(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4464256号
(P4464256)

(45)発行日　平成22年5月19日(2010.5.19)　(24)登録日　平成22年2月26日(2010.2.26)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　400Z
H04L 12/46 (2006.01)　H04L 12/46　M

請求項の数 1　(全 13 頁)

(21)出願番号　特願2004-333825 (P2004-333825)
(22)出願日　平成16年11月18日 (2004.11.18)
(65)公開番号　特開2006-148376 (P2006-148376A)
(43)公開日　平成18年6月8日 (2006.6.8)
審査請求日　平成19年6月15日 (2007.6.15)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(72)発明者　三浦　健次郎
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

審査官　石田　紀之

最終頁に続く

(54)【発明の名称】ネットワーク上位監視装置

(57)【特許請求の範囲】
【請求項１】
クライアント端末からサーバまでの１つ以上のルータを経由する経路を示す経路情報であって、上記１つ以上のルータを示すリストを含む経路情報を記憶するネットワーク管理用データベースと、
上記クライアント端末からサーバまでの経路の変化を通知するメッセージと、経路の変化後に経由する１つ以上のルータを示すリストとを含む変化した経路情報を通信回線を介して受信するインターネットプロトコル（ＩＰ）通信ソフトウェア部と、
上記ＩＰ通信ソフトウェア部が受信した変化した経路情報が含む１つ以上のルータを示すリストから上記クライアント端末からサーバまでの経路の変化後に使用する経路使用数を求め、求めた経路使用数とあらかじめ記憶した所定の基準値とを比較して経路使用数が上記所定の基準値を超える場合、上記所定の基準値を超える上記変化した経路情報が含む１つ以上のルータを示すリストに基づく経路と、上記ネットワーク管理用データベースに記憶された経路情報が含む１つ以上のルータを示すリストに基づく経路とを表示装置に表示するデータ制御部と
を備えたことを特徴とするネットワーク上位監視装置。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、多数のサーバを多数の中継機器を経由して分散配置したネットワークにお

いて、サーバや中継機器の動作を効果的に監視する監視装置、監視システムに関するものである。

【背景技術】

【０００２】

データ通信ネットワークとして普及している、ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）ネットワークのネットワーク管理システムにおいては、管理の対象である複数のノードの障害（動作している、動作していない）を監視するために、各ノードに対して定期的なポーリングを行っている。その結果、ノードからの応答が得られなかったときは、時間を置いて何度かポーリングを行い、それでも応答が無いときは、ノードが停止していると判断し、表示画面上にそのノードの障害を示すようにしている。通常このポーリングはＩＣＭＰ（Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）の「エコー要求及びエコー応答」メッセージにより行うことが多い。ＩＣＭＰは必須プロトコルであるからである。

ＳＮＭＰ（Ｓｉｍｐｌｅ Ｎｅｔｗｏｒｋ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ）は、ＩＰネットワークを管理するプロトコルとして標準となっているプロトコルである。ＳＮＭＰではマネージャから管理対象内で動作するエージェントに管理情情報のＩＤ（ＭＩＢ－ＯＩＤ＋インスタンスＩＤ）を指定して監視対象内のエージェントソフトウェアに問い合わせる。エージェントは該当するＩＤに対応する値をマネージャに応答する。

ＳＮＭＰはその名の通り、プロトコルの仕様が簡素であることから実装が比較的容易であり、現在では広く普及している。上記ポーリングをＳＮＭＰ要求／応答により行う場合もある。

【０００３】

上記方式の一例として、以下の特許文献１の、「ネットワーク管理システムおよびデータ記憶媒体」がある。このシステムによれば、サーバからのポーリングへの応答が無かった時点で障害と判定できるが、サーバ自体に問題があるのか、途中の経路に問題があるのか、など真の障害部位が特定できないという課題を解決するとしている。そのため、稼働監視をしているターゲットからの応答がなかった場合に、監視装置とポーリング対象の接続構成データベースを検索し、監視装置から近い順に順次中継ノードに対しポーリングをかけ、最初に応答がなかった部分が障害障害であると推定する障害部位特定を行うというものである。

しかし、引用発明で想定する監視装置は、公開公報に添付された図面の記載から明らかなように、データセンターに設置された（集中）監視装置である。この場合監視装置とターゲットサーバ間のルートのチェックは可能であるが、データセンターからは途中にあり、ターゲットのクライアントは利用しない中継ノードが障害であるような場合は、利用者はサーバＡを使えているにもかかわらず、サーバＡが使えない（障害）と判断してしまう。これは単純な例であるが、実際のネットワークはもっと複雑であるため、上記の主旨を適用できるケースはさらに限定される。

【０００４】

第２の従来例として特許文献２に示される、「ネットワーク監視機構」においては、ポーリングする各インタフェースについて一次故障と二次故障を区別する手段を備えることにより、管理者に障害の根本原因を明確に提示することが提案されている。この方式によれば、一次故障と二次故障を区別するための手段として複数のネットワーク・インタフェースの各々に関する臨界ルート属性を設定し、接続状態や影響を分析しようとしている。分析用の情報収集手段としては、ＳＮＭＰのＭＩＢ、ＩＣＭＰ、ＩＰＸパケットなどが利用される。

しかしこの方式では、ネットワークの構成を間接的に把握するので、直ちに障害機器を特定はできない。

【０００５】

第３の従来例として特許文献３に示される、「ネットワーク監視システム及びネットワーク監視方法」においては、上記の中央監視装置からのポーリングまたは問合せと共に、

末端のサーバに並行して「監視プローブサーバ」を設けて、この監視プローブサーバからも担当機器に個別に問合せを行い、中央の監視サーバと監視プローブサーバとによる、それぞれの個別応答結果の組み合わせに基づいて故障機器を推定するシステムを提案している。

上記のシステムによれば、中央の監視サーバが監視プローブサーバからの個別応答結果を得て、中央監視サーバからの個別応答と突合わせて、初めて故障機器を推定ができる。しかし層間接続はこのように単一で単純な接続形態ばかりであるとは限らず、冗長度のある層間接続に対しては、必ずしも簡単に障害機器を特定出来るとは限らず、複数の並列機器に順次問合せを行うことは、多大の時間がかかって実用的でない。何よりもこのままではこの経路が使えなくなってしまう。

なおＳＮＭＰのプロトコルの一般的な解説については、例えば非特許文献１で述べられている。

【０００６】

従来のネットワーク監視では、利用者が十分な応答性能でネットワークアプリケーションを利用できているかどうかとういう視点での監視が十分ではなかった。これは、クライアント端末とサーバは同一のネットワークセグメントに設置されているということを前提とし、またＩＰプロトコルがベストエフォートサービスを前提としていたため、アプリケーションの多くは通信できれば（遅延が起こっても）動作するので、応答性能の監視は重要項目になりにくかったからである。

しかし、近年ネットワーク運用形態が変化し、ＩＰネットワーク上で利用されるアプリケーションも変化してきている。まず、通信事業者が提供するＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）回線の高速化・常時接続化が進展し、これに伴って各支店に設置していたサーバをデータセンターに集約することが多くなっている。すなわち、クライアント端末とサーバは、同一ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）内ではなく、常時接続ネットワークを介して離れた位置に設置される場合が多くなっている。このような運用形態においても、ネットワーク監視装置はデータセンター内に設置されることが多い。そしてデータセンター内の監視装置からサーバを監視しても、クライアントからサーバまでの経路が異なり、かつデーターセンター内は高速ＬＡＮで接続されていてＷＡＮ回線より高速なので、その応答速度は、クライアント端末からの応答速度と異なることが多い。

またＩＰネットワークが進展したことにより、ＩＰネットワーク上でＶｏＩＰ電話を初めとする応答性能に敏感なアプリケーションが利用され初めている。従ってネットワークの応答遅延や、応答速度の揺らぎがアプリケーションの使用感を大きく左右するものが増えつつあり、応答性能の監視が重要になっている。

更に、中継路では２重化技術、動的経路変更技術などにより、冗長化がすすんでいる。従来の監視方法のみでは、ネットワーク機器が故障した場合に、故障によりバックアップ経路に切り替わったかどうかの判断を簡単な方法で行うことは困難で一次故障による影響範囲も判断しにくいという問題があった。

【特許文献１】特開平１１－４２２３号公報

【特許文献２】特開平１１－１８４７８１号公報

【特許文献３】特開２００１－３５６９７２号公報

【非特許文献１】「シンプルブック　インターネット管理入門」Ｍ・Ｔ・Ｒｏｓｅ（プレンティスホール出版発行）発行１９９５年１２月１５日

【発明の開示】

【発明が解決しようとする課題】

【０００７】

従来の監視機構は上記のように構成されており、ある業務を成立させる（ある業務アプリケーションを正常に動作させる）のに必要な検査対象機器（サーバ、ルータ等）間の関連付けが弱いか、関連付けがあっても固定的にプログラムに組み込まれていた。このため、ある業務が停止した場合に、その原因を追及するためには、その業務に関連する（検査

対象）機器（複数の場合が多い）を、ネットワーク管理者が類推特定し、それに対する各障害検査手段を適用し、障害を追求していかなければならず、解析・復旧に時間がかかるという課題がある。上記第３の従来例も、同様の課題がある。そもそもこうしたシステムは多重化されていることが多く、１つの障害で全てが使用不可になるのではなく、複数の障害によりダウンすることが多い。こうした場合に１つの障害を早めに取り除くことでシステムの信頼性が向上する。しかし従来の障害検出方式では、こうした障害の度合いは、まして判らないという課題がある。

【０００８】

この発明は上記の課題を解決するためになされたもので、監視装置により、事前に各検査対象機器、特にサーバとクライアントの端末間を結ぶ複数のルートの接続状態を知り、またルータ等の特定中継経路機器の状態を知り、システムの稼動状態を把握して、重大障害を事前に予防することを目的とする。

【課題を解決するための手段】

【０００９】

この発明に係るネットワーク監視システムは、所定のサーバに接続する中継路グループを構成する各機器に対して経路問合せを行う経路問合せ部と、経路問合せに対する応答結果をモニタするネットワークモニタ部と、応答結果を経路情報として記憶するネットワーク管理用データベースと、を備えて、前に記憶している経路情報と上記応答結果の経路情報とが異なると、変化した経路情報を送信する下位監視装置と、

上記下位監視装置からの上記経路の変化情報を受信して記憶する上位ネットワーク管理用データベースと、複数の上記下位監視装置からの上記上位ネットワーク管理用データベースに記憶した変化した経路情報が所定の基準値を超えると、基準値を超えた経路の関連情報を出力するデータ制御部と、を備えた上位監視装置と、で構成される。

【発明の効果】

【００１０】

上記のようにこの発明によれば、エッジ（下位）監視装置が定期的にルート情報を監視し、ルートの変更があれば直ちに統合ネットワーク（上位）監視装置に通報し、ルート接続状態と障害情報とを併せ出力するようにしたので、重大障害を予防できる効果がある。

【発明を実施するための最良の形態】

【００１１】

実施の形態１．

実システムでは、冗長度のある機器構成と接続となっているので、単一の機器に障害が生じても、直ぐにはシステムに影響が現れず、しかしそれが進展すると重大障害となる事態が多々ある。ここでは、中央にあるサーバと末端にあるクライアントの端末間の、特に中継経路が多重化されているシステムについて、その状況を絶えず把握して、重大障害の可能性が生じた場合に直ちに障害部分を出力する形態を説明する。

図１は、本実施の形態における監視装置と監視対象グループとの接続関係を示すシステム構成図である。先ずシステムの構成を図１により説明する。図において、監視対象機器グループとしてこの場合には、エッジ監視装置からみたネットワークをクライアント端末近傍のクライアントネットワークグループ１、中継路グループ２、サーバグループ３の単位のグループとする。

各グループは更に、クライアントネットワークグループ１として複数のクライアント端末Ｃ　４ａと下位監視装置の一種としてのエッジ監視装置５ａ、及びルータＲｃ１ａ　１１、Ｒｃ２ａ　１２とで構成される。このようにルータまたはＩＰパケットルーティングをサポートするスイッチは冗長構成されていて、実アドレスに対して一つの仮想インタフェースが設定されている。組にしたアドレスには優先付けがされて仮想インターフェースにマッピングする優先度を定める（Ａｃｔｉｖｅ／Ｓｔａｎｄｂｙ）。通常、クライアント端末に設定するデフォルトゲートウェイには仮想アドレスを設定する。ＶＲＲＰ／ＨＳＲＰは仮想インタフェースに対する通信を正常動作している実インタフェースに対応させる役割をもつ。

また中継路グループ２として、異なる通信業者（ＩＳＰまたはＩｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）が提供するＷＡＮ等のネットワークＩＳＰ－１　２１、ＩＳＰ－２　２２、及びルータＲ１ａ　２３、Ｒ２ａ　２４、で構成される。サーバグループ３として、複数のサーバＳ１　６、Ｓ２　７とこれらを統合した仮想ホスト（ＶＲ－Ｓ）３２と、スイッチまたはルータＲｓ　３１及びエッジ監視装置５と協働してネットワーク全体の状況を監視・制御する上位監視装置の一種としての統合ネットワーク監視装置８とで構成される。

また中継路グループ２と、その上位のサーバグループ３では、ＲＩＰ（Ｒｏｕｔｉｎｇ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）またはＯＳＰＦ（Ｏｐｅｎ　Ｓｈｏｒｔｅｓｔ　Ｐａｔｈ　Ｆｉｒｓｔ）等で代表されるダイナミックルーティング技術により、機器の故障時に２重化された経路の代替経路に自動的に切換わるようにネットワーク設計されている。

【００１２】

図２は下位監視装置であるエッジ監視装置５ａ等（以下、５で代表）、及び上位監視装置である統合ネットワーク監視装置８のハードウェア構成を示す図であり、典型的にはシステムバス５１にＣＰＵ５３とメモリ例えばＲＡＭ５４と表示装置（ＤＩＳＰ）５２とキーボード等の入力インタフェース（Ｉ／Ｆ）５５と、ＬＡＮ１１と接続する通信Ｉ／Ｆ５６とハードディスク（ＨＤＤ）５７と、ＣＤやＦＤやフラッシュメモリ等の外部記憶装置群と接続する外部記憶装置Ｉ／Ｆ５８とが接続されている。

図３はエッジ監視装置５、及び統合ネットワーク監視装置８の、同じくソフトウェア構成を示す図であり、以下の各構成要素、例えば管理プロトコル制御部６１は、図２に示すＲＡＭ５４にプログラムとしてＨＤＤ５７等から読込まれて図３に記載する機能を持つ。各ソフトウェア構成要素として、ＩＣＭＰやＳＮＭＰやＴＥＬＮＥＴ等のプロトコルを管理する管理プロトコル制御部６１、通信回線等からのデータを制御し、また差異情報に基づいて統合ネットワーク監視装置８へ差異情報を送信するデータ制御部６２、それらのデータに基づいて管理用のデータベースを構成するネットワーク管理用データベース（ＤＢ）６３、モニタ結果も考慮して問合せ内容である構成・経路情報を作成・検索する構成・経路情報作成・検索（経路・機器問合せ）部６４と、応答結果をモニタするネットワークモニタ部６５と、性能計測部６６と、ローカルな通信回線（ＬＡＮ等）１１に接続するＩＰ通信ソフトウェア部６７とで構成される。なおデータ制御部６２は、統合ネットワーク監視装置８においては上位ネットワーク管理用データベース６３のデータと基準値６２ｂとに基づいてＤＩＳＰ５２に情報を出力する。

なお、サーバグループ３に近いエッジ監視装置ＥＭ、またはサーバＳが、他のエッジ監視装置ＥＭからクライアントネットワークグループの障害報告を受けて蓄積して、統合ネットワーク監視装置の役割を果たす場合は、その装置が上位監視装置になる。

同様に、端末Ｃ等が図２のハードウェア構成を持ち、図３の機能を持てば、その端末が下位監視装置となる。

【００１３】

また図４は、障害通知時に、対応して監視装置から各監視対象グループに対して送信される問い合わせ内容の一例を示す検査内容テーブルであり、図５は中継路グループにおける経路特定の問い合わせ、応答を説明するための経路説明図であり、図６は装置間のシーケンスを示す図であり、図７はエッジ監視装置５と、統合監視装置８が行う動作を示すフローチャートである。

これらの図を用いて動作を説明する。問い合わせテーブルを示す図４において、各グループに対して異なる問い合わせを行うために、個々の監視対象を１つのグループにまとめて管理する、それぞれシステムでユニークな名前を付けられたグループ名７１、グループの対象構成要素を抽出する式、例えばグループの構成要素を全てリストする方法や、ＳＱＬデータベースの検索式を指定するなどの対象抽出式の種別７２、対象抽出式の種別がＬＩＳＴなら要素名をあげ、ＳＱＬならその式を記載した対象抽出式７３、監視コマンド７４、及び監視コマンドに対応して発生させる発生イベント７４を規定しておく。中継路グ

ループ２に対する例では、＄ＥＭＩＤ、＄ＩＰ、@ＲＯＵＴＥ＿ＩＰ等は（予約）変数であり、エッジ監視装置のＩＤ（識別子）、対象となっているＩＰアドレス、ＩＰアドレスのリスト等が入る。

【００１４】

対象抽出式７３について補足する。対象抽出式は対象をいくつかのグループにまとめて監視したい場合に、監視の対象を特定するための式である。

具体的には対象抽出式種別７２で示されるように、監視対象を個別に指定してリストすることによりグループ化する方式（ＬＩＳＴ）、ＳＱＬ文によりデータベースから監視対象を抽出し、グループ化する方式（ＳＱＬ）の他、経路情報のような場合はエンドノードを指定しその経路上の中継機器（ルータ等）を自動検出しグループ化する方式（ＧＲＯＵＰＥＤ＿ＢＹ＿ＥＮＤＮＯＤＥ）などが考えられる。

また、発生イベント７５について補足すると、監視コマンドの結果ステータスやエッジ監視装置の出力（＄ＥＭ＿ＯＵＴＰＵＴ）等を使って、発生させるイベントを運用管理者が自由に変更することを可能なように実装することもできる。

【００１５】

エッジ監視装置５の構成・経路情報作成／検索（この場合は経路問合せ）部６４は、例えば定期的に中継路グループ（ＲＯＵＴＥ＿ＧＲＯＵＰ）２に対して問合せ動作を開始する。

経路問合せの方法としてＩＣＭＰ　ＴＩＭＥ　ＥＸＣＥＥＤエラーを応用して行う方法を経路説明の図５とシーケンスを示す図６により説明する。図６において、先ず端末Ｃに代わってエッジ監視装置ＥＭの構成・経路情報作成／検索部６４はステップＳ８１で、宛先アドレスをサーバＳ（インタフェースＩ１）、送信元アドレスをＥＭ（Ｉ１）、ＩＣＭＰヘッダーのＴＴＬ（Ｔｉｍｅ　Ｔｏ　Ｌｉｖｅ）値を初期値（＝１）にしてサーバＳ宛にパケットを送信する。このパケットは送信元であるエッジ監視装置ＥＭのメモリ上にあるルーティング情報に基づいて最初のルータＲｃ（Ｉ１）に到達する。ルータＲｃ（Ｉ１）は最終的な宛先アドレス（サーバＳ（Ｉ１））ではないため、ルータＲｃは次のルータに転送する準備を行う。ここでＴＴＬ値はルータを経由する際に１減らされるため、ルータＲｃでＴＴＬは１減らされ０となる。

ＴＴＬ値が０になるとＳ８２で、ルータＲｃはＩＣＭＰ　ＴＩＭＥ－ＥＸＣＥＥＤエラーを送信元アドレスにあるエッジ監視装置ＥＭに返信して終了する（転送しなくなる）。

エッジ監視装置ＥＭのネットワークモニタ部６５はルータＲｃからＩＣＭＰ　ＴＩＭＥ－ＥＸＣＥＥＤエラーを受信するが、エラーパケット内にはエラーを返したルータＲｃ（Ｉ１）のＩＰアドレスが入っているため、これを調べることでエッジ監視装置ＥＭからのホップ数（経由するルータの数）１のルータ（最も近いルータ）はルータＲｃ（Ｉ１）であると判別できる。これをＳ８１の開始時刻と共にネットワーク管理用データベース（ＤＢ）６３に記録する。

【００１６】

次にエッジ監視装置ＥＭの構成・経路情報作成／検索部６４はネットワークモニタ部６５からの通知を受けてＳ８１と同様に、宛先アドレスをルータＳ１（Ｉ１）、送信元アドレスをエッジ監視装置ＥＭ（Ｉ１）、ＩＣＭＰヘッダーのＴＴＬ値を前回設定した値（初期値）に１加えた値（２）に設定してＳ８３でパケットを送信する。

このパケットはルータＲｃ－Ｉ１で受信され、ＴＴＬ値が１減らされる。ルータＲｃは内部に保持しているルーティング情報を検索し、サーバＳに到達するための次のルータＲ１（Ｉ１）に同じＳ８３でパケットを転送する。

このパケットを受信したルータＲ１でも、ルータＲｃが行ったと同様なＴＴＬ減算処理を行う。すると、ルータＲ１でＴＴＬ値が０となり、ルータＲ１からＩＣＭＰ　ＴＩＭＥ－ＥＸＣＥＥＤエラーがＳ８４でエッジ監視装置ＥＭに送信される。

エッジ監視装置ＥＭではこの受信により、ＴＴＬ値２（すなわちホップ数２）のルータはルータＲ１（Ｉ１）であることがわかるので、これをＳ８１の開始時刻と共にデータベースに記録する。

次にエッジ監視装置ＥＭはＴＴＬ値を３にしてＳ８５のように上記の手順を繰り返すと、ホップ数３のルータＲｓ（Ｉ１）がわかるので、これを開始時刻とともにデータベースに記録する。

この手順をパケットがＳ８５以降もサーバＳに到達できるまで繰り返し、やがてＳ８６でサーバＳに到達し、レスポンスＳ８７を得る。

【００１７】

こうして最終的には図５の経路Ｉ１の場合は、エッジ監視装置ＥＭ→ルータＲｃ（Ｉ１）→ルータＲ１（Ｉ１）→ルータＲｓ（Ｉ１）→サーバＳ（Ｉ１）と経路を確定することができる。

こうして図７で経路問い合わせ動作Ｓ９１とネットワークモニタＳ９２とを繰り返してサーバＳまでの経路情報が蓄積されてＳ９３でネットワーク管理用ＤＢ６３に記憶されると、この経路情報はＳ９４で統合ネットワーク監視装置Ｍ８に送信される。

統合ネットワーク監視装置８は、あるトリガ、例えば定期的にエッジ監視装置からの経路情報を収集する。勿論Ｓ９４で記載のように、エッジ監視装置５が経路の変化を検出すると、その変化した経路情報を送信してくる。そして中継路のルータまたはスイッチ毎に所定の基準値６２ｂを設定しておき、後で述べるようにそれに基いてＤＩＳＰ５２にその超えたルータとその経路情報群を表示する。

一方、統合ネットワーク監視装置Ｍは、その構成・経路情報作成／検索（この場合は機器問合せ）部６４により、従来の方式によりルータの各インタフェース（Ｒｓ（Ｉ１～Ｉ４）、Ｒ１（Ｉ１～Ｉ２）、Ｒ２（Ｉ１～Ｉ２）、Ｒｃ（Ｉ１～Ｉ３）にポーリングをかけることにより、障害を検出しているものとする。

【００１８】

ここでルータＲ１が停止（またはルータＲ１のインタフェースＩ１が停止でもよい）すると、ルータＲ１を経由していたエッジ監視装置ＥＭまたは端末Ｃからサーバへの通信が一時的に途絶える。しかし、ＯＳＰＦ等のダイナミックルーティングプロトコルにより、システムとしては自動的にルートが切換わって、ルータＲｃ（Ｉ３）からルータＲ２（Ｉ１）に転送されるようになる。

なお統合ネットワーク監視装置Ｍからルータ１の故障は検出できるが、利用者端末Ｃからサーバに通信ができているかどうの判定は難しい。これを推定するアルゴリズムも幾つか提案されているが、制限付きの場合が多く、全てのネットワークに適用はできない。即ち、実際にはネットワークの冗長化は全ての部分で行われ、１つの中継ノードに接続する回線ももっと多いので複雑化であり、推定が難しい。従ってエッジ監視装置ＥＭからの現在生きている経路情報が非常に重要である。

エッジ監視装置ＥＭは各支店（クライアント）側に設置されており、各エッジ監視装置ＥＭ（ｎ）は端末Ｃ（ｎ）の代わりに定期的に経路探索を行っており、上記で説明した経路問合せにより、例えばルータＲｃからルータＲ２に転送されたＳ８３’に対するルータＲ２からのエラー応答Ｓ８４’により経路が変わったことを検知する。サーバＳに到達するまでに経由するルータが全て判明したら、エッジ監視装置ＥＭは最終的に得た経路の変化を統合ネットワーク監視装置Ｍに、到達確認を行わない通知型のプロトコルであるＳＮＭＰ－ＴＲＡＰ、応答確認型のプロトコルであるＳＮＭＰ－ＩＮＦＯＲＭ－ＲＥＱＵＥＳＴ）またはＸＭＬ形式の情報に変換してＨＴＴＰプロトコル等で送信する。ＴＲＡＰで送信するデータとしては、例えば、ルートが変化した旨のメッセージ、エッジ監視装置ＥＭ５のＩＤ及びＩＰアドレス、宛先のＩＰアドレス、経由するルータのＩＰリスト（ホップ数１から順に）を、先に述べた図７のＳ９４で送信する。

対応して統合ネットワーク監視装置８は、Ｓ９６で各エッジ監視装置５からの経路情報を受けて、これらの経路情報をネットワーク管理用ＤＢ６３に記憶する。

【００１９】

統合ネットワーク監視装置Ｍ８では、個別ポーリング監視方法等によりルータＲ１の故障を検出しているとする。即ちその構成・経路情報作成／検索部６４は、図７のＳ９７で機器問合せを行っている。この状態で更に、エッジ監視装置ＥＭ（ｎ）からステップＳ９

６の変化した経路情報を受けることで、端末Ｃ（ｎ）とサーバＳとの経路は変更されたが、通信はできていると判断できる。言い換えれば、経路中に縮退動作をしている中継ノードがあることを表している。なお、このＳ９６とＳ９７のステップは、どちらを先に行ってもよいし、Ｓ９７は常に行うようにしなくてもよい。

この切換えが一つの支店（クライアントネットワークグループ）からの経路であればまだ余裕があるかも知れないが、幹線経路を多数の支店が共用していて、冗長ルータの一部が故障している状態（縮退運転状態）であると、現状では各支店からサーバに通信は出来ていても、次に重大障害が発生する可能性を持っている。そこでＳ９８において統合ネットワーク監視装置８のデータ制御部６２は、各支店とサーバ間で行われている支所からの通信経路毎の経路使用数を加算して、支店から使用する経路数が基準値６２ｂより多くなる経路があると、その支店からの経路数が多くなった経路またはルータを画面上線路の色を変えるなどしてその影響・状況を表示することができる。図７でエンドからスタートへ戻るループは、問合せ等の動作が定期的に繰返されることを意味している。

例えば図１において、ルータＲ１ａに障害が発生して、それまで太い実線で示される経路で通信を行っていた支店端末４ａ（即ち、ＥＭ５ａ）が点線経路のルータＲ２ａ経路に変ると、ルータＲ２ａとルータＲｓ間の経路数は２になる。そして基準値が２であると、この経路をアラーム表示する。同時に支店端末４ｂからルータＲ１ａ経由の太い実線経路も、ルータＲ１ｂ経由の点線経路に変り、変更前経路を点滅させ、または変更後経路を別色の実線表示で表示する、等の注意表示を行う。これによりルータＲ１ａ　２３に障害が生じていることが推定でき、構成・経路情報作成／検索部６４での、それまで使用されていたルータが代替された情報によりそのルータに対する検索を行うプログラムにより図７のＳ９７で、ルータＲ１ａ　２３にポーリングをかけて、時間を置かずルータＲ１ａの機器障害を確認できる。そして基準値６２ｂ以上に支店が集中して使用する経路があって、同時にその近辺で障害がある機器があると、その機器は早急に復旧が必要であると判る。

【００２０】

なお必要があれば支店の重要度（大規模店など）に応じて支店毎の経路に重み付けして、重み付け係数付きで経路数を加算して加算合計経路数を得るようにしてもよい。

こうして表示形式や表示色の変化で重大障害の発生可能性を出力し、障害機器の早期置き換えの必要性が迅速かつ容易にわかる。

また、統合ネットワー監視装置８において、宛先サーバ毎に、関連する各中継機器を、各中継機器の（重み付け係数付き経路数を加算した）加算合計経路数に基づいてソートし、昇順（重要度順）にならべて表示すること（ＴｏｐＮ表示）で、ネットワーク上で重要な中継機器を俯瞰的に把握することができるネットワーク運用管理上の効果がある。

さらに、別途収集可能な各中継機器の冗長度設定情報を加えて表示することもできる。こうすることで経路上重要な中継器とその冗長度がわかり、重要な中継機器に対するバックアップ設定ができているかどうかを確認することもできる。

【００２１】

本ケースはルータＲ１の全面障害の場合で説明したが、ルータＲ（ｎ）のバグや設定ミスによって、経路が不安定になり、経路のフラッピング（一定周期で経路が切り替わる）などの現象が生じる場合がある。このような現象は従来のポーリング手法では検出が難しく（経路フラップの場合は統合ネットワーク監視装置Ｍ８からのポーリングには、リトライによって応答してしまう場合が多い）、上記の手順によるルート検出情報を統合ネットワーク監視装置へ上げるシステム・方法が有効である。即ち途中の機器の応答が不安定である場合でも、上記したように各エッジ監視装置５からの経路情報を収集して、統合的な経路上の機器の動作を把握できる。

上記図５と図６による経路検索は、ＩＣＭＰ　ＴＩＭＥ　ＥＸＣＥＥＤエラーによる方法であった。これをＳＮＭＰで行うことも出来る。

即ち各ルータのＳＮＭＰ　ＭＩＢを調査し、各ルータのｉｐ　Ｒｏｕｔｅ　Ｄｅｓｔ，ｉｐ　Ｒｏｕｔｅ　ＩＦ　Ｉｎｄｅｘ，ｉｐ　Ｒｏｕｔｅ　ＮｅｘｔＨｏｐ　ＭＩＢ（ＲＦＣ１２１３）を順次読みとり、これを監視装置の構成データベースに反映させることで

経路を特定する方法もある。しかしこの方法は、ルータでＳＮＭＰエージェントモジュールが動作していなかったり、適切なアクセス権限（コミュニティパスワード）がないと適用できない等の制約があり、ＩＣＭＰ方式の方が好ましい。

なおシステムによっては、現用系から予備系への切換わりに時間がかかり場合があり、アプリケーションによってはこの予備系への移行時間内にタイムアウトとなって、見かけ上は不具合に見えることもある。しかし上記の構成と動作によると、統合ネットワーク監視装置８が出力する経路情報と故障機器とを見れば、アプリケーションの不具合か、経路変更または機器の不具合かが判定できる。

【００２２】

実施の形態２．

上記の実施の形態では、ルート情報に変更があった場合に統合ネットワーク監視装置で複数のエッジ監視装置からのルート情報と、それらに基づく障害機器とを出力してシステム上の重大障害予防を行う動作を説明した。ここではルート情報に変更が無くて、システムの応答が悪くなった場合に障害部分を推測する構成と動作を説明する。

システム構成は図１と同様である。またエッジ監視装置５ａには、性能計測部６６があり、またネットワーク管理用データベース６３には、応答時間を計測する対象となるサーバ６のＩＰアドレスまたはホスト名、及び計測周期、計測プロトコル、ＴＲＡＰ敷居値、パケットサイズ等が設定されている。

【００２３】

次にこの構成による動作を説明する。

定期的に、または機器からの応答がシステムで定めた遅延時間を超すと、エッジ監視装置５ａの性能計測部６６は、例えば、計測プロトコルが‘ＩＰ（ＩＣＭＰ）’の場合は指定されたサイズのＩＣＭＰパケット要求をサーバ６に送信し、その応答時間を計測する。そして先の実施の形態で述べた動作と同様に、各ルータ等のどの部分がボトルネックになっているか、性能劣化があるのか、応答時間が計測できる。計測した値は、エッジ監視装置５ａ内のデータベース（リレーショナルデータベースであることが多い）に記録する。図１の構成では、ネットワーク管理用ＤＢ６３に計測した値がＴＲＡＰしきい値（所定基準値）を超えている場合は、内部的に性能劣化をログに記録する（ＳＮＭＰ－ＴＡＲＰを内部的に発生させ、ＴＲＡＰログに記録することが多い）と共に、統合ネットワーク監視装置８に対してもＳＮＭＰ－ＴＲＡＰ（またはＳＮＭＰ－ＩＮＦＯＲＭ－ＥＲＱＵＥＳＴ／ＲＥＳＰＯＮＳＥ等の別の通知手段）により、しきい値を超えてネットワーク性能の劣化が起こったことを通知する。ＴＲＡＰの通知パケットには、性能劣化が起こった監視対象のＩＰアドレスの他、エッジ監視装置のＩＤやエリア情報を付加して送信する。

【００２４】

遅延情報を通知すべき統合ネットワーク監視装置８のアドレス等は、エッジ監視装置５ａに事前に定義されているものとする。

なお、計測プロトコルはＩＣＭＰプロトコル他、ＨＴＴＰ（ＷＥＢ）、ＳＭＴＰ（メール）、その他のアプリケーション（ＵＤＰ／ＴＣＰポート）であってもよい。

ＨＴＴＰ－ＧＥＴであれば、ＵＲＬを指定してそのページが表示される時間を計測することができる。

なおポーリングを定期的に行うことは、通信経路の利用効率を低下させることになる。従って定期的に行うのは、実は終端ノードのみにＩＣＭＰエコー要求／応答パケットを用いて監視する。そして一定の性能以下に低下した場合に、サーバに向けて関連する経路をたどって順次、機器の応答性能を計測する。

こうして中継路グループ２に性能低下が無ければ、システムの性能低下はサーバ側の障害またはサーバ負荷増大によることが推定される。

いずれにせよ、統合監視装置８では、各クライアントネットワークグループ１に設けたエッジ監視装置５からの性能報告情報を出力して、しきい値を超えて性能低下した場合でも、その原因が経路上のどの部分がボトルネックであるか経路情報を出力して、または経路情報が基準値６２ｂに満たない場合はサーバ側に問題があると出力して、重大障害に至る

前に注意を喚起できる効果がある。

【００２５】

実施の形態３.

上記の各実施の形態では、エッジ監視装置５と統合ネットワーク監視装置８の各構成要素は、専用の要素であるとして説明した。

しかし、汎用の計算機でこれらの構成要素の機能、図７の各ステップをプログラムでステップとして記述して、メモリ上に記憶してエッジ監視装置相当を構成してもよい。つまり図６に記載の中継路への問合せを行い、また応答をモニタして設定変更とデータ記憶を行って経路問合せを繰返し、トリガで指定されるか、または経路変更を検出すると、統合ネットワーク監視装置８に向けて経路変更情報を送信する、各ステップを備える。

また統合ネットワーク監視装置についても同様であり、機器問合せを行い、縮退動作を検出して、または所定のトリガで使用経路数が基準値を超えることを検出すると、その経路情報と障害と推定される機器を出力するステップ、つまりＳ９１ないしＳ９８のステップを備える。

このようにしても、上記の各実施の形態と同様の効果が得られる。

【図面の簡単な説明】

【００２６】

【図１】この発明の実施の形態１における監視装置と監視対象との接続関係を示すシステム構成図である。

【図２】実施の形態１等における監視装置のハードウェア構成を示す図である。

【図３】実施の形態１等における監視装置のソフトウェア構成を示す図である。

【図４】実施の形態１等における検査内容テーブルの例を示す図である。

【図５】実施の形態１等の中継路グループにおける経路特定の問合せ、応答を説明するための経路説明図である。

【図６】実施の形態１等における装置間のシーケンスを示す図である。

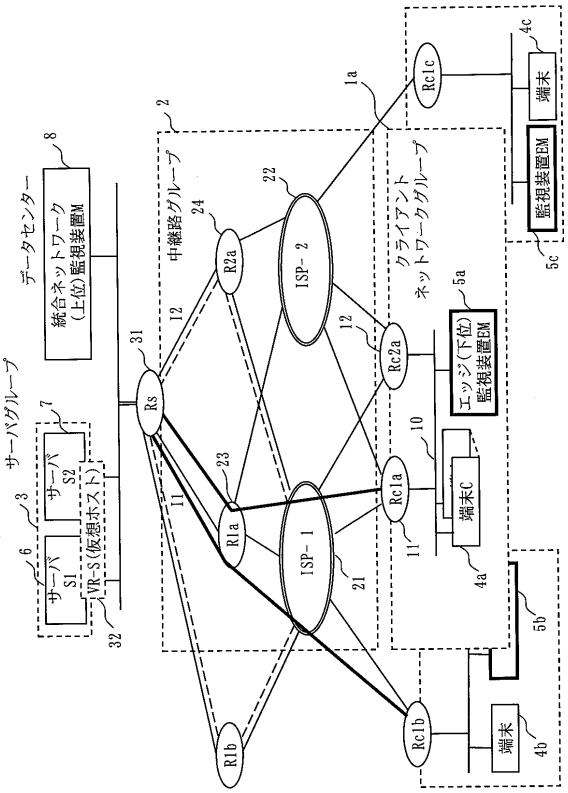
【図７】実施の形態１等における監視装置の動作を示すフロー図である。

【符号の説明】

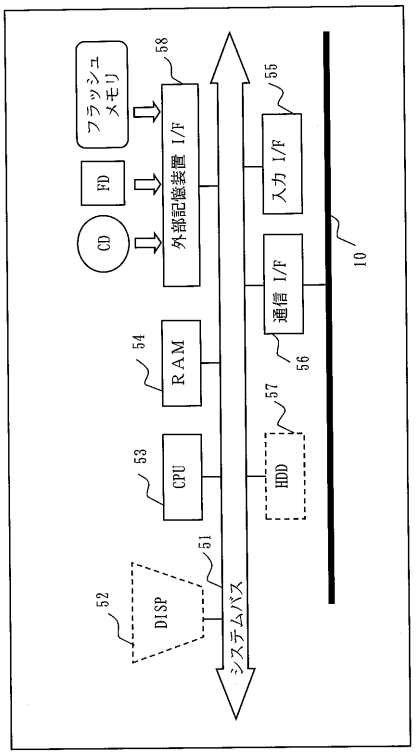
【００２７】

１，１ａ クライアントネットワークグループ、２ 中継路グループ、３ サーバグループ、４，４ａ，４ｂ，４ｃ 端末（Ｃ）、５，５ａ，５ｂ，５ｃ エッジ（下位）監視装置（ＥＭ）、６ サーバＳ１、７ サーバＳ２、８ 統合ネットワーク（上位）監視装置（Ｍ）、１０ ＬＡＮ，１１ ルータＲｃ１ａ、１２ ルータＲｃ２ａ、２１ ＩＳＰ－１、２２ ＩＳＰ－２、２３ ルータＲ１ａ、２４ ルータＲ２ａ、３１ ルータＲｓ、３２ ＶＲ－Ｓ、５１ システムバス、５２ 表示装置（ＤＩＳＰ）、５３ ＣＰＵ、５４ ＲＡＭ、５５ 入力Ｉ／Ｆ、５６ 通信Ｉ／Ｆ、５７ ハードディスク（ＨＤＤ）、５８ 外部記憶装置Ｉ／Ｆ、６１ 管理プロトコル制御部、６２ データ制御部、６２ｂ 基準値、６３ ネットワーク管理用データベース（ＤＢ）、６４ 構成・経路情報作成／検索部、６５ ネットワークモニタ部、６６ 性能計測部、６７ ＩＰ通信ソフトウェア部、Ｓ９１ 経路問い合わせステップ、Ｓ９２ 経路モニタ結果蓄積ステップ、Ｓ９３ ＤＢ記憶ステップ、Ｓ９４ 経路情報送信ステップ、Ｓ９６ ＤＢ記憶ステップ、Ｓ９７ 危機問合せステップ、Ｓ９８ 基準値を超える機器，経路情報出力ステップ。

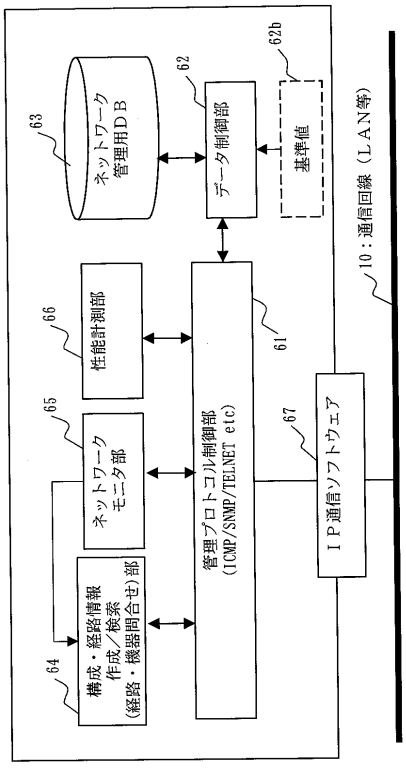
【図１】



【図２】



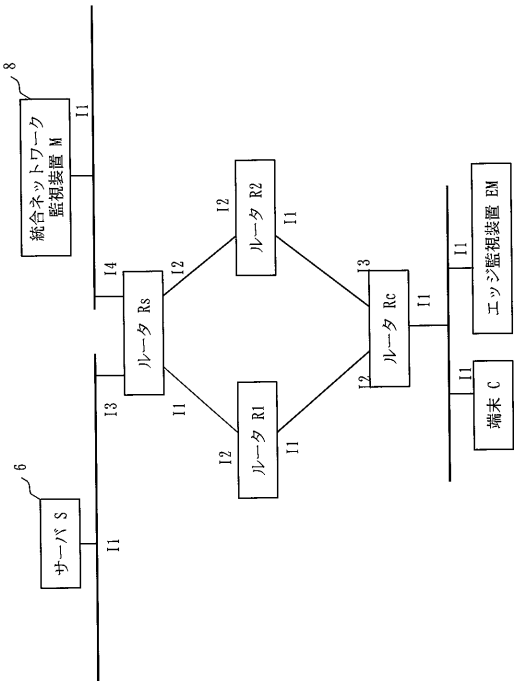
【図３】



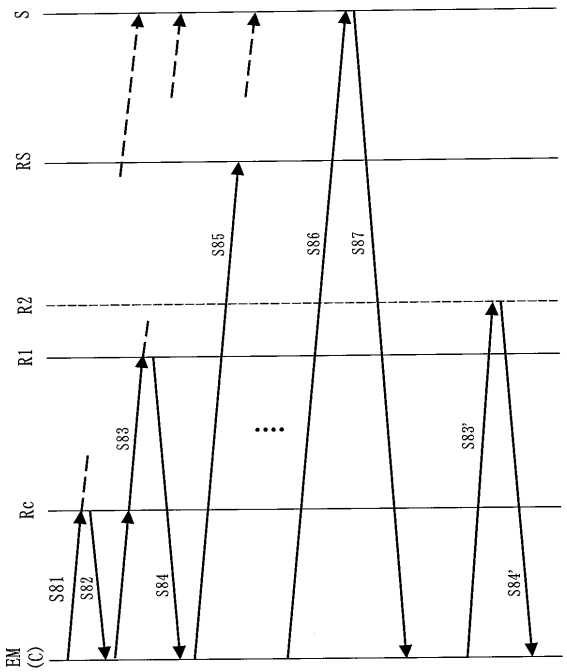
【図４】

71 グループ名	72 対象抽出式種別	73 対象抽出式	74 監視コマンド	75 発生イベント
CLIENT_GROUP (クライアント)	SQL	TARGETS=' select IP_addr from host_table where hostname LIKE 'tokyo%' ;'	ping	if ($STATUS = ERROR) { trapprint "client($IP) response error from($EMID)" ; }
ROUTE_GROUP (中継路グループ)	GROUPED_BY_ENDNODE	# ENDNODE TARGETS=192.168.254.10	traceroute	if($STATUS = ERROR){ trapprint "no route to $IP(from $EMID)" ; } elsif($EM_OUTPUT="/route change/){ print trapbuf "ROUTE CHANGED¥n" ; print trapbuf "NEW ROUTE LIST FROM $EMID to $TARGETS" ; foreach $IP(IP @ROUTE_IP { print trapbuf "ROUTE $IP¥IP; } trapprint trapbuf; }
SERVER_GROUP (サーバグループ)	LIST	TARGETS=192.168.254.10, 192.168.254.11	ping	if ($STATUS = ERROR) { trapprint "server($IP) response error (from $EMID)" ; }

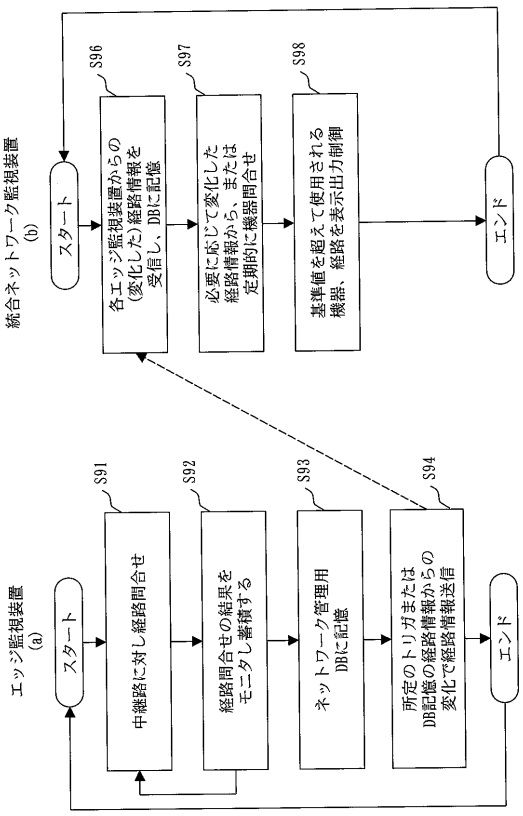
【図５】


統合ネットワーク
監視装置 M
8
I1
I4
I2
I2
ルータ R2
I1
I3
ルータ Rs
I3
ルータ Rc
I1
エッジ監視装置 EM
I1
I1
I2
I1
I2
ルータ R1
I1
I2
I1
端末 C
6
サーバ S
I1

【図６】


S
RS
R2
R1
Rc
EM
(C)
S81
S82
S83
S84
S85
S86
S87
S83'
S84'

【図７】


エッジ監視装置
(a)
スタート
S91
中継路に対し経路問合せ
S92
経路問合せの結果を
モニタし蓄積する
S93
ネットワーク管理用
DBに記憶
S94
所定のトリガまたは
DB記憶の経路情報からの
変化で経路情報送信
エンド
統合ネットワーク監視装置
(b)
スタート
S96
各エッジ監視装置からの
(変化した)経路情報を
受信し、DBに記憶
S97
必要に応じて変化した
経路情報から、または
定期的に機器問合せ
S98
基準値を超えて使用される
機器、経路を表示出力制御
エンド

フロントページの続き

(56)参考文献 特開平０９－３２１７６０（ＪＰ，Ａ）
特開２００３－０６０７０４（ＪＰ，Ａ）
特開２０００－３２４１０６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／５６
Ｈ０４Ｌ　１２／４６