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

特許第4128974号
(P4128974)

(45)発行日　平成20年7月30日(2008.7.30)　(24)登録日　平成20年5月23日(2008.5.23)

(51)Int.Cl.　　F I
H04L 12/24 (2006.01)　　H04L 12/24
H04L 12/44 (2006.01)　　H04L 12/44　M

請求項の数 5　(全 38 頁)

(21)出願番号　特願2004-107481 (P2004-107481)
(22)出願日　平成16年3月31日 (2004.3.31)
(65)公開番号　特開2005-295209 (P2005-295209A)
(43)公開日　平成17年10月20日 (2005.10.20)
審査請求日　平成18年6月23日 (2006.6.23)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100090516
弁理士　松倉　秀実
(74)代理人　100113608
弁理士　平川　明
(74)代理人　100105407
弁理士　高田　大輔
(74)代理人　100089244
弁理士　遠山　勉

最終頁に続く

(54)【発明の名称】レイヤ２ループ検知システム

(57)【特許請求の範囲】
【請求項１】
複数のレイヤ２スイッチを有するレイヤ２ネットワークを監視対象とするＳＮＭＰマネージャによるレイヤ２ループ検知装置であって；
前記複数のレイヤ２スイッチからこれらレイヤ２スイッチのポートに関する情報を含むＭＩＢ情報をＳＮＭＰ通信により収集して、前記レイヤ２ネットワークの正常時のトポロジを認識する手段と；
スパニングツリープロトコルＳＴＰに則ってそれぞれ設定された、トラフィック遮断のためのブロッキングポート及びポート無能状態のディセーブルポートを前記トポロジ認識処理に基づいて識別する手段と；
識別した前記ブロッキングポート及び前記ディセーブルポートを監視ポイントにそれぞれ設定してその状態を定期的に監視する手段と；
前記ブロッキングポート及び前記ディセーブルポートのいずれかの状態が変動したときをトリガに前記複数のレイヤ２スイッチから前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集して、前記レイヤ２ネットワークのトポロジを再認識し、レイヤ２ループを検知する手段と；
を備えるレイヤ２ループ検知装置。
【請求項２】
前記監視ポイントの状態として、前記ブロッキングポート及び前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポート及び前記ディセーブルポートの

いずれかからトラフィックが転送されているときをトリガにレイヤ２ループを検知する；
請求項１記載のレイヤ２ループ検知装置。
【請求項３】
前記監視ポイントの状態として、前記ブロッキングポート及び前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポート及び前記ディセーブルポートのいずれかのポートステータスが変化したときをトリガにレイヤ２ループを検知する；
請求項１記載のレイヤ２ループ検知装置。
【請求項４】
前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集する際に、そのＭＩＢ情報を収集できない前記レイヤ２スイッチがある場合、そのレイヤ２スイッチに接続されたポートが全て指定ポートになっていることを検知することにより、前記レイヤ２ループ箇所を検知する；
請求項１記載のレイヤ２ループ検知装置。
【請求項５】
前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集する際に、リンクの両端がどちらも指定ポートになっているリンクを検知することにより、前記レイヤ２ループ箇所を推定する；
請求項１記載のレイヤ２ループ検知装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数のレイヤ２スイッチを有するレイヤ２ネットワークを監視対象とするＳＮＭＰマネージャによるレイヤ２ループの検知を可能にするレイヤ２ループ検知システムに関する。
【背景技術】
【０００２】
エンタープライズネットワーク等を構築するためのレイヤ２ネットワークにおいては、ループ（レイヤ２ループ）を排除してネットワークの冗長性を確保する一手法として、ＩＥＥＥ（Institute of Electrical and Electronic Engineers）８０２．１Ｄで標準化されているスパニングツリープロトコル（ＳＴＰ：Spanning Tree Protocol）を動作させる。
【０００３】
これはＭＡＣ（Media Access Control）フレームにはＩＰ（Internet Protocol）でいうところのＴＴＬ（Time to Live）に相当するものがないため、ネットワークがループしている箇所では、ＭＡＣフレームはそのまま巡回してしまうからである。
【０００４】
ＳＴＰは、隣接ノード（レイヤ２スイッチ）間でＢＰＤＵ（Bridge Protocol Data Unit）と呼ばれる監視用パケットを送受信し、ネットワークがループしている箇所を検知すると、ブロッキングポート（Blocking Port）と呼ばれるＭＡＣフレームを遮断するポート（トラフィック遮断ポート）を作成して、ループを論理的に遮断する。
【０００５】
上記ＳＴＰを利用した手法によりレイヤ２ループの発生は回避されるが、レイヤ２スイッチであるブリッジのＣＰＵ障害等のために、ＳＴＰが崩壊してしまう場合がある。ＳＴＰが崩壊してしまうと、ブロッキングポートが消失してしまうので、ループの発生を免れない。この結果、そのレイヤ２ネットワークは輻輳状態になってしまい、レスポンス低下またはメルトダウン等の障害に陥ったりすることもある。
【０００６】
このような障害に陥った場合に、ブリッジのログが上書きされたり、簡易ネットワーク管理プロトコル（ＳＮＭＰ：Simple Network Management Protocol）通信を利用するときはその通信が不可能になるため、障害箇所が特定できない事態も発生してしまう。

【特許文献１】特開平５－３１６１３６号公報
【特許文献２】特開２００２－３３５２５８号公報
【特許文献３】特表２００１－５０９６５７号公報
【特許文献４】特開２００２－１６４８９０号公報
【非特許文献１】http://www.nic.ad.jp/ja/materials/iw/2002/proceeding/T18-1.pdf
【発明の開示】
【発明が解決しようとする課題】
【０００７】
本発明の課題は、複数のレイヤ２スイッチを有するレイヤ２ネットワークを監視対象とするＳＮＭＰマネージャによりレイヤ２ループの検知を確実に可能にする手法（技術）を提供することにある。
【課題を解決するための手段】
【０００８】
上記課題を解決するために、本発明のレイヤ２ループ検知装置は、複数のレイヤ２スイッチを有するレイヤ２ネットワークを監視対象とするＳＮＭＰマネージャによるレイヤ２ループ検知装置であって；
前記複数のレイヤ２スイッチからこれらレイヤ２スイッチのポートに関する情報を含むＭＩＢ情報をＳＮＭＰ通信により収集して、前記レイヤ２ネットワークの正常時のトポロジを認識する手段と；
スパニングツリープロトコルＳＴＰに則ってそれぞれ設定された、トラフィック遮断のためのブロッキングポート及びポート無能状態のディセーブルポートを前記トポロジ認識処理に基づいて識別する手段と；
識別した前記ブロッキングポート及び前記ディセーブルポートを監視ポイントにそれぞれ設定してその状態を定期的に監視する手段と；
前記ブロッキングポート及び前記ディセーブルポートのいずれかの状態が変動したときをトリガに前記複数のレイヤ２スイッチから前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集して、前記レイヤ２ネットワークのトポロジを再認識し、レイヤ２ループを検知する手段とを備える。
【０００９】
この構成において、レイヤ２ループ検知装置は、前記監視ポイントの状態として、前記ブロッキングポート及び前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポート及び前記ディセーブルポートのいずれかからトラフィックが転送されているときをトリガにレイヤ２ループを検知する。
【００１０】
また、レイヤ２ループ検知装置は、前記監視ポイントの状態として、前記ブロッキングポート及び前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポート及び前記ディセーブルポートのいずれかのポートステータスが変化したときをトリガにレイヤ２ループを検知する。
【００１１】
また、レイヤ２ループ検知装置は、前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集する際に、そのＭＩＢ情報を収集できない前記レイヤ２スイッチがある場合、そのレイヤ２スイッチに接続されたポートが全て指定ポートになっていることを検知することにより、前記レイヤ２ループ箇所を検知する。
【００１２】
さらに、レイヤ２ループ検知装置は、前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集する際に、リンクの両端がどちらも指定ポートになっているリンクを検知することにより、前記レイヤ２ループ箇所を推定する。
【発明の効果】
【００１３】
本発明によれば、レイヤ２ネットワーク障害時に発生する工数及び人件費を大幅に削減

することが可能になる。また、障害を早急に復旧させること、障害発生を防止するといったことも可能となる。

【００１４】

また、本発明によれば、ＳＴＰが構築されているリンクのうち、あるリンクの両端のポートが指定ポートで対になっている箇所を特定することにより、障害箇所を特定することができる。

【００１５】

さらに、本発明によれば、ＳＮＭＰ通信の応答の無いレイヤ２スイッチと接続されている全ての対向のポートが指定ポートであることを特定することにより、障害箇所を特定することができる。

【００１６】

本発明の他の課題、特徴及び利点は、図面及び併記の特許請求の範囲とともに取り上げられる際に、以下に記載される明細書を読むことにより明らかになるであろう。

【発明を実施するための最良の形態】

【００１７】

以下、添付図面を参照して、本発明について更に詳細に説明する。図面には本発明の好ましい実施形態が示されている。しかし、本発明は、多くの異なる形態で実施されることが可能であり、本明細書に記載される実施形態に限定されると解釈されてはならない。むしろ、これらの実施形態は、本明細書の開示が徹底的かつ完全となり、当業者に本発明の範囲を十分に伝えるように提供される。

【００１８】

［第１の実施の形態］

（システム構成）

本発明の第１の実施の形態におけるシステムの構成を示す図１を参照すると、レイヤ２ループ検知システムＳＹＳは、簡易ネットワーク管理プロトコル（ＳＮＭＰ：Simple Network Management Protocol）のマネージャ・エージェント構造を持ち、ＩＰ(Internet Protocol)ネットワークとしてのイーサネットワーク（イーサネット：登録商標）などのローカルエリアネットワーク（ＬＡＮ：Local Area Network）１（１１，１２，１３，１４，１５）にそれぞれ接続されるＳＮＭＰマネージャ２及び複数のエージェント３（３１，３２，３３，３４）を備え、ネットワーク管理（監視）機能を有するシステムを構成する。

【００１９】

管理（監視）ステーション上のＳＮＭＰマネージャ（以下、単にマネージャと記載することもある）２は、厳密にはＳＮＭＰマネージャを搭載するパーソナルコンピータ（ＰＣ）などの装置であり、ここではレイヤ２（Ｌ２）ループ検知装置を構成する。ＳＮＭＰマネージャ２は、管理（監視）対象システムとしてのレイヤ２（Ｌ２）ネットワークＮＷ上のＬＡＮ１及び複数のエージェント３を監視する。このＳＮＭＰマネージャ２は、図２に詳細機能構成を示すように、トポロジ認識部２１、ポート識別部２２、ポーリング部２３、トリガ検出部２４、トポロジ再認識部２５、及び障害判別部２６を備える。

【００２０】

Ｌ２ネットワークＮＷを構成する複数のエージェント３は、厳密にはエージェントを搭載する装置であり、ここではレイヤ２（Ｌ２）スイッチとしてのブリッジ（１～４）３１，３２，３３，３４に対応する。ブリッジ３１及びブリッジ３２はＬＡＮ１１、ブリッジ３２及びブリッジ３３はＬＡＮ１２、ブリッジ３３及びブリッジ３４はＬＡＮ１３、及びブリッジ３４及びブリッジ３１はＬＡＮ１４によってそれぞれ物理的に接続されている。また、ブリッジ３１はＳＮＭＰマネージャ２とＬＡＮ１５によって物理的に接続されている。ただし、ブリッジ３２及びブリッジ３３は、後に詳述するように、ＬＡＮ１２を通して論理的には接続されていない状態である。

【００２１】

このレイヤ２ループ検知システムＳＹＳにおけるマネージャ２はブリッジ３１に接続さ

れているＬＡＮ１５上に配置されているが、ＬＡＮ１５に接続される他のＩＰネットワークに収容されている形態でもよい。

【００２２】

（システム動作／レイヤ２ループ検知処理）

次に、図１に示す本発明の第１の実施の形態のレイヤ２ループ検知システムＳＹＳにおける動作例を図１、図２、図３、及び図４を併用して説明する。

【００２３】

上述したようなマネージャ・エージェント構造を持つこのレイヤ２ループ検知システムＳＹＳにおいては、ＳＮＭＰはＵＤＰ(User Datagram Protocol)上で動作するネットワーク管理のための管理ステーションと管理対象システムとの間における管理情報の交換プロトコルである。この第１の実施の形態のシステムＳＹＳのＳＮＭＰでは、管理ステーション上のＳＮＭＰマネージャ２からの処理要求（コマンド）に対して、管理対象システムであるＬ２ネットワークＮＷ上のブリッジ３１～３４が管理情報（レスポンス）をマネージャ２に通知する。

【００２４】

このような要求・応答に基づくトポロジ認識部２１の機能により、ＳＮＭＰマネージャ２は、監視対象ブリッジ３１～３４のＩＰアドレス、つまりＳＮＭＰ通信したいブリッジを指定する際に使用するアドレスと、監視対象ブリッジ３１～３４のＣｏｍｍｕｎｉｔｙＳｔｒｉｎｇ、つまりブリッジとＳＮＭＰ通信を行うための文字列（パスワード）とを予め取得する。図１及び図４中に例示するように、ブリッジ３１～３４のＩＰアドレスは、１９２．１６８．１０．１０、１９２．１６８．１０．３０、１９２．１６８．１０．４０、１９２．１６８．１０．２０である。

【００２５】

また、マネージャ２とブリッジ３１～３４間では、ＳＮＭＰメッセージの交換という形態で要求・応答を行うが、ＳＮＭＰに則ったメッセージのうちの自律メッセージとしてのトラップ（ＴＲＡＰ）は、ブリッジ３１～３４からマネージャ２に自律的に（単方向に）送信するＵＤＰのメッセージであり、ＬＡＮ１１～１４の状態（輻輳や障害等）やブリッジ３１～３４の状態等を通知するために使用される。この自律メッセージ・ＴＲＡＰの利用については後に詳述する。

【００２６】

エンタープライズネットワーク等を構築するためのＬ２ネットワークＮＷにおいては、ＭＡＣ（Media Access Control）フレームが巡回してしまうループ（レイヤ２ループ）を排除してネットワークの冗長性を確保する一手法として、ＩＥＥＥ８０２．１Ｄで標準化されているスパニングツリープロトコル（ＳＴＰ：Spanning Tree Protocol）を動作させる。

【００２７】

ＳＴＰは、Ｌ２スイッチであるブリッジ３１～３４間でＢＰＤＵ（Bridge Protocol Data Unit）と呼ばれる監視用パケットを送受信し、ネットワークがループしている箇所を検知すると、ブロッキングポート（ＢＰ：Blocking Port）と呼ばれるＭＡＣフレームを遮断するポート（トラフィック遮断ポート）を作成して、ループを論理的に遮断する。これにより、Ｌ２ループの発生を回避することができる。

【００２８】

また、ＳＴＰは、ルートブリッジと呼ばれる１つのブリッジをルート（根）としたツリー（木）構造のネットワーク構成（トポロジ）を作成するプロトコルである。Ｌ２ネットワークＮＷは、ＳＴＰに則ってブリッジ３１～３４間でＣｏｎｆｉｇｕｒａｔｉｏｎＢＰＤＵを送受信して、ルートブリッジを決定する。

【００２９】

Ｌ２ネットワークＮＷにおいてＳＴＰを動作させることにより、各ブリッジ３２～３４のルートブリッジ（ブリッジ３１）、つまり根に近いポートが１つだけルートポート（ＲＰ：Root Port）になる。また、各ＬＡＮ１１～１４で一番ルートパスコスト（Root Path

Cost）が小さいポートがそのＬＡＮの指定（選定）ポート（ＤＰ：Designated Port）となる。ルートブリッジのポートは、ルートパスコストが０であるので、全て指定ポートＤＰとなる。

【００３０】

ルートポートＲＰ及び指定ポートＤＰはＦｏｒｗａｒｄｉｎｇ、またそれ以外のポートはＢｌｏｃｋｉｎｇというポートステータス（ステート）となる。

【００３１】

この結果、Ｌ２ネットワークＮＷにおいては、ブリッジ３１はその第１のポート及び第２のポートを指定ポートＤＰとするルートブリッジとなる。なお、図１中、ポート番号は丸付き数字で示している。また、ブリッジ３２，３３，３４の第１のポートはそれぞれルートポートＲＰとなり、ブリッジ３２，３４の第２のポートはそれぞれ指定ポートＤＰとなる。ブリッジ３３の第２のポートは本来指定ポートＤＰであるが、Ｌ２ループの発生を回避するためにブロッキングポート（１）ＢＰとなる。

【００３２】

ＳＮＭＰマネージャ２のトポロジ認識部２１は、監視対象のＬ２ネットワークＮＷを構成するブリッジ３１～３４からのＭＩＢ（Management Information Base）情報をブリッジ（第３のポート）３１及びＬＡＮ１５を介して、ＳＮＭＰ通信により収集する。

【００３３】

ここで、トポロジ認識部２１により収集されるＭＩＢ情報は、次の（１）～（１０）のスクリプト言語で表され、ブリッジ３１～３４間を接続するポートに関する情報を含んでいる。

（１）ｄｏｔ１ｄＳｔｐＰｒｉｏｒｉｔｙ：ＳＮＭＰ通信対象ブリッジのプライオリティ

（２）ｄｏｔ１ｄＢａｓｅＢｒｉｄｇｅＡｄｄｒｅｓｓ：ＳＮＭＰ通信対象ブリッジのＭＡＣアドレス

（３）ｄｏｔ１ｄＳｔｐＰｏｒｔ：ＳＮＭＰ通信対象ブリッジ内でＳＴＰに所属するポートＩＤ

（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅ：上記ポートのステータス。このステータスの値は、１：Ｄｉｓａｂｌｅ、２：Ｂｌｏｃｋｉｎｇ、３：Ｌｉｓｔｅｎｉｎｇ、４：Ｌｅａｒｎｉｎｇ、５：Ｆｏｒｗａｒｄｉｎｇのいずれかである。

（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔ：ＳＮＭＰ通信対象ブリッジにおけるルートポートＩＤ

（６）ｄｏｔ１ｄＳｔｐＰｏｒｔＤｅｓｉｇｎａｔｅｄＲｏｏｔ：ＳＮＭＰ通信対象のポートが所属するＳＴＰのルートブリッジＩＤ

（７）ｄｏｔ１ｄＳｔｐＰｏｒｔＤｅｓｉｇｎａｔｅｄＢｒｉｄｇｅ：ＳＮＭＰ通信対象のポートにおけるＤｅｓｉｇｎａｔｅｄブリッジＩＤ

（８）ｄｏｔ１ｄＳｔｐＰｏｒｔＤｅｓｉｇｎａｔｅｄＰｏｒｔ：ＳＮＭＰ通信対象のポートにおけるＤｅｓｉｇｎａｔｅｄポートＩＤ

（９）ｉｆＩｎＯｃｔｅｔｓ：ＳＮＭＰ通信対象のポートにおける受信した総バイト数

（１０）ｉｆＯｕｔＯｃｔｅｔｓ：ＳＮＭＰ通信対象のポートにおける送信した総バイト数

また、トポロジ認識部２１により収集されたＭＩＢ情報の一覧を図４に示す。トポロジ認識部２１は、収集したＭＩＢ情報を図４に示すように、ブリッジ３１～３４のＩＰアドレス及びポート番号をキー情報として、図示省略の記憶部（ハードディスク）に格納する。

トポロジ認識部２１は、収集したＭＩＢ情報に基づき、（７）ｄｏｔ１ｄＳｔｐＰｏｒｔＤｅｓｉｎａｔｅｄＢｒｉｄｇｅ及び（８）ｄｏｔ１ｄＳｔｐＰｏｒｔＤｅｓｉｇｎａｔｅｄＰｏｒｔの値が等しいブリッジのポート同士が隣接していると解析する。

【００３４】

また、トポロジ認識部２１は、（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅに基づいて、ブリッジ３１～３４の各ポートのＳＴＰのステータスを把握する。その内、Ｆｏｒｗａ

ｒｄｉｎｇステータス「５」については、（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔで示されたポート番号「１」のポートはルートポートＲＰと解析され、そうでなければ指定ポートＤＰであると解析される。トポロジ認識部２１は、これらの処理により、Ｌ２ネットワークＮＷのトポロジを解析する。

【００３５】

次に、ポート識別部２２は、トポロジ認識部２１によるトポロジ認識処理で得られた各ポートのＳＴＰのステータス「２」からブロッキングポート（１）ＢＰを識別し、このブロッキングポート（１）ＢＰを監視ポイントに設定する。この例では、ブリッジ３３の第２のポートが監視ポイントに設定される。

【００３６】

ポーリング部２３は、設定された監視ポイント対応のブロッキングポート（１）ＢＰのＭＩＢ情報を定期的（周期的に）に監視して収集し、変動状態をトリガ検出部２４に伝える。トリガ検出部２４は、ポーリング部２３からブロッキングポート（１）ＢＰのＭＩＢ情報の変化が入力された場合、これをトリガ（契機）に障害発生を認識して、トポロジ再認識部２５に伝える。

【００３７】

トリガ検出部２４から障害発生を入力されたトポロジ再認識部２５は、監視対象のＬ２ネットワークＮＷのブリッジ３１～３４からＭＩＢ情報（ここでは、（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅ、（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔ、（９）ｉｆＩｎＯｃｔｅｔｓ）を再度取得し、各ポートのＳＴＰのステータスを更新することによってトポロジを再び解析し、Ｌ２ループを検知する。

【００３８】

このＬ２ループの検知をトポロジ再認識部２５から入力された障害判別部２６は、Ｌ２ネットワークＮＷにおける障害発生を認識する。

【００３９】

次に、ＳＮＭＰマネージャ２のポーリング部２３及びトリガ検出部２４による処理を一層具体的に説明する。

【００４０】

上述した一連のＬ２ループ検知処理において、ポーリング部２３は、監視ポイント対応のブロッキングポート（１）ＢＰを定期監視するためのＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を収集することで、ブロッキングポート（１）ＢＰからトラフィック（パケット）がＳＮＭＰマネージャ２で予め決めた任意の閾値以上、転送された場合に、障害発生のトリガとするように変動状態をトリガ検出部２４に伝える。これにより、トリガ検出部２４は、これをトリガに障害発生を認識して、トポロジ再認識部２５に伝える。なお、この閾値はＬ２ネットワークＮＷの正常時にブロッキングポート（１）ＢＰから出力されているトラフィックがトリガにかからないように設定する必要がある。

【００４１】

また、上述した一連のＬ２ループ検知処理において、ポーリング部２３は、監視ポイント対応のブロッキングポート（１）ＢＰを定期監視するためのＭＩＢ情報として（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅの値を収集することで、ブロッキングポート（１）ＢＰのポートステータスがＢｌｏｃｋｉｎｇから変化した場合に、障害発生のトリガとするように変動状態をトリガ検出部２４に伝える。これにより、トリガ検出部２４は、これをトリガに障害発生を認識して、トポロジ再認識部２５に伝える。

【００４２】

さらに、上述した一連のＬ２ループ検知処理において、ポーリング部２３及びトリガ検出部２４は、監視ポイント対応のブロッキングポート（１）ＢＰを定期監視するためのＭＩＢ情報の変化以外をトリガとして、Ｌ２ネットワークＮＷの障害発生を認識することも可能である。

【００４３】

具体的には、ポーリング部２３及びトリガ検出部２４は、各ブリッジ３１～３４が送信

する自律メッセージ・ＴＲＡＰの内のトポロジチェンジトラップ：ｔｏｐｏｌｏｇｙＣｈａｎｇｅ　ｔｒａｐの受信をトリガとして障害発生を認識する。このトポロジチェンジトラップは、各ブリッジ３１～３４においてポートステータスがＬｅａｒｎｉｎｇからＦｏｒｗａｒｄｉｎｇに、またＦｏｒｗａｒｄｉｎｇからＢｌｏｃｋｉｎｇに変化した際に発生される。

【００４４】

また、ポーリング部２３及びトリガ検出部２４は、各ブリッジ３１～３４が送信する自律メッセージ・ＴＲＡＰの内のニュールートトラップ：ｎｅｗＲｏｏｔ　ｔｒａｐの受信をトリガとして障害発生を認識する。このニュールートトラップは、各ブリッジにおいて新たなルートポートＲＰが選出された際に発生される。

【００４５】

［第２の実施の形態］

（システム構成）

本発明の第２の実施の形態におけるシステムの構成を示す図５を参照すると、レイヤ２ループ検知システムＳＹＳは、上述した第１の実施の形態のシステムＳＹＳと同様に、ＳＮＭＰのマネージャ・エージェント構造を持ち、ＩＰネットワークとしてのイーサネットワーク（イーサネット：登録商標）などのローカルエリアネットワーク（ＬＡＮ）１（１１，１２，１３，１４，１５）にそれぞれ接続されるＳＮＭＰマネージャ２及び複数のエージェント３（３１，３２，３３，３４）を備え、ネットワーク管理（監視）機能を有するシステムを構成する。

【００４６】

管理（監視）ステーション上のＳＮＭＰマネージャ２は、厳密にはＳＮＭＰマネージャを搭載するパーソナルコンピータ（ＰＣ）などの装置であり、ここではＬ２ループ検知装置を構成する。ＳＮＭＰマネージャ２は、管理（監視）対象システムとしてのＬ２ネットワークＮＷ上のＬＡＮ１及び複数のエージェント３を監視する。このＳＮＭＰマネージャ２は、図２に詳細機能構成を示すように、トポロジ認識部２１、ポート識別部２２、ポーリング部２３、トリガ検出部２４、トポロジ再認識部２５、及び障害判別部２６を備える。

【００４７】

Ｌ２ネットワークＮＷを構成する複数のエージェント３は、厳密にはエージェントを搭載する装置であり、ここではＬ２スイッチとしてのブリッジ（１～４）３１，３２，３３，３４に対応する。ブリッジ３１及びブリッジ３２はＬＡＮ１１、ブリッジ３２及びブリッジ３３はＬＡＮ１２、ブリッジ３３及びブリッジ３４はＬＡＮ１３、及びブリッジ３４及びブリッジ３１はＬＡＮ１４によってそれぞれ物理的に接続されている。また、ブリッジ３１はＳＮＭＰマネージャ２とＬＡＮ１５によって物理的に接続されている。ただし、ブリッジ３２及びブリッジ３３は、後に詳述するように、ＬＡＮ１２を通して論理的には接続されていない状態である。

【００４８】

このレイヤ２ループ検知システムＳＹＳにおけるマネージャ２はブリッジ３１に接続されているＬＡＮ１５上に配置されているが、ＬＡＮ１５に接続される他のＩＰネットワークに収容されている形態でもよい。

【００４９】

（システム動作／レイヤ２ループ検知処理）

次に、図５に示す本発明の第２の実施の形態のレイヤ２ループ検知システムＳＹＳにおける動作例を図２、図５、図６、及び図７を併用して説明する。

【００５０】

上述したようなマネージャ・エージェント構造を持つこのレイヤ２ループ検知システムＳＹＳにおいては、ＳＮＭＰはＵＤＰ上で動作するネットワーク管理のための管理ステーションと管理対象システムとの間における管理情報の交換プロトコルである。この第２の実施の形態のシステムＳＹＳのＳＮＭＰでは、管理ステーション上のＳＮＭＰマネージャ

２からの処理要求（コマンド）に対して、管理対象システムであるＬ２ネットワークＮＷ上のブリッジ３１～３４が管理情報（レスポンス）をマネージャ２に通知する。

【００５１】

このような要求・応答に基づくトポロジ認識部２１の機能により、ＳＮＭＰマネージャ２は、監視対象ブリッジ３１～３４のＩＰアドレス、つまりＳＮＭＰ通信したいブリッジを指定する際に使用するアドレスと、監視対象ブリッジ３１～３４のＣｏｍｍｕｎｉｔｙＳｔｒｉｎｇ、つまりブリッジとＳＮＭＰ通信を行うための文字列（パスワード）とを予め取得する。図５及び図７中に例示するように、ブリッジ３１～３４のＩＰアドレスは、１９２．１６８．１０．１０、１９２．１６８．１０．３０、１９２．１６８．１０．４０、１９２．１６８．１０．２０である。

【００５２】

また、マネージャ２とブリッジ３１～３４間では、ＳＮＭＰメッセージの交換という形態で要求・応答を行うが、ＳＮＭＰに則ったメッセージのうちの自律メッセージとしてのトラップ（ＴＲＡＰ）は、ブリッジ３１～３４からマネージャ２に自律的に（単方向に）送信するＵＤＰのメッセージであり、ＬＡＮ１１～１４の状態（輻輳や障害等）やブリッジ３１～３４の状態等を通知するために使用される。この自律メッセージ・ＴＲＡＰの利用については後に詳述する。

【００５３】

エンタープライズネットワーク等を構築するためのＬ２ネットワークＮＷにおいては、ＭＡＣフレームが巡回してしまうループ（レイヤ２ループ）を排除してネットワークの冗長性を確保する一手法として、ＩＥＥＥ８０２．１Ｄで標準化されているスパニングツリープロトコル（ＳＴＰ）を動作させる。

【００５４】

ＳＴＰは、Ｌ２スイッチであるブリッジ３１～３４間でＢＰＤＵと呼ばれる監視用パケットを送受信し、ネットワークがループしている箇所を検知すると、ブロッキングポート（ＢＰ）と呼ばれるＭＡＣフレームを遮断するポート（トラフィック遮断ポート）を作成して、ループを論理的に遮断する。これにより、Ｌ２ループの発生を回避することができる。

【００５５】

また、ＳＴＰは、ルートブリッジと呼ばれる１つのブリッジをルート（根）としたツリー（木）構造のネットワーク構成（トポロジ）を作成するプロトコルである。Ｌ２ネットワークＮＷは、ＳＴＰに則ってブリッジ３１～３４間でＣｏｎｆｉｇｕｒａｔｉｏｎＢＰＤＵを送受信して、ルートブリッジを決定する。

【００５６】

Ｌ２ネットワークＮＷにおいてＳＴＰを動作させることにより、各ブリッジ３２～３４のルートブリッジ（ブリッジ３１）、つまり根に近いポートが１つだけルートポート（ＲＰ）になる。また、各ＬＡＮ１１～１４で一番ルートパスコストが小さいポートがそのＬＡＮの指定ポート（ＤＰ）となる。ルートブリッジのポートは、ルートパスコストが０であるので、全て指定ポートＤＰとなる。

【００５７】

ルートポートＲＰ及び指定ポートＤＰはＦｏｒｗａｒｄｉｎｇ、またそれ以外のポートはＢｌｏｃｋｉｎｇまたはＤｉｓａｂｌｅというポートステータス（ステート）となる。

【００５８】

この結果、Ｌ２ネットワークＮＷにおいては、ブリッジ３１はその第１のポート及び第２のポートを指定ポートＤＰとするルートブリッジとなる。なお、図５中、ポート番号は丸付き数字で示している。また、ブリッジ３２，３３，３４の第１のポートはそれぞれルートポートＲＰとなり、ブリッジ３４の第２のポートは指定ポートＤＰとなる。ブリッジ３３の第２のポートは、本来Ｌ２ループの発生を回避するためにブロッキングポートＢＰとなるが、この例ではブリッジ３２の第２のポートと共に、ディセーブルポート（ＤｉｓＰ：Disable Port）である。

【００５９】
ＳＮＭＰマネージャ２のトポロジ認識部２１は、監視対象のＬ２ネットワークＮＷを構成するブリッジ３１～３４からのＭＩＢ情報をブリッジ（第３のポート）３１及びＬＡＮ１５を介して、ＳＮＭＰ通信により収集する。トポロジ認識部２１により収集されるＭＩＢ情報は、第１の実施の形態と同様に上記（１）～（１０）である。
【００６０】
また、トポロジ認識部２１により収集されたＭＩＢ情報の一覧を図７に示す。トポロジ認識部２１は、収集したＭＩＢ情報を図７に示すように、ブリッジ３１～３４のＩＰアドレス及びポート番号をキー情報として、図示省略の記憶部（ハードディスク）に格納する。
【００６１】
トポロジ認識部２１は、収集したＭＩＢ情報に基づき、（７）ｄｏｔ１ｄＳｔｐＰｏｒｔＤｅｓｉｎａｔｅｄＢｒｉｄｇｅ及び（８）ｄｏｔ１ｄＳｔｐＰｏｒｔＤｅｓｉｇｎａｔｅｄＰｏｒｔの値が等しいブリッジのポート同士が隣接していると解析する。
【００６２】
また、トポロジ認識部２１は、（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅに基づいて、ブリッジ３１～３４の各ポートのＳＴＰのステータスを把握する。その内、Ｆｏｒｗａｒｄｉｎｇステータス「５」については、（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔで示されたポート番号「１」のポートはルートポートＲＰと解析され、そうでなければ指定ポートＤＰであると解析される。トポロジ認識部２１は、これらの処理により、Ｌ２ネットワークＮＷのトポロジを解析する。
【００６３】
次に、ポート識別部２２は、トポロジ認識部２１によるトポロジ認識処理で得られた各ポートのＳＴＰのステータス「２」からブロッキングポートＢＰを識別するが、このＬ２ネットワークＮＷの構成ではブロッキングポートＢＰが存在しないので、ポートステータス「１」から無能ポートを示すディセーブルポート（１，２）ＤｉｓＰを識別して、これらを監視ポイントに設定する。この例では、ブリッジ３２，３３の第２のポートがそれぞれ監視ポイントに設定される。
【００６４】
ポーリング部２３は、設定された監視ポイント対応のディセーブルポート（１，２）ＤｉｓＰのＭＩＢ情報を定期的（周期的に）に監視して収集し、変動状態をトリガ検出部２４に伝える。トリガ検出部２４は、ポーリング部２３からディセーブルポート（１，２）ＤｉｓＰのいずれかのＭＩＢ情報の変化が入力された場合、これをトリガ（契機）に障害発生を認識して、トポロジ再認識部２５に伝える。
【００６５】
トリガ検出部２４から障害発生を入力されたトポロジ再認識部２５は、監視対象のＬ２ネットワークＮＷのブリッジ３１～３４からＭＩＢ情報（ここでは、（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅ、（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔ、（９）ｉｆＩｎＯｃｔｅｔｓ）を再度取得し、各ポートのＳＴＰのステータスを更新することによってトポロジを再び解析し、Ｌ２ループを検知する。
【００６６】
このＬ２ループの検知をトポロジ再認識部２５から入力された障害判別部２６は、Ｌ２ネットワークＮＷにおける障害発生を認識する。
【００６７】
次に、ＳＮＭＰマネージャ２のポーリング部２３及びトリガ検出部２４による処理を一層具体的に説明する。
【００６８】
上述した一連のＬ２ループ検知処理において、ポーリング部２３は、監視ポイント対応のディセーブルポート（１，２）ＤｉｓＰを定期監視するためのＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を収集することで、ディセーブルポート（１，２）Ｄｉｓ

Ｐのいずれかからトラフィック（パケット）が転送された場合に、障害発生のトリガとするように変動状態をトリガ検出部２４に伝える。これにより、トリガ検出部２４は、これをトリガに障害発生を認識して、トポロジ再認識部２５に伝える。また、トラフィック量は前回との差分をポーリング部２３によって計算することにより求める。

【００６９】

また、上述した一連のＬ２ループ検知処理において、ポーリング部２３は、監視ポイント対応のディセーブルポート（１，２）ＤｉｓＰを定期監視するためのＭＩＢ情報として（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅの値を収集することで、ディセーブルポート（１，２）ＤｉｓＰのポートステータスがＤｉｓａｂｌｅから変化した場合に、障害発生のトリガとするように変動状態をトリガ検出部２４に伝える。これにより、トリガ検出部２４は、これをトリガに障害発生を認識して、トポロジ再認識部２５に伝える。

【００７０】

さらに、上述した一連のＬ２ループ検知処理において、ポーリング部２３及びトリガ検出部２４は、監視ポイント対応のディセーブルポート（１，２）ＤｉｓＰを定期監視するためのＭＩＢ情報の変化以外をトリガとして、Ｌ２ネットワークＮＷの障害発生を認識することも可能である。

【００７１】

具体的には、ポーリング部２３及びトリガ検出部２４は、各ブリッジ３１～３４が送信する自律メッセージ・ＴＲＡＰの内のトポロジチェンジトラップ：ｔｏｐｏｌｏｇｙＣｈａｎｇｅ　ｔｒａｐの受信をトリガとして障害発生を認識する。このトポロジチェンジトラップは、各ブリッジ３１～３４においてポートステータスがＬｅａｒｎｉｎｇからＦｏｒｗａｒｄｉｎｇに、またＦｏｒｗａｒｄｉｎｇからＢｌｏｃｋｉｎｇに変化した際に発生される。

【００７２】

また、ポーリング部２３及びトリガ検出部２４は、各ブリッジ３１～３４が送信する自律メッセージ・ＴＲＡＰの内のニュールートトラップ：ｎｅｗＲｏｏｔ　ｔｒａｐの受信をトリガとして障害発生を認識する。このニュールートトラップは、各ブリッジにおいて新たなルートポートＲＰが選出された際に発生される。

【００７３】

［第３の実施の形態］

（システム構成）

本発明の第３の実施の形態におけるシステムの構成を示す図８を参照すると、レイヤ２ループ検知システムＳＹＳは、上述した第１の実施の形態のシステムＳＹＳと同様に、ＳＮＭＰのマネージャ・エージェント構造を持ち、ＩＰネットワークとしてのイーサネットワーク（イーサネット：登録商標）などのローカルエリアネットワーク（ＬＡＮ）１（１１，１２，１３，１４，１５）にそれぞれ接続されるＳＮＭＰマネージャ２及び複数のエージェント３（３１，３２，３３，３４）を備え、ネットワーク管理（監視）機能を有するシステムを構成する。

【００７４】

管理（監視）ステーション上のＳＮＭＰマネージャ２は、厳密にはＳＮＭＰマネージャを搭載するパーソナルコンピータ（ＰＣ）などの装置であり、ここではＬ２ループ検知装置を構成する。ＳＮＭＰマネージャ２は、管理（監視）対象システムとしてのＬ２ネットワークＮＷ上のＬＡＮ１及び複数のエージェント３を監視する。このＳＮＭＰマネージャ２は、図２に詳細機能構成を示すように、トポロジ認識部２１、ポート識別部２２、ポーリング部２３、トリガ検出部２４、トポロジ再認識部２５、及び障害判別部２６を備える。

【００７５】

Ｌ２ネットワークＮＷを構成する複数のエージェント３は、厳密にはエージェントを搭載する装置であり、ここではＬ２スイッチとしてのブリッジ（１～４）３１，３２，３３，３４に対応する。ブリッジ３１及びブリッジ３２はＬＡＮ１１、ブリッジ３２及びブリ

ッジ３３はＬＡＮ１２、ブリッジ３３及びブリッジ３４はＬＡＮ１３、及びブリッジ３４及びブリッジ３１はＬＡＮ１４によってそれぞれ物理的に接続されている。また、ブリッジ３１はＳＮＭＰマネージャ２とＬＡＮ１５によって物理的に接続されている。ただし、ブリッジ３２及びブリッジ３３は、後に詳述するように、ＬＡＮ１２を通して論理的には接続されていない状態である。

【００７６】

このレイヤ２ループ検知システムＳＹＳにおけるマネージャ２はブリッジ３１に接続されているＬＡＮ１５上に配置されているが、ＬＡＮ１５に接続される他のＩＰネットワークに収容されている形態でもよい。

【００７７】

（システム動作／レイヤ２ループ検知処理）

次に、図８に示す本発明の第３の実施の形態のレイヤ２ループ検知システムＳＹＳにおける動作例を図２、図８、図９、及び図１０を併用して説明する。

【００７８】

上述したようなマネージャ・エージェント構造を持つこのレイヤ２ループ検知システムＳＹＳにおいては、ＳＮＭＰはＵＤＰ上で動作するネットワーク管理のための管理ステーションと管理対象システムとの間における管理情報の交換プロトコルである。この第３の実施の形態のシステムＳＹＳのＳＮＭＰでは、管理ステーション上のＳＮＭＰマネージャ２からの処理要求（コマンド）に対して、管理対象システムであるＬ２ネットワークＮＷ上のブリッジ３１～３４が管理情報（レスポンス）をマネージャ２に通知する。

【００７９】

このような要求・応答に基づくトポロジ認識部２１の機能により、ＳＮＭＰマネージャ２は、監視対象ブリッジ３１～３４のＩＰアドレス、つまりＳＮＭＰ通信したいブリッジを指定する際に使用するアドレスと、監視対象ブリッジ３１～３４のＣｏｍｍｕｎｉｔｙＳｔｒｉｎｇ、つまりブリッジとＳＮＭＰ通信を行うための文字列（パスワード）とを予め取得する。図８及び図１０中に例示するように、ブリッジ３１～３４のＩＰアドレスは、１９２．１６８．１０．１０、１９２．１６８．１０．３０、１９２．１６８．１０．４０、１９２．１６８．１０．２０である。

【００８０】

また、マネージャ２とブリッジ３１～３４間では、ＳＮＭＰメッセージの交換という形態で要求・応答を行うが、ＳＮＭＰに則ったメッセージのうちの自律メッセージとしてのトラップ（ＴＲＡＰ）は、ブリッジ３１～３４からマネージャ２に自律的に（単方向に）送信するＵＤＰのメッセージであり、ＬＡＮ１１～１４の状態（輻輳や障害等）やブリッジ３１～３４の状態等を通知するために使用される。この自律メッセージ・ＴＲＡＰの利用については後に詳述する。

【００８１】

エンタープライズネットワーク等を構築するためのＬ２ネットワークＮＷにおいては、ＭＡＣフレームが巡回してしまうループ（レイヤ２ループ）を排除してネットワークの冗長性を確保する一手法として、ＩＥＥＥ８０２．１Ｄで標準化されているスパニングツリープロトコル（ＳＴＰ）を動作させる。

【００８２】

ＳＴＰは、Ｌ２スイッチであるブリッジ３１～３４間でＢＰＤＵと呼ばれる監視用パケットを送受信し、ネットワークがループしている箇所を検知すると、ブロッキングポート（ＢＰ）と呼ばれるＭＡＣフレームを遮断するポート（トラフィック遮断ポート）を作成して、ループを論理的に遮断する。これにより、Ｌ２ループの発生を回避することができる。

【００８３】

また、ＳＴＰは、ルートブリッジと呼ばれる１つのブリッジをルート（根）としたツリー（木）構造のネットワーク構成（トポロジ）を作成するプロトコルである。Ｌ２ネットワークＮＷは、ＳＴＰに則ってブリッジ３１～３４間でＣｏｎｆｉｇｕｒａｔｉｏｎＢＰ

ＤＵを送受信して、ルートブリッジを決定する。

【００８４】

Ｌ２ネットワークＮＷにおいてＳＴＰを動作させることにより、各ブリッジ３２～３４のルートブリッジ（ブリッジ３１）、つまり根に近いポートが１つだけルートポート（ＲＰ）になる。また、各ＬＡＮ１１～１４で一番ルートパスコストが小さいポートがそのＬＡＮの指定ポート（ＤＰ）となる。ルートブリッジのポートは、ルートパスコストが０であるので、全て指定ポートＤＰとなる。

【００８５】

ルートポートＲＰ及び指定ポートＤＰはＦｏｒｗａｒｄｉｎｇ、またそれ以外のポートはＢｌｏｃｋｉｎｇまたはＤｉｓａｂｌｅというポートステータス（ステート）となる。

【００８６】

この結果、Ｌ２ネットワークＮＷにおいては、ブリッジ３１はその第１のポート及び第２のポートを指定ポートＤＰとするルートブリッジとなる。なお、図８中、ポート番号は丸付き数字で示している。また、ブリッジ３２，３３，３４の第１のポートはそれぞれルートポートＲＰとなり、ブリッジ３２，３４の第２のポートは指定ポートＤＰとなる。ブリッジ３３の第２のポートは本来指定ポートＤＰであるが、Ｌ２ループの発生を回避するためにブロッキングポートＢＰとなる。ブリッジ３２，３３の第３のポートはディセーブルポート（ＤｉｓＰ）である。

【００８７】

ＳＮＭＰマネージャ２のトポロジ認識部２１は、監視対象のＬ２ネットワークＮＷを構成するブリッジ３１～３４からのＭＩＢ情報をブリッジ（第３のポート）３１及びＬＡＮ１５を介して、ＳＮＭＰ通信により収集する。トポロジ認識部２１により収集されるＭＩＢ情報は、第１の実施の形態と同様に上記（１）～（１０）である。

【００８８】

また、トポロジ認識部２１により収集されたＭＩＢ情報の一覧を図１０に示す。トポロジ認識部２１は、収集したＭＩＢ情報を図１０に示すように、ブリッジ３１～３４のＩＰアドレス及びポート番号をキー情報として、図示省略の記憶部（ハードディスク）に格納する。

【００８９】

トポロジ認識部２１は、収集したＭＩＢ情報に基づき、（７）ｄｏｔ１ｄＳｔｐＰｏｒｔＤｅｓｉｎａｔｅｄＢｒｉｄｇｅ及び（８）ｄｏｔ１ｄＳｔｐＰｏｒｔＤｅｓｉｇｎａｔｅｄＰｏｒｔの値が等しいブリッジのポート同士が隣接していると解析する。

【００９０】

また、トポロジ認識部２１は、（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅに基づいて、ブリッジ３１～３４の各ポートのＳＴＰのステータスを把握する。その内、Ｆｏｒｗａｒｄｉｎｇステータス「５」については、（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔで示されたポート番号「１」のポートはルートポートＲＰと解析され、そうでなければ指定ポートＤＰであると解析される。トポロジ認識部２１は、これらの処理により、Ｌ２ネットワークＮＷのトポロジを解析する。

【００９１】

次に、ポート識別部２２は、トポロジ認識部２１によるトポロジ認識処理で得られた各ポートのＳＴＰのステータス「２」からブロッキングポート（１）ＢＰを識別するとともに、ポートステータス「１」から無能ポートを示すディセーブルポート（１，２）ＤｉｓＰを識別して、これらを監視ポイントに設定する。この例では、ブリッジ３３の第２のポート及びブリッジ３２，３３の第３のポートがそれぞれ監視ポイントに設定される。

【００９２】

ポーリング部２３は、設定された監視ポイント対応のブロッキングポート（１）ＢＰ及びディセーブルポート（１，２）ＤｉｓＰのＭＩＢ情報を定期的（周期的に）に監視して収集し、変動状態をトリガ検出部２４に伝える。トリガ検出部２４は、ポーリング部２３からブロッキングポート（１）ＢＰ及びディセーブルポート（１，２）ＤｉｓＰのいずれ

かのＭＩＢ情報の変化が入力された場合、これをトリガ（契機）に障害発生を認識して、トポロジ再認識部２５に伝える。

【００９３】

トリガ検出部２４から障害発生を入力されたトポロジ再認識部２５は、監視対象のＬ２ネットワークＮＷのブリッジ３１～３４からＭＩＢ情報（ここでは、（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅ、（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔ、（９）ｉｆＩｎＯｃｔｅｔｓ）を再度取得し、各ポートのＳＴＰのステータスを更新することによってトポロジを再び解析し、Ｌ２ループを検知する。

【００９４】

このＬ２ループの検知をトポロジ再認識部２５から入力された障害判別部２６は、Ｌ２ネットワークＮＷにおける障害発生を認識する。

【００９５】

次に、ＳＮＭＰマネージャ２のポーリング部２３及びトリガ検出部２４による処理を一層具体的に説明する。

【００９６】

上述した一連のＬ２ループ検知処理において、ポーリング部２３は、監視ポイント対応のブロッキングポート（１）ＢＰを定期監視するためのＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を収集することで、ブロッキングポート（１）ＢＰからトラフィック（パケット）がＳＮＭＰマネージャ２で予め決めた任意の閾値以上、転送された場合に、障害発生のトリガとするように変動状態をトリガ検出部２４に伝える。これにより、トリガ検出部２４は、これをトリガに障害発生を認識して、トポロジ再認識部２５に伝える。なお、この閾値はＬ２ネットワークＮＷの正常時にブロッキングポート（１）ＢＰから出力されているトラフィックがトリガにかからないように設定する必要がある。

【００９７】

また、ポーリング部２３は、監視ポイント対応のディセーブルポート（１，２）ＤｉｓＰを定期監視するためのＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を収集することで、ディセーブルポート（１，２）ＤｉｓＰのいずれかからトラフィック（パケット）が転送された場合に、障害発生のトリガとするように変動状態をトリガ検出部２４に伝える。これにより、トリガ検出部２４は、これをトリガに障害発生を認識して、トポロジ再認識部２５に伝える。また、トラフィック量は前回との差分をポーリング部２３によって計算することにより求める。

【００９８】

また、上述した一連のＬ２ループ検知処理において、ポーリング部２３は、監視ポイント対応のブロッキングポート（１）ＢＰ及びディセーブルポート（１，２）ＤｉｓＰを定期監視するためのＭＩＢ情報として（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅの値を収集することで、ブロッキングポートＢＰのポートステートがＢｌｏｃｋｉｎｇから変化した場合、またはディセーブルポート（１，２）ＤｉｓＰのいずれかのポートステータスがＤｉｓａｂｌｅから変化した場合に、障害発生のトリガとするように変動状態をトリガ検出部２４に伝える。これにより、トリガ検出部２４は、これをトリガに障害発生を認識して、トポロジ再認識部２５に伝える。

【００９９】

さらに、上述した一連のＬ２ループ検知処理において、ポーリング部２３及びトリガ検出部２４は、監視ポイント対応のブロッキングポート（１）ＢＰ及びディセーブルポート（１，２）ＤｉｓＰを定期監視するためのＭＩＢ情報の変化以外をトリガとして、Ｌ２ネットワークＮＷの障害発生を認識することも可能である。

【０１００】

具体的には、ポーリング部２３及びトリガ検出部２４は、各ブリッジ３１～３４が送信する自律メッセージ・ＴＲＡＰの内のトポロジチェンジトラップ：ｔｏｐｏｌｏｇｙＣｈａｎｇｅ　ｔｒａｐの受信をトリガとして障害発生を認識する。このトポロジチェンジトラップは、各ブリッジ３１～３４においてポートステータスがＬｅａｒｎｉｎｇからＦｏ

ｒｗａｒｄｉｎｇに、またＦｏｒｗａｒｄｉｎｇからＢｌｏｃｋｉｎｇに変化した際に発生される。

【０１０１】

また、ポーリング部２３及びトリガ検出部２４は、各ブリッジ３１～３４が送信する自律メッセージ・ＴＲＡＰの内のニュールートトラップ：ｎｅｗＲｏｏｔ　ｔｒａｐの受信をトリガとして障害発生を認識する。このニュールートトラップは、各ブリッジにおいて新たなルートポートＲＰが選出された際に発生される。

【０１０２】

［第４の実施の形態］

（システム構成）

本発明の第４の実施の形態におけるシステムの構成を示す図１１を参照すると、レイヤ２ループ検知システムＳＹＳは、上述した第１の実施の形態のシステムＳＹＳの変形例としてのＳＮＭＰのマネージャ・エージェント構造を持ち、ＩＰネットワークとしてのイーサネットワーク（イーサネット：登録商標）などのローカルエリアネットワーク（ＬＡＮ）１（１１，１２，１３，１４，１５，１６）にそれぞれ接続される第１及び第２のＳＮＭＰマネージャ２，４及び複数のエージェント３（３１，３２，３３，３４）を備え、ネットワーク管理（監視）機能を有するシステムを構成する。

【０１０３】

管理（監視）ステーション上の第１のＳＮＭＰマネージャ（１）２及び第２のＳＮＭＰマネージャ（２）４は、厳密にはＳＮＭＰマネージャを搭載するパーソナルコンピータ（ＰＣ）などの装置であり、ここでは第１のＳＮＭＰマネージャ（１）２がＬ２ループ検知装置を構成する。第１のＳＮＭＰマネージャ（１）２は、管理（監視）対象システムとしてのＬ２ネットワークＮＷ上のＬＡＮ１及び複数のエージェント３を監視する。また、各第２のＳＮＭＰマネージャ（２）４は、管理対象システムとしてのＬ２ネットワークＮＷ上のＬＡＮ１及び対応のエージェント３を監視する。これらのＳＮＭＰマネージャ２，４は、図２に詳細機能構成を示すように、トポロジ認識部２１、ポート識別部２２、ポーリング部２３、トリガ検出部２４、トポロジ再認識部２５、及び障害判別部２６を備える。

【０１０４】

Ｌ２ネットワークＮＷを構成する複数のエージェント３は、厳密にはエージェントを搭載する装置であり、ここではＬ２スイッチとしてのブリッジ（１～４）３１，３２，３３，３４に対応する。ブリッジ３１及びブリッジ３２はＬＡＮ１１、ブリッジ３２及びブリッジ３３はＬＡＮ１２、ブリッジ３３及びブリッジ３４はＬＡＮ１３、及びブリッジ３４及びブリッジ３１はＬＡＮ１４によってそれぞれ物理的に接続されている。また、ブリッジ３１はＳＮＭＰマネージャ２とＬＡＮ１５によって物理的に接続されている。ブリッジ３２，３３，３４は対応のＳＮＭＰマネージャ４とＬＡＮ１６によって物理的に接続されている。ただし、ブリッジ３２及びブリッジ３３は、後に詳述するように、ＬＡＮ１２を通して論理的には接続されていない状態である。

【０１０５】

このレイヤ２ループ検知システムＳＹＳにおけるマネージャ２，４は、ブリッジ（第３のポート）３１に接続されているＬＡＮ１５またはブリッジ（第３のポート）３２，３３，３４にそれぞれ接続されているＬＡＮ１６上に配置されているが、ＬＡＮ１５，１６に接続される他のＩＰネットワークに収容されている形態でもよい。

【０１０６】

また、第２のＳＮＭＰマネージャ４は、各ブリッジ３２，３３，３４に接続されている多数のユーザ端末の内、ＳＮＭＰマネージャを搭載するパーソナルコンピータとして設けることが可能であり、これによりＳＮＭＰマネージャのために新たに端末を用意する必要がなくなる。

【０１０７】

（システム動作／レイヤ２ループ検知処理）

次に、図１１に示す本発明の第４の実施の形態のレイヤ２ループ検知システムＳＹＳに

おける動作例を説明する。なお、この動作説明は発明の実施に支障を来さない程度に上述した第１の実施の形態と相異する事項に限定して行う。したがって、説明のない事項は上述した第１の実施の形態と同様である。

【０１０８】

この第４の実施の形態のシステムＳＹＳのＳＮＭＰでは、管理ステーション上のＳＮＭＰマネージャ２からの処理要求（コマンド）に対して、管理対象システムであるＬ２ネットワークＮＷ上のブリッジ３１～３４が管理情報（レスポンス）をマネージャ２に通知する。また、管理ステーション上の各ＳＮＭＰマネージャ４からの処理要求に対して、管理対象システムであるＬ２ネットワークＮＷ上のブリッジ３２～３４が管理情報を対応のマネージャ４に通知する。

【０１０９】

このような要求・応答に基づくトポロジ認識部２１（図２参照）の機能により、ＳＮＭＰマネージャ２は、監視対象ブリッジ３１～３４のＩＰアドレス、つまりＳＮＭＰ通信したいブリッジを指定する際に使用するアドレスと、監視対象ブリッジ３１～３４のＣｏｍｍｕｎｉｔｙ　Ｓｔｒｉｎｇ、つまりブリッジとＳＮＭＰ通信を行うための文字列（パスワード）とを予め取得する。同様に、各ＳＮＭＰマネージャ４は、監視対象ブリッジ３２～３４の対応するもののＩＰアドレス及びＣｏｍｍｕｎｉｔｙ　Ｓｔｒｉｎｇを予め取得する。ブリッジ３１～３４のＩＰアドレスは、１９２．１６８．１０．１０、１９２．１６８．１０．３０、１９２．１６８．１０．４０、１９２．１６８．１０．２０である。

【０１１０】

マネージャ２とブリッジ３１～３４間では、ＳＮＭＰメッセージの交換という形態で要求・応答を行うが、ＳＮＭＰに則ったメッセージのうちの自律メッセージとしてのＴＲＡＰは、ブリッジ３１～３４からマネージャ２に自律的に（単方向に）送信するＵＤＰのメッセージであり、ＬＡＮ１１～１４の状態（輻輳や障害等）やブリッジ３１～３４の状態等を通知するために使用される。

【０１１１】

また、各マネージャ４と対応のブリッジ３２～３４間では、ＳＮＭＰメッセージの交換という形態で要求・応答を行うが、ＳＮＭＰに則ったメッセージのうちの自律メッセージとしてのＴＲＡＰは、ブリッジ３２～３４から対応のマネージャ４に自律的に（単方向に）送信するＵＤＰのメッセージであり、ＬＡＮ１１～１４の状態（輻輳や障害等）やブリッジ３２～３４の状態等を通知するために使用される。この自律メッセージ・ＴＲＡＰの利用については後に詳述する。

【０１１２】

ＳＮＭＰマネージャ２は、各ブリッジ３１～３４のＭＩＢ情報（上記（１）～（１０））を収集し、それらを基にしてＬ２ネットワークＮＷのトポロジを解析する。そして、ＳＮＭＰマネージャ２は、ブリッジ３１のみについてブロッキングポートＢＰを識別し、ブロッキングポートＢＰがあればそのポートのＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を定期監視し、ブロッキングポートＢＰからトラフィックが予め決めた任意の閾値以上、転送されたことを障害発生のトリガにする。なお、この閾値はＬ２ネットワークＮＷの正常時にブロッキングポートＢＰより出力されているトラフィックがトリガにかからないように設定する必要がある。

【０１１３】

また、ブリッジ３２，３３，３４に接続されている各ＳＮＭＰマネージャ４は、対応のブリッジのブロッキングポートＢＰ（ここでは、ブリッジ３３に接続されているＳＮＭＰマネージャ４がブロッキングポート（１）ＢＰ）を認識し、そのポート（ポート２）のＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を定期監視し、ブロッキングポートＢＰからトラフィックが予め決めた任意の閾値以上、転送されるとトポロジチェンジトラップをＳＮＭＰマネージャ２に向けて送信する。

【０１１４】

ブリッジ３３対応のＳＮＭＰマネージャ４からのトポロジチェンジトラップを受信した

ＳＮＭＰマネージャ２は、このトラップの受信を障害発生のトリガにする。このとき、ＳＮＭＰマネージャ２は、再度ＭＩＢ情報（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅ、（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔ、（９）ｉｆＩｎＯｃｔｅｔを取得し、各ポートのＳＴＰのステータスを更新してトポロジを再び解析することにより、Ｌ２ループを検知する。このＬ２ループ検知処理手法によると、第１のＳＮＭＰマネージャ２からの定期監視のトラフィックを抑制することができる。

【０１１５】

上述した一連のＬ２ループ検知処理において、第１のＳＮＭＰマネージャ（１）２は、ブリッジ３１のみについて監視ポイント対応のブロッキングポートＢＰを識別し、ブロッキングポートＢＰがあればそのポートを定期監視するためのＭＩＢ情報として（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅの値を収集することで、ブロッキングポートＢＰのポートステータスがＢｌｏｃｋｉｎｇから変化した場合に、障害発生のトリガとするように変形可能である。

【０１１６】

また、ブリッジ３２，３３，３４に接続されている第２のＳＮＭＰマネージャ（２）４は、対応のブリッジのブロッキングポートＢＰ（ここでは、ブリッジ３３に接続されているＳＮＭＰマネージャ４がブロッキングポート（１）ＢＰ）を認識し、そのポートのＭＩＢ情報として（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅの値を定期監視し、ブロッキングポート（１）ＢＰのポートステータスがＢｌｏｃｋｉｎｇから変化した場合に、トポロジチェンジトラップをＳＮＭＰマネージャ２に向けて送信する。ブリッジ３３対応のＳＮＭＰマネージャ４からのトポロジチェンジトラップを受信したＳＮＭＰマネージャ２は、このトラップの受信を障害発生のトリガにするように変形可能である。

【０１１７】

［第５の実施の形態］

（システム構成）

本発明の第５の実施の形態におけるシステムの構成を示す図１２を参照すると、レイヤ２ループ検知システムＳＹＳは、上述した第２の実施の形態のシステムＳＹＳの変形例としてのＳＮＭＰのマネージャ・エージェント構造を持ち、ＩＰネットワークとしてのイーサネットワーク（イーサネット：登録商標）などのローカルエリアネットワーク（ＬＡＮ）１（１１，１２，１３，１４，１５，１６）にそれぞれ接続されるＳＮＭＰマネージャ２，４及び複数のエージェント３（３１，３２，３３，３４）を備え、ネットワーク管理（監視）機能を有するシステムを構成する。

【０１１８】

管理（監視）ステーション上の第１のＳＮＭＰマネージャ（１）２及び第２のＳＮＭＰマネージャ（２）４は、厳密にはＳＮＭＰマネージャを搭載するパーソナルコンピータ（ＰＣ）などの装置であり、ここでは第１のＳＮＭＰマネージャ（１）２がＬ２ループ検知装置を構成する。第１のＳＮＭＰマネージャ（１）２は、管理（監視）対象システムとしてのＬ２ネットワークＮＷ上のＬＡＮ１及び複数のエージェント３を監視する。また、各第２のＳＮＭＰマネージャ（２）４は、管理対象システムとしてのＬ２ネットワークＮＷ上のＬＡＮ１及び対応のエージェント３を監視する。これらのＳＮＭＰマネージャ２，４は、図２に詳細機能構成を示すように、トポロジ認識部２１、ポート識別部２２、ポーリング部２３、トリガ検出部２４、トポロジ再認識部２５、及び障害判別部２６を備える。

【０１１９】

Ｌ２ネットワークＮＷを構成する複数のエージェント３は、厳密にはエージェントを搭載する装置であり、ここではＬ２スイッチとしてのブリッジ（１～４）３１，３２，３３，３４に対応する。ブリッジ３１及びブリッジ３２はＬＡＮ１１、ブリッジ３２及びブリッジ３３はＬＡＮ１２、ブリッジ３３及びブリッジ３４はＬＡＮ１３、及びブリッジ３４及びブリッジ３１はＬＡＮ１４によってそれぞれ物理的に接続されている。また、ブリッジ３１はＳＮＭＰマネージャ２とＬＡＮ１５によって物理的に接続されている。ブリッジ３２，３３，３４は対応のＳＮＭＰマネージャ４とＬＡＮ１６によって物理的に接続され

ている。ただし、ブリッジ３２及びブリッジ３３は、後に詳述するように、ＬＡＮ１２を通して論理的には接続されていない状態である。

【０１２０】

このレイヤ２ループ検知システムＳＹＳにおけるマネージャ２，４は、ブリッジ（第３のポート）３１に接続されているＬＡＮ１５またはブリッジ（第３のポート）３２，３３，３４にそれぞれ接続されているＬＡＮ１６上に配置されているが、ＬＡＮ１５，１６に接続される他のＩＰネットワークに収容されている形態でもよい。

【０１２１】

また、第２のＳＮＭＰマネージャ４は、各ブリッジ３２，３３，３４に接続されている多数のユーザ端末の内、ＳＮＭＰマネージャを搭載するパーソナルコンピータとして設けることが可能であり、これによりＳＮＭＰマネージャのために新たに端末を用意する必要がなくなる。

【０１２２】

（システム動作／レイヤ２ループ検知処理）

次に、図１２に示す本発明の第５の実施の形態のレイヤ２ループ検知システムＳＹＳにおける動作例を説明する。なお、この動作説明は発明の実施に支障を来さない程度に上述した第２の実施の形態と相異する事項に限定して行う。したがって、説明のない事項は上述した第２の実施の形態と同様である。

【０１２３】

この第５の実施の形態のシステムＳＹＳのＳＮＭＰでは、管理ステーション上のＳＮＭＰマネージャ２からの処理要求（コマンド）に対して、管理対象システムであるＬ２ネットワークＮＷ上のブリッジ３１～３４が管理情報（レスポンス）をマネージャ２に通知する。また、管理ステーション上の各ＳＮＭＰマネージャ４からの処理要求に対して、管理対象システムであるＬ２ネットワークＮＷ上のブリッジ３２～３４が管理情報を対応のマネージャ４に通知する。

【０１２４】

このような要求・応答に基づくトポロジ認識部２１（図２参照）の機能により、ＳＮＭＰマネージャ２は、監視対象ブリッジ３１～３４のＩＰアドレス、つまりＳＮＭＰ通信したいブリッジを指定する際に使用するアドレスと、監視対象ブリッジ３１～３４のＣｏｍｍｕｎｉｔｙ　Ｓｔｒｉｎｇ、つまりブリッジとＳＮＭＰ通信を行うための文字列（パスワード）とを予め取得する。同様に、各ＳＮＭＰマネージャ４は、監視対象ブリッジ３２～３４の対応するもののＩＰアドレス及びＣｏｍｍｕｎｉｔｙ　Ｓｔｒｉｎｇを予め取得する。ブリッジ３１～３４のＩＰアドレスは、１９２．１６８．１０．１０、１９２．１６８．１０．３０、１９２．１６８．１０．４０、１９２．１６８．１０．２０である。

【０１２５】

マネージャ２とブリッジ３１～３４間では、ＳＮＭＰメッセージの交換という形態で要求・応答を行うが、ＳＮＭＰに則ったメッセージのうちの自律メッセージとしてのＴＲＡＰは、ブリッジ３１～３４からマネージャ２に自律的に（単方向に）送信するＵＤＰのメッセージであり、ＬＡＮ１１～１４の状態（輻輳や障害等）やブリッジ３１～３４の状態等を通知するために使用される。

【０１２６】

また、各マネージャ４と対応のブリッジ３２～３４間では、ＳＮＭＰメッセージの交換という形態で要求・応答を行うが、ＳＮＭＰに則ったメッセージのうちの自律メッセージとしてのＴＲＡＰは、ブリッジ３２～３４から対応のマネージャ４に自律的に（単方向に）送信するＵＤＰのメッセージであり、ＬＡＮ１１～１４の状態（輻輳や障害等）やブリッジ３２～３４の状態等を通知するために使用される。この自律メッセージ・ＴＲＡＰの利用については後に詳述する。

【０１２７】

ＳＮＭＰマネージャ２は、各ブリッジ３１～３４のＭＩＢ情報（上記（１）～（１０））を収集し、それらを基にしてＬ２ネットワークＮＷのトポロジを解析する。そして、Ｓ

ＮＭＰマネージャ２は、ブリッジ３１のみについてブロッキングポートＢＰを識別し、ブロッキングポートＢＰが存在しなければディセーブルポート（１，２）ＤｉｓＰを識別し、ディセーブルポート（１，２）ＤｉｓＰがあればそのポートのＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を定期監視し、ディセーブルポート（１，２）ＤｉｓＰからトラフィックが転送されたことを障害発生のトリガにする。

【０１２８】

また、ブリッジ３２，３３，３４に接続されている各ＳＮＭＰマネージャ４は、対応のブリッジのブロッキングポートＢＰを識別し、ブロッキングポートＢＰが存在しなければディセーブルポート（１，２）ＤｉｓＰ（ここでは、ブリッジ３２，３３に接続されている各ＳＮＭＰマネージャ４がディセーブルポート（１，２）ＤｉｓＰ）を認識し、そのポート（ポート２）のＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を定期監視し、ディセーブルポート（１，２）ＤｉｓＰのいずれかからトラフィックが転送されるとトポロジチェンジトラップをＳＮＭＰマネージャ２に向けて送信する。

【０１２９】

ブリッジ３２，３３対応のＳＮＭＰマネージャ４のいずれかからのトポロジチェンジトラップを受信したＳＮＭＰマネージャ２は、このトラップの受信を障害発生のトリガにする。このとき、ＳＮＭＰマネージャ２は、再度ＭＩＢ情報（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅ、（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔ、（９）ｉｆＩｎＯｃｔｅｔを取得し、各ポートのＳＴＰのステータスを更新してトポロジを再び解析することにより、Ｌ２ループを検知する。このＬ２ループ検知処理手法によると、第１のＳＮＭＰマネージャ２からの定期監視のトラフィックを抑制することができる。

【０１３０】

上述した一連のＬ２ループ検知処理において、第１のＳＮＭＰマネージャ（１）２は、ブリッジ３１のみについて監視ポイント対応のディセーブルポートＤｉｓＰを識別し、ディセーブルポートＤｉｓＰがあればそのポートを定期監視するためのＭＩＢ情報として（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅの値を収集することで、ディセーブルポートＤｉｓＰのポートステータスがＤｉｓａｂｌｅから変化した場合に、障害発生のトリガとするように変形可能である。

【０１３１】

また、ブリッジ３２，３３，３４に接続されている第２のＳＮＭＰマネージャ（２）４は、対応のブリッジのディセーブルポートＤｉｓＰ（ここでは、ブリッジ３２，３３に接続されているＳＮＭＰマネージャ４がディセーブルポート（１，２）ＤｉｓＰ）を認識し、そのポートのＭＩＢ情報として（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅの値を定期監視し、ディセーブルポート（１，２）ＤｉｓＰのいずれかのポートステータスがＤｉｓａｂｌｅから変化した場合に、トポロジチェンジトラップをＳＮＭＰマネージャ２に向けて送信する。ブリッジ３３対応のＳＮＭＰマネージャ４からのトポロジチェンジトラップを受信したＳＮＭＰマネージャ２は、このトラップの受信を障害発生のトリガにするように変形可能である。

【０１３２】

［第６の実施の形態］

（システム構成）

本発明の第６の実施の形態におけるシステムの構成を示す図１３を参照すると、レイヤ２ループ検知システムＳＹＳは、上述した第３の実施の形態のシステムＳＹＳの変形例としてのＳＮＭＰのマネージャ・エージェント構造を持ち、ＩＰネットワークとしてのイーサネットワーク（イーサネット：登録商標）などのローカルエリアネットワーク（ＬＡＮ）１（１１，１２，１３，１４，１５，１６）にそれぞれ接続されるＳＮＭＰマネージャ２，４及び複数のエージェント３（３１，３２，３３，３４）を備え、ネットワーク管理（監視）機能を有するシステムを構成する。

【０１３３】

管理（監視）ステーション上の第１のＳＮＭＰマネージャ（１）２及び第２のＳＮＭＰ

マネージャ（２）４は、厳密にはＳＮＭＰマネージャを搭載するパーソナルコンピータ（ＰＣ）などの装置であり、ここでは第１のＳＮＭＰマネージャ（１）２がＬ２ループ検知装置を構成する。第１のＳＮＭＰマネージャ（１）２は、管理（監視）対象システムとしてのＬ２ネットワークＮＷ上のＬＡＮ１及び複数のエージェント３を監視する。また、各第２のＳＮＭＰマネージャ（２）４は、管理対象システムとしてのＬ２ネットワークＮＷ上のＬＡＮ１及び対応のエージェント３を監視する。これらのＳＮＭＰマネージャ２，４は、図２に詳細機能構成を示すように、トポロジ認識部２１、ポート識別部２２、ポーリング部２３、トリガ検出部２４、トポロジ再認識部２５、及び障害判別部２６を備える。

【０１３４】

Ｌ２ネットワークＮＷを構成する複数のエージェント３は、厳密にはエージェントを搭載する装置であり、ここではＬ２スイッチとしてのブリッジ（１～４）３１，３２，３３，３４に対応する。ブリッジ３１及びブリッジ３２はＬＡＮ１１、ブリッジ３２及びブリッジ３３はＬＡＮ１２、ブリッジ３３及びブリッジ３４はＬＡＮ１３、及びブリッジ３４及びブリッジ３１はＬＡＮ１４によってそれぞれ物理的に接続されている。また、ブリッジ３１はＳＮＭＰマネージャ２とＬＡＮ１５によって物理的に接続されている。ブリッジ３２，３３，３４は対応のＳＮＭＰマネージャ４とＬＡＮ１６によって物理的に接続されている。ただし、ブリッジ３２及びブリッジ３３は、後に詳述するように、ＬＡＮ１２を通して論理的には接続されていない状態である。

【０１３５】

このレイヤ２ループ検知システムＳＹＳにおけるマネージャ２，４は、ブリッジ（第３のポート）３１に接続されているＬＡＮ１５またはブリッジ（第３または第４のポート）３２，３３，３４にそれぞれ接続されているＬＡＮ１６上に配置されているが、ＬＡＮ１５，１６に接続される他のＩＰネットワークに収容されている形態でもよい。

【０１３６】

また、第２のＳＮＭＰマネージャ４は、各ブリッジ３２，３３，３４に接続されている多数のユーザ端末の内、ＳＮＭＰマネージャを搭載するパーソナルコンピータとして設けることが可能であり、これによりＳＮＭＰマネージャのために新たに端末を用意する必要がなくなる。

【０１３７】

（システム動作／レイヤ２ループ検知処理）

次に、図１３に示す本発明の第６の実施の形態のレイヤ２ループ検知システムＳＹＳにおける動作例を説明する。なお、この動作説明は発明の実施に支障を来さない程度に上述した第３の実施の形態と相異する事項に限定して行う。したがって、説明のない事項は上述した第３の実施の形態と同様である。

【０１３８】

この第６の実施の形態のシステムＳＹＳのＳＮＭＰでは、管理ステーション上のＳＮＭＰマネージャ２からの処理要求（コマンド）に対して、管理対象システムであるＬ２ネットワークＮＷ上のブリッジ３１～３４が管理情報（レスポンス）をマネージャ２に通知する。また、管理ステーション上の各ＳＮＭＰマネージャ４からの処理要求に対して、管理対象システムであるＬ２ネットワークＮＷ上のブリッジ３２～３４が管理情報を対応のマネージャ４に通知する。

【０１３９】

このような要求・応答に基づくトポロジ認識部２１（図２参照）の機能により、ＳＮＭＰマネージャ２は、監視対象ブリッジ３１～３４のＩＰアドレス、つまりＳＮＭＰ通信したいブリッジを指定する際に使用するアドレスと、監視対象ブリッジ３１～３４のＣｏｍｍｕｎｉｔｙ　Ｓｔｒｉｎｇ、つまりブリッジとＳＮＭＰ通信を行うための文字列（パスワード）とを予め取得する。同様に、各ＳＮＭＰマネージャ４は、監視対象ブリッジ３２～３４の対応するもののＩＰアドレス及びＣｏｍｍｕｎｉｔｙ　Ｓｔｒｉｎｇを予め取得する。ブリッジ３１～３４のＩＰアドレスは、１９２．１６８．１０．１０、１９２．１６８．１０．３０、１９２．１６８．１０．４０、１９２．１６８．１０．２０である。

【０１４０】
マネージャ２とブリッジ３１～３４間では、ＳＮＭＰメッセージの交換という形態で要求・応答を行うが、ＳＮＭＰに則ったメッセージのうちの自律メッセージとしてのＴＲＡＰは、ブリッジ３１～３４からマネージャ２に自律的に（単方向に）送信するＵＤＰのメッセージであり、ＬＡＮ１１～１４の状態（輻輳や障害等）やブリッジ３１～３４の状態等を通知するために使用される。
【０１４１】
また、各マネージャ４と対応のブリッジ３２～３４間では、ＳＮＭＰメッセージの交換という形態で要求・応答を行うが、ＳＮＭＰに則ったメッセージのうちの自律メッセージとしてのＴＲＡＰは、ブリッジ３２～３４から対応のマネージャ４に自律的に（単方向に）送信するＵＤＰのメッセージであり、ＬＡＮ１１～１４の状態（輻輳や障害等）やブリッジ３２～３４の状態等を通知するために使用される。この自律メッセージ・ＴＲＡＰの利用については後に詳述する。
【０１４２】
ＳＮＭＰマネージャ２は、各ブリッジ３１～３４のＭＩＢ情報（上記（１）～（１０））を収集し、それらを基にしてＬ２ネットワークＮＷのトポロジを解析する。そして、ＳＮＭＰマネージャ２は、ブリッジ３１のみについてブロッキングポートＢＰまたはディセーブルポートＤｉｓＰを識別し、ブロッキングポートＢＰまたはディセーブルポートＤｉｓＰがあればそのポートのＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を定期監視し、ブロッキングポートＢＰからトラフィックが予め決めた任意の閾値以上、転送されたことを障害発生のトリガにし、またディセーブルポートＤｉｓＰからトラフィックが転送されたことを障害発生のトリガにする。なお、この閾値はＬ２ネットワークＮＷの正常時にブロッキングポートＢＰより出力されているトラフィックがトリガにかからないように設定する必要がある。
【０１４３】
また、ブリッジ３２，３３，３４に接続されている各ＳＮＭＰマネージャ４は、対応のブリッジのブロッキングポートＢＰ（ここでは、ブリッジ３３に接続されているＳＮＭＰマネージャ４がブロッキングポート（１）ＢＰ）を認識し、そのポート（ポート２）のＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を定期監視し、ブロッキングポート（１）ＢＰからトラフィックが予め決めた任意の閾値以上、転送されるとトポロジチェンジトラップをＳＮＭＰマネージャ２に向けて送信する。
【０１４４】
また、ブリッジ３２，３３，３４に接続されている各ＳＮＭＰマネージャ４は、対応のブリッジのディセーブルポートＤｉｓＰ（ここでは、ブリッジ３２，３３に接続されている各ＳＮＭＰマネージャ４がディセーブルポート（１，２）ＤｉｓＰ）を認識し、そのポート（ポート３）のＭＩＢ情報として（１０）ｉｆＯｕｔＯｃｔｅｔｓの値を定期監視し、ディセーブルポート（１，２）ＤｉｓＰのいずれかからトラフィックが転送されるとトポロジチェンジトラップをＳＮＭＰマネージャ２に向けて送信する。
【０１４５】
ブリッジ３２，３３対応のＳＮＭＰマネージャ４のいずれかからのトポロジチェンジトラップを受信したＳＮＭＰマネージャ２は、このトラップの受信を障害発生のトリガにする。このとき、ＳＮＭＰマネージャ２は、再度ＭＩＢ情報（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅ、（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔ、（９）ｉｆＩｎＯｃｔｅｔを取得し、各ポートのＳＴＰのステータスを更新してトポロジを再び解析することにより、Ｌ２ループを検知する。このＬ２ループ検知処理手法によると、第１のＳＮＭＰマネージャ２からの定期監視のトラフィックを抑制することができる。
【０１４６】
上述した一連のＬ２ループ検知処理において、第１のＳＮＭＰマネージャ（１）２は、ブリッジ３１のみについて監視ポイント対応のブロッキングポートＢＰまたはディセーブルポートＤｉｓＰを識別し、ブロッキングポートＢＰまたはディセーブルポートＤｉｓＰ

があればそのポートを定期監視するためのＭＩＢ情報として（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅの値を収集することで、ブロッキングポートＢＰのポートステータスがＢｌｏｃｋｉｎｇから変化した場合またはディセーブルポートＤｉｓＰのポートステータスがＤｉｓａｂｌｅから変化した場合に、障害発生のトリガとするように変形可能である。

【０１４７】

また、ブリッジ３２，３３，３４に接続されている第２のＳＮＭＰマネージャ（２）４は、対応のブリッジのブロッキングポートＢＰ（ここでは、ブリッジ３３に接続されているＳＮＭＰマネージャ４がブロッキングポート（１）ＢＰ）を認識、または対応のブリッジのディセーブルポートＤｉｓＰ（ここでは、ブリッジ３２，３３に接続されているＳＮＭＰマネージャ４がディセーブルポート（１，２）ＤｉｓＰ）を認識し、そのポートのＭＩＢ情報として（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅの値を定期監視する。そして、ＳＮＭＰマネージャ４は、ブロッキングポート（１）ＢＰのポートステータスがＢｌｏｃｋｉｎｇから変化した場合、またはディセーブルポート（１，２）ＤｉｓＰのいずれかのポートステータスがＤｉｓａｂｌｅから変化した場合に、トポロジチェンジトラップをＳＮＭＰマネージャ２に向けて送信する。ブリッジ３２，３３対応のＳＮＭＰマネージャ４のいずれかからのトポロジチェンジトラップを受信したＳＮＭＰマネージャ２は、このトラップの受信を障害発生のトリガにするように変形可能である。

【０１４８】

［第７の実施の形態］

次に、本発明の第７の実施の形態のレイヤ２ループ検知システムＳＹＳについて説明する。なお、この第７の実施の形態の説明は発明の実施に支障を来さない程度に上述した第１の実施の形態と相異する事項に限定して行う。したがって、説明のない事項は上述した第１の実施の形態と同様である。また、この第７の実施の形態の発明は上述した第２～第６の実施の形態のレイヤ２ループ検知システムＳＹＳに適用することも可能である。

【０１４９】

（第１のＭＩＢ情報収集法）

図１４に示すレイヤ２ループ検知システムＳＹＳにおいては、管理ステーション上のＳＮＭＰマネージャ２のポーリング部２３（図２参照）は、監視ポイント対応のブロッキングポート（１）ＢＰのＭＩＢ情報を定期的（周期的に）に監視して収集し、変動状態をトリガ検出部２４に伝える。この例では、ブリッジ３３の第２のポートが監視ポイントに設定されている。

【０１５０】

ＳＮＭＰマネージャ２のトリガ検出部２４は、ポーリング部２３からブロッキングポート（１）ＢＰのＭＩＢ情報の変化が入力された場合、これをトリガに障害発生を認識して、トポロジ再認識部２５に伝える。

【０１５１】

トリガ検出部２４から障害発生を入力されたトポロジ再認識部２５は、監視対象のＬ２ネットワークＮＷのブリッジ３１～３４からＭＩＢ情報（ここでは、（４）ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅ、（５）ｄｏｔ１ｄＳｔｐＲｏｏｔＰｏｒｔ、（９）ｉｆＩｎＯｃｔｅｔｓ）を再度取得し、各ポートのＳＴＰのステータスを更新することによってトポロジを再び解析し、Ｌ２ループを検知する。

【０１５２】

このＬ２ループの検知をトポロジ再認識部２５から入力された障害判別部２６は、Ｌ２ネットワークＮＷにおける障害発生を認識する。

【０１５３】

このレイヤ２ループ検知システムＳＹＳのＳＮＭＰマネージャ２は、このＬ２ループ検知処理におけるＭＩＢ情報をｉｎ－ｂａｎｄでＳＮＭＰ通信を行うことによって収集（取得）する。つまり、ＳＮＭＰマネージャ２は、Ｌ２ネットワークＮＷを構成するＬＡＮ１における主信号（ＭＡＣフレーム）伝送のための物理リンクと同一の物理リンク上に設けられた同一論理的経路であるＶＬＡＮ（Virtual Local Area Network）（１）を通してＭ

ＩＢ情報収集のためのＳＮＭＰ通信を行う。

【０１５４】

ここで、実線の矢印は主信号伝送用の論理的経路であるＶＬＡＮ（１）を示し、点線の矢印はＭＩＢ情報伝送用の論理的経路であるＶＬＡＮ（１）を示す。

【０１５５】

これにより、ＳＮＭＰマネージャ２は、新たな監視経路を必要とすることなく、主信号系の経路を用いてＭＩＢ情報を収集できる。

【０１５６】

（第２のＭＩＢ情報収集法）

図１５に示すレイヤ２ループ検知システムＳＹＳにおいては、管理ステーション上のＳＮＭＰマネージャ２は、上述した第１のＭＩＢ情報収集法に代替して、Ｌ２ネットワークＮＷを構成するＬＡＮ１における主信号（ＭＡＣフレーム）伝送のための物理リンクと同一の物理リンク上に設けられ異なる論理的経路であるＶＬＡＮ（２）を通してＭＩＢ情報収集のためのＳＮＭＰ通信を行う。

【０１５７】

ここで、実線の矢印は主信号伝送用の論理的経路であるＶＬＡＮ（１）を示し、点線の矢印はＭＩＢ情報伝送用の論理的経路であるＶＬＡＮ（２）を示す。

【０１５８】

これにより、ＳＮＭＰマネージャ２は、主信号の影響を受けることなく、ＭＩＢ情報を取得できる。

【０１５９】

（第３のＭＩＢ情報収集法）

図１６に示すレイヤ２ループ検知システムＳＹＳにおいては、管理ステーション上のＳＮＭＰマネージャ２は、上述した第１のＭＩＢ情報収集法に代替して、Ｌ２ネットワークＮＷを構成するＬＡＮ１における主信号（ＭＡＣフレーム）伝送のための物理リンクと異なる物理リンク上に設けられ異なる論理的経路であるＶＬＡＮ（２）を通してＭＩＢ情報収集のためのＳＮＭＰ通信を行う。

【０１６０】

ここで、実線の矢印は主信号伝送用の論理的経路であるＶＬＡＮ（１）を示し、点線の矢印はＭＩＢ情報伝送用の論理的経路であるＶＬＡＮ（２）を示す。

【０１６１】

これにより、ＳＮＭＰマネージャ２は、主信号の影響を受けることなく、ＭＩＢ情報を取得できる。

【０１６２】

（第４のＭＩＢ情報収集法）

図１７に示すレイヤ２ループ検知システムＳＹＳのＳＮＭＰマネージャ２は、上述した第１のＭＩＢ情報収集法に代替して、Ｌ２ループ検知処理におけるＭＩＢ情報をｏｕｔ－ｂａｎｄでＳＮＭＰ通信を行うことによって収集（取得）する。つまり、ＳＮＭＰマネージャ２は、Ｌ２ネットワークＮＷを構成するＬＡＮ１における主信号（ＭＡＣフレーム）伝送のためのネットワークと異なるネットワークである他のＬＡＮ１Ａを通してＭＩＢ情報収集のためのＳＮＭＰ通信を行う。

【０１６３】

ここで、実線の矢印は主信号伝送用のネットワーク上の論理的経路であるＶＬＡＮ（１）を示し、点線の矢印はＭＩＢ情報伝送用のネットワーク上の論理的経路を示す。

【０１６４】

また、ＭＩＢ情報伝送用のネットワークを構成するＳＷは、ブリッジ及びハブなどのＬ２スイッチである。各Ｌ２スイッチＳＷはブリッジ３１～３４に接続され、ルートブリッジ３１対応のＬ２スイッチＳＷはＳＮＭＰマネージャ２に接続されている。

【０１６５】

これにより、ＳＮＭＰマネージャ２は、主信号の影響を受けることなく、ＭＩＢ情報を

取得できる。

【０１６６】

［第８の実施の形態］

次に、本発明の第８の実施の形態のレイヤ２ループ検知システムＳＹＳについて説明する。なお、この第８の実施の形態の説明は発明の実施に支障を来さない程度に上述した第１の実施の形態と相異する事項に限定して行う。したがって、説明のない事項は上述した第１の実施の形態と同様である。また、この第８の実施の形態の発明は上述した第２～第６の実施の形態のレイヤ２ループ検知システムＳＹＳに適用することも可能である。

【０１６７】

（第１のＬ２ループ検知法）

図１８に示すレイヤ２ループ検知システムＳＹＳにおいては、Ｌ２ネットワークＮＷを構成するブリッジ３２に障害（ＣＰＵ障害）が発生し、ルートブリッジ（ブリッジ３１）に接続されているＳＮＭＰマネージャ２（図示省略）との間のＭＩＢ情報収集のためのＳＮＭＰ通信の応答がなくなった場合、そのブリッジ３２に接続されているポート１（ブリッジ３１）及びポート２（ブリッジ３３）がルートポートＲＰでなく、かつポートステータスがＦｏｒｗａｒｄｉｎｇのときに（すなわち、指定ポートＤＰのときに）、ＳＮＭＰマネージャ２はブリッジ３２を原因としたＬ２ループが発生していることを検知する。

【０１６８】

つまり、このレイヤ２ループ検知システムＳＹＳにおいては、ＭＩＢ情報を収集できないブリッジがＬ２ネットワークＮＷにある場合、そのブリッジに接続された他のブリッジのポートが全て指定ポートＤＰであることを検知することにより、ループ箇所を検知する。換言すれば、ＳＮＭＰ通信の応答の無いブリッジと接続されている全ての対向のポートが指定ポートＤＰであることを特定することにより、障害発生のループ箇所を特定している。

【０１６９】

（第２のＬ２ループ検知法）

図１９に示すレイヤ２ループ検知システムＳＹＳにおいては、Ｌ２ネットワークＮＷを構成するルートブリッジ（ブリッジ３１）の第１のポート（１）にて障害が発生し、ブリッジ３１の第１のポート（１）及びブリッジ３２の第２のポート（２）がルートポートＲＰでなく、かつポートステータスがＦｏｒｗａｒｄｉｎｇで対向しているときに（すなわち、指定ポートＤＰのときに）、これらのポート（１，２）を原因としたＬ２ループが発生していることを検知する。

【０１７０】

つまり、このレイヤ２ループ検知システムＳＹＳにおいては、ＬＡＮ１のリンクの両端がどちらも指定ポートＤＰであるリンクを検知することにより、ループ箇所を推定する。

【０１７１】

（第３のＬ２ループ検知法）

図１８または図１９に示すレイヤ２ループ検知システムＳＹＳにおいては、ＳＮＭＰマネージャ２は、推定したＬ２ループ発生箇所のポート（１，２）のＭＩＢ情報としての（９）ｉｆＩｎＯｃｔｅｔｓの値を参照し、それらのポートにトラフィックが流入していることを検知することにより、Ｌ２ループ箇所を特定する。

【０１７２】

つまり、このレイヤ２ループ検知システムＳＹＳにおいては、推定したループ箇所のＭＩＢ情報を収集し、矛盾の起こったポートにトラフィックが流れていることを検知することにより、ループ箇所を特定する。

【０１７３】

（第４のＬ２ループ検知法）

図１８または図１９に示すレイヤ２ループ検知システムＳＹＳにおいては、ＳＮＭＰマネージャ２は、推定したＬ２ループ発生箇所のポート（１，２）のＭＩＢ情報としての（９）ｉｆＩｎＯｃｔｅｔｓの値を参照し、それらのポートにトラフィックが流入していな

いことを検知することにより、ブリッジ障害またはリンク障害が発生していることを推定する。

【０１７４】

つまり、このレイヤ２ループ検知システムＳＹＳにおいては、推定したループ箇所のＭＩＢ情報を収集し、矛盾の起こったポートにトラフィックが流れていないことを検知することにより、Ｌ２スイッチ障害またはリンク障害が発生していることを推定する。

【０１７５】

（第５のＬ２ループ検知法）

図２０に示すレイヤ２ループ検知システムＳＹＳにおいては、ＳＮＭＰマネージャ２は、上記第３のＬ２ループ検知法のようにＬ２ループ箇所を特定後、ＳＮＭＰ通信により、ブリッジ３３の第２のポート（２）だけのＭＩＢ情報（ｉｆＡｄｍｉｎｓｔａｔｕｓ）をｕｐからｄｏｗｎにセットすることによりこのポート（２）をＤｉｓａｂｌｅ（ポート遮断）にし、ループの発生を防止する。

【０１７６】

つまり、このレイヤ２ループ検知システムＳＹＳにおいては、矛盾している隣接ポートを特定した後、ＳＮＭＰ通信により、矛盾ポートの一部のポートのＭＩＢ情報をｕｐからｄｏｗｎにセットすることにより、ループ発生を防止する。

【０１７７】

（第６のＬ２ループ検知法）

図２１に示すレイヤ２ループ検知システムＳＹＳにおいては、ＳＮＭＰマネージャ２は、上記第３のＬ２ループ検知法のようにＬ２ループ箇所を特定後、ＳＮＭＰ通信により、ブリッジ３１の第１のポート（１）及びブリッジ３３の第２のポート（２）のＭＩＢ情報（ｉｆＡｄｍｉｎｓｔａｔｕｓ）をｕｐからｄｏｗｎにセットすることによりこれらのポート（１，２）をＤｉｓａｂｌｅ（ポート遮断）にし、ループの発生を防止する。

【０１７８】

つまり、このレイヤ２ループ検知システムＳＹＳにおいては、矛盾している隣接ポートを特定した後、ＳＮＭＰ通信により、矛盾ポートの全てのポートのＭＩＢ情報をｕｐからｄｏｗｎにセットすることにより、ループ発生を防止する。

【０１７９】

［変形例］

上述した各実施の形態における処理はコンピュータで実行可能なプログラムとして提供され、ＣＤ－ＲＯＭやフレキシブルディスクなどの記録媒体、さらには通信回線を経て提供可能である。　また、上述した各実施の形態における各処理はその任意の複数または全てを選択し組合せて実施することもできる。

【０１８０】

［その他］

（付記１）複数のレイヤ２スイッチを有するレイヤ２ネットワークを監視対象とするＳＮＭＰマネージャによるレイヤ２ループ検知方法であって；

前記複数のレイヤ２スイッチからこれらレイヤ２スイッチのポートに関する情報を含むＭＩＢ情報をＳＮＭＰ通信により収集して、前記レイヤ２ネットワークの正常時のトポロジを認識し；

スパニングツリープロトコルＳＴＰに則って設定されたトラフィック遮断のためのブロッキングポートを前記トポロジ認識処理に基づいて識別し；

識別した前記ブロッキングポートを監視ポイントに設定してその状態を定期的に監視し；

前記ブロッキングポートの状態が変動したときをトリガに前記複数のレイヤ２スイッチから前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集して、前記レイヤ２ネットワークのトポロジを再認識し、レイヤ２ループを検知する；

レイヤ２ループ検知方法。

【０１８１】

（付記２）前記監視ポイントの状態として、前記ブロッキングポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポートからトラフィックが転送されているときをトリガにレイヤ２ループを検知する；
付記１記載のレイヤ２ループ検知方法。
【０１８２】
（付記３）前記監視ポイントの状態として、前記ブロッキングポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポートのポートステータスが変化したときをトリガにレイヤ２ループを検知する；
付記１記載のレイヤ２ループ検知方法。
【０１８３】
（付記４）複数のレイヤ２スイッチを有するレイヤ２ネットワークを監視対象とするＳＮＭＰマネージャによるレイヤ２ループ検知方法であって；
前記複数のレイヤ２スイッチからこれらレイヤ２スイッチのポートに関する情報を含むＭＩＢ情報をＳＮＭＰ通信により収集して、前記レイヤ２ネットワークの正常時のトポロジを認識し；
スパニングツリープロトコルＳＴＰに則って設定されたトラフィック遮断のためのブロッキングポートを前記トポロジ認識処理に基づいて識別できない場合、ポート無能状態のディセーブルポートを識別し；
識別した前記ディセーブルポートを監視ポイントに設定してその状態を定期的に監視し；
前記ディセーブルポートの状態が変動したときをトリガに前記複数のレイヤ２スイッチから前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集して、前記レイヤ２ネットワークのトポロジを再認識し、レイヤ２ループを検知する；
レイヤ２ループ検知方法。
【０１８４】
（付記５）前記監視ポイントの状態として、前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ディセーブルポートからトラフィックが転送されているときをトリガにレイヤ２ループを検知する；
付記４記載のレイヤ２ループ検知方法。
【０１８５】
（付記６）前記監視ポイントの状態として、前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ディセーブルポートのポートステータスが変化したときをトリガにレイヤ２ループを検知する；
付記４記載のレイヤ２ループ検知方法。
【０１８６】
（付記７）複数のレイヤ２スイッチを有するレイヤ２ネットワークを監視対象とするＳＮＭＰマネージャによるレイヤ２ループ検知方法であって；
前記複数のレイヤ２スイッチからこれらレイヤ２スイッチのポートに関する情報を含むＭＩＢ情報をＳＮＭＰ通信により収集して、前記レイヤ２ネットワークの正常時のトポロジを認識し；
スパニングツリープロトコルＳＴＰに則ってそれぞれ設定された、トラフィック遮断のためのブロッキングポート及びポート無能状態のディセーブルポートを前記トポロジ認識処理に基づいて識別し；
識別した前記ブロッキングポート及び前記ディセーブルポートを監視ポイントにそれぞれ設定してその状態を定期的に監視し；
前記ブロッキングポート及び前記ディセーブルポートのいずれかの状態が変動したときをトリガに前記複数のレイヤ２スイッチから前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集して、前記レイヤ２ネットワークのトポロジを再認識し、レイヤ２ループを検知する；
レイヤ２ループ検知方法。

【０１８７】
（付記８）前記監視ポイントの状態として、前記ブロッキングポート及び前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポート及び前記ディセーブルポートのいずれかからトラフィックが転送されているときをトリガにレイヤ２ループを検知する；
付記７記載のレイヤ２ループ検知方法。
【０１８８】
（付記９）前記監視ポイントの状態として、前記ブロッキングポート及び前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポート及び前記ディセーブルポートのいずれかのポートステータスが変化したときをトリガにレイヤ２ループを検知する；
付記７記載のレイヤ２ループ検知方法。
【０１８９】
（付記１０）前記レイヤ２スイッチから自律的に送信されるトポロジチェンジトラップの受信をトリガにレイヤ２ループを検知する；
付記１，４または７記載のレイヤ２ループ検知方法。
【０１９０】
（付記１１）前記レイヤ２スイッチから自律的に送信されるニュールートトラップの受信をトリガにレイヤ２ループを検知する；
付記１，４または７記載のレイヤ２ループ検知方法。
【０１９１】
（付記１２）前記レイヤ２スイッチはブリッジであり、前記レイヤ２ネットワークはイーサネットワーク（イーサネット：登録商標）である
付記１，４または７記載のレイヤ２ループ検知方法。
【０１９２】
（付記１３）前記ブロッキングポートまたは前記ディセーブルポートのＭＩＢ情報は、スクリプト言語ｉｆＯｕｔＯｃｔｅｔｓで示されるＳＮＭＰ通信対象のポートにおいて送信した総バイト数である
付記２，５または８記載のレイヤ２ループ検知方法。
【０１９３】
（付記１４）前記ブロッキングポートまたは前記ディセーブルポートのＭＩＢ情報は、スクリプト言語ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅで示されるＳＮＭＰ通信対象のポートのステータスの値である
付記３，６または９記載のレイヤ２ループ検知方法。
【０１９４】
（付記１５）複数のレイヤ２スイッチを有するレイヤ２ネットワークを監視対象とするＳＮＭＰマネージャによるレイヤ２ループ検知装置であって；
前記複数のレイヤ２スイッチからこれらレイヤ２スイッチのポートに関する情報を含むＭＩＢ情報をＳＮＭＰ通信により収集して、前記レイヤ２ネットワークの正常時のトポロジを認識する手段と；
スパニングツリープロトコルＳＴＰに則って設定されたトラフィック遮断のためのブロッキングポートを前記トポロジ認識処理に基づいて識別する手段と；
識別した前記ブロッキングポートを監視ポイントに設定してその状態を定期的に監視する手段と；
前記ブロッキングポートの状態が変動したときをトリガに前記複数のレイヤ２スイッチから前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集して、前記レイヤ２ネットワークのトポロジを再認識し、レイヤ２ループを検知する手段と；
を備えるレイヤ２ループ検知装置。
【０１９５】
（付記１６）前記監視ポイントの状態として、前記ブロッキングポートのＭＩＢ情報を

定期的に監視し、前記ブロッキングポートからトラフィックが転送されているときをトリガにレイヤ２ループを検知する；
付記１５記載のレイヤ２ループ検知装置。
【０１９６】
（付記１７）前記監視ポイントの状態として、前記ブロッキングポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポートのポートステータスが変化したときをトリガにレイヤ２ループを検知する；
付記１５記載のレイヤ２ループ検知装置。
【０１９７】
（付記１８）複数のレイヤ２スイッチを有するレイヤ２ネットワークを監視対象とするＳＮＭＰマネージャによるレイヤ２ループ検知装置であって；
前記複数のレイヤ２スイッチからこれらレイヤ２スイッチのポートに関する情報を含むＭＩＢ情報をＳＮＭＰ通信により収集して、前記レイヤ２ネットワークの正常時のトポロジを認識する手段と；
スパニングツリープロトコルＳＴＰに則って設定されたトラフィック遮断のためのブロッキングポートを前記トポロジ認識処理に基づいて識別できない場合、ポート無能状態のディセーブルポートを識別する手段と；
識別した前記ディセーブルポートを監視ポイントに設定してその状態を定期的に監視する手段と；
前記ディセーブルポートの状態が変動したときをトリガに前記複数のレイヤ２スイッチから前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集して、前記レイヤ２ネットワークのトポロジを再認識し、レイヤ２ループを検知する手段と；
を備えるレイヤ２ループ検知装置。
【０１９８】
（付記１９）前記監視ポイントの状態として、前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ディセーブルポートからトラフィックが転送されているときをトリガにレイヤ２ループを検知する；
付記１８記載のレイヤ２ループ検知装置。
【０１９９】
（付記２０）前記監視ポイントの状態として、前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ディセーブルポートのポートステータスが変化したときをトリガにレイヤ２ループを検知する；
付記１８記載のレイヤ２ループ検知装置。
【０２００】
（付記２１）複数のレイヤ２スイッチを有するレイヤ２ネットワークを監視対象とするＳＮＭＰマネージャによるレイヤ２ループ検知装置であって；
前記複数のレイヤ２スイッチからこれらレイヤ２スイッチのポートに関する情報を含むＭＩＢ情報をＳＮＭＰ通信により収集して、前記レイヤ２ネットワークの正常時のトポロジを認識する手段と；
スパニングツリープロトコルＳＴＰに則ってそれぞれ設定された、トラフィック遮断のためのブロッキングポート及びポート無能状態のディセーブルポートを前記トポロジ認識処理に基づいて識別する手段と；
識別した前記ブロッキングポート及び前記ディセーブルポートを監視ポイントにそれぞれ設定してその状態を定期的に監視する手段と；
前記ブロッキングポート及び前記ディセーブルポートのいずれかの状態が変動したときをトリガに前記複数のレイヤ２スイッチから前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集して、前記レイヤ２ネットワークのトポロジを再認識し、レイヤ２ループを検知する手段と；
を備えるレイヤ２ループ検知装置（１）。
【０２０１】

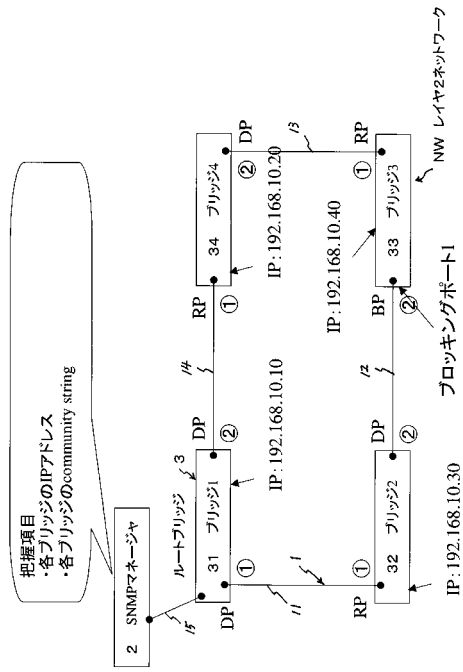
（付記２２）前記監視ポイントの状態として、前記ブロッキングポート及び前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポート及び前記ディセーブルポートのいずれかからトラフィックが転送されているときをトリガにレイヤ２ループを検知する；
付記２１記載のレイヤ２ループ検知装置（２）。
【０２０２】
（付記２３）前記監視ポイントの状態として、前記ブロッキングポート及び前記ディセーブルポートのＭＩＢ情報を定期的に監視し、前記ブロッキングポート及び前記ディセーブルポートのいずれかのポートステータスが変化したときをトリガにレイヤ２ループを検知する；
付記２１記載のレイヤ２ループ検知装置（３）。
【０２０３】
（付記２４）前記レイヤ２スイッチから自律的に送信されるトポロジチェンジトラップの受信をトリガにレイヤ２ループを検知する；
付記１５，１８または２１記載のレイヤ２ループ検知装置。
【０２０４】
（付記２５）前記レイヤ２スイッチから自律的に送信されるニュールートトラップの受信をトリガにレイヤ２ループを検知する；
付記１５，１８または２１記載のレイヤ２ループ検知装置。
【０２０５】
（付記２６）前記レイヤ２スイッチはブリッジであり、前記レイヤ２ネットワークはイーサネットワーク（イーサネット：登録商標）である；
付記１５，１８または２１記載のレイヤ２ループ検知装置。
【０２０６】
（付記２７）前記ブロッキングポートまたは前記ディセーブルポートのＭＩＢ情報は、スクリプト言語ｉｆＯｕｔＯｃｔｅｔｓで示されるＳＮＭＰ通信対象のポートにおいて送信した総バイト数である；
付記１６，１９または２２記載のレイヤ２ループ検知装置。
【０２０７】
（付記２８）前記ブロッキングポートまたは前記ディセーブルポートのＭＩＢ情報は、スクリプト言語ｄｏｔ１ｄＳｔｐＰｏｒｔＳｔａｔｅで示されるＳＮＭＰ通信対象のポートのステータスの値である；
付記１６，１９または２２記載のレイヤ２ループ検知装置。
【０２０８】
（付記２９）前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集する際に、そのＭＩＢ情報を収集できない前記レイヤ２スイッチがある場合、そのレイヤ２スイッチに接続されたポートが全て指定ポートになっていることを検知することにより、前記レイヤ２ループ箇所を検知する；
付記１５，１８または２１記載のレイヤ２ループ検知装置（４）。
【０２０９】
（付記３０）前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集する際に、リンクの両端がどちらも指定ポートになっているリンクを検知することにより、前記レイヤ２ループ箇所を推定する；
付記１５，１８または２１記載のレイヤ２ループ検知装置（５）。
【０２１０】
（付記３１）推定した前記レイヤ２ループ箇所の前記ＭＩＢ情報を収集し、矛盾の起こったポートにトラフィックが流れていることを検知することにより、前記レイヤ２ループ箇所を特定する；
付記２９または３０記載のレイヤ２ループ検知装置。
【０２１１】

（付記３２）推定した前記レイヤ２ループ箇所の前記ＭＩＢ情報を収集し、矛盾の起こったポートにトラフィックが流れていないことを検知することにより、前記レイヤ２スイッチまたは前記リンクの障害が発生していることを推定する；
付記２９または３０記載のレイヤ２ループ検知装置。
【０２１２】
（付記３３）矛盾している隣接ポートを特定した後、ＳＮＭＰ通信により、矛盾ポートの一部または全部のポートのＭＩＢ情報をアップからダウン（ｕｐ→ｄｏｗｎ）にセットすることにより、前記レイヤ２ループの発生を防止する；
付記３１記載のレイヤ２ループ検知装置。
【０２１３】
（付記３４）前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集する際に、そのＭＩＢ情報を収集できない前記レイヤ２スイッチがある場合、そのレイヤ２スイッチに接続されたポートが全て指定ポートになっていることを検知することにより、前記レイヤ２ループ箇所を検知する；
付記１，４または７記載のレイヤ２ループ検知方法。
【０２１４】
（付記３５）前記ＭＩＢ情報の一部をＳＮＭＰ通信により再収集する際に、リンクの両端がどちらも指定ポートになっているリンクを検知することにより、前記レイヤ２ループ箇所を推定する；
付記１，４または７記載のレイヤ２ループ検知方法。
【０２１５】
（付記３６）推定した前記レイヤ２ループ箇所の前記ＭＩＢ情報を収集し、矛盾の起こったポートにトラフィックが流れていることを検知することにより、前記レイヤ２ループ箇所を特定する；
付記３４または３５記載のレイヤ２ループ検知方法。
【０２１６】
（付記３７）推定した前記レイヤ２ループ箇所の前記ＭＩＢ情報を収集し、矛盾の起こったポートにトラフィックが流れていないことを検知することにより、前記レイヤ２スイッチまたは前記リンクの障害が発生していることを推定する；
付記３４または３５記載のレイヤ２ループ検知方法。
【０２１７】
（付記３８）矛盾している隣接ポートを特定した後、ＳＮＭＰ通信により、矛盾ポートの一部または全部のポートのＭＩＢ情報をアップからダウン（ｕｐ→ｄｏｗｎ）にセットすることにより、前記レイヤ２ループの発生を防止する；
付記３６記載のレイヤ２ループ検知方法。
【図面の簡単な説明】
【０２１８】
【図１】本発明の第１の実施の形態のレイヤ２ループ検知システムの構成を示すブロック図。
【図２】ＳＮＭＰマネージャの機能構成を示すブロック図。
【図３】第１の実施の形態のシステムにおけるＬ２ループ検知処理の説明図。
【図４】第１の実施の形態のシステムにおけるＭＩＢ情報の一覧を示す図。
【図５】本発明の第２の実施の形態のレイヤ２ループ検知システムの構成を示すブロック図。
【図６】第２の実施の形態のシステムにおけるＬ２ループ検知処理の説明図。
【図７】第２の実施の形態のシステムにおけるＭＩＢ情報の一覧を示す図。
【図８】本発明の第３の実施の形態のレイヤ２ループ検知システムの構成を示すブロック図。
【図９】第３の実施の形態のシステムにおけるＬ２ループ検知処理の説明図。
【図１０】第３の実施の形態のシステムにおけるＭＩＢ情報の一覧を示す図。

【図１１】本発明の第４の実施の形態のレイヤ２ループ検知システムの構成を示すブロック図。
【図１２】本発明の第５の実施の形態のレイヤ２ループ検知システムの構成を示すブロック図。
【図１３】本発明の第６の実施の形態のレイヤ２ループ検知システムの構成を示すブロック図。
【図１４】本発明の第７の実施の形態の第１のレイヤ２ループ検知システムの構成を示すブロック図。
【図１５】本発明の第７の実施の形態の第２のレイヤ２ループ検知システムの構成を示すブロック図。
【図１６】本発明の第７の実施の形態の第３のレイヤ２ループ検知システムの構成を示すブロック図。
【図１７】本発明の第７の実施の形態の第４のレイヤ２ループ検知システムの構成を示すブロック図。
【図１８】本発明の第８の実施の形態の第１のレイヤ２ループ検知システムの構成を示すブロック図。
【図１９】本発明の第８の実施の形態の第２のレイヤ２ループ検知システムの構成を示すブロック図。
【図２０】本発明の第８の実施の形態の第３のレイヤ２ループ検知システムの構成を示すブロック図。
【図２１】本発明の第８の実施の形態の第４のレイヤ２ループ検知システムの構成を示すブロック図。
【符号の説明】
【０２１９】

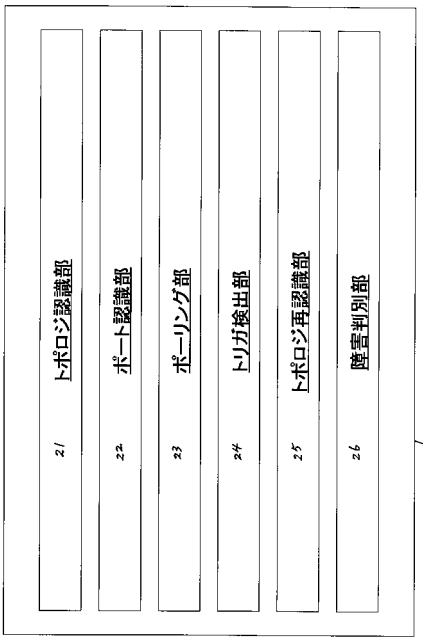
ＳＹＳ	レイヤ２ループ検知システム
ＮＷ	Ｌ２ネットワーク
１	ＬＡＮ
１１～１６	ＬＡＮ
２	ＳＮＭＰマネージャ（Ｌ２ループ検知装置）
３	ブリッジ（Ｌ２スイッチ）
３１～３４	ブリッジ（Ｌ２スイッチ）
４	ＳＮＭＰマネージャ
ＲＰ	ルートポート
ＤＰ	指定ポート
ＢＰ	ブロッキングポート
ＤｉｓＰ	ディセーブルポート

【図１】

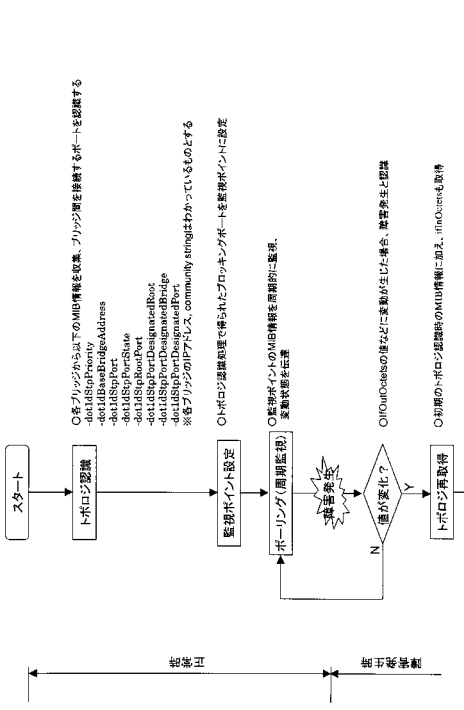


SYS 第1の実施の形態のレイヤ2ループ検知システム

【図２】



【図３】



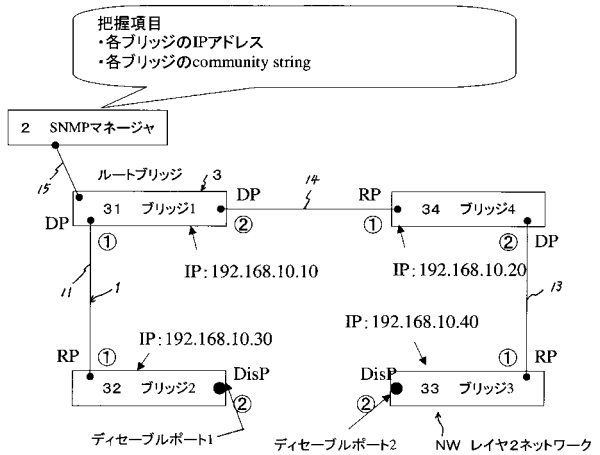
第1の実施の形態のL2ループ検知処理

【図４】

取得したMIB情報の一覧

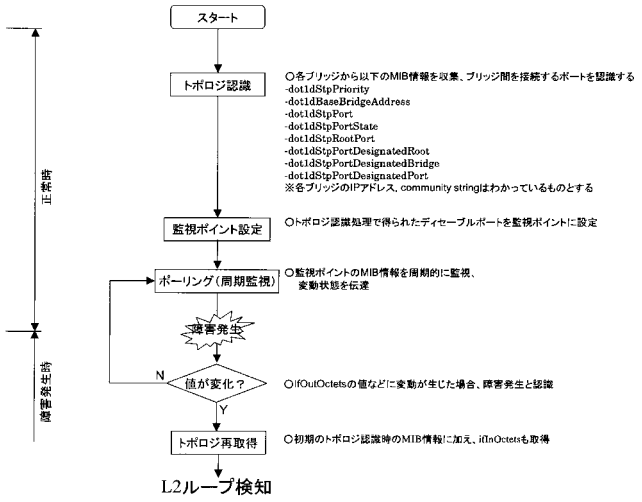
対象ブリッジIP	ポート	StpPriority	BaseBridgeAddress	StpRootPort	StpPort	StpPortState	StpDesignatedBridge	StpDesignatedPort
192.168.10.10	1	8032	00:00:00:00:00:01	なし	1	5	00:00:00:00:00:01	8001
	2				2	5	00:00:00:00:00:01	8002
192.168.10.20	1	8032	00:00:00:00:00:02	1	1	5	00:00:00:00:00:01	8002
	2				2	5	00:00:00:00:00:02	8002
192.168.10.30	1	8032	00:00:00:00:00:03	1	1	5	00:00:00:00:00:01	8001
	2				2	5	00:00:00:00:00:03	8002
192.168.10.40	1	8032	00:00:00:00:00:04	1	1	5	00:00:00:00:00:02	8002
	2				2	2	00:00:00:00:00:03	8002

【図５】



SYS 第2の実施の形態のレイヤ2ループ検知システム

【図６】



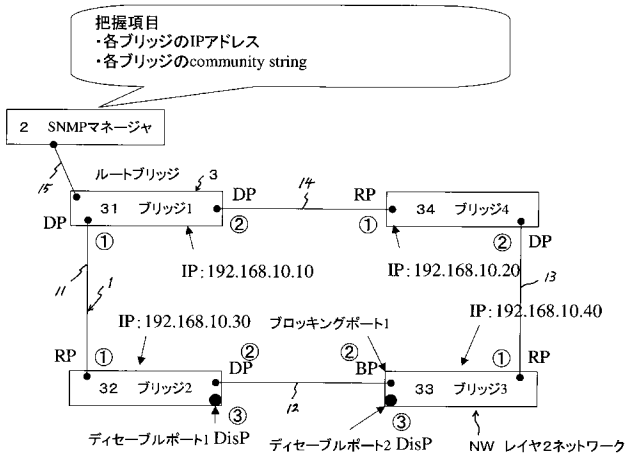
第2の実施の形態のL2ループ検知処理

【図７】

対象ブリッジIP	ポート	StpPriority	BaseBridgeAddress	StpRootPort	StpPort	StpPortState	StpdesignatedBridge	StpDesignatedPort
192.168.10.10	1	8032	00:00:00:00:00:01	なし	1	5	00:00:00:00:00:01	8001
	2				2	5	00:00:00:00:00:01	8002
192.168.10.20	1	8032	00:00:00:00:00:02	1	1	5	00:00:00:00:00:01	8002
	2				2	5	00:00:00:00:00:02	8002
192.168.10.30	1	8032	00:00:00:00:00:03	1	1	5	00:00:00:00:00:01	8001
	2				2	1		
192.168.10.40	1	8032	00:00:00:00:00:04	1	1	5	00:00:00:00:00:02	8002
	2				2	1		

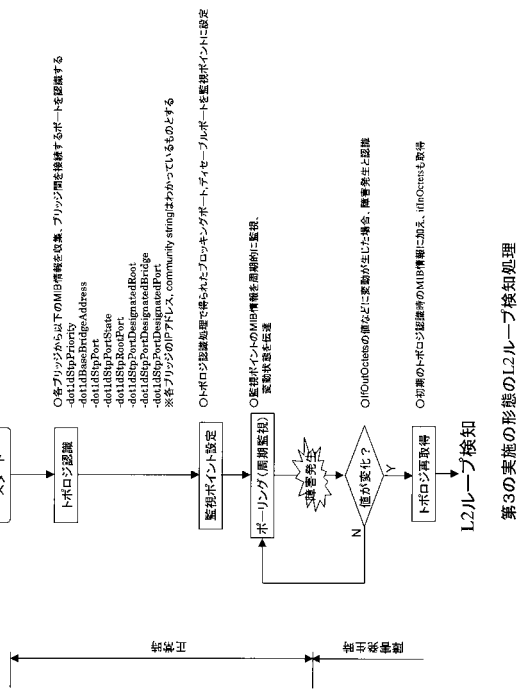
取得したMIB情報の一覧

【図８】



SYS 第3の実施の形態のレイヤ2ループ検知システム

【図９】



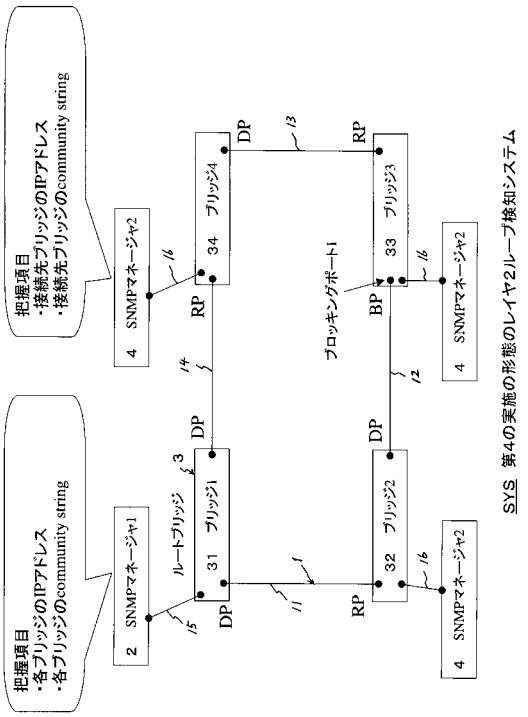
第3の実施の形態のL2ループ検知処理

【図１０】

対象ブリッジIP	ポート	StpPriority	BaseBridgeAddress	StpRootPort	StpPort	StpPortState	StpdesignatedBridge	StpDesignatedPort
192.168.10.10	1	8032	00:00:00:00:00:01	なし	1	5	00:00:00:00:00:01	8001
	2				2	5	00:00:00:00:00:01	8002
192.168.10.20	1	8032	00:00:00:00:00:02	1	1	5	00:00:00:00:00:01	8002
	2				2	5	00:00:00:00:00:02	8002
192.168.10.30	1	8032	00:00:00:00:00:03	1	1	5	00:00:00:00:00:01	8001
	2				2	5	00:00:00:00:00:03	8002
	3				3	1		
192.168.10.40	1	8032	00:00:00:00:00:04	1	1	5	00:00:00:00:00:02	8002
	2				2	2	00:00:00:00:00:03	8002
	3				3	1		

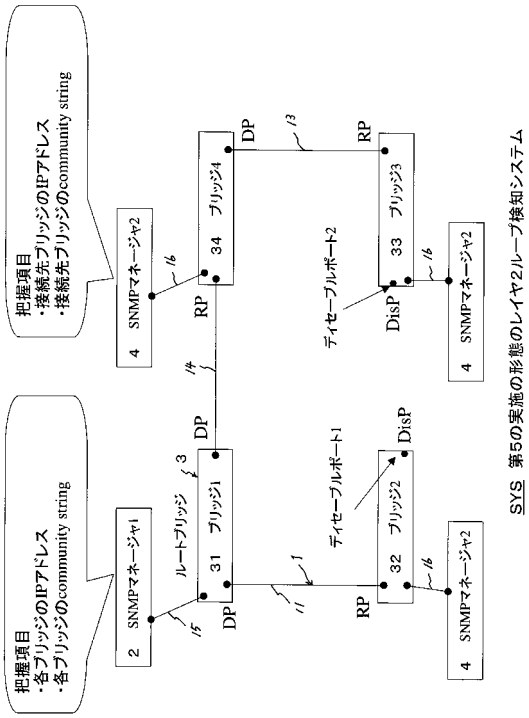
取得したMIB情報の一覧

【図１１】



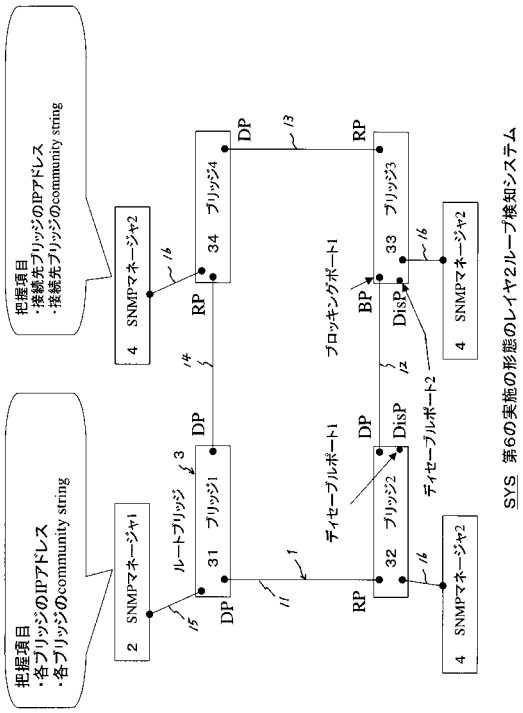
SYS 第4の実施の形態のレイヤ2ループ検知システム

【図１２】



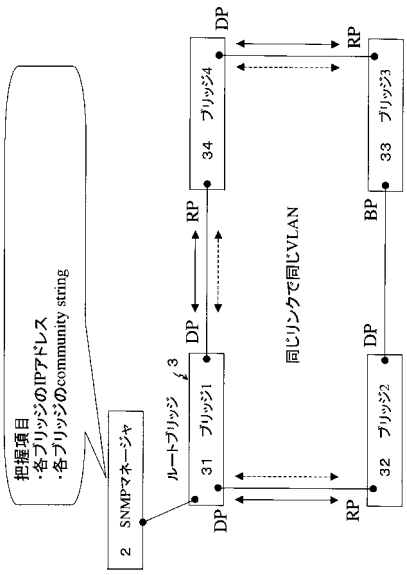
SYS 第5の実施の形態のレイヤ2ループ検知システム

【図１３】



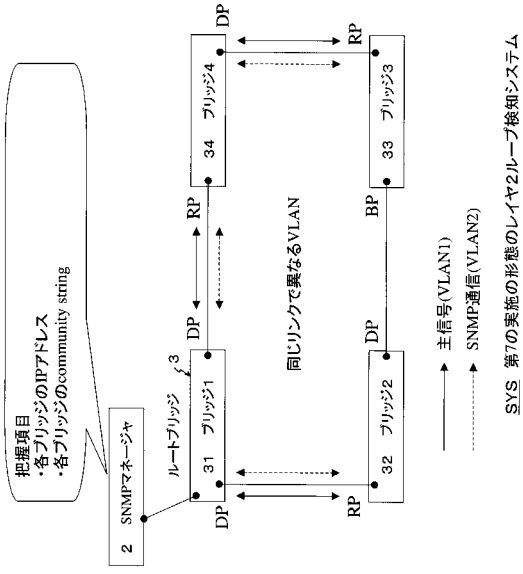
SYS 第6の実施の形態のレイヤ2ループ検知システム

【図１４】



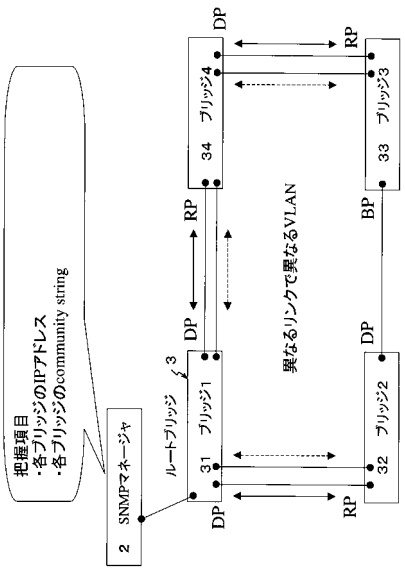
SYS 第7の実施の形態のレイヤ2ループ検知システム

【図１５】



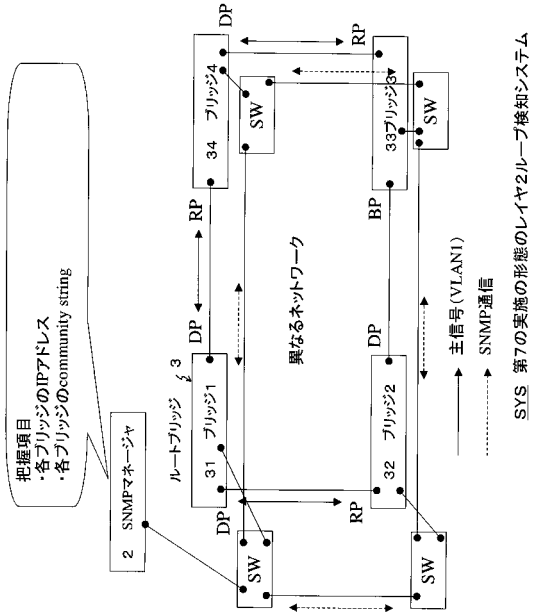
SYS 第7の実施の形態のレイヤ2ループ検知システム

【図１６】



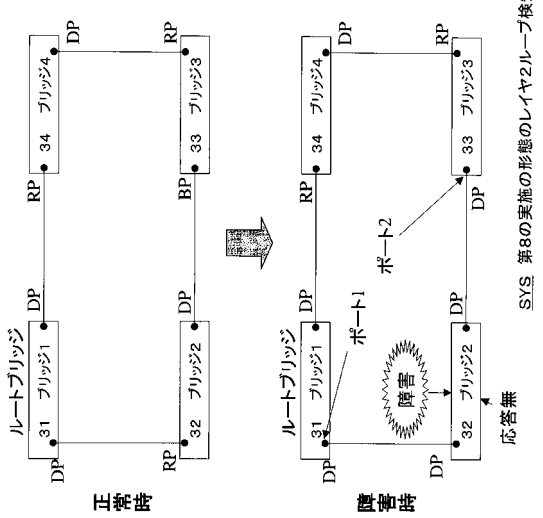
SYS 第7の実施の形態のレイヤ2ループ検知システム

【図１７】



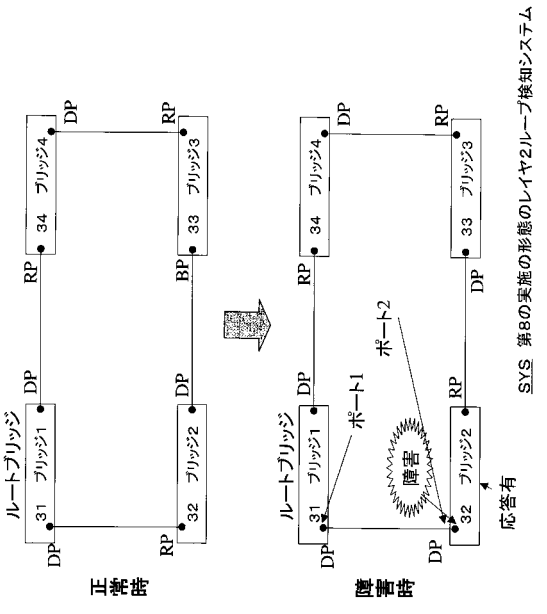
SYS 第7の実施の形態のレイヤ2ループ検知システム

【図１８】



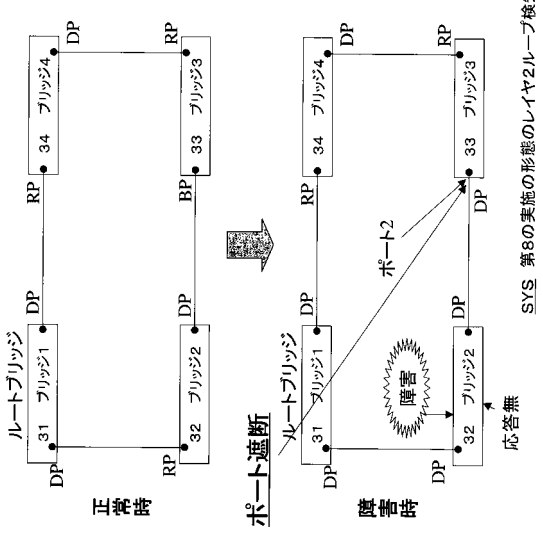
SYS 第8の実施の形態のレイヤ2ループ検知システム

【図１９】



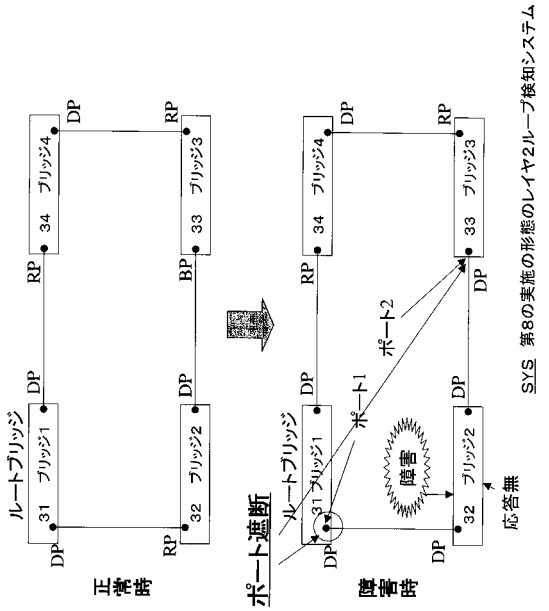
SYS 第8の実施の形態のレイヤ2ループ検知システム

【図２０】



SYS 第8の実施の形態のレイヤ2ループ検知システム

【図２１】



SYS 第8の実施の形態のレイヤ2ループ検知システム

フロントページの続き

(72)発明者　杉谷　樹一
神奈川県横浜市港北区新横浜三丁目９番１８号　富士通ネットワークテクノロジーズ株式会社内
(72)発明者　武藤　亮一
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　西　哲也
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　吉田　隆之

(56)参考文献　特開２００４－３６４０６５（ＪＰ，Ａ）
特開平８－３２６０９（ＪＰ，Ａ）
特開２００２－３００１６４（ＪＰ，Ａ）
特開２００２－３６８７７１（ＪＰ，Ａ）
特表２００５－５３９４０９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２