

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4454516号
(P4454516)

(45) 発行日 平成22年4月21日(2010.4.21)

(24) 登録日 平成22年2月12日(2010.2.12)

(51) Int.Cl.		F I		
HO 4 L 12/56	(2006.01)	HO 4 L 12/56	4 O O Z	
HO 4 L 29/14	(2006.01)	HO 4 L 13/00	3 1 1	

請求項の数 5 (全 21 頁)

(21) 出願番号	特願2005-39528 (P2005-39528)	(73) 特許権者	000005223 富士通株式会社
(22) 出願日	平成17年2月16日(2005.2.16)		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2006-229477 (P2006-229477A)	(74) 代理人	100092152 弁理士 服部 毅巖
(43) 公開日	平成18年8月31日(2006.8.31)	(72) 発明者	笹川 靖 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
審査請求日	平成20年1月11日(2008.1.11)	(72) 発明者	瓦井 健一 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	百海 正実 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】 障害検出装置

(57) 【特許請求の範囲】

【請求項1】

ネットワーク上の障害検出を行う障害検出装置において、
 障害監視制御パケットを生成し、自装置と同一プロトコルで障害検出のための相互動作が不要な対向装置に対して、前記障害監視制御パケットを送信する障害監視制御パケット送信部と、
 前記障害監視制御パケットの送信パケット数をカウントする送信パケットカウンタと、
 前記対向装置から送信される、前記送信パケットと同一プロトコルのパケット以外の制御パケットを受信して、受信パケット数をカウントする受信パケットカウンタと、
 前記送信パケット数と前記受信パケット数を監視して、一定時間内に少なくともいずれか一方のパケット数に変化がなければ、障害発生と認識し、外部へ通知する障害検出部と、
 を有することを特徴とする障害検出装置。

【請求項2】

前記障害監視制御パケット送信部は、装置内の上位レイヤの処理部に配置し、前記送信パケットカウンタは、装置内の前記対向装置と自装置が接続する物理レイヤまたはリンクレイヤの処理部に配置することで、前記障害検出部は、前記送信パケット数の監視を行って、前記上位レイヤと前記物理レイヤの処理部間の経路に発生する障害検出を保證することを特徴とする請求項1記載の障害検出装置。

10

20

【請求項 3】

前記受信パケットカウンタは、装置内の上位レイヤの処理部に配置することで、前記障害検出部は、前記受信パケット数の監視を行って、前記対向装置から前記上位レイヤの処理部までの経路に発生する障害検出を保証することを特徴とする請求項 1 記載の障害検出装置。

【請求項 4】

前記障害監視制御パケット送信部は、ユーザトラフィックが流れていないときであっても、誤った障害検出がされないように、ユーザトラフィックとは独立な前記障害監視制御パケットを常時一定間隔で送信することを特徴とする請求項 1 記載の障害検出装置。

【請求項 5】

自装置と前記対向装置とが、複数リンクを仮想的な 1 つのリンクとみなすリンク・アグリゲーションで接続している場合には、前記障害監視制御パケット送信部は、前記複数リンクの各リンクから前記障害監視制御パケットを送信し、前記送信パケットカウンタは、前記複数リンクのリンク毎に送信パケット数をカウントし、前記受信パケットカウンタは、前記複数リンクの各リンクから前記対向装置から送信された制御パケットを受信して、リンク毎に受信パケット数をカウントし、前記障害検出部は、リンク毎に障害検出を行うことを特徴とする請求項 1 記載の障害検出装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、障害検出装置に関し、特にネットワーク上の障害検出を行う障害検出装置に関する。

【背景技術】

【0002】

近年、通信事業者が提供する、LAN (Local Area Network) を利用してのキャリアサービスとして、広域イーサネット (イーサネットは登録商標) があり、現在広がりを見せている。広域イーサネットは、イーサネットの LAN 環境を、レイヤ 2 スイッチを使ってネットワークを接続し、複数の LAN 環境を 1 つに統合するサービスである。

【0003】

広域イーサネットは、高価なルータ (レイヤ 3 スイッチ) を用いずに、安価なスイッチングハブ (レイヤ 2 スイッチ) を使うので、ネットワークの構築や運用管理に関わるコストが削減でき、例えば、企業の構内 LAN をつなげて、都市全体のエリアにまで拡張することが可能である。

【0004】

また、このようなキャリアネットワークにおいて、ネットワーク障害が発生し、復旧が遅れると、被害も重篤なものになるため、装置内の各種パッケージの二重化、装置自身の二重化、リンクの二重化、エンド - エンド間のパスの二重化等の様々なレベルでの冗長構成が採用されており、障害検出時には冗長系側にすみやかに切り替えを行うことで耐障害性の向上を図っている。

【0005】

ただし、冗長構成をいくら設けていても、装置自身が障害をすばやく的確に検出できなければ意味がなく、サイレント障害 (冗長側への自動的な切り替えが行われず、またオペレータへのアラーム通知もなく、異常動作が生じていることが認識しにくい障害) が発生すると、障害期間が長時間続き、またイーサネット網においては、ループ (loop) が生じて、フレーム輻輳が発生してしまうおそれがある。

【0006】

図 11、図 12 はループによるネットワーク障害を説明するための図である。ネットワーク 50 は、ノード 51 ~ 54 で構成され、ノード 51 ~ ノード 54 はリング状に互いに接続し、ノード 51 とノード 54 が接続している (図中、細実線が物理的な回線)。

【0007】

10

20

30

40

50

ここで、イーサネット網を構築する場合には、ループ状の経路が生じないように、ツリー（tree）構造の経路となるように構築する。なぜなら、もし、ネットワーク上にループ状の経路が存在すると、フレームのブロードキャスト時に、ブロードキャスト・ストーム（broadcast storm）と呼ばれるフレーム輻輳が発生するからである。

【0008】

すなわち、あるノードからブロードキャスト・フレームを送出したとき、ブロードキャスト・フレームは、各ノードにおいて、受信ポート以外のすべてのポートからフラディング（flooding）されるので、ネットワーク内にループがあると、ブロードキャスト・フレームは、ループ内を無限に流れることになり、同じ経路を延々とブロードキャスト・フレームが巡ってしまう。

10

【0009】

すると、帯域が瞬時にブロードキャスト・フレームで埋まってしまい、通常の通信ができなくなってしまう。例えば、図11のように、ネットワーク50にはループRがあるので、ブロードキャスト・フレームがノード51 ノード52 ノード53 ノード54 ノード51 …とるように、ループR上を無限に流れて輻輳が発生してしまう。

【0010】

したがって、イーサネット網を構築する場合には、レイヤ2ネットワークでのループを論理的に遮断する必要がある。例えば、図12のように、回線L1、L2を論理的に遮断すれば、すべてのループがなくなって、ツリーTの構造が形成される（図中、太実線）。

【0011】

20

このようなツリー（スパニングツリー（Spanning Tree）と呼ばれる）を形成するためには、例えば、STP（Spanning Tree Protocol）の制御により、各ノード間でBPDU（Bridge Protocol Data Unit）と呼ばれる制御情報をやりとりし、トラフィック経路をダイナミックに変更する運用を行う（スタティックに運用する場合には、各ノードに対してあらかじめツリー経路となるように設定しておく）。これにより、物理的にループを形成しているネットワークであっても、フレームがループの中を巡り続ける事態を防ぐことができる。

【0012】

ところが、図12のようなスパニングツリーが形成されていても、ネットワーク50にサイレント障害が発生して障害検出機能が効果的に働かないと、そのために各ノードでの経路認識が食い違ってきて、ツリー構造が崩れ、ループが生じてしまうおそれがある。したがって、サイレント障害の対策には、冗長構成を設けることの他にさらに、いかに高精度に障害を検出できるかということが重要な事項となる。

30

【0013】

従来のイーサネットの障害検出として、LAN内の装置でループバックテストを実行する技術が提案されている（例えば、特許文献1）。

【特許文献1】特開2003-304264号公報（段落番号【0020】～【0027】，第1図）

【発明の開示】

【発明が解決しようとする課題】

40

【0014】

上記のような、サイレント障害が発生すると、運用系から冗長系への切替え契機は、顧客からの苦情によるしかなく、サービスの長時間の断となるため、各ベンダでは独自のプロトコルによって、ネットワーク障害を検出する取り組みがなされている。

【0015】

図13はネットワーク障害検出の流れを示す図である。ベンダ独自プロトコルによる一般的なネットワーク障害を検出する一動作例を示している。ノードA、BがリンクL3、L4で接続している。

【0016】

〔S21〕ノードAは、リンクL3を通じて、フレームFaをノードBへ送信する。フ

50

フレーム F a には、自ノード識別欄と他ノード識別欄があり、ノード A では、フレーム F a の自ノード識別欄に、自分がノード A である旨の “ A ” を挿入し、他ノード識別欄には、リンク L 4 から受信したフレーム F b の自ノード識別欄に記されている “ B ” を折り返す形で挿入して送信する。

【 0 0 1 7 】

〔 S 2 2 〕 ノード B は、リンク L 4 を通じて、フレーム F b をノード A へ送信する。フレーム F b は、自ノード識別欄と他ノード識別欄があり、ノード B では、フレーム F b の自ノード識別欄に、自分がノード B である旨の “ B ” を挿入し、他ノード識別欄には、リンク L 3 から受信したフレーム F a の自ノード識別欄に記されている “ A ” を折り返す形で挿入して送信する。

10

【 0 0 1 8 】

〔 S 2 3 〕 ノード A は、フレーム F b を受信すると、フレーム F b の自ノード識別欄に記されている “ B ” という情報をメモリに記憶させる（すなわち、相手ノードが B であることを記憶する）。なお、メモリのエージング時間（メモリをクリアする更新時間）を 1 分とし、フレーム F b の送信間隔は 2 0 秒とする。

【 0 0 1 9 】

〔 S 2 4 〕 ノード B は、フレーム F a を受信すると、フレーム F a の自ノード識別欄に記されている “ A ” という情報をメモリに記憶させる（すなわち、相手ノードが A であることを記憶する）。なお、メモリのエージング時間を 1 分とし、フレーム F a の送信間隔は 2 0 秒とする。

20

【 0 0 2 0 】

〔 S 2 5 〕 ノード A は、フレーム F b が 3 回来ないとメモリをクリアすることになり、このとき他ノード識別欄に “ 0 ” を挿入したフレーム F a - 1 を生成してノード B へ送信する。また、ノード A は、フレーム F b が 3 回来ないことで、リンク L 4（または対向のノード B）に障害が発生していることを検出する。

【 0 0 2 1 】

〔 S 2 6 〕 ノード B は、フレーム F a - 1 を受信すると、他ノード識別欄に “ 0 ” が挿入されていることを認識する。すなわち、自分のノード識別名（ B ）がノード A に伝わっておらず、自分が送信しているフレーム F b がノード A に正常受信されていないことを認識し、リンク L 4（または対向のノード A）に障害が発生していることを検出する。

30

【 0 0 2 2 】

このように、「対向装置から制御フレームを一定期間受信しないこと」及び「対向装置から受信する制御フレーム中の折り返し情報が、自装置が送信した情報と異なること」によって、送受信ノード間で障害検出を行うことができる。

【 0 0 2 3 】

しかし、このような現状のベンダ独自プロトコルによるネットワーク障害検出では、上記の例のような、対向装置側の監視内容を意識した上での制御を行うことを前提としているため、ネットワーク内の自社装置間で接続されたリンクしか対応できないといった問題があった。

【 0 0 2 4 】

このため、マルチベンダ化が進んでいる現在のキャリアネットワークに対して、利便性が乏しいといった問題があり、さらにネットワーク検出障害のプロトコルの標準化も進展していないのが現状である。

40

【 0 0 2 5 】

このため、マルチベンダ環境において、自装置と対向装置間で同一プロトコルによる相互動作をすることなく、対向装置側が障害の監視を何ら意識せずに、ネットワーク障害を検出できれば、非常に耐障害性の向上という意味での効果が期待され、このような技術の実現が強く要望されている。

【 0 0 2 6 】

本発明はこのような点に鑑みてなされたものであり、対向装置間で同一プロトコルによ

50

る相互動作をすることなく、自装置のみでネットワーク障害を高精度に検出する障害検出装置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】

【0027】

本発明では上記課題を解決するために、図1に示すような、ネットワーク上の障害検出を行う障害検出装置10において、障害監視制御パケットを生成し、自装置と同一プロトコルで障害検出のための相互動作が不要な対向装置20に対して、障害監視制御パケットを送信する障害監視制御パケット送信部11と、障害監視制御パケットの送信パケット数をカウントする送信パケットカウンタ12と、対向装置20から送信される制御パケットを受信して、受信パケット数をカウントする受信パケットカウンタ13と、送信パケット数と受信パケット数を監視して、一定時間内に少なくともいずれか一方のパケット数に変化がなければ、障害発生と認識し、外部へ通知する障害検出部14と、を有することを特徴とする障害検出装置10が提供される。

10

【0028】

ここで、障害監視制御パケット送信部11は、障害監視制御パケットを生成し、自装置と同一プロトコルで障害検出のための相互動作が不要な対向装置20に対して、障害監視制御パケットを送信する。送信パケットカウンタ12は、障害監視制御パケットの送信パケット数をカウントする。受信パケットカウンタ13は、対向装置20から送信される制御パケットを受信して、受信パケット数をカウントする。障害検出部14は、送信パケット数と受信パケット数を監視して、一定時間内に少なくともいずれか一方のパケット数に変化がなければ、障害発生と認識し、外部へ通知する。

20

【発明の効果】

【0029】

本発明の障害検出装置は、自装置と同一プロトコルで障害検出のための相互動作が不要な対向装置に対して、障害監視制御パケットを送信して障害監視制御パケットの送信パケット数をカウントし、対向装置から送信される制御パケットを受信して、受信パケット数をカウントし、送信パケット数と受信パケット数に対して、一定時間内に少なくともいずれか一方のパケット数に変化がなければ、障害発生と認識する構成とした。これにより、マルチベンダ環境において、自装置と対向装置間で同一プロトコルによる相互動作をすることなく、自装置のみでネットワーク障害を高精度に検出することが可能になる。

30

【発明を実施するための最良の形態】

【0030】

以下、本発明の実施の形態を図面を参照して説明する。図1は障害検出装置の原理図である。障害検出装置10は、障害監視制御パケット送信部11、送信パケットカウンタ12、受信パケットカウンタ13、障害検出部14から構成され、ネットワーク上の障害検出を行う装置である。障害検出装置10の機能は、例えば、広域イーサネット内のレイヤ2スイッチなどに適用可能である。

【0031】

障害監視制御パケット送信部11は、障害監視制御パケットを生成し、自装置と同一プロトコルで障害検出のための相互動作が不要な対向装置20に対して（すなわち、自社製品とは異なる他社の製品に対して）、障害監視制御パケットを送信する。送信パケットカウンタ12は、障害監視制御パケットの送信パケット数をカウントする。

40

【0032】

受信パケットカウンタ13は、対向装置20から送信される制御パケットを受信して、受信パケット数をカウントする。障害検出部14は、送信パケット数と受信パケット数を監視して、一定時間内に少なくともいずれか一方のパケット数に変化がなければ、障害発生と認識し、外部へ通知する。

【0033】

次に障害監視制御パケット送信部11、送信パケットカウンタ12及び受信パケットカウンタ13の障害検出装置10内の配置位置について説明する。図2は障害検出装置10

50

のブロック構成を示す図である。障害検出装置 10 は、スイッチング処理部 101、出力パケット処理部 (Egress Process) 102a、入力パケット処理部 (Ingress Process) 102b、MAC (Media Access Control) 処理部 103a、103b、リンクインタフェース部 104a、104b、CPU 105 から構成される。

【0034】

出力パケット処理部 102a は、スイッチング処理部 101 でスイッチングされたパケットの入力処理を行い、MAC 処理部 103a は、MAC レイヤの終端処理を行う。リンクインタフェース部 104a は、物理レイヤでの送信インタフェース処理を行って、パケットを対向装置 20 へリンク L を介して送信する。

【0035】

また、リンクインタフェース部 104b は、リンク L を介して送信された対向装置 20 からのパケットに、物理レイヤでの受信インタフェース処理を行い、MAC 処理部 103a は、MAC レイヤの終端処理を行う。入力パケット処理部 102b は、パケットの出力処理を行ってスイッチング処理部 101 へ送信する。CPU 105 は、各構成ブロックの全体制御を行う。

【0036】

ここで、障害監視制御パケット送信部 11 の機能は、出力パケット処理部 102a に配置し、送信パケットカウンタ 12 は、リンクインタフェース部 104a に配置する。そして、出力パケット処理部 102a から障害監視制御パケットを一定間隔で流して、リンクインタフェース部 104a でその障害監視制御パケットをカウントする。

【0037】

障害検出部 14 の機能を有する CPU 105 は、送信パケットカウンタ 12 でカウントされる送信パケット数を監視して、一定時間内にパケット数に変化がなければ障害発生とみなす (障害監視制御パケット送信部 11 から一定間隔で障害監視制御パケットが送信されるので、一定時間カウントアップされていないとすれば障害が発生していることになる)。

【0038】

この場合、出力パケット処理部 102a MAC 処理部 103a リンクインタフェース部 104a の経路が、障害検出の保証範囲となる (ただし、この送信側の障害検出では、対向装置 20 に確実にパケットが送信されていることは確認できないが、リンク L が確立した状態で、少なくともリンクインタフェース部 104a までが正常であれば、トラフィックが対向装置 20 に届かない確率は非常に低いので、障害検出のカバー範囲は広がる)。

【0039】

一方、受信パケットカウンタ 13 は、入力パケット処理部 102b に配置し、入力パケット処理部 102b において、対向装置 20 から送信されたパケットをカウントする。

障害検出部 14 の機能を有する CPU 105 は、受信パケットカウンタ 13 でカウントされる受信パケット数を監視して、一定時間内にパケット数に変化がなければ障害発生とみなす (対向装置 20 から一定間隔で制御パケットが送信されるので、一定時間カウントアップされていないとすれば障害が発生していることになる)。この場合、対向装置 20 リンクインタフェース部 104b MAC 処理部 103b 入力パケット処理部 102b の経路が、障害検出の保証範囲となる。

【0040】

このように、障害監視制御パケットを送信して障害検出を行う場合は、障害監視制御パケット送信部 11 を装置の上位レイヤ処理側 (装置の内側) に配置し、送信パケットカウンタ 12 を物理レイヤ処理 (装置の外側) に配置する。また、対向装置 20 から送信される制御パケットによる障害検出を行う場合は、受信パケットカウンタ 13 を装置の上位レイヤ処理側に配置する。このような配置にすることで、上記のように障害検出の保証範囲を最も広くとることが可能になる。

【0041】

次に 1 本のリンクにおける障害検出動作について説明する。図 3 は装置間が 1 本のリン

10

20

30

40

50

クで接続された際の障害検出動作を示すシーケンス図である。障害検出装置 10 の機能を有する装置を自社装置 10 a、対向装置 20 を他社装置 20 a とし、互いに 1 本のリンク L で接続している。

【0042】

〔S1〕自社装置 10 a 内の障害監視制御パケット送信部 11 は、障害監視用の独自のパケットである障害監視制御パケットを一定間隔で他社装置 20 a へ送信する。なお、この障害監視制御パケットは、他社装置 20 a で受信されたときに廃棄されるものであり、ペイロードには何の制御内容をも含まないパケットである。

【0043】

〔S2〕自社装置 10 a 内の送信パケットカウンタ 12 は、障害監視制御パケットをカウントする。

10

〔S3〕自社装置 10 a 内の障害検出部 14 は、カウントされる送信パケット数を監視する。カウント値に変化がなければ（カウントアップされてなければ）ステップ S4 へいき、変化があれば監視を続ける。

【0044】

〔S4〕障害検出部 14 は、自社装置 10 a に障害が発生しているものとみなし外部へアラーム通知する。

〔S5〕他社装置 20 a は、制御パケットを送信する。この制御パケットは、他社装置 20 a から送信される何らかの制御パケットであり（カウント動作のみに用いるためどのような制御パケットでもよい）、一定間隔で送信されるものである。

20

【0045】

〔S6〕自社装置 10 a 内の受信パケットカウンタ 13 は、制御パケットを受信してカウントする。

〔S7〕自社装置 10 a 内の障害検出部 14 は、カウントされる受信パケット数を監視する。カウント値に変化がなければステップ S8 へいき、変化があれば監視を続ける。

【0046】

〔S8〕障害検出部 14 は、他社装置 20 a から自社装置 10 a 間の経路に障害が発生しているものとみなし外部へアラーム通知する。

ここで、ステップ S1、S5 において、障害監視制御パケットと制御パケットは、常時一定間隔でリンク L 上に送出されるユーザトラフィックとは独立したパケットとする。

30

【0047】

なぜなら、もしユーザトラフィックに関連するパケットを使用して、パケット数のカウント値による障害検出を行うと、夜間などではユーザトラフィックが減少しカウント値の変化が起こらず、通信状態が正常であっても障害が発生していると誤って検出するおそれがあるからである。

【0048】

このため、自社装置 10 a からはユーザトラフィックとは無関係な独自の障害監視制御パケットを送信し、また他社装置 20 a から送信されるユーザトラフィックとは無関係な何らかの制御パケットを受信することで、ユーザトラフィックが流れていないときであっても、誤検出のない障害検出を可能にしている。

40

【0049】

また、ステップ S4、S8 ではアラーム通知を行ってオペレータに保守動作を促しているが、その後の障害検出装置 10 の動作として、該当ポートを無効化する処理が行われる（対向装置 20 はリンク断を検出することになる）。無効化されたポートの復旧は、手動または定期的に自動復旧が行われる。さらに、障害検出をリンク冗長 / 装置冗長への切り替え契機として、冗長系へ切り替えることも可能である。

【0050】

以上説明したように、障害検出装置 10 では、自装置側で統計情報として送信パケット数及び受信パケット数を計測して、これらの統計情報を収集し、障害検出を行う構成とした。このような構成により、対向装置 20 側の監視内容を意識せずに障害検出を行うこと

50

ができる。すなわち、マルチベンダ環境において、自装置と対向装置間で同一プロトコルによる相互動作をすることなく、対向装置 20 側が障害の監視を何ら意識せずに、また冗長ポートを追加するなどといった作業も不要であり、効率よくネットワーク障害を検出できる。このため、従来のように、自社装置間でのみ接続されたリンクしか障害検出ができないといった不便さがなくなり、他ベンダ装置に接続しても、高精度にネットワーク障害を検出できるので、マルチベンダ環境において対耐障害性の向上を図ることが可能になる。

【 0 0 5 1 】

次に自社装置 10 a と他社装置 20 a がリンク・アグリゲーション (Link Aggregation (以降 LA と呼ぶ)) で接続している際の障害検出動作について説明する。なお、LA は、複数リンクを仮想的な 1 つのリンクとみなす接続方式であり、IEEE.802.3ad で規定されている。

10

【 0 0 5 2 】

図 4 は装置間が LA で接続された際の障害検出動作を示すシーケンス図である。自社装置 10 a と他社装置 20 a が 3 本のリンク L 1 ~ L 3 で接続し、このリンク L 1 ~ L 3 を仮想的な 1 本のリンクとして使用するものとする。

【 0 0 5 3 】

〔 S 1 1 〕 自社装置 10 a 内の障害監視制御パケット送信部 1 1 は、障害監視用の独自のパケットである障害監視制御パケットをリンク L 1 ~ L 3 を介して、一定間隔で他社装置 20 a へ送信する。

20

【 0 0 5 4 】

〔 S 1 2 〕 自社装置 10 a 内の送信パケットカウンタ 1 2 は、リンク L 1 ~ L 3 毎に流れる障害監視制御パケットをカウントする。

〔 S 1 3 〕 自社装置 10 a 内の障害検出部 1 4 は、リンク L 1 ~ L 3 毎にカウントされる送信パケット数を監視する。カウント値に変化がなければステップ S 1 4 へいき、変化があれば監視を続ける。

【 0 0 5 5 】

〔 S 1 4 〕 障害検出部 1 4 は、自社装置 10 a に障害が発生しているものとみなし外部へアラーム通知する。

〔 S 1 5 〕 他社装置 20 a は、リンク L 1 ~ L 3 を介して、制御パケットを送信する。

30

【 0 0 5 6 】

〔 S 1 6 〕 自社装置 10 a 内の受信パケットカウンタ 1 3 は、リンク L 1 ~ L 3 毎に制御パケットを受信してカウントする。

〔 S 1 7 〕 自社装置 10 a 内の障害検出部 1 4 は、リンク L 1 ~ L 3 毎にカウントされる受信パケット数を監視する。カウント値に変化がなければステップ S 1 8 へいき、変化があれば監視を続ける。

【 0 0 5 7 】

〔 S 1 8 〕 障害検出部 1 4 は、他社装置 20 a から自社装置 10 a 間の経路に障害が発生しているものとみなし外部へアラーム通知する。

次に障害検出装置 10 を具体的に実現した際の構成及び動作について説明する。図 5 は障害検出装置 10 の機能を有する通信装置の構成を示す図である。通信装置 30 は、装置管理部 31、CL (command line) / NMS (network management system) インタフェース部 32、LCC (Link Connectivity Check) プロトコル処理部 34、フィルタリングデータベース処理部 35、回線 / スイッチ制御部 36、スイッチング処理部 37、回線インタフェース処理部 38 - 1 ~ 38 - n から構成される。

40

【 0 0 5 8 】

なお、障害監視制御パケット送信部 11、送信パケットカウンタ 12 及び受信パケットカウンタ 13 の機能は、回線インタフェース処理部 38 - 1 ~ 38 - n に含まれ、障害検出部 14 の機能は、LCC プロトコル処理部 34 に含まれる。

【 0 0 5 9 】

50

装置管理部 3 1 は、装置全体の管理を行う。具体的にはプロビジョニング情報管理部 3 3 と連携し、装置のプロビジョニング情報にもとづき、スイッチング処理部 3 7、回線インタフェース処理部 3 8 - 1 ~ 3 8 - n、LCC プロトコル処理部 3 4 に動作条件を指示する。

【 0 0 6 0 】

また、スイッチング処理部 3 7 / 回線インタフェース処理部 3 8 - 1 ~ 3 8 - n / LCC プロトコル処理部 3 4 から、動作状態 / 障害発生 / 障害復旧等に関する情報を入手し、必要なアクションを取る。障害検出制御を行う装置管理部 3 1 に対する機能拡張例を以下の (A 1) ~ (A 4) に示す。

【 0 0 6 1 】

(A 1) プロビジョニング情報管理部 3 3 との連携によりポート毎にadminstatusパラメータの設定情報を読み出し、これにもとづき、LCC プロトコル処理部 3 4 に動作条件の指示を行う。

【 0 0 6 2 】

(A 2) LCC プロトコル処理部 3 4 からの通知により、障害検出をオペレータへ通知する。

(A 3) LCC プロトコル処理部 3 4 からの通知により、障害検出を知り、必要によりフィルタリングデータベース処理部 3 5 に対して、フィルタリングデータベースのフラッシュを指示する。

【 0 0 6 3 】

(A 4) LCC プロトコル処理部 3 4 からの通知により、障害検出を知り、必要により回線 / スイッチ制御部 3 6 を経由し、回線インタフェース処理部 3 8 - 1 ~ 3 8 - n に対して、Disable状態への遷移を指示する。

【 0 0 6 4 】

CL / NMS インタフェース部 3 2 は、CL (コマンドライン) / NMS (ネットワーク管理システム) とのインタフェースを司り、ここでは、プロビジョニング情報管理部 3 3 と連携し、管理情報の設定及び表示を行う。

【 0 0 6 5 】

プロビジョニング情報管理部 3 3 は、CL / NMS インタフェース部 3 2 からの指示に従い、プロビジョニング情報を設定 / 表示すると共に、該当プロビジョニング情報を各機能ブロックに対して参照可能とする。

【 0 0 6 6 】

LCC プロトコル処理部 3 4 は、LCC の動作主体であり、装置管理部 3 1 から指示された動作条件に従い、障害を検出した場合は、その旨を装置管理部 3 1 に通知する。障害検出制御を行うLCC プロトコル処理部 3 4 に対する機能拡張例を以下の (B 1) ~ (B 5) に示す。

【 0 0 6 7 】

(B 1) 装置管理部 3 1 からの指示により、ポート毎に障害監視機能 / 制御パケット送信機能の有効化 / 無効化を行い、ポート状態ステートマシン # 1 ~ # n に動作指示を出すとともに、必要に応じて、回線インタフェース処理部 3 8 - 1 ~ 3 8 - n に障害監視の開始 / 停止を指示する。

【 0 0 6 8 】

(B 2) 制御パケット送信機能が有効の場合、必要に応じて、回線インタフェース処理部 3 8 - 1 ~ 3 8 - n に障害監視用制御パケットを装置管理部 3 1 から指示された間隔で送信する事を指示する。

【 0 0 6 9 】

(B 3) 障害監視機能が有効の場合、回線インタフェース処理部 3 8 - 1 ~ 3 8 - n からの障害検出通知 / 復旧通知を受信し、ポート状態ステートマシン # 1 ~ # n に該当イベントの発生を通知する。

【 0 0 7 0 】

10

20

30

40

50

(B 4) ポート状態ステートマシン # 1 ~ # n の動作により、障害を認識し、該当ポートが障害である旨を、装置管理部 3 1 に通知する。

(B 5) 装置管理部 3 1 からの指示により、回線 / スイッチ制御部 3 6 を経由し、回線インタフェース処理部 3 8 - 1 ~ 3 8 - n に対して、Disable ステートへの遷移を指示する。

【 0 0 7 1 】

フィルタリングデータベース処理部 3 5 は、プロビジョニング情報管理部 3 3、装置管理部 3 1、回線インタフェース処理部 3 8 - 1 ~ 3 8 - n と連携し、M A C フィルタリングデータベースの原本を管理し、各回線インタフェース処理部に対して、必要な M A C フィルタリングデータベースを提供するとともに、スイッチング制御部 3 7 に対して、必要

10

【 0 0 7 2 】

回線 / スイッチ制御部 3 6 は、装置管理部 3 1 からの指示に従い、スイッチング処理部 3 7 / 回線インタフェース処理部 3 8 - 1 ~ 3 8 - n に対して、動作条件を通知するとともに、スイッチング処理部 3 7 / 回線インタフェース処理部 3 8 - 1 ~ 3 8 - n からの動作状態 / 障害発生 / 障害復旧等に関する情報を装置管理部 3 1 に通知する。

【 0 0 7 3 】

スイッチング処理部 3 7 は、回線 / スイッチ制御部 3 6 からの指示に従い、各回線インタフェース処理部及び自装置内の必要な機能ブロックとのスイッチングを行う。

回線インタフェース処理部 3 8 - 1 ~ 3 8 - n は、回線 / スイッチ制御部 3 6 からの指示に従い、M A C フィルタリングデータベースを参照することによるパケットの送受信を行う。障害検出制御を行う回線インタフェース処理部 3 8 - 1 ~ 3 8 - n に対する機能拡張例を以下の (C 1)、(C 2) に示す。

20

【 0 0 7 4 】

(C 1) L C C プロトコル処理部 3 4 からの指示により、障害監視ステートマシン # 1 ~ # n に対して、障害監視の開始 / 停止を指示する。

(C 2) 障害監視ステートマシン # 1 ~ # n は、統計情報 (カウント値) の受信パケット数と送信パケット数の変化を周期的に監視し、障害検出 / 復旧検出を L C C プロトコル処理部 3 4 に通知する。

【 0 0 7 5 】

次に通信装置 3 0 における障害検出の動作設定について説明する。

(1) 障害検出用監視統計情報

(1 a) 受信パケット数 : M A C チップの受信ユニキャストパケット数と受信非ユニキャストパケット数との和の変化を監視する。ただし、C L I によりクリアされないカウンタを監視する。

【 0 0 7 6 】

(1 b) 送信パケット数 : M A C チップの送信ユニキャストパケット数と送信非ユニキャストパケット数との和の変化を監視する。ただし、C L I によりクリアされないカウンタを監視する。

【 0 0 7 7 】

(2) 単一物理ポートに対して、以下の動作指定を行う。

(2 a) 特定の M A C D A (マルチキャストアドレス / 対向装置のユニキャストアドレス)、Ethertype を付与した制御パケットを特定の送信間隔で送信する事を指定する。

【 0 0 7 8 】

(2 b) 障害検出時の動作モードを指定する。

(T R A P 通知のみ (障害検出時にアラーム通知をして保守動作を促すこと) / T R A P 通知 + s h u t s o w n (障害検出時にアラーム通知をして保守動作を促し、該当ポートを無効化すること) / T R A P 通知 + s h u t s o w n + 自動復旧 (障害検出時にアラーム通知をして保守動作を促し、該当ポートを無効化し、定期的に自動復旧を試みること))。

40

【 0 0 7 9 】

50

(2 c) 障害検出保護回数を指定する。

障害検出タイマ値 × 障害検出保護回数 この期間障害が継続した場合障害とする。障害検出タイマは 8 秒固定とする (受信パケット数または / 送信パケット数がこのタイマの期間変化しなかった場合障害とする) 。

【 0 0 8 0 】

(3) 障害監視制御パケットの送信開始契機は以下とする。

「該当ポートが L C C 機能を指定されている状態」かつ「該当ポートの物理ポートが UP 状態」へ遷移時で該当ポートがパケットの送受信が可能となった時。

【 0 0 8 1 】

(4) 送信パケット数 / 受信パケット数の変化の監視開始契機は以下とする (物理ポートの LINK UP / DOWN を考慮する) 。

(4 a) 「該当ポートが L C C 機能を指定されている状態」かつ「該当ポートがリンクアップ中」へ遷移時。

【 0 0 8 2 】

(4 b) 「監視正常状態」で該当ポートのリンクダウンを検出後、リンクアップを検出時。

(4 c) TRAP 通知モードで障害検出後、自動復旧した場合。

【 0 0 8 3 】

(4 d) TRAP 通知モードで障害検出後、復旧待ち状態で、該当ポートのリンクダウンを検出後、リンクアップを検出時。

(4 e) TRAP 通知 + shutdown モードで、障害検出による shutdown を実施後、オペレータからの復旧指示によりリンクアップを試み、リンクアップした時。

【 0 0 8 4 】

なお、上記リンクアップ検出時は常に、該当ポートがパケットの送受信が可能となったことが条件として加わる。

(5) 送信パケット数 / 受信パケット数の変化の監視停止契機は以下とする (物理ポートの LINK UP / DOWN を考慮する) 。

【 0 0 8 5 】

(5 a) 該当ポートが L C C 機能の指定を解除された時。

(5 b) 該当ポートがリンクダウンした時。

(5 c) 該当ポートが TRAP 通知 + shutdown 及び TRAP 通知 + shutdown + 自動復旧モードで運用中に、障害検出による shutdown を実施した場合。

【 0 0 8 6 】

(6) shutdown と通常の shutdown の識別と復旧方法

(6 a) 新たに本機能で認識するポート状態 (LccOperStatus) を設け、 ifOperStatus が down 状態で、LccOperStatus が failure の時に、本機能により shutdown を実施したものと判断する。

【 0 0 8 7 】

(6 b) 上記状態からの復旧は、noshutdown コマンドにより行う。

(6 c) 障害の検出そのものは、システムとしての警報の扱いの対象外とする。つまり、本機能による障害の検出そのものでは、TRAP 通知のみとする。

【 0 0 8 8 】

(7) 障害監視方式を以下に示す。

(7 a) (4) に示す条件を障害監視のトリガとする。

(7 b) (2) で規定した障害検出タイマを周期として、(1) で規定した「受信パケット数」と「送信パケット数」の変化を監視する。

【 0 0 8 9 】

(7 c) 前の周期で収集した「受信パケット数」 / 「送信パケット数」と現周期で収集した「受信パケット数」 / 「送信パケット数」を比較し、どちらかが一致した場合、障害と判断し、この障害検出が指定された保護回数連続した時、一致したカウンタ名及びポー

10

20

30

40

50

トIDを付加情報として障害検出を通知する。

【 0 0 9 0 】

(7 d) 障害検出中は、上記と同様の方式で復旧を監視する。復旧の判定は前の周期で収集した「受信パケット数」 / 「送信パケット数」と現周期で収集した「受信パケット数」 / 「送信パケット数」を比較し、双方が不一致の場合とし、ポートIDを付加情報として障害検出を通知する。

【 0 0 9 1 】

(7 e) (5) で規定した条件をトリガとして、障害監視を停止する。

次に障害監視制御パケットのフォーマットについて説明する。図 6 は障害監視制御パケットのフォーマットを示す図である。図中の数値はbyteを表す。各フィールドの説明を以下に示す。

【 0 0 9 2 】

MAC DA[6]は、宛先MACアドレスであり、コマンドにて指定されたアドレスを設定する。デフォルトで01-00-0E-00-00-01。MAC SA[6]は、送出元MACアドレスであり、自装置のMACアドレスを設定する。

【 0 0 9 3 】

L/T[2]は、障害監視制御パケットのEther-Typeであり、コマンドにて指定された値を設定する。Sub Type[1]は、0x20固定とする(0x20が障害監視制御パケットであることを示す識別番号となる)。

【 0 0 9 4 】

Flags[1]は、0固定とする。Code[2]は、<02-00>とし、LCC機能の制御パケットを示す。TTL (Time to Live) [1]はリザーブとする(255固定)。TTL base[1]は、リザーブ(255固定)とする。

【 0 0 9 5 】

Sequence number[2]は、0固定とする。Slot-ID[1]は、パケットを送信するポートのスロット識別子である。Port-ID[1]は、パケットを送信するポートのポート識別子である。Padding[3 6]は、ALL " 0 " を設定する。

【 0 0 9 6 】

次に通信装置 3 0 のポート状態ステートマシン及び障害監視ステートマシンについて説明する。図 7、図 8 はポート状態ステートマシン # 1 ~ # n の状態遷移を示す図である。変数の定義を以下に示す。

【 0 0 9 7 】

LccAdminStatus : LCC機能の該当ポートへの設定状態。disable, enableの状態を持つ。

ifOperStatus : 該当ポートのオペレーショナルリンク状態。up, down, dormant (新規追加) の3つの状態を持つ。dormant状態へは、本機能によりshutdownされた場合に遷移し、他状態への遷移は通常のshutdownコマンドが投入された場合のみ遷移する。

【 0 0 9 8 】

LccOperStatus : 本機能における該当ポートの状態であり、監視機能無効、監視正常、障害中、監視休止中の状態を持つ。監視機能無効 (disable) は、本機能が指定されていない状態または指定されたがリンクがアップしていない状態である。監視正常 (normal) は、本機能による監視状態にあり、正常な状態である。障害中 (failure) は、本機能による障害を検出した状態で、動作モードにより、該当ポートのifOperStatusはdormant状態の場合とup状態の場合がある。監視休止中 (unknown) は、本機能による監視正常時にリンクダウンを検出 (ifOperStatusがdown) し、監視を休止している状態である。

【 0 0 9 9 】

LccMonStartInd : 障害監視ステートマシンへの動作指示。動作指示内容として、trueは、この値に変化したことにより、障害監視ステートマシンは監視を開始する。falseは、この値に変化したことにより、障害監視ステートマシンは監視を停止する。

【 0 1 0 0 】

10

20

30

40

50

LccMode：本機能による障害検出時の動作モードを意味する（コマンドにより指定）。動作モードには、shutdown（障害検出時、shutdownするモード）とnoShutdown（障害検出時、shutdownしないモード）がある。

【0101】

次にポート状態ステートマシン # 1 ~ # n の関数の定義を示す。

noticeNormalTrap（）：障害監視を開始した事を示すTRAPを送信する。付加情報として、検出portidを付与する。

【0102】

noticeFailTrap（）：本機能による障害を検出した事を示すTRAPを送信する。付加情報として、検出portid, 障害種別（Rx / Tx / RxTx）を付与する。

10

LccShutdown（）：LCC機能によるshutdownを実行する。

【0103】

図9、図10は障害監視ステートマシン # 1 ~ # n の状態遷移を示す図である。変数の定義を以下に示す。

prevRxCount：直前の周期で収集した受信パケットカウンタの内容を示す。

【0104】

prevTxCount：直前の周期で収集した送信パケットカウンタの内容を示す。

currRxCount：現周期で収集した受信パケットカウンタの内容を示す。

currTxCount：現周期で収集した送信パケットカウンタの内容を示す。

【0105】

rxCount：getStatistics関数で収集した受信パケットカウンタの内容を示す。

txCount：getStatistics関数で収集した送信パケットカウンタの内容を示す。

rxFail：受信パケットカウンタの監視が正常か否かを示す変数（障害監視で使用）。

20

【0106】

txFail：送信パケットカウンタの監視が正常か否かを示す変数（障害監視で使用）。

rxFail2：受信パケットカウンタの監視が正常か否かを示す変数（復旧監視で使用）。

txFail2：送信パケットカウンタの監視が正常か否かを示す変数（復旧監視で使用）。

【0107】

timerExp：タイマステートマシンにより、登録されたタイマが満了時、trueに設定される変数。

30

monTimer：タイマステートマシンに登録されるタイマ変数。タイマステートマシンは、本変数が0以外の時に1秒周期で1減算し、0になるとtimerExpをtrueに設定する。

【0108】

adminMonTimer：監視タイマとして設定された変数（R2.3では8固定）。

rxCompRslt：compStatistics関数の実行結果が格納される変数（受信パケットカウンタ）。

【0109】

txCompRslt：compStatistics関数の実行結果が格納される変数（送信パケットカウンタ）。

detectGuardTimes：保護回数連続障害検出判定用変数。

40

【0110】

adminGuardTimes：CLIにより指定された保護回数。

次に障害監視ステートマシン # 1 ~ # n における関数の定義を示す。

getStatistics（）：統計情報の受信パケットカウンタと送信パケットカウンタを参照し、その結果を、それぞれrxCount, txCountに格納する。

【0111】

compStatistics（）：prevRxCountとcurrRxCount / prevTxCountとcurrTxCountを比較し、その結果をそれぞれ、rxCompRslt / txCompRsltに格納する（一致したらtrueを一致しなかったらfalseを設定する）。

【0112】

50

failNotics () : LccOperStatusにfailureを設定する事によりポート状態ステートマシンに障害検出を通知する (rxFail / txFailは付加情報としてポート状態ステートマシンにより参照される) 。

【 0 1 1 3 】

recovNotics () : LccOperStatusにnormalを設定する事によりポート状態ステートマシンに障害復旧の検出を通知する。

制御パラメータ (送信) は、宛先MACアドレス、Ether Type、制御パケット送信間隔 (固定 : 3 秒) からなる。制御パラメータ (監視) は、監視タイマ (固定 : 8 秒とし、この時間送受信パケット数のどちらかが変化しない場合、障害と判定する) 。動作モード、保護回数からなる。

【 0 1 1 4 】

保守者への通知 (TRAP) は、障害を検出したことを通知する。このとき、付加情報として、障害検出ポートや障害種別 (Rx / Tx / RxTx) を通知する。また、TRAPにより、障害が復旧したことを通知し、このとき付加情報として、復旧検出ポートを通知する。

【 0 1 1 5 】

保守者への通知 (CLI) は、Link Connectivity Check (L C C) 機能に関する設定状態をコマンドにより、参照可能とする。または監視ポートの状態をコマンドにより、参照可能とする (ポート状態 : 正常 (normal) 、障害中 (failure) 、未知 (unknown) 、監視無効 (disable)) 。

【 0 1 1 6 】

フィルタリング条件は、受信制御パケットは障害監視用統計情報収集後、廃棄することとする。

以上説明したように、障害検出装置 1 0 は、マルチベンダ環境のキャリアネットワークにおけるリンクのサイレント障害の検出に有効であり、ネットワークの耐障害性の向上を図ることが可能になる。特に、障害検出装置 1 0 は、独自機能でありながら、他社装置に何ら変更を必要としないためキャリアにとって、マルチベンダ環境における導入を容易にする。

【 0 1 1 7 】

(付記 1) ネットワーク上の障害検出を行う障害検出装置において、
障害監視制御パケットを生成し、自装置と同一プロトコルで障害検出のための相互動作が不要な対向装置に対して、前記障害監視制御パケットを送信する障害監視制御パケット送信部と、

前記障害監視制御パケットの送信パケット数をカウントする送信パケットカウンタと、
前記対向装置から送信される制御パケットを受信して、受信パケット数をカウントする受信パケットカウンタと、

前記送信パケット数と前記受信パケット数を監視して、一定時間内に少なくともいずれか一方のパケット数に変化がなければ、障害発生と認識し、外部へ通知する障害検出部と、

を有することを特徴とする障害検出装置。

【 0 1 1 8 】

(付記 2) 前記障害監視制御パケット送信部は、装置内の上位レイヤの処理部に配置し、前記送信パケットカウンタは、装置内の前記対向装置と自装置が接続する物理レイヤまたはリンクレイヤの処理部に配置することで、前記障害検出部は、前記送信パケット数の監視を行って、前記上位レイヤと前記物理レイヤの処理部間の経路に発生する障害検出を保証することを特徴とする付記 1 記載の障害検出装置。

【 0 1 1 9 】

(付記 3) 前記受信パケットカウンタは、装置内の上位レイヤの処理部に配置することで、前記障害検出部は、前記受信パケット数の監視を行って、前記対向装置から前記上位レイヤの処理部までの経路に発生する障害検出を保証することを特徴とする付記 1 記載の障害検出装置。

10

20

30

40

50

【 0 1 2 0 】

(付記 4) 前記障害監視制御パケット送信部は、ユーザトラフィックが流れていないときであっても、誤った障害検出がされないように、ユーザトラフィックとは独立な前記障害監視制御パケットを常時一定間隔で送信することを特徴とする付記 1 記載の障害検出装置。

【 0 1 2 1 】

(付記 5) 前記障害監視制御パケット送信部は、前記対向装置で受信されたときに廃棄され、ペイロードに制御内容を含まない前記障害監視制御パケットを生成し送信することを特徴とする付記 4 記載の障害検出装置。

【 0 1 2 2 】

(付記 6) 自装置と前記対向装置とが、複数リンクを仮想的な 1 つのリンクとみなすリンク・アグリゲーションで接続している場合には、前記障害監視制御パケット送信部は、前記複数リンクの各リンクから前記障害監視制御パケットを送信し、前記送信パケットカウンタは、前記複数リンクのリンク毎に送信パケット数をカウントし、前記受信パケットカウンタは、前記複数リンクの各リンクから前記対向装置から送信された制御パケットを受信して、リンク毎に受信パケット数をカウントし、前記障害検出部は、リンク毎に障害検出を行うことを特徴とする付記 1 記載の障害検出装置。

【 0 1 2 3 】

(付記 7) ネットワーク上の障害検出を行う障害検出方法において、障害監視制御パケットを生成して、自装置と同一プロトコルで障害検出のための相互動作が不要な対向装置に対して、前記障害監視制御パケットを送信し、

前記障害監視制御パケットの送信パケット数を、送信パケットカウンタでカウントし、前記対向装置から送信される制御パケットを、受信パケットカウンタで受信して、受信パケット数をカウントし、

前記送信パケット数と前記受信パケット数を監視して、一定時間内に少なくともいずれか一方のパケット数に変化がなければ、障害発生と認識して外部へ通知することで、前記対向装置の側で障害の監視を認識することなく、自装置側のみで障害検出を行うことを特徴とする障害検出方法。

【 0 1 2 4 】

(付記 8) 装置内の上位レイヤの処理部で障害監視制御パケットの生成、送信を行い、前記送信パケットカウンタは、装置内の前記対向装置と自装置が接続する物理レイヤまたはリンクレイヤの処理部に配置することで、前記送信パケット数の監視により、前記上位レイヤと前記物理レイヤの処理部間の経路に発生する障害検出を保証することを特徴とする付記 7 記載の障害検出方法。

【 0 1 2 5 】

(付記 9) 前記受信パケットカウンタは、装置内の上位レイヤの処理部に配置することで、前記受信パケット数の監視により、前記対向装置から前記上位レイヤの処理部までの経路に発生する障害検出を保証することを特徴とする付記 7 記載の障害検出方法。

【 0 1 2 6 】

(付記 10) ユーザトラフィックが流れていないときであっても、誤った障害検出がされないように、ユーザトラフィックとは独立な前記障害監視制御パケットを常時一定間隔で送信することを特徴とする付記 7 記載の障害検出方法。

【 0 1 2 7 】

(付記 11) 前記対向装置で受信されたときに廃棄され、ペイロードに制御内容を含まない前記障害監視制御パケットを生成し送信することを特徴とする付記 10 記載の障害検出方法。

【 0 1 2 8 】

(付記 12) 自装置と前記対向装置とが、複数リンクを仮想的な 1 つのリンクとみなすリンク・アグリゲーションで接続している場合には、前記複数リンクの各リンクから前記障害監視制御パケットを送信し、前記送信パケットカウンタは、前記複数リンクのリン

10

20

30

40

50

ク毎に送信パケット数をカウントし、前記受信パケットカウンタは、前記複数リンクの各リンクから前記対向装置から送信された制御パケットを受信して、リンク毎に受信パケット数をカウントすることで、リンク毎に障害検出を行うことを特徴とする付記7記載の障害検出方法。

【図面の簡単な説明】

【0129】

【図1】障害検出装置の原理図である。

【図2】障害検出装置のブロック構成を示す図である。

【図3】装置間が1本のリンクで接続された際の障害検出動作を示すシーケンス図である

10

。【図4】装置間がLAで接続された際の障害検出動作を示すシーケンス図である。

【図5】障害検出装置の機能を有する通信装置の構成を示す図である。

【図6】障害監視制御パケットのフォーマットを示す図である。

【図7】ポート状態ステートマシンの状態遷移を示す図である。

【図8】ポート状態ステートマシンの状態遷移を示す図である。

【図9】障害監視ステートマシンの状態遷移を示す図である。

【図10】障害監視ステートマシンの状態遷移を示す図である。

【図11】ループによるネットワーク障害を説明するための図である。

【図12】ループによるネットワーク障害を説明するための図である。

【図13】ネットワーク障害検出の流れを示す図である。

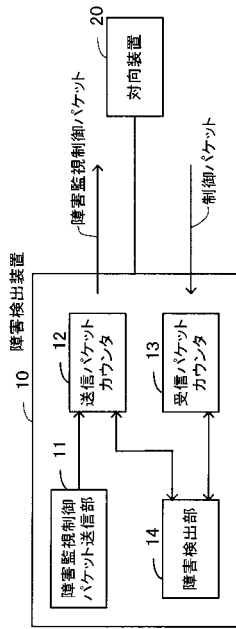
20

【符号の説明】

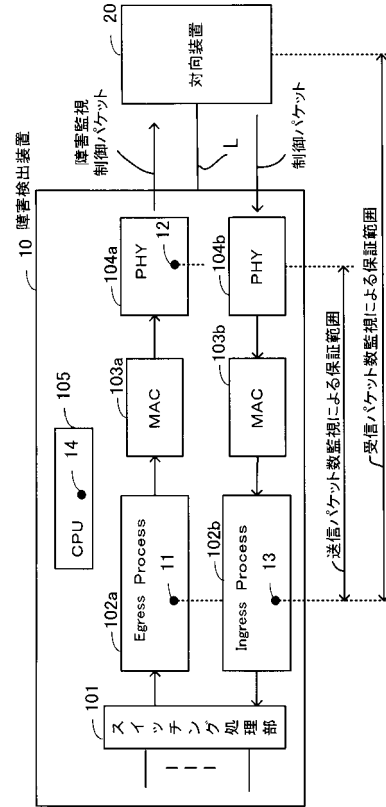
【0130】

- 10 障害検出装置
- 11 障害監視制御パケット送信部
- 12 送信パケットカウンタ
- 13 受信パケットカウンタ
- 14 障害検出部
- 20 対向装置

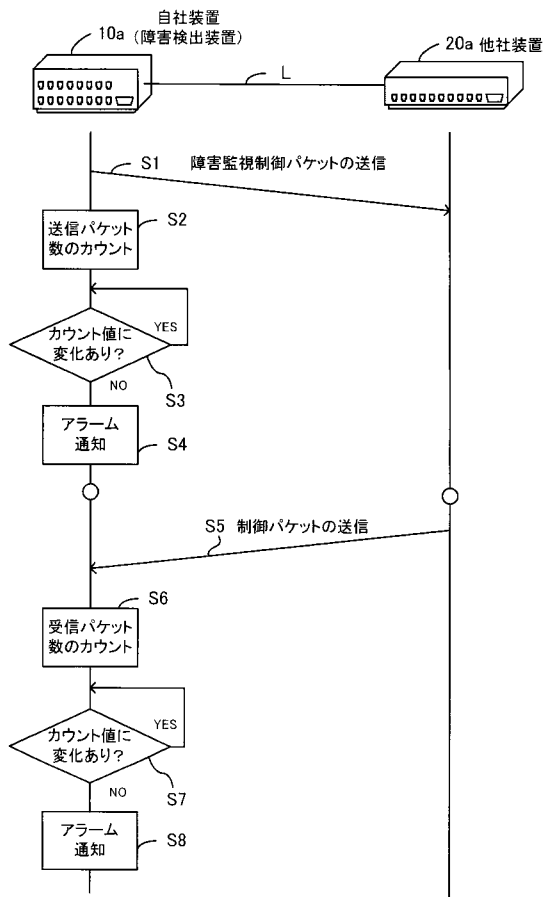
【図1】



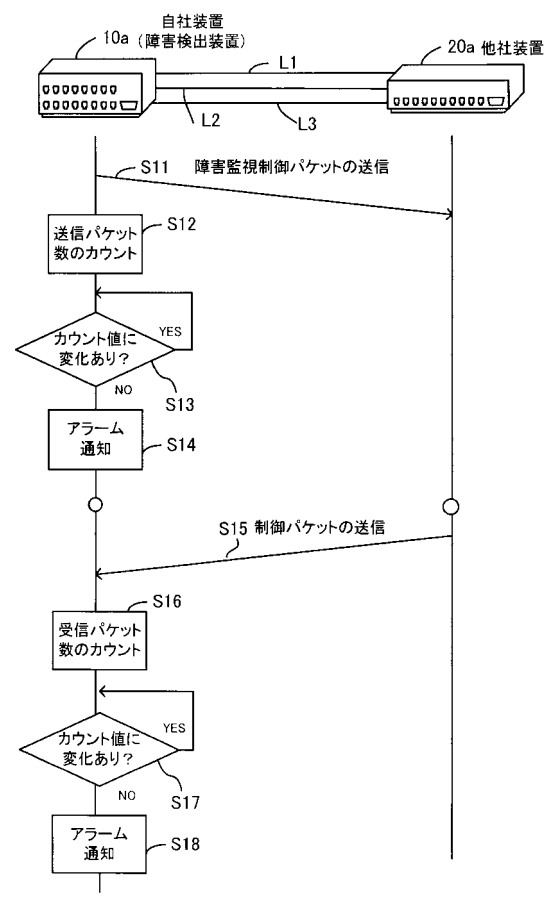
【図2】



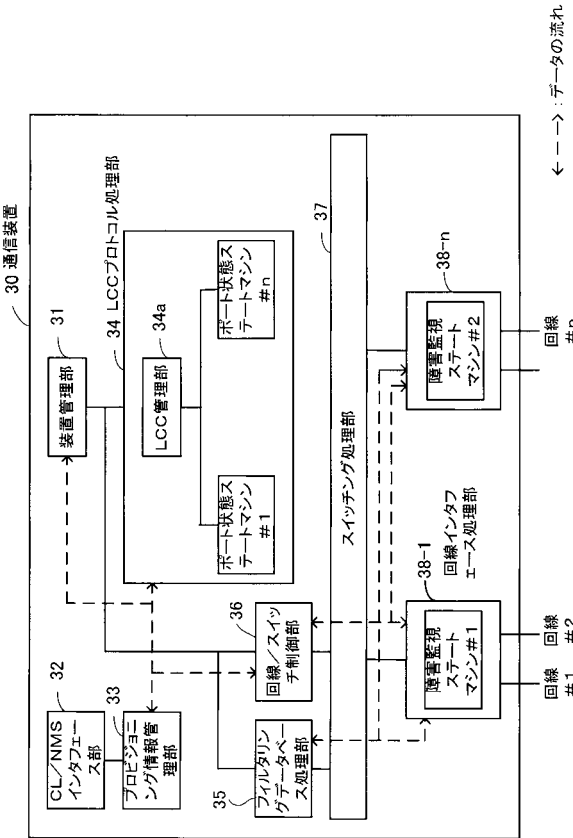
【図3】



【図4】



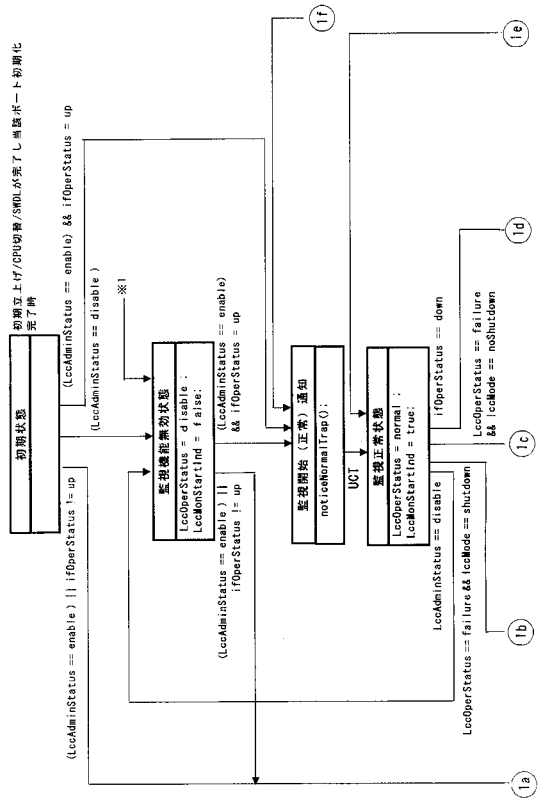
【 図 5 】



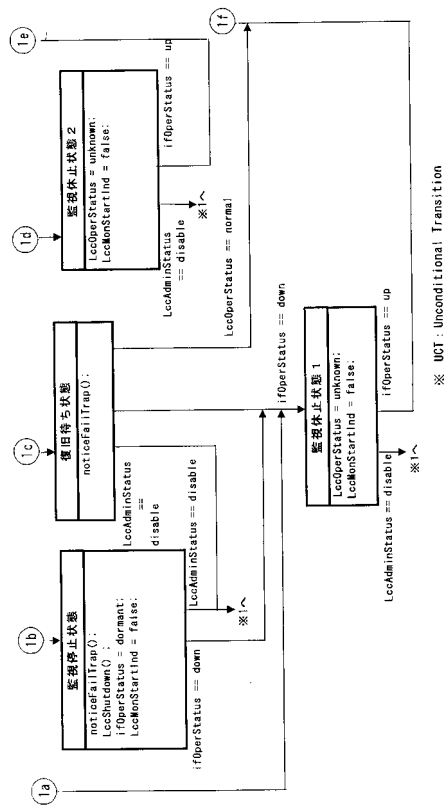
【 図 6 】

ヘッダ		ペイロード									
MAC DA	MAC SA	L/T	Sub Type	Flag	Code	TTL base	TTL	Sequence number	Slot ID	Port ID	Padding
6	6	2	1	1	2	1	1	2	1	1	36

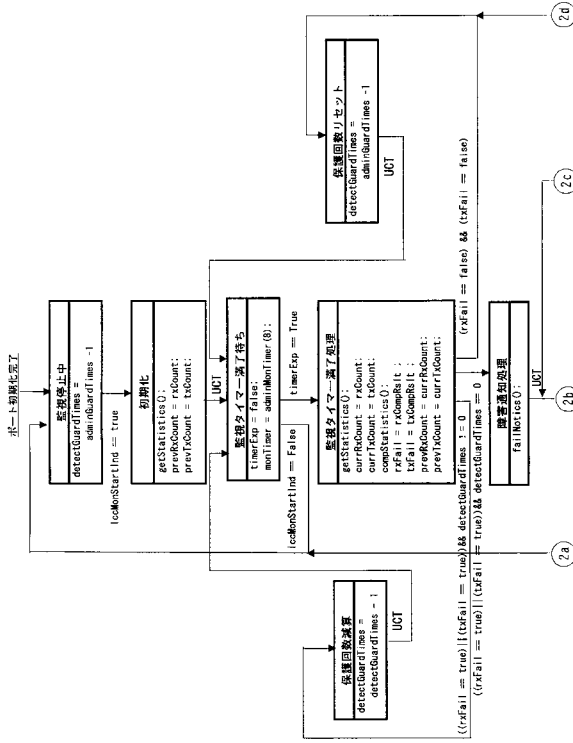
【 図 7 】



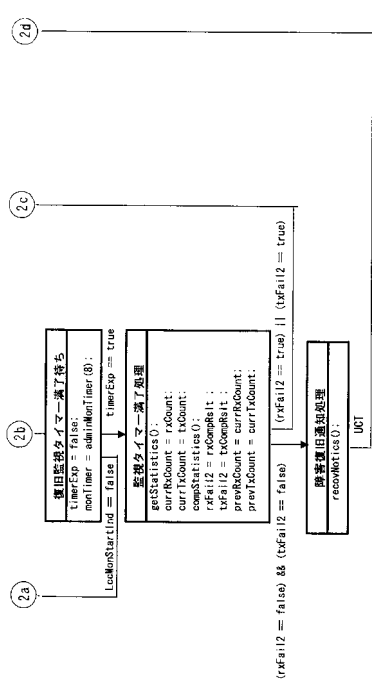
【 図 8 】



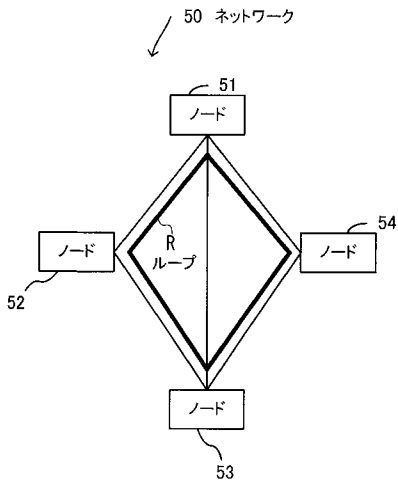
【図 9】



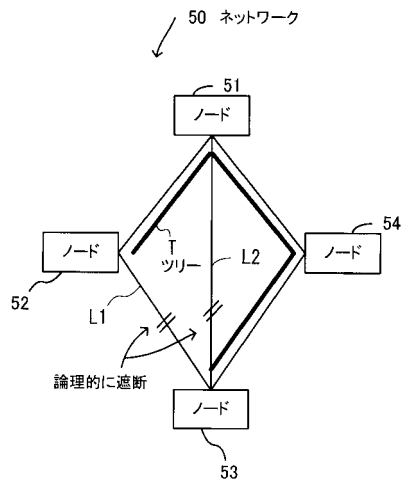
【図 10】



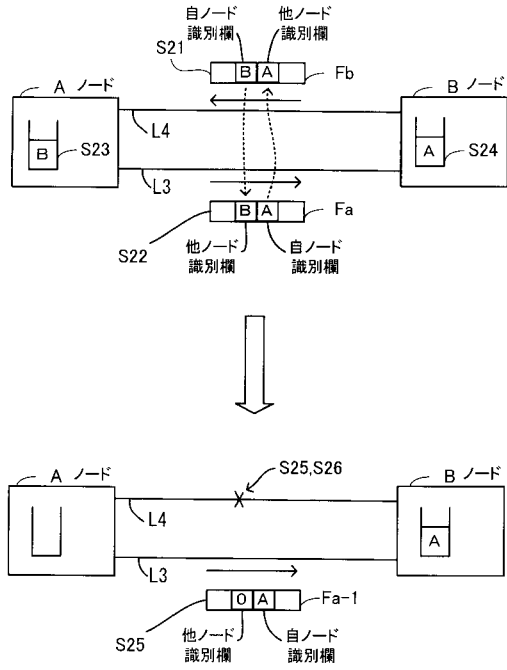
【図 11】



【図 12】



【図13】



フロントページの続き

(72)発明者 鷹取 孝

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

審査官 玉木 宏治

(56)参考文献 特開平09-130358(JP,A)

特開2005-033485(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/00-66

H04L 29/14