）を行う。2つの処理により、それぞれ異なるプローブパケットが生成される。

【0059】

図6（A）及び（B）は、プローブパケットの例を示す図である。プローブパケット530は、送信元と宛て先のIPアドレスが夫々格納される送信元（Src）IPアドレス532及び宛て先（Dst）IPアドレスフィールド533と、シーケンス番号が格納されるシーケンス番号フィールド535と、TTLカウンタ値が格納されるTTLフィールド536とを有する。 30

【0060】

同図に示す例では、S24の処理により図6（A）に示すプローブパケットが生成され、S25の処理により図6（B）に示すプローブパケットが生成される。

【0061】

まず、S24の処理において、パケット生成部31は、ユーザトラフィック抽出部20により取得したHTTPパケットの宛て先アドレスを、プローブパケットの宛て先IPアドレスフィールド533に格納する。また、送信元IPアドレスフィールド532にキャプチャ端末1自身のIPアドレスを格納する。 40

【0062】

そして、シーケンス番号フィールド535に、「シーケンスカウンタ値×バイアス値（D）+TTLカウンタ値」を格納する。上記設定では、シーケンスカウンタ値は「1」、TTLカウンタ値はS23により「1」となる。また、バイアス値（D）は本実施例では「100」とすると、シーケンス番号は、 $1 \times 100 + 1 = 101$ となる。

【0063】

また、S25の処理において、パケット生成部31は、取得したパケットの送信元アドレスを、さらに別のプローブパケット530の宛て先IPアドレスフィールド533に格 50

納する。送信元IPアドレスフィールド532は、キャプチャ端末1自身のIPアドレスが格納される。

【0064】

そして、シーケンス番号フィールド535に、「シーケンス値カウンタ×バイアス値(S1)+バイアス値(S2)+TTLカウンタ値」を格納する。バイアス値(S1)を「100」、バイアス値(S2)を「50」とすると、シーケンス番号は、 $1 \times 100 + 50 + 1 = 151$ となる。

【0065】

次いで、パケット生成部31は、生成したプローブパケットをパケット送信部13に転送する(S26)。生成された2つのプローブパケットが網に送信されることになるが、一方のプローブパケットは、宛て先が「取得した宛て先アドレス」のため、HTTPパケットの送信先(例えば、サーバ400)に送信される。

10

【0066】

他方のプローブパケットは、宛て先が「取得した送信元アドレス」のため、HTTPパケットの送信元(例えば、端末200)に送信される。

【0067】

そして、設定したホップ数分(m回)繰り返したか否か判断する(S27)。上述の例では、ホップ数は「5」のため、上述の処理を5回繰り返すことになる。

【0068】

2回目の処理のときは、S23により、TTLカウンタ値が「2」となり、S24の処理により、シーケンス番号が $1 \times 100 + 2 = 102$ であるプローブパケットが生成される。また、3回目の処理のときは、シーケンス番号が $1 \times 100 + 3 = 103$ であるプローブパケットが生成される。このように、ユーザトラフィックのパケットの送信先(例えば、サーバ400)に送信されるプローブパケットのシーケンス番号は、パケットごとに夫々異なる番号を有することになる。

20

【0069】

一方、S25の処理により生成されるプローブパケットは、2回目の処理で、 $1 \times 100 + 50 + 2 = 152$ のシーケンス番号、3回目の処理で $1 \times 100 + 50 + 3 = 153$ のシーケンス番号を、夫々有することになる。このように、ユーザトラフィックのパケットの送信元(例えば、端末200)に送信されるプローブパケットもパケットごとに夫々異なる番号を有する。更に、サーバ400に送信されるプローブパケットと端末200に送信されるプローブパケットとも夫々異なる番号を有し、ユニークな番号となる。

30

【0070】

上述の例では、ホップ数は「5」(=m)のため、夫々「5」個の計「10」個のプローブパケットが生成される(夫々異なるシーケンス番号を有する)。

【0071】

図5に戻り、m回繰り返したとき(S27でYES)、パケット生成部31は、シーケンス値カウンタ33を「+1」加算する。この加算により、更に、キャプチャ端末1から送信されるプローブパケットのユニーク性が保証される。

【0072】

即ち、シーケンス値カウンタ33が「+1」加算され、更に別途HTTPパケットを受信すると、S24の処理により生成されるプローブパケットのシーケンス番号は「 $2 \times 100 + 1 = 201$ 」、2回目の処理では、「 $2 \times 100 + 2 = 202$ 」となる。最初の処理で生成されたプローブパケットの各シーケンス番号と比較しても、ユニークなものとなる。

40

【0073】

そして、パケット送信部13から、生成されたプローブパケットが送信される。図7(A)は、プローブパケットの構成例を示す図である。図6(A)等と同一部分には同一の符号を付している。

【0074】

50

このプローブパケット530を受けた各ノード310～370等は、プローブ応答パケットを生成してキャプチャ端末1に順次送信する。

【0075】

図7(B)は、プローブ応答パケット550の構成例を示す図である。全体の構成は、プローブパケット530と同様である。送信元IPアドレスフィールド552には、各ノード310～370等のIPアドレスが格納される。また、宛て先IPアドレスフィールド553には、キャプチャ端末1のIPアドレスが格納される。

【0076】

プローブパケットを送信後、しばらくすると、パケット受信部11は、プローブ応答パケットとプローブパケットを相次いで受信(又は、キャプチャ)する。

【0077】

ここでプローブパケットは、パケット送信部13からノード310～370等を介さずに直接パケット受信部11で受信される。これは、パケット送信部13やパケット受信部11がループバック機能を用いているからである。このようなループバック機能は、パケット受信部11等を構成するインターフェースが標準的に装備している。

【0078】

振り分け部12は、ループバック機能によるプローブパケット及びプローブ応答パケットと、ユーザトラフィックのパケットとを振り分ける。上述のように、パケットのプロトコルフィールドに格納された値により振り分ける。

【0079】

プローブ受信部40は、振り分けられたプローブパケットとプローブ応答パケットとに対して結果保存機能の処理を実行する。図8は、結果保存部41におけるフローチャートの例である。

【0080】

結果保存部41は、結果保存機能を実行するための処理を開始すると(S40)、パケット(プローブパケット又はプローブ応答パケット)からシーケンス番号を抽出し、シーケンス番号からシーケンスカウンタ値を逆算する(S41)。

【0081】

前述の例では、シーケンス番号の「100」の位を確認すれば判明できる。例えば、シーケンス番号が「101」のとき、シーケンス値カウンタは「1」、シーケンス番号が「203」のとき、シーケンス値カウンタは「2」とであると判明できる。

【0082】

次いで、結果保存部41は、シーケンス値カウンタと宛て先(Dst)アドレスとをキーにして、結果保存DB42に既存エントリが存在するか否かを判断する(S42)。

【0083】

これにより、受信したパケットが既に受信している途中の経路調査用のプローブパケット群の一部であるか、又は、新たに調査を始めた経路調査用のプローブパケットであるかを判別することができる。

【0084】

図9は、結果保存DB42の構成例である。1エントリは、プローブパケットに基づくサブエントリ421～425と、サブエントリ421～425の要素431～435とから構成される。各エントリ421～425等は、TTL順に並べられる。本フローチャートによりこの結果保存DB42が構築される。

【0085】

既に受信している途中の経路調査用のプローブパケットとは、結果保存DB42に、サブエントリ421～425のいずれかが存在している場合のパケットである。また、新たに調査を始めた経路調査用のプローブパケットとは、結果保存DB42に該当するサブエントリ421～425等が存在しない場合のパケットである。

【0086】

図8に戻り、受信したパケットが新たに調査を始めた経路調査用のプローブパケットの

10

20

30

40

50

とき（結果保存DB42に既存エントリが存在しないとき、S42で「エントリ存在しない」）、シーケンス値カウンタと、プローブパケットの宛て先アドレスをキーにして、結果保存DB42に新たにエントリを追加する（S46）。そして、結果保存機能の処理が終了する（S47）。

【0087】

一方、受信したプローブパケットが現在受信途中の経路調査用のプローブパケットのとき（結果保存DB42に既存エントリが存在するとき、S42で「エントリ存在する」）、結果保存部41は、受信したパケットがプローブパケットかプローブ応答パケットかを判別する（S43）。

【0088】

この判別は、図7（A）又は同図（B）に示すように、リクエスト又はレスポンスを示す値が格納されるフィールド554から判別できる。例えば、プローブパケットの場合、このフィールド554にリクエストを示す「0」、プローブ応答パケットの場合、このフィールド554にレスポンスを示す「1」が格納されているので、この値から判別する。

【0089】

プローブパケットのとき（S43で「プローブパケット」）、結果保存部41はシーケンス値カウンタと受信パケットの宛て先（Dst）アドレスをキーとして、結果保存DB42の該当するエントリに、TTL順にサブエントリを追加する（S48）。

【0090】

図9の例では、サブエントリ421～424に対して、更にサブエントリ425を追加する処理等が本処理（S48）に該当する。

【0091】

一方、プローブ応答パケットのとき（S43で「応答パケット」）、結果保存部41は、結果保存DB42に該当するサブエントリが存在しているため、TTLを参照して、該当するサブエントリに要素として自パケットの送信元（Src）アドレスを格納する（S44）。

【0092】

図9の例では、サブエントリ421に要素431として、プローブ応答パケットの送信元（Src）アドレスを格納する処理が本処理（S44）に該当する。そして、結果保存機能の一連の処理が終了する。

【0093】

結果保存部41は、プローブパケットやプローブ応答パケットを受信するごとに、上述の処理を行い、結果保存DB42を構築する。そして、最終的に構築された結果保存DB42では、プローブ応答パケットの送信元（Src）アドレスが順番に並べられている。この送信元アドレスは、プローブパケットを送信したノード310～370等のアドレスを示す。従って、結果保存DB42の順番に並べられた送信元アドレスが経路を示すことになり、その経路が結果保存DB42に蓄積される。

【0094】

図10は、本実施例1における効果を説明するための図である。端末200から、ユーザトラフィックのパケットを、ノード310、330、340を経由して、サーバ400に送信するとき、キャプチャ端末1は、ノード310を通過するパケットを受信（キャプチャ）する。

【0095】

そして、キャプチャ端末1は、キャプチャしたパケットから、そのパケットの送信先（又は送信元）を宛て先とするプローブパケットを生成して網に送信する。即ち、端末200からのユーザトラフィックのパケットと、プローブパケットとが略同時にノード310を経由して、順次同じ経路に伝送される。その後キャプチャ端末1は、プローブ応答パケットを受信することで、結果保存DB42に経路が蓄積される。

【0096】

従って、本実施例1では、経路状態をユーザトラフィックに応じて即時的に取得するこ

10

20

30

40

50

とが可能となる。また、キャプチャ端末 1 を操作する網オペレータがプローブパケットを生成するためのトリガとなる操作を別途行う必要がない。よって、経路状態を即時的に取得できるため、障害発生時点での経路状態も即時取得できる。

【 0 0 9 7 】

上述した例では、キャプチャ端末 1 を備えるネットワークシステム 1 0 0 の例で説明したが、例えば、ユーザが使用する端末 2 1 0 に、上述したキャプチャ端末 1 の機能を備えるようにしてもよい。図 1 1 は、そのような場合のネットワークシステム 1 0 0 の構成例を示す図である。

【 0 0 9 8 】

この場合、端末 2 1 0 は、網を流れる多数のユーザのトラフィックをキャプチャするのではなく、ユーザ自身が（端末 2 1 0 自身が）送受信するトラフィックを対象としてキャプチャする。

【 0 0 9 9 】

また、プローブパケットは、ユーザトラフィックの宛て先アドレスにのみ送信される。ユーザトラフィックの送信元アドレスは端末 2 1 0 のアドレスのため、例えば図 6 (B) のようなプローブパケットは生成されず、送信されない。

【 0 1 0 0 】

更に、結果保存 D B 4 2 に蓄積される経路情報は、ユーザがアクセスした先（ユーザトラフィックの宛て先アドレスを持つサーバ 4 0 0 など）に関するものとなる。

【 0 1 0 1 】

この場合でも、上述した例と同様に経路状態を即時取得可能で、障害発生時点での経路状態も取得可能である。

【 実施例 2 】

【 0 1 0 2 】

次に実施例 2 について説明する。本実施例 2 は、以前に保存した経路情報と、新たに抽出した経路情報とを比較し、変動があればその旨を網オペレータやユーザに通知するようにした例である。

【 0 1 0 3 】

図 1 2 は、本実施例 2 において適用されるキャプチャ端末 1 の構成例である。実施例 1 のキャプチャ端末 1 と同一の構成部分には同一の符号を付している。異なるのは、プローブ受信部 4 0 において、結果比較部 4 3 と差分データベース (D B) 4 4 とを更に備える点である。

【 0 1 0 4 】

結果保存部 4 1 により結果保存 D B 4 2 が構築されるまでは実施例 1 と同様である。結果保存機能の処理 (図 8) が終了した後、結果比較機能を実行するための処理が開示され、経路の変動が網オペレータやユーザに通知される。図 1 3 は、結果比較機能を実行するためのフローチャートの例である。

【 0 1 0 5 】

結果比較部 4 3 は、結果比較機能を実行するための処理を開始すると (S 5 0)、以前の結果比較処理でメモリに展開された結果 (後述) を差分 D B 4 4 に記録する (S 5 1) 。そして、結果保存機能の処理 (図 8) と同様に、結果保存部 4 1 は受信したパケット (プローブパケット又はプローブ応答パケット) に対してメモリに結果保存 D B 4 2 と同様のエントリの作成等を行う。メモリに記憶されたエントリは、その後、差分 D B 4 4 と比較することで経路の比較に用いられる。

【 0 1 0 6 】

次いで、結果比較部 4 3 は、パケットが最終応答パケットか否かを判断する (S 5 2) 。即ち、受信したパケット (プローブパケット又はプローブ応答パケット) が最終ホップ目の宛て先 (D s t) アドレスに対する応答パケットか否かを判断する。

【 0 1 0 7 】

これは、受信パケットの送信元アドレスが、差分 D B 4 4 のエントリにあるプローブパ

10

20

30

40

50

ケットの宛て先 (Dst) アドレスと同一か否かにより判断する。或いは、プローブパケットを受信した各ノード 310 ~ 370 等は、プローブパケットをプローブ応答パケットのペイロード 557 に格納しているため (図 7 (A) 及び同図 (B) 参照)、ペイロード 557 に格納されたプローブパケットの宛て先アドレスを参照して、差分 DB 44 のエントリと比較するようにしてもよい。又は、受信パケットの TTL フィールド 536、556 に格納された値が、例えば「5」(ホップ数として最初に設定した値)であれば、最終応答パケットと判断してもよい。

【0108】

受信したパケットが最終応答パケットではないとき (S52 で「最終応答パケットではない」)、結果比較処理は終了する (S56)。これは、最終パケットを受信するまでは、同一エントリ内のサブエントリや要素が全て構築されておらず、その後の処理で経路の比較を行うことができないからである。

10

【0109】

一方、受信パケットが最終応答パケットのとき (S52 で、「最終応答パケット」)、経路の比較作業を実際に行うことになる。まず、結果比較部 43 は差分 DB 44 を参照し、メモリに記憶されたエントリのうち宛て先 (Dst) アドレスと同一のエントリが差分 DB 44 に存在するか否かを判断する (S53)。過去に同一経路について経路の比較調査を行ったか否かを判断するためである。

【0110】

同じ宛て先 (Dst) アドレスのエントリが差分 DB 44 に存在しないとき (S53 で「存在しない」)、処理は終了する (S57)。その経路については始めて調査することになるため差分は抽出することはできないからである。

20

【0111】

一方、同じ宛て先 (Dst) アドレスのエントリが差分 DB 44 に存在するとき (S53 で「存在する」)、結果比較部 43 は、差分 DB 44 の内容 (エントリ内のシーケンス値カウンタや Src アドレス等) とメモリに記憶された内容を全て比較して、差分 DB 44 の内容が一致するか否かを判断する (S54)。

【0112】

一つでも内容が異なれば (S54 で「一致しない」)、結果比較部 43 は経路に差異が存在することになるため、変動があった旨を網オペレータ又はユーザに通知する (S58)。

30

【0113】

通知は、例えば、結果比較部 43 が変動があった旨をモニタ等の表示部に表示させるようにしてもよいし、メモリ等に発生時間とともに記憶してログを取るようにしてもよい。

【0114】

一方、差異がないとき (S54 で「一致する」)、又は差異があつて変動があった旨を通知した後、結果比較部 43 は差分 DB 44 の既存エントリを削除して終了する (S55)。この処理と、上述のメモリに展開された結果の差分 DB 44 への記録 (S51) により、常に、新しい結果が差分 DB 44 に保存されることになる。

【0115】

このように、本実施例 2 では、ある時点で突然経路の変動が生じた場合、差分 DB 44 の内容とメモリに記憶された内容とが一致なくなり、その旨が網オペレータやユーザに通知されるため、経路の変動を網オペレータ等が把握することができる。

40

【0116】

尚、結果比較機能の処理が実行される前までは、実施例 1 と同様の処理が実行されるため、本実施例 2 においても実施例 1 と同様の作用効果を奏する。

【0117】

上述した例において、結果比較部 43 は差分 DB 44 のすべての内容を比較するようにしたが (図 13 の S54)、例えば、比較対象をサブエントリの要素のみを比較するようにしてもよい。図 9 の例では、要素 431 ~ 435、451 のみ比較するようにしてもよ

50

い。差分DB44（結果保存DB42と同一の構成）のサブエントリ421～425、441～442、461は、経路が変動してもしなくても、その内容に変化はなく、経路に変動があったとき、プローブ応答パケットの送信元（Src）アドレスが変化するためである。この場合、結果比較部43は、すべての内容を比較していないため、その分処理を早くすることができる。勿論、上述した例と同様の作用効果も奏する。

【実施例3】

【0118】

次に実施例3について説明する。本実施例3は、重複したプローブパケットの送信を防止し、網に対する調査を低負荷で行い得るようにした例である。

【0119】

図2において、パケット生成部31は、アドレス抽出部21から抽出されたアドレスが入力される度にプローブパケットを生成することになる。以前に送信した同じアドレスに対して、プローブパケットを重複して生成し、網に送信することもある。

【0120】

そこで、本実施例3では、同じアドレスにプローブパケットを送信するような、重複したプローブパケットの送信を防止するようにしている。

【0121】

図14は、本実施例3におけるキャプチャ端末1の構成例を示す図である。実施例1（図2）と異なるのは、ユーザトラフィック抽出部20において、ユーザトラフィックテーブル22とタイムアウト部23とを備える点である。

【0122】

ユーザトラフィックテーブル22は、アドレス抽出部21により抽出された送信元（Src）アドレスと宛て先（Dst）アドレスとの組が記憶される。

【0123】

また、タイムアウト部23は、網オペレータ等により設定された時間が経過すると、ユーザトラフィックテーブル22に記憶されたエントリを削除する。

【0124】

図15は、重複プローブ防止機能を実行するための処理の動作を示すフローチャートの例である。タイムアウトの処理も付加されている。

【0125】

アドレス抽出部21は、アドレス抽出機能を実行する処理を開始すると（S60）、ユーザトラフィックの packets から送信元（Src）アドレスと、宛て先（Dst）アドレスとを抽出する（S61）。実施例1と同様である。

【0126】

次いで、アドレス抽出部21は、ユーザトラフィックテーブル22を参照して、アドレスの組によるエントリが存在するか否かを判断する（S62）。

【0127】

ユーザトラフィックテーブル22には、以前にプローブパケットを送信したアドレスの組が記憶されている。従って、アドレス抽出部21が、例えば、宛て先アドレスをキーにして検索し、マッチするアドレスが存在すれば以前にプローブパケットを送信したことを意味することになる。

【0128】

よって、ユーザトラフィックテーブル22にエントリが存在すれば（S62で「エントリ存在する」）、アドレス抽出部21はパケットを破棄して処理を終了させる（S63）。この場合、パケット生成部31に各アドレスが出力されないため、プローブパケットは生成されない。

【0129】

一方、ユーザトラフィックテーブル22にエントリが存在しなければ（S62で「エントリ存在しない」）、アドレス抽出部21は、ユーザトラフィックテーブル22に対して、送信元（Src）と宛て先（Dst）のアドレスの組である新たなエントリを作成する

10

20

30

40

50

(S64)。このとき、アドレス抽出部21は、テーブル22にエントリを作成した時間(タイムスタンプ)も同時に記憶する。

【0130】

そして、アドレス抽出部21は各アドレスをパケット生成部31に出力し、プローブパケットが生成される。その後の処理は実施例1と同様である。

【0131】

また、タイムアウト部23では、予め網オペレータ等が設定した時間(n分:例えば、メモリに記憶されたタイムアウト時間)から、エントリの「タイムスタンプ」が現在よりn分前か否かを判断する(S71)。つまり、タイムアウト部23は「タイムスタンプ」の時間から、「タイムアウト時間」経過したか否かを判断する。勿論、タイムアウト時間は「分」単位ではなく、「秒」単位でもよい。

10

【0132】

設定したタイムアウト時間経過したとき(S71で「はい」)、タイムアウト部23はユーザトラフィックテーブル22の該当エントリを削除する(S72)。これにより、ユーザトラフィックテーブル22のエントリが増大するのを防止できる。

【0133】

一方、決定したタイムアウト時間経過していないとき(S71で「いいえ」)、又は該当エントリ削除後、タイムアウト部23はテーブル22内の全エントリを走査し(S73)、常にタイムアウト時間経過したか否か調査することになる。

【0134】

20

一定時間経過してもパケットを網に送信し続けるトラフィックに対しては、エントリが削除された後、再度、エントリがテーブル22内に作成されるため、プローブパケットの送信は継続することができる。

【0135】

このように、本実施例3では、ユーザトラフィックテーブル22に同一のアドレスが記憶されていれば、プローブパケットが生成、送信されないため、重複したプローブパケットの送信を防止することができ、網に対して低負荷で実施例1と同様の調査を行うことができる。

【0136】

また、この際にユーザトラフィックテーブル22に対して一定時間経過後、該当エントリを削除してエントリの増大を防ぐとともに、一定時間経過しても通信が継続するトラフィックに対しては継続調査を行うこともできる。

30

【0137】

尚、本実施例3は、上述した実施例2においても実施可能であり、実施例2と同様の作用効果を奏する。

【0138】

以上まとめると付記のようになる。

【0139】

(付記1)

網の経路状態を調査する管理装置において、
前記網からのトラフィックを受信するパケット送受信部と、
受信した前記トラフィックから、アドレス情報を抽出するアドレス抽出部と、
抽出された前記アドレス情報を送信先とするプローブパケットを生成するプローブパケット生成部とを備え、

40

前記パケット送受信部は、生成された前記プローブパケットを前記網に送信するとともに、前記トラフィックが転送される前記網の経路に沿って送信された前記プローブパケットに対するプローブ応答パケットを受信することを特徴とする管理装置。

【0140】

(付記2)

更に、前記プローブ応答パケットから経路情報を作成し、前記経路情報を保存する結果

50

保存部を備えることを特徴する付記 1 記載の管理装置。

【 0 1 4 1 】

(付記 3)

前記結果保存部は、保存した第 1 の経路情報と、新たに受信した前記プローブ応答パケットから作成した第 2 の経路情報とを比較することで、前記網に転送される前記トラフィックの経路の変動を検出することを特徴とする付記 2 記載の管理装置。

【 0 1 4 2 】

(付記 4)

前記ユーザトラフィック抽出部は、抽出した前記アドレス情報を保存し、新たに受信した前記トラフィックから抽出した前記アドレス情報と同一のときは、前記プローブパケット生成部に対し前記プローブパケットを生成させないようにすることを特徴とする付記 1 記載の管理装置。

10

【 0 1 4 3 】

(付記 5)

前記ユーザトラフィック抽出部は、保存した前記アドレス情報を一定時間経過後消去することを特徴とする付記 4 記載の管理装置。

【 0 1 4 4 】

(付記 6)

前記パケット送受信部は、前記プローブ応答パケットを受信するとともに、前記網に転送されずループバック機能により前記プローブパケットを受信し、

20

前記結果保存部は、前記プローブ応答パケットと、前記ループバック機能により受信した前記プローブパケットとから前記経路情報を作成することを特徴とする付記 2 記載の管理装置。

【 0 1 4 5 】

(付記 7)

前記プローブパケット生成部は、抽出された前記アドレス情報に対して、予め設定されたホップ数分の前記プローブパケットを生成することを特徴とする付記 1 記載の管理装置。

【 0 1 4 6 】

(付記 8)

前記プローブパケット生成部は、前記プローブパケットごとに異なる識別子を、生成された前記プローブパケットに付加することを特徴とする付記 1 記載の管理装置。

30

【 0 1 4 7 】

(付記 9)

前記識別子は、前記プローブパケットの送信先であるターゲットごとにユニークなシーケンス番号と、送信される前記プローブパケットのホップ数を示す値とを含むことを特徴とする付記 8 記載の管理装置。

【 0 1 4 8 】

(付記 10)

前記結果保存部は、前記シーケンス番号が同一の前記プローブ応答パケットを同一エンタリ内にまとめて保存することを特徴とする付記 9 記載の管理装置。

40

【 0 1 4 9 】

(付記 11)

前記プローブ応答パケットには前記プローブパケットの送信された前記ターゲットのアドレス情報が含まれ、前記結果保存部には前記アドレス情報が前記エンタリ内に含まれることを特徴とする付記 10 記載の管理装置。

【 0 1 5 0 】

(付記 12)

網の経路状態を調査する管理方法において、
前記網からのトラフィックを受信し、

50

受信した前記トラフィックから、アドレス情報を抽出し、
抽出された前記アドレス情報を送信先とするプローブパケットを生成し、
生成された前記プローブパケットを前記網に送信するとともに、前記トラフィックが転送される前記網の経路に沿って送信された前記プローブパケットに対するプローブ応答パケットを受信することを特徴とする管理方法。

【0151】

(付記13)

網の経路状態を調査する管理プログラムにおいて、
前記網からのトラフィックを受信する処理と、
受信した前記トラフィックから、アドレス情報を抽出する処理と、
抽出された前記アドレス情報を送信先とするプローブパケットを生成する処理と、
生成された前記プローブパケットを前記網に送信するとともに、前記トラフィックが転送される前記網の経路に沿って送信された前記プローブパケットに対するプローブ応答パケットを受信する処理と、
をコンピュータに実行させることを特徴とする管理プログラム。

10

【0152】

(付記14)

端末とサーバとが網を介して接続されるとともに、網の経路状態を調査する管理装置が前記網に接続された網システムにおいて、
前記管理装置には、
前記端末から前記サーバに転送されるトラフィックを受信するパケット送受信部と、
受信した前記トラフィックから、アドレス情報を抽出するアドレス抽出部と、
抽出された前記アドレス情報を送信先とするプローブパケットを生成するプローブパケット生成部とを備え、
前記パケット送受信部は、生成された前記プローブパケットを前記網に送信するとともに、前記トラフィックが転送される前記網の経路に沿って送信された前記プローブパケットに対するプローブ応答パケットを受信することを特徴とする網システム。

20

【図面の簡単な説明】

【0153】

【図1】ネットワークシステムの構成例を示す図である。

30

【図2】キャプチャ/プローブ端末の構成例を示す図である。

【図3】図3(A)はIPパケットの構成例、同図(B)はターゲット定義テーブルの構成例を示す図である。

【図4】ユーザトラフィック抽出部における処理の動作を示すフローチャートの例である。

【図5】プローブパケット生成部における処理の動作を示すフローチャートの例である。

【図6】図6(A)及び(B)は、プローブパケットの例を示す図である。

【図7】図7(A)はプローブパケットの例、同図(B)はプローブ応答パケットの例を示す図である。

【図8】結果保存部における処理の動作を示すフローチャートの例である。

40

【図9】結果保存データベースの構成例を示す図である。

【図10】ネットワークシステムにおけるパケットの転送例を示す図である。

【図11】ネットワークシステムにおけるパケットの転送例を示す図である。

【図12】キャプチャ/プローブ端末の他の構成例を示す図である。

【図13】結果比較機能を実行するための処理の動作を示すフローチャートの例である。

【図14】キャプチャ/プローブ端末の他の構成例を示す図である。

【図15】重複プローブ防止機能を実行するための処理の動作を示すフローチャートの例である。

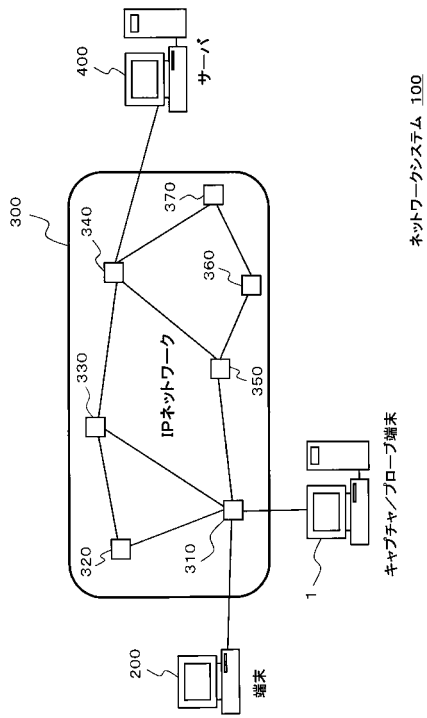
【符号の説明】

【0154】

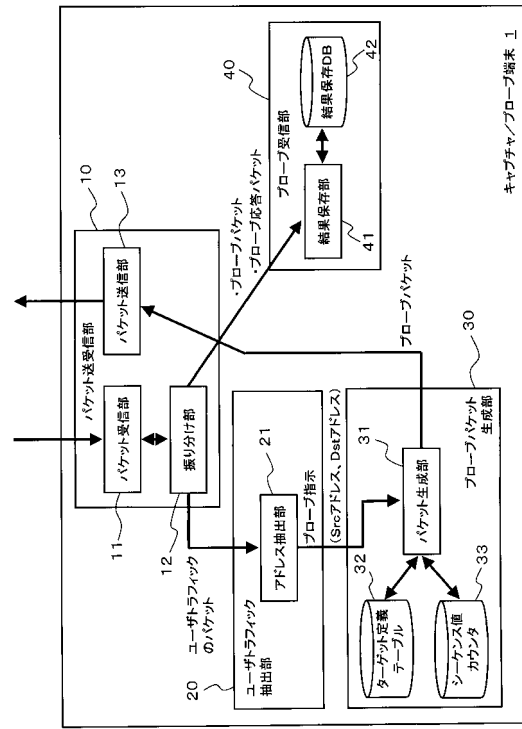
50

1	キャプチャ/プローブ端末	
1 0	パケット送受信部	
1 1	パケット受信部	
1 2	振り分け部	
1 3	パケット送信部	
2 0	ユーザトラフィック抽出部	
2 1	アドレス抽出部	
2 2	ユーザトラフィックテーブル	
2 3	タイムアウト部	
3 0	プローブパケット生成部	10
3 1	パケット生成部	
3 2	ターゲット定義テーブル	
3 3	シーケンス値カウンタ	
4 0	プローブ受信部	
4 1	結果保存部	
4 2	結果保存データベース(結果保存DB)	
4 3	結果比較部	
4 4	差分データベース(差分DB)	
2 0 0、2 1 0	端末	
3 0 0	IPネットワーク	20
3 1 0 ~ 3 7 0	ノード	
4 0 0	サーバ	
5 0 0	IPパケット	
5 3 0	プローブパケット	
5 5 0	プローブ応答パケット	
4 2 1 ~ 4 2 5、4 4 1 ~ 4 4 2、4 6 1	サブエントリ	
4 3 1 ~ 4 3 5、4 5 1	サブエントリの要素	

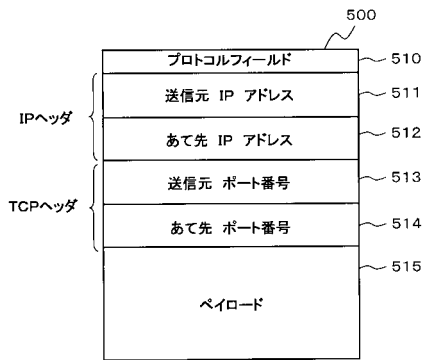
【図1】



【図2】



【図3】



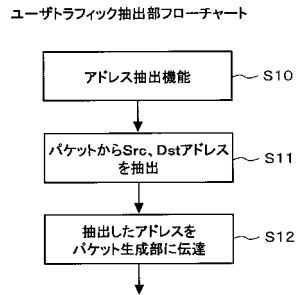
(A) IPパケットの構成例

送信元アドレス	宛て先アドレス
0.0.0.0/0	1.2.3.4
0.0.0.0/0	10.25.30.0/24
...	...

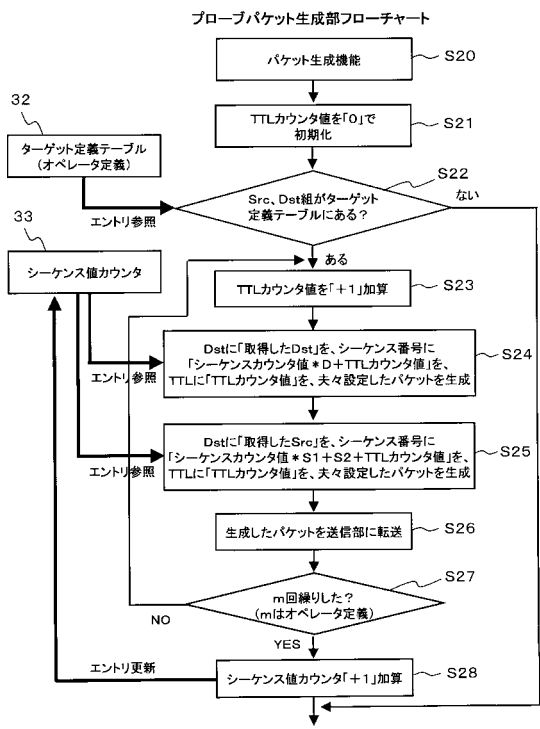
32

(B) ターゲット定義テーブルの例

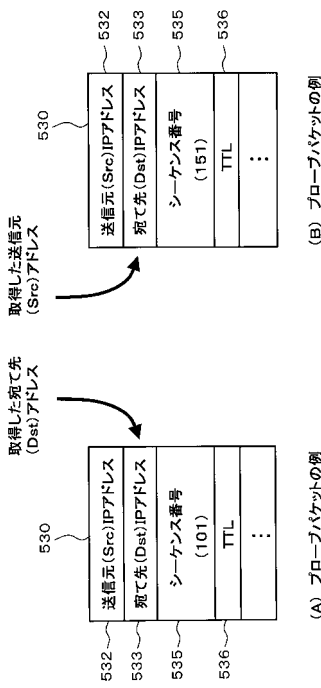
【図4】



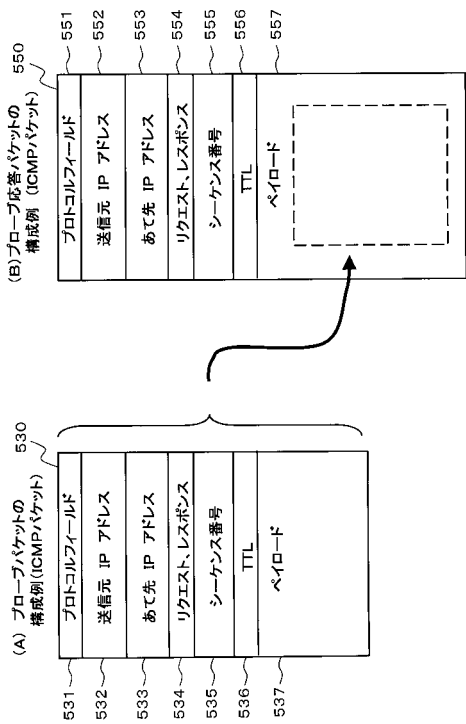
【図5】



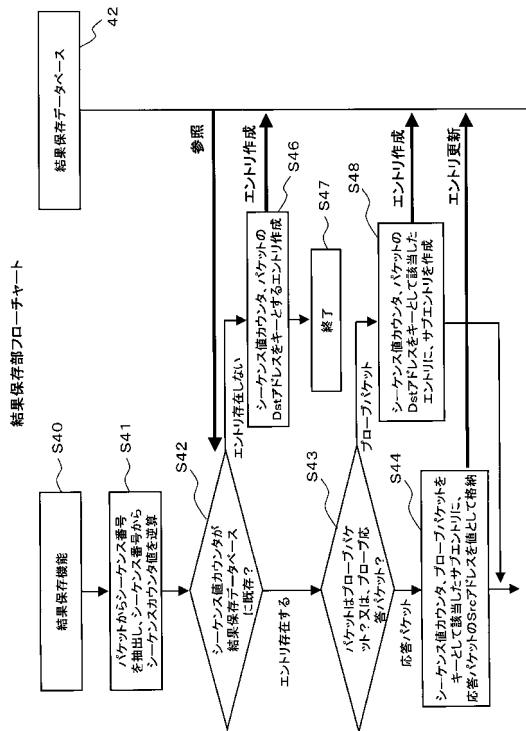
【図6】



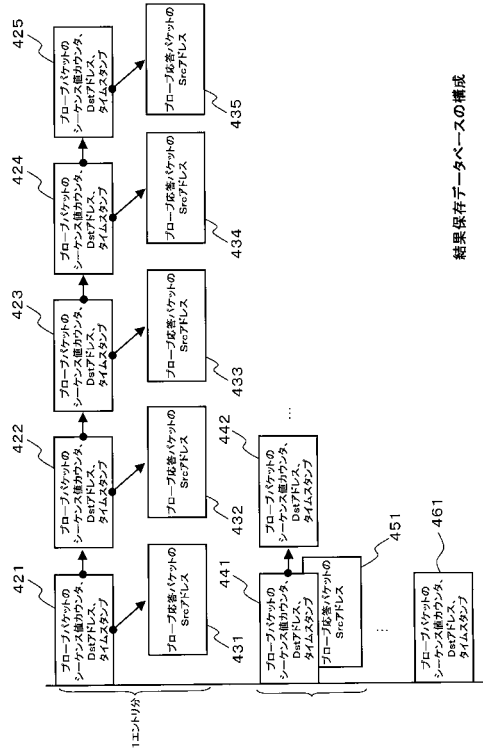
【図7】



【図8】

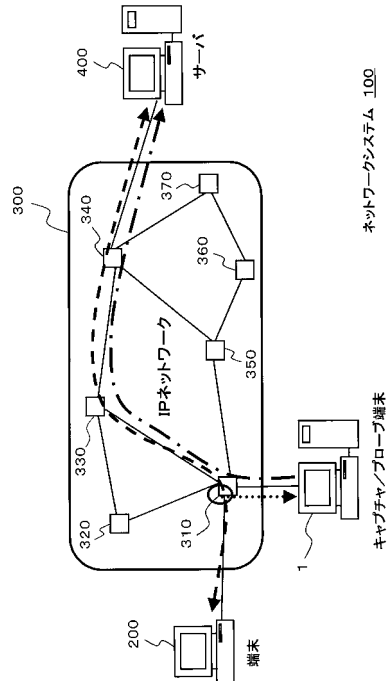


【 図 9 】



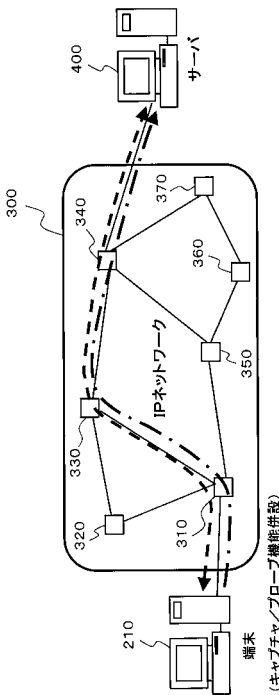
結果保存データベースの構成

【 図 10 】



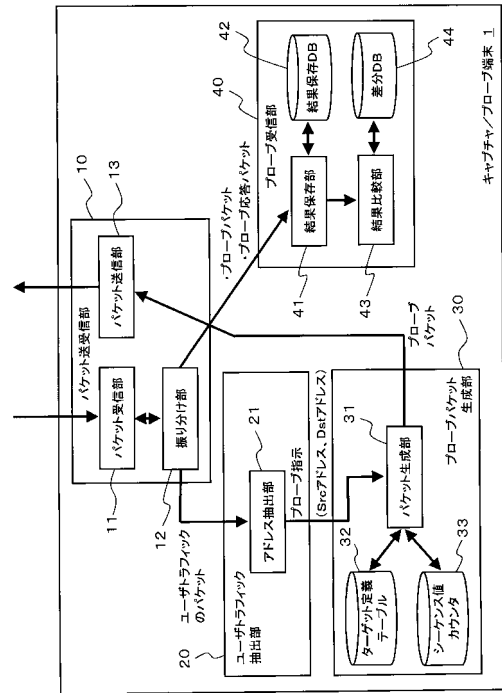
ネットワークシステム 100

【 図 11 】



ネットワークシステム 100

【 図 12 】



キャプチャ/プロローブ端末 1

フロントページの続き

審査官 吉田 隆之

(56)参考文献 特開2004-88747(JP,A)
特開2007-324642(JP,A)
信学技報 IN2001-54

(58)調査した分野(Int.Cl., DB名)
H04L 12