(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-56743
(P2010-56743A)
(43)公開日　平成22年3月11日(2010.3.11)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	(2006.01)	H04L	12/56	100A	5K028
H04J 3/00	(2006.01)	H04J	3/00	R	5K030
		H04J	3/00	U	

審査請求 未請求　請求項の数 6　OL　（全 17 頁）

(21)出願番号　特願2008-218139 (P2008-218139)
(22)出願日　平成20年8月27日 (2008.8.27)

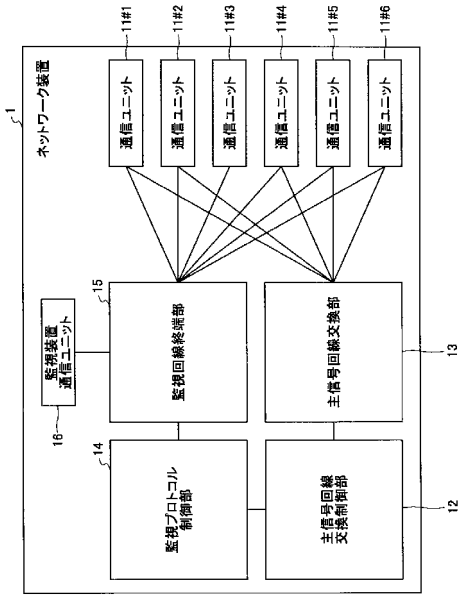
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　番場　正和
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5K028 AA14 BB08 CC05 LL02 QQ01
5K030 GA12 HA08 JA07 MA04 MB09
MD02

(54)【発明の名称】ネットワーク装置および回線設定制御方法

(57)【要約】
【課題】ＧＭＰＬＳ等の自律的な回線設定であっても、従来のＳＯＮＥＴ／ＳＤＨ等がサポートしていたリバーティブモードの機能をサポートする。
【解決手段】冗長化のためのワーク側とプロテクト側の回線の識別子を指定し、自律的に回線の設定を行う機能を有するネットワーク装置であって、回線の設定に関するメッセージに、リバーティブモードであるか否かを示すモード情報、パススイッチのデフォルト方向を示すデフォルト方向情報、および、リバーティブモードである場合に障害を起こした回線への切り戻しを監視するタイマ値を示すタイマ値情報を含めて他のネットワーク装置に送信する手段を備える。
【選択図】図６

本発明の一実施形態にかかるネットワーク装置の構成例を示す図



【特許請求の範囲】
【請求項１】
冗長化のためのワーク側とプロテクト側の回線の識別子を指定し、自律的に回線の設定を行う機能を有するネットワーク装置であって、
回線の設定に関するメッセージに、リバーティブモードであるか否かを示すモード情報、パススイッチのデフォルト方向を示すデフォルト方向情報、および、リバーティブモードである場合に障害を起こした回線への切り戻しを監視するタイマ値を示すタイマ値情報を含めて他のネットワーク装置に送信する手段
を備えたことを特徴とするネットワーク装置。
【請求項２】
前記メッセージを受信した場合に、当該メッセージに含まれるパススイッチのデフォルト方向から回線の設定を行う手段
を備えたことを特徴とする請求項１に記載のネットワーク装置。
【請求項３】
前記モード情報および前記タイマ値情報は、前記メッセージ中で使用されていないリザーブ領域に格納する
ことを特徴とする請求項１または２のいずれか一項に記載のネットワーク装置。
【請求項４】
前記デフォルト方向情報は、前記メッセージ中でワーク側とプロテクト側の区別をつけるためのプロテクティングビットを用いる
ことを特徴とする請求項１乃至３のいずれか一項に記載のネットワーク装置。
【請求項５】
前記メッセージを受信し、当該メッセージに前記モード情報および前記タイマ値情報が含まれない場合、非リバーティブモードとして回線の設定を行う
ことを特徴とする請求項１乃至４のいずれか一項に記載のネットワーク装置。
【請求項６】
冗長化のためのワーク側とプロテクト側の回線の識別子を指定し、自律的に回線の設定を行う機能を有するネットワーク装置の制御方法であって、
回線の設定に関するメッセージに、リバーティブモードであるか否かを示すモード情報、パススイッチのデフォルト方向を示すデフォルト方向情報、および、リバーティブモードである場合に障害を起こした回線への切り戻しを監視するタイマ値を示すタイマ値情報を含めて他のネットワーク装置に送信する工程
を備えたことを特徴とする回線設定制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＧＭＰＬＳ（Generalized Multi-Protocol Label Switching）等の自律的な回線設定の機能を有するネットワーク装置および回線設定制御方法に関する。
【背景技術】
【０００２】
信頼性の要求されるネットワークでは、障害時にサービスを中断させないため、１＋１プロテクトパス（1+1 protected path）といった回線の冗長構成がとられている。これは、ワーク（Work）側とプロテクト（Protect）側の２本の回線（パス：path）を設定し、ワーク側に障害が発生した場合にはプロテクト側に切り替えることでサービスの継続運用を可能とするものである。
【０００３】
従来のＳＯＮＥＴ（Synchronous Optical NETwork）／ＳＤＨ（Synchronous Digital Hierarchy）等において、回線の設定はネットワーク管理装置の集中管理のもとに行われており、１＋１プロテクトパスの設定にはＵＰＳＲ（Unidirectional Path Switched Ring）技術が利用されている。

【０００４】
パス切替（Path Switch）については、属性として、「リバーティブ（Revertive）モード」と、「パススイッチ（Path Switch）デフォルト方向」と、「ウエイトツーリストア（Wait To Restore）タイマ値」とが用いられている。
【０００５】
リバーティブモードとは、以下の動作をするモードである。
【０００６】
原則としてパススイッチデフォルト方向側を運用回線とし、ワーク側に障害が発生したとき一時的にプロテクト側へ運用回線を切り替えて運用を続ける。そして、ワーク側の障害が復旧してウエイトツーリストアタイマ値の時間にわたって障害が検出されなかったとき、再びパススイッチデフォルト方向側、すなわち、ワーク側へ運用回線を切り戻す。以上がリバーティブモードにおける動作である。
【０００７】
非リバーティブモードとは、以下の動作をするモードである。
【０００８】
現在運用している回線を運用回線とし、障害が起こったら他方の回線へ運用回線を切り替えて運用を続け、切り替えを起こした障害が復旧しても引き続き現在の運用回線で運用を続ける。以上が非リバーティブモードにおける動作である。
【０００９】
パススイッチデフォルト方向とは、リバーティブモード時の動作において、通常使われる回線を示し、これにより示される回線を通常の運用回線とする。ウエイトツーリストアタイマ値とは、リバーティブモード時の動作において、プロテクト側へ切り替わって運用されていて、かつ、ワーク側の障害がクリアになったとき、どのくらいの時間の監視時間をもってワーク側に切り戻るのかを決めるタイマ値である。
【００１０】
図１はモードによる属性値の必要不要の関係を示す図であり、リバーティブモードではパススイッチデフォルト方向とウエイトツーリストアタイマ値が必要とされ、非リバーティブモードではパススイッチデフォルト方向は必要とされるが、ウエイトツーリストアタイマ値は不要となる。
【００１１】
ところで、ＳＯＮＥＴ／ＳＤＨやＤＷＤＭ（Dense Wavelength Division Multiplexing）を利用したネットワークにおいて、ＧＭＰＬＳを利用した回線設定方法が注目されている。ＧＭＰＬＳでは自律的にネットワーク内に回線を設定することができるため、ネットワークの保守を簡略化できるものと期待されている。
【００１２】
現在、ＧＭＰＬＳの標準化が行われており、その中で１＋１プロテクトパスの実装方法が検討されている（例えば、ＲＦＣ４８７２）。そこでは、ワーク側（１本目）とプロテクト側（２本目）を関連付けるのに、ラベルスイッチパスＩＤ（LSP ID）（ＲＦＣ３２０９で定義されている。）とアソシエーションＩＤ（Association ID）（ＲＦＣ４８７２で定義されている。）という識別子を利用している。ラベルスイッチパスＩＤはエンドツーエンド（End to End）の回線（パス）を識別する識別子であり、アソシエーションＩＤはその回線と冗長構成のペアになる他の回線（パス）を識別する識別子である。
【００１３】
また、ワーク側とプロテクト側の区別をつけるために、プロテクティングビット（Protecting Bit）（ＲＦＣ４８７２で定義されている。）という識別子を利用している。プロテクティングビットのデフォルトは「０」であり、ワーク側であることを示す。「１」の場合はプロテクト側であることを示す。この方法により、自動で生成したパスのワーク側とプロテクト側を区別することが可能となった。
【００１４】
図２は回線設定を要求するパスメッセージ（Path Msg）および回線設定の完了を通知す

るリザーブメッセージ（Resv Msg）のフォーマット例を示す図であり、ＲＳＶＰ－ＴＥ（Resource Reservation Protocol - Traffic Engineering）で利用されているＴＬＶ（Type Length Value）により記述されたものである。ＴＬＶでは、値（Value）の型（Type）と構造体（オブジェクト）の長さ（Length）を記述することにより、任意の情報を伝達できるようにしている。

【００１５】

図２において、先頭の２行のブロックＢＬ１はメッセージ全体について記述したものであり、「Msg Type」が「１」の場合はパスメッセージ、「２」の場合はリザーブメッセージとなる。ブロックＢＬ２はセンダテンプレートオブジェクト（Sender Template Object）であり、ラベルスイッチパスＩＤ「LSP ID」が含まれる。ブロックＢＬ３はアソシエーションオブジェクト（Association Object）であり、アソシエーションＩＤ「Association ID」が含まれる。ブロックＢＬ４はプロテクションオブジェクト（Protection Object）であり、プロテクティングビット「Ｐ」が含まれる。

【００１６】

一方、特許文献１には、ＲＦＣ４８７２と同様に、ワーク側とプロテクト側を区別して管理するためのシグナリング技術が開示されている。

【特許文献１】特開２００８－６０７５５号公報

【発明の開示】

【発明が解決しようとする課題】

【００１７】

上述したように、ＧＭＰＬＳにおける１＋１プロテクトパスの実装方法が検討され、いくつかの拡張がなされているが、この拡張によっても、まだ従来の集中管理していたときに利用していたパラメータに関して不足している部分がある。すなわち、従来のＳＯＮＥＴ／ＳＤＨ規格で提供されているＵＰＳＲ技術の属性である「リバーティブモード」、「パススイッチデフォルト方向」、「ウエイトツーリストアタイマ値」については考慮されていない。

【００１８】

従って、ＧＭＰＬＳにおいて１＋１プロテクトパスを構築した場合、これらの属性を始点から終点へ伝達する手段がないため、運用形態としては非リバーティブモード形態しかサポートできない。

【００１９】

また、ＲＦＣ４８７２などで定義されている情報を用いて実際に回線設定を行うときには、２つの方式がある。１つは、ワーク側を設定したのち、プロテクト側を設定する逐次式と呼ばれる方式である。もう一つは、ワーク側とプロテクト側を同時に設定する同時設定式と呼ばれる方式である。逐次式は同時設定式に比べて回線設定に要する時間が長くかかるという短所がある。

【００２０】

そして、ＧＭＰＬＳにおいて１＋１プロテクトパスを構築した場合、運用形態としては非リバーティブモード形態のみとなり、更に、逐次式で運用しない限り、ワーク側から運用させるという制御ができない。別のいい方をすると、同時設定式で運用した場合、必ずワーク側が最初の運用回線となる保証がない。もし、期待するワーク側を選択していない状況になった場合には、ネットワーク監視装置から手動でワーク側を選択するように制御する必要が出てくる。

【００２１】

以下、これらの問題につき詳細に説明する。

【００２２】

図３は従来の逐次式による１＋１プロテクトパス構築の処理例を示すシーケンス図である。図３において、始点ノードＡではワーク側およびプロテクト側のＬＳＰ　ＩＤを決定したのち、ワーク側から回線設定処理を始める。すなわち、ワーク側の回線設定には、ＬＳＰ　ＩＤにワーク側のＬＳＰ　ＩＤを、Ａｓｓｏｃｉａｔｉｏｎ　ＩＤには　プロテク

ト側のＬＳＰ　ＩＤを設定し、これらを含めたパスメッセージを中間点ノードｎを経由して終点ノードＺに送信する（ステップＳ１、Ｓ２）。終点ノードＺでは中間点ノードｎを経由して始点ノードＡに向かい、回線設定をしてリザーブメッセージを送信する（ステップＳ３、Ｓ４）。

【００２３】

ワーク側の回線設定に成功すると、始点ノードＡではプロテクト側の回線設定処理を開始する。すなわち、ＬＳＰ　ＩＤにプロテクト側のＬＳＰ　ＩＤを、Ａｓｓｏｃｉａｔｉｏｎ　ＩＤにはワーク側のＬＳＰ　ＩＤを設定し、これらを含めたパスメッセージを中間点ノードｎを経由して終点ノードＺに送信する（ステップＳ５、Ｓ６）。終点ノードＺでは中間点ノードｎを経由して始点ノードＡに向かい、回線設定をしてリザーブメッセージを送信する（ステップＳ７、Ｓ８）。

【００２４】

このように、逐次式の場合は、ワーク側から設定を開始し、ワーク側の回線設定が成功しない限り、プロテクト側の回線設定を確立する処理を行わないので、必ずワーク側が運用側で、プロテクト側が予備側となる。

【００２５】

しかし、この方式の欠点は、逐次式のため、１回で２本の回線設定を行う同時設定式に比べて時間がかかることである。特に、実運用の回線設定で数十本から百本程度の回線を取り扱うケースを考えると顕著である。

【００２６】

図４はそのような複数の回線を取り扱う場合の処理例である。図４において、始点ノードＡから回線設定の命令を発呼する時点においては、すべての回線分同時に発呼される（ステップＳ１１）。これらが終点ノードＺへ向けて、中間点ノードｎ（中間ノード群）で処理される（ステップＳ１２）。明示的に同じ経路を発呼時に指示しない限り、同じ経路を通ることは保証されないため、設定する回線によって、異なる経路を通る場合がある。そのため、終点ノードＺへはランダムな順番で到達する。同様に、終点ノードＺから始点ノードＡへのメッセージも、中間ノード群の影響を受けて、ランダムな順番で到達する（ステップＳ１３、Ｓ１４）。

【００２７】

始点ノードＡでは到着順に逐次処理し、プロテクト側のパスメッセージを終点ノードＺに送信する（ステップＳ１５、Ｓ１６）。終点ノードＺでも到着順に逐次処理し、リザーブメッセージを始点ノードＡに送信する（ステップＳ１７、Ｓ１８）。なお、図では等間隔に到達しているように見えるが、実際には、到達する順序もその間隔も保証できない状態となっている。

【００２８】

逐次式の欠点は、始点ノードＡと終点ノードＺの間で、１発呼あたり２回もメッセージを往復させるため、この不安定な要素を増幅させている。例えば、同時設定式と比較してみると次のようなことがいえる。始点ノードＡから終点ノードＺへメッセージが到達する時間を３０秒、始点ノードＡと終点ノードＺでメッセージを処理する時間を３０秒としたときを考える。ワーク側のメッセージが、始点ノードＡから終点ノードＺを経て始点ノードＡまで戻ってくるときに必要な時間は、０秒（Ａでの処理がないため）＋３０秒（Ａ→Ｚ）＋３０秒（Ｚでの処理）＋３０秒（Ｚ→Ａ）で、トータル９０秒かかる。更に、プロテクト側のメッセージが、始点ノードＡから終点ノードＺを経て始点ノードＡに戻るときに必要な時間は、３０秒（Ａでの処理）＋３０秒（Ａ→Ｚ）＋３０秒（Ｚでの処理）＋３０秒（Ｚ→Ａ）＋３０秒（Ａでの処理）で、トータル１５０秒かかる。合計すると２４０秒かかる。これを同時式でやると、０秒（Ａでの処理がないため）＋３０秒（Ａ→Ｚ）＋６０秒（Ｚでの処理。ワーク側およびプロテクト側の分で３０×２）＋３０秒（Ｚ→Ａ）＋６０秒（Ｚでの処理。ワーク側およびプロテクト側の分で３０×２）で、トータル１８０秒かかる。逐次式ではプロテクト側のメッセージを往復させる分、確実に遅くなる（この例だと６０秒）。

【００２９】
図５は従来の同時設定式による１＋１プロテクトパス構築の処理例を示すシーケンス図であり、（ａ）は途中で逆転が起こらないケース、（ｂ）は途中で逆転が起こるケースである。
【００３０】
図５（ａ）（ｂ）のいずれにおいても、始点ノードＡではワーク側とプロテクト側のＬＳＰ　ＩＤを設定したのち、ワーク側のＡｓｓｏｃｉａｔｉｏｎ　ＩＤにプロテクト側のＬＳＰ　ＩＤを、プロテクト側のＡｓｓｏｃｉａｔｉｏｎ　ＩＤにワーク側のＬＳＰ　ＩＤを設定し、同時に回線設定処理を行う。すなわち、２つのパスメッセージをそれぞれ中間点ノードｎ１、ｎ２を経由して終点ノードＺに送信し（ステップＳ２１、Ｓ２２、Ｓ２５、Ｓ２６）、終点ノードＺでは始点ノードＡに向かい、回線設定をしてリザーブメッセージを送信する（ステップＳ２３、Ｓ２４、Ｓ２７、Ｓ２８）。
【００３１】
同時設定式の場合は、ワーク側とプロテクト側が同時に回線設定されるため、ワーク側が必ず先に構築されるとは限らない。つまり、プロテクト側が運用側で、ワーク側が予備側となる場合がある。なぜなら、ワーク側の処理とプロテクト側の処理は非同期であり、始点ノードＡから終点ノードＺまでのノード数の違いや、中継するノードのプロトコル処理速度により、終点ノードＺまでの到達時間は異なるためである。図５（ａ）の場合は途中で逆転が起こらないためワーク側が運用側となるが、図５（ｂ）の場合は途中で逆転が起こるためプロテクト側が運用側となってしまう。
【００３２】
同時設定式のメリットは、回線設定処理をワーク側とプロテクト側で同時に行うので、前述のように、逐次式よりも早く完了することである。しかし、先に処理を終了した方が一意に運用側となるため、ユーザからするとどちらが運用側になるかわからないという欠点を持つ。ユーザはこの欠点をフォローするため、ネットワーク監視装置からどちら側が現用回線になっているのかを確認し、場合によってはネットワーク監視装置から希望する回線を現用回線とする操作を行う必要がある。なお、従来のＳＯＮＥＴ／ＳＤＨ等では上位装置の集中管理のもとに回線設定が行われるため、リバーティブモード／非リバーティブモードにかかわらず、このような問題は発生しない。
【００３３】
上記の従来の問題点に鑑み、ＧＭＰＬＳ等の自律的な回線設定であっても、従来のＳＯＮＥＴ／ＳＤＨ等がサポートしていたリバーティブモードの機能をサポートすることのできるネットワーク装置および回線設定制御方法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】
【００３４】
このネットワーク装置の一実施態様では、冗長化のためのワーク側とプロテクト側の回線の識別子を指定し、自律的に回線の設定を行う機能を有するネットワーク装置であって、回線の設定に関するメッセージに、リバーティブモードであるか否かを示すモード情報、パススイッチのデフォルト方向を示すデフォルト方向情報、および、リバーティブモードである場合に障害を起こした回線への切り戻しを監視するタイマ値を示すタイマ値情報を含めて他のネットワーク装置に送信する手段を備える。
【発明の効果】
【００３５】
開示のネットワーク装置にあっては、ＧＭＰＬＳ等の自律的な回線設定であっても、従来のＳＯＮＥＴ／ＳＤＨ等がサポートしていたリバーティブモードの機能をサポートすることができる。
【発明を実施するための最良の形態】
【００３６】
以下、本発明の好適な実施形態につき説明する。
【００３７】

<構成>
図６は本発明の一実施形態にかかるネットワーク装置の構成例を示す図である。
【００３８】
図６において、ネットワーク装置１は、通信ユニット１１（１１＃１～１１＃６）と主信号回線交換制御部１２と主信号回線交換部１３と監視プロトコル制御部１４と監視回線終端部１５と監視装置通信ユニット１６とを備えている。
【００３９】
通信ユニット１１は、光信号（ＯＣｎ）や電気信号（ＥＣｎ）を終端する装置であり、他の装置と主信号（ユーザデータ）や制御データ（ネットワーク監視装置の信号やＯＳＰＦ－ＴＥ（Open Shortest Path First - Traffic Engineering）プロトコル、ＲＳＶＰ－ＴＥプロトコルの信号）をやりとりするインターフェースである。
【００４０】
主信号回線交換制御部１２は、主信号回線交換部１３に対して回線設定を行い、通信ユニット１１間の接続を制御する。
【００４１】
主信号回線交換部１３は、通信ユニット１１から伝達される主信号を別の通信ユニット１１へ回線接続するための装置であり、主信号回線交換制御部１２の指示に従って回線交換を行う。この主信号回線交換部１３を介して、複数ある通信ユニット１１は任意のチャネル（ＳＴＳ－ｃｈ）間で接続される。
【００４２】
監視プロトコル制御部１４は、実際にＧＭＰＬＳネットワーク維持に必要なＯＳＰＦ－ＴＥやＲＳＶＰ－ＴＥの処理を司る部分であり、監視回線終端部１５を通じて送受信されるプロトコルを解析し、プロトコルに応じた処理を行う。ここでは、主信号回線交換制御部１２と絶えず連携し、ユーザやＲＳＶＰ－ＴＥとして回線設定要求がきた場合には、主信号回線交換制御部１２に対して回線設定を要求する。
【００４３】
監視回線終端部１５は、他装置やネットワーク監視装置と送受信するプロトコルを生成したり終端したりする部分であり、ＯＳＩ（Open Systems Interconnection）ネットワークやＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）ネットワークとして伝搬されてくるＧＭＰＬＳネットワーク関連情報を終端し、監視プロトコル制御部１４が処理しやすい形にフォーマットし直す。
【００４４】
監視装置通信ユニット１６は、ネットワーク監視装置とネットワーク装置１を接続するためのインターフェースである。ネットワーク監視装置を接続するときに利用する。
【００４５】
図７は複数のネットワーク装置１（１Ａ～１Ｅ、１Ｚ）を用いたネットワークの例を示す図である。図７において、ＧＭＰＬＳネットワーク内にネットワーク装置１Ａ～１Ｅ、１Ｚが存在し、ネットワーク装置１Ａには外部ネットワーク３Ｐが接続され、ネットワーク装置１Ｚには外部ネットワーク３Ｑが接続されている。また、ネットワーク監視装置２がネットワーク装置１Ａに接続されている。ユーザは、ネットワーク装置１Ａ～１Ｅ、１Ｚで構成されるネットワークを経由して、外部ネットワーク３Ｐと外部ネットワーク３Ｑを接続したいと考えている場合を想定している（SPC Soft Permanent Connectionモデル）。また、ネットワーク装置１Ａを始点ノード、ネットワーク装置１Ｚを終点ノードとしている。ネットワーク装置１Ｂ～１Ｅは中間点ノードとなる。
【００４６】
<動作>
処理上で考慮すべき点は２つある。１つは、従来方式で取り扱えなかったリバーティブモード、パススイッチデフォルト方向、ウエイトツーリストアタイマ値をどうやって始点ノードと終点ノードで共有するか、という点である。もう１つは、どうやって効率よく、ワーク側（１本目）を正しく運用回線として設定させるかである。前者は、パススイッチ

管理に必要な事項である。後者は、回線設定において、無駄なスイッチ（ネットワーク監視装置からの制御によるスイッチ）を必要とすることなく、ワーク側回線を運用回線とするために必要となる。

【００４７】

パススイッチを管理するパラメータを始点ノードと終点ノードとで共有するために、本実施形態では、ＲＦＣ４８７２に定義しているプロテクションオブジェクトのリザーブ（Reserved）領域を利用している。図８はプロテクションオブジェクトのフォーマット例を示す図であり、最後の行（リザーブ領域）に、リバーティブモードを示す「Ｒ」ビットと、ウエイトツーリストアタイマ値を示す「Ｗａｉｔ　Ｔｏ　Ｒｅｓｔｏｒｅ」とを割り当てている。このプロテクションオブジェクトは、図２のパスメッセージのブロックＢＬ４に置き換えられる。これにより、リバーティブモードおよびウエイトツーリストアタイマ値の設定を始点ノードから終点ノードへ送信できるようになる。また、パススイッチデフォルト方向の設定は、プロテクションオブジェクトのプロテクティングビット「Ｐ」（図８のフォーマットの２行目）を利用し、後述する回線設定ロジックで求めることにする。

【００４８】

以下、図７に示したネットワーク構成を前提に、ネットワーク装置１Ａに対しユーザがＲＳＶＰ－ＴＥの回線設定要求を発行し、ネットワーク装置１Ａが経路計算を行い、ネットワーク装置１Ａからネットワーク装置１Ｚまで１＋１プロテクトパスを確立する場合を考える。

【００４９】

この場合、始点ノードのネットワーク装置１Ａは、ユーザから入力されたパラメータ（リバーティブモード、パススイッチデフォルト方向、ウエイトツーリストアタイマ値）をプロテクションオブジェクトに設定し、パスメッセージに設定する。終点ノードのネットワーク装置１Ｚは、そのプロテクションオブジェクトを含むパスメッセージを受信する。そして、受信したパスメッセージを回線設定ロジックに従って解析する。ここでは、先ず、パススイッチデフォルト方向をプロテクティングビットから決定する。その後、プロテクションオブジェクトの拡張した部分を読み出し、リバーティブモードかどうか判定する。リバーティブモードであった場合、引き続き、ウエイトツーリストアタイマ値をプロテクションオブジェクトの拡張した部分から読み出す。そして、これらの値を利用して、回線設定を行う。効率よくワーク側を運用回線とするためには、始点ノード、終点ノードそれぞれにおいて、ワーク側の回線設定処理がプロテクト側の回線設定処理よりも先に行われるように処理順序を制御する必要がある。

【００５０】

以下、より詳細に動作を説明する。

【００５１】

図９は始点ノードの処理例を示すフローチャート、図１０は終点ノードの処理例を示すフローチャート、図１１は回線設定ロジックの例を示すフローチャートである。

【００５２】

図９において、始点ノードのネットワーク装置１Ａにおいては、先ず、ユーザからユーザの希望するパラメータ（リバーティブモード、パススイッチデフォルト方向、ウエイトツーリストアタイマ値）が入力される（ステップＳ１０１）。その後、必要に応じて経路計算が行われる（ステップＳ１０２～Ｓ１０４）。

【００５３】

回線設定を行う経路が求まった段階で、プロテクションオブジェクトの生成処理を行う。すなわち、プロテクティングビットは、デフォルト方向用のパスメッセージには「０」を、そうでないパスメッセージには「１」を設定する（ステップＳ１０５）。次いで、リバーティブモードおよびウエイトツーリストアタイマ値をプロテクションオブジェクトに設定する（ステップＳ１０６）。そして、プロテクションオブジェクトを含むパスメッセージを終点ノードのネットワーク装置１Ｚへ送信する（ステップＳ１０７、Ｓ１０８）。このとき、同時に２本分送信する。逐次式のように、ワーク側の設定結果を待たなくてよ

い。始点ノードのネットワーク装置１Ａから送られたパスメッセージは、終点ノードのネットワーク装置１Ｚで処理される。

【００５４】

次に、図１０において、終点ノードのネットワーク装置１Ｚは、パスメッセージを受信すると、先ず、アソシエーションＩＤがあるか否かチェックし（ステップＳ１２１、Ｓ１２２）、アソシエーションＩＤがない場合は１＋１プロテクトパス確立要求でないとして従来通りのパスメッセージの処理を行って処理を終了する（ステップＳ１２３、Ｓ１２４）。

【００５５】

アソシエーションＩＤがある場合は、受信したパスメッセージのプロテクションオブジェクトのプロテクティングビットをみて、ワーク側か、プロテクト側かを判定する（ステップＳ１２５、Ｓ１２６）。そして、ワーク側であった場合は、受信したパスメッセージに含まれるリバーティブモード、パススイッチデフォルト方向、ウエイトツーリストアタイマ値を用いて回線の設定を行う（ステップＳ１２７、Ｓ１２９）。プロテクト側であった場合は、設定情報をワーク側を受信するまで退避しておき（ステップＳ１２８）、ワーク側の設定が終了した時点で、プロテクト側のパスメッセージ処理を同様に行って回線設定を行う（ステップＳ１３０～Ｓ１３４）。

【００５６】

そして、２本とも終わった時点で、始点ノードのネットワーク装置１Ａに向かって、リザーブメッセージを送信する（ステップＳ１３５、Ｓ１３７、Ｓ１３８）。もし、パスメッセージ受信処理において、ワーク側もしくはプロテクト側を受信し損ねた場合は、従来技術を踏襲し、パスエラーメッセージ（Path Err Message）を送信することによって、始点ノードのネットワーク装置１Ａに対しエラーが発生したことを通知する（ステップＳ１３６）。

【００５７】

図９に戻り、終点ノードのネットワーク装置１Ｚから送られたリザーブメッセージを受信した始点ノードのネットワーク装置１Ａは、先ず、プロテクションオブジェクトのプロテクティングビットをみて、ワーク側のリザーブメッセージか、プロテクト側のリザーブメッセージかを判定する（ステップＳ１０９、Ｓ１１０）。もし、プロテクト側を受信していたら、ワーク側を受信し、その回線設定が終わるまで退避させる（ステップＳ１１１）。もし、ワーク側を受信した場合は、受信したリザーブメッセージのプロテクションオブジェクトが自己が送信したパスメッセージのプロテクションオブジェクトと同じかどうか判断し（ステップＳ１１２）、同じである場合はそのまま回線設定を行う（ステップＳ１１４）。同じでない場合は、対向装置が今回の拡張に対応していない装置であるとして、非リバーティブモードとなるように回線設定情報を作り（ステップＳ１１３）、回線設定を行う（ステップＳ１１４）。これは、終点ノードのネットワーク装置１Ｚが今回の拡張に対応していない従来装置であって、始点ノードが送出したプロテクションオブジェクトの内容を返信できない場合に対応するものである。そのため、始点ノードのネットワーク装置１Ａにおいて、受信したプロテクションオブジェクトの内容と、始点ノード自身が送出したプロテクションオブジェクトの内容を比較することによって拡張に対応しているか否か判断が可能である。そして、自分の送った内容が戻ってこなかった場合には、拡張したプロトコルをサポートしていないと認識し、非リバーティブモードとして回線設定を行うように動作している。

【００５８】

続いて、プロテクト側についても同様に回線設定処理を行う（ステップＳ１１５～Ｓ１１９）。

【００５９】

図１１は回線設定ロジックの例を示すフローチャートである。図１１において、回線設定を開始すると、プロテクションオブジェクトのプロテクティングビットが「０」かどうか判断する（ステップＳ１４１）。プロテクティングビットが「０」である場合にはパス

スイッチデフォルト方向を自分側とし（ステップＳ１４２）、「０」でない場合はパススイッチデフォルト方向をアソシエーションＩＤで指定されている側とする（ステップＳ１４３）。

【００６０】

次いで、リバーティブモードの値をプロテクションオブジェクトから読み出し（ステップＳ１４４）、リバーティブモードであるか否か判断する（ステップＳ１４５）。リバーティブモードである場合はウエイトツーリストアタイマ値をプロテクションオブジェクトから読み出し（ステップＳ１４６）、収集した値をもとに回線設定を行う（ステップＳ１４７）。リバーティブモードでない場合は上段で収集した値をもとに回線設定を行う（ステップＳ１４７）。

【００６１】

次に、具体的に、始点ノード・終点ノード間の動作について説明する。

【００６２】

図１２はネットワーク上の回線設定の例を示す図であり、図７と同じネットワーク構成を前提としている。また、図１３～図１５はその際の処理例を示すシーケンス図であり、図１３はパスメッセージの処理中に逆転が起こるケース、図１４はリザーブメッセージの処理中に逆転が起こるケース、図１５はパスメッセージおよびリザーブメッセージの処理中に逆転が起こるケースである。

【００６３】

図１３に示すケース、すなわち始点ノードのネットワーク装置１Ａから終点ノードのネットワーク装置１Ｚへ行く間、つまりパスメッセージを処理する過程において、ワーク側のパスメッセージとプロテクト側のパスメッセージに逆転が起こるケースを考える。このケースにおいては、始点ノードのネットワーク装置１Ａよりワーク側、プロテクト側のパスメッセージが送信される（ステップＳ２０１、Ｓ２０２）。その後、何らかの理由により、終点ノードのネットワーク装置１Ｚへは、プロテクト側が先に届く（ステップＳ２０３）。パスメッセージを受信した終点ノードのネットワーク装置１Ｚは、ワーク側のパスメッセージか、プロテクト側のパスメッセージかを判定し、プロテクト側のパスメッセージということで、メッセージを受領するが処理せず保管しておく。その後、異なるパスメッセージを受信し（ステップＳ２０４）、ワーク側のパスメッセージであることを判定できたら、パスメッセージの情報にしたがって回線設定を行う。この処理により、図１２における（１）の回線設定が実施される。終点ノードのネットワーク装置１Ｚでのワーク側の回線設定が完了すると、プロテクト側の回線設定が行われる。この処理により、図１２の（２）の回線設定が実施される。その後、ワーク側、プロテクト側のリザーブメッセージが終点ノードのネットワーク装置１Ｚから始点ノードのネットワーク装置１Ａへ送信される（ステップＳ２０５～Ｓ２０８）。

【００６４】

始点ノードのネットワーク装置１Ａでは、受信したリザーブメッセージを解析し、ワーク側のリザーブメッセージか、プロテクト側のリザーブメッセージかを判定する。その後、ワーク側と判定されたとき、図１２の（３）の回線設定が実施される。その後、異なるリザーブメッセージを受信し、解析し、プロテクト側と判定されたとき、図１２の（４）の回線設定が実施される。最後に、（３）→（４）と設定することで、必ずワーク側の方が先に無障害状態になり、現用回線として選択されることになる。

【００６５】

次に、図１４に示すケース、すなわち始点ノードのネットワーク装置１Ａから終点ノードのネットワーク装置１Ｚへ行く間にはパスメッセージの逆転が起こらず、終点ノードのネットワーク装置１Ｚから始点ノードのネットワーク装置１Ａへ行く間、つまりリザーブメッセージを処理する過程において、ワーク側とプロテクト側のリザーブメッセージに逆転が起こるケースを考える。このケースにおいては、始点ノードのネットワーク装置１Ａから送出されたパスメッセージ（ステップＳ２１１、Ｓ２１２）は、ワーク側、プロテクト側の順序で、終点ノードのネットワーク装置１Ｚへ到達する（ステップＳ２１３、Ｓ２

１４）。終点ノードのネットワーク装置１Ｚは、受信したパスメッセージのプロテクションオブジェクトに含まれるプロテクティングビットをみて、ワーク側のパスメッセージかプロテクト側のパスメッセージかを判定する。そして、ワーク側のパスメッセージであることを認識したら、図１２の（１）の回線設定が実施される。その後、受信したパスメッセージのプロテクティングビットを解析し、プロテクト側と認識したら、図１２の（２）の回線設定が実施される。そして、ワーク側、プロテクト側それぞれのリザーブメッセージが終点ノードのネットワーク装置１Ｚから始点ノードのネットワーク装置１Ａへ送信される（ステップＳ２１５、Ｓ２１６）。

【００６６】

その途中の過程において、ワーク側とプロテクト側のメッセージ処理時間の差が生じ、始点ノードのネットワーク装置１Ａには、プロテクト側、ワーク側という順序で到達する（ステップＳ２１７、Ｓ２１８）。始点ノードのネットワーク装置１Ａは、受信したリザーブメッセージからプロテクションオブジェクトのプロテクティングビットを見て、プロテクト側のリザーブメッセージか、ワーク側のリザーブメッセージかを判定する。プロテクト側のものを受信した場合は、リザーブメッセージは受領するが、回線設定処理（図１２の（４）の設定）は行わない。そして、ワーク側のリザーブメッセージを受信するまで待つ。ワーク側のリザーブメッセージの受信は、受信したリザーブメッセージのプロテクションオブジェクトのプロテクティングビットをみる。そして、ワーク側と判定されたとき、図１２の（３）の回線設定が実施される。その後、受領していたプロテクト側のリザーブメッセージの処理（図１２の（４）の回線設定）を行う。ここも、（１）→（２）と（３）→（４）と回線を設定することで、ワーク側から現用回線となるようにコントロールしている。

【００６７】

次に、図１５に示すケース、すなわち始点ノードのネットワーク装置１Ａから終点ノードのネットワーク装置１Ｚへのパスメッセージでも、終点ノードのネットワーク装置１Ｚから始点ノードのネットワーク装置１Ａへのリザーブメッセージでもメッセージを処理する過程において逆転が起こるケースを考える。このケースは、図１３と図１４を複合したものとなる。パスメッセージの逆転に関しては、図１３で説明した動作を行う。リザーブメッセージの逆転に関しては、図１４で説明した動作を行う。これにより、このケースにおいても、図１２において（１）→（２）と（３）→（４）と回線を設定することができ、ワーク側から現用回線となるようにコントロールしている。

【００６８】

最後に、今回の拡張に対応していない従来装置が対向装置（ネットワーク装置１Ａが拡張に対応しているならネットワーク装置１Ｚが対向装置。ネットワーク装置１Ｚが拡張に対応しているならネットワーク装置１Ａが対向装置）となるケースについて考える。始点ノードが拡張に対応し、終点ノードが従来装置の場合については、図９のリザーブメッセージの処理（ステップＳ１１２、Ｓ１１３、Ｓ１１７、Ｓ１１８）において対応している。

【００６９】

その他の場合については、次のような動作となる。すなわち、本実施形態においては、パススイッチデフォルト方向をプロテクションオブジェクトのプロテクティングビットより収集する。これは、発明如何によらず同じ使い方をする。従って、対向装置がプロテクションオブジェクトをＲＦＣ４８７２の定義のまま利用すると、対向装置が拡張をサポートしているか否かによらず、拡張に対応している側ではパススイッチデフォルト方向を設定することが可能となる。本実施形態では、リバーティブモードの判定とウエイトツーリストアタイマ値の授受に際し、プロテクションオブジェクトのリザーブ領域を利用している。一般に、ＲＦＣの動作として、リザーブ領域は「０」で埋めることを行っている。このルールに従った対向装置であれば、リザーブ領域を「０」として取り扱うため、拡張に対応している側からみると、非リバーティブモード（Ｒ　ｂｉｔが「０」）でウエイトツーリストアタイマ値が「０」ということが要求されていることになる。これにより、対向

装置が拡張をサポートしていなくても、ＩＥＴＦに従って動作しているケースにおいては、問題なく非リバーティブモードとして動作することができる。

【００７０】

<総括>

以上説明したように、本実施形態によれば次のような利点がある。

（１）ＧＭＰＬＳ等の自律的な回線設定であっても、従来のＳＯＮＥＴ／ＳＤＨ等のオペレーションで提供していたリバーティブモードの機能をサポートすることができる。

（２）パスレベルに必要な情報はシグナリングメッセージ内に埋め込まれ、回線の始点ノードと終点ノードがパスレベルに必要な情報を別途送受する必要がない。特に、メッセージのフォーマットに必要最小限の拡張を行い、別のメッセージオブジェクトを定義してそこでこれらの情報を取り扱うことはしていないため、既存技術との親和性が高い。

（３）シグナリングメッセージ内に埋め込まれた、ワーク側／プロテクト側の情報を判断することにより、リバーティブモード／非リバーティブモードにかかわらず始点ノードおよび終点ノードにおいて、必ずワーク側から回線設定を行うことができる。

（４）今回の拡張をサポートしていない機器と対向しても、必ずパススイッチデフォルト方向が判別でき、かつ、非リバーティブモードとして動作することができる。

【００７１】

以上、本発明の好適な実施の形態により本発明を説明した。ここでは特定の具体例を示して本発明を説明したが、特許請求の範囲に定義された本発明の広範な趣旨および範囲から逸脱することなく、これら具体例に様々な修正および変更を加えることができることは明らかである。すなわち、具体例の詳細および添付の図面により本発明が限定されるものと解釈してはならない。

（付記１）　冗長化のためのワーク側とプロテクト側の回線の識別子を指定し、自律的に回線の設定を行う機能を有するネットワーク装置であって、

回線の設定に関するメッセージに、リバーティブモードであるか否かを示すモード情報、パススイッチのデフォルト方向を示すデフォルト方向情報、および、リバーティブモードである場合に障害を起こした回線への切り戻しを監視するタイマ値を示すタイマ値情報を含めて他のネットワーク装置に送信する手段

を備えたことを特徴とするネットワーク装置。

（付記２）　前記メッセージを受信した場合に、当該メッセージに含まれるパススイッチのデフォルト方向から回線の設定を行う手段

を備えたことを特徴とする付記１に記載のネットワーク装置。

（付記３）　前記モード情報および前記タイマ値情報は、前記メッセージ中で使用されていないリザーブ領域に格納する

ことを特徴とする付記１または２のいずれか一項に記載のネットワーク装置。

（付記４）　前記デフォルト方向情報は、前記メッセージ中でワーク側とプロテクト側の区別をつけるためのプロテクティングビットを用いる

ことを特徴とする付記１乃至３のいずれか一項に記載のネットワーク装置。

（付記５）　前記メッセージを受信し、当該メッセージに前記モード情報および前記タイマ値情報が含まれない場合、非リバーティブモードとして回線の設定を行う

ことを特徴とする付記１乃至４のいずれか一項に記載のネットワーク装置。

（付記６）　冗長化のためのワーク側とプロテクト側の回線の識別子を指定し、自律的に回線の設定を行う機能を有するネットワーク装置の制御方法であって、

回線の設定に関するメッセージに、リバーティブモードであるか否かを示すモード情報、パススイッチのデフォルト方向を示すデフォルト方向情報、および、リバーティブモードである場合に障害を起こした回線への切り戻しを監視するタイマ値を示すタイマ値情報を含めて他のネットワーク装置に送信する工程

を備えたことを特徴とする回線設定制御方法。

（付記７）　前記メッセージを受信した場合に、当該メッセージに含まれるパススイッチのデフォルト方向から回線の設定を行う工程

を備えたことを特徴とする付記６に記載の回線設定制御方法。
（付記８）　前記モード情報および前記タイマ値情報は、前記メッセージ中で使用されていないリザーブ領域に格納する
ことを特徴とする付記６または７のいずれか一項に記載の回線設定制御方法。
（付記９）　前記デフォルト方向情報は、前記メッセージ中でワーク側とプロテクト側の区別をつけるためのプロテクティングビットを用いる
ことを特徴とする付記６乃至８のいずれか一項に記載の回線設定制御方法。
（付記１０）　前記メッセージを受信し、当該メッセージに前記モード情報および前記タイマ値情報が含まれない場合、非リバーティブモードとして回線の設定を行う
ことを特徴とする付記６乃至９のいずれか一項に記載の回線設定制御方法。

【図面の簡単な説明】
【００７２】
【図１】モードによる属性値の必要不要の関係を示す図である。
【図２】メッセージのフォーマット例を示す図である。
【図３】従来の逐次式による１＋１プロテクトパス構築の処理例を示すシーケンス図（その１）である。
【図４】従来の逐次式による１＋１プロテクトパス構築の処理例を示すシーケンス図（その２）である。
【図５】従来の同時設定式による１＋１プロテクトパス構築の処理例を示すシーケンス図である。
【図６】本発明の一実施形態にかかるネットワーク装置の構成例を示す図である。
【図７】複数のネットワーク装置を用いたネットワークの例を示す図である。
【図８】プロテクションオブジェクトのフォーマット例を示す図である。
【図９】始点ノードの処理例を示すフローチャートである。
【図１０】終点ノードの処理例を示すフローチャートである。
【図１１】回線設定ロジックの例を示すフローチャートである。
【図１２】ネットワーク上の回線設定の例を示す図である。
【図１３】実施形態の処理例を示すシーケンス図（その１）である。
【図１４】実施形態の処理例を示すシーケンス図（その２）である。
【図１５】実施形態の処理例を示すシーケンス図（その３）である。

【符号の説明】
【００７３】
１　　ネットワーク装置
１１　　通信ユニット
１２　　主信号回線交換制御部
１３　　主信号回線交換部
１４　　監視プロトコル制御部
１５　　監視回線終端部
１６　　監視装置通信ユニット
２　　ネットワーク監視装置
３　　外部ネットワーク

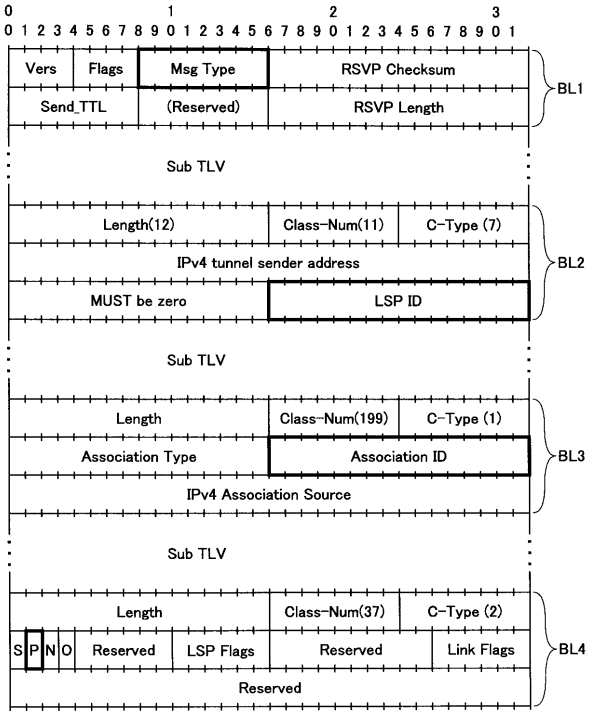
【図１】

モードによる属性値の必要不要の関係を示す図

	Path Switch デフォルト方向	Wait To Restore タイマ値
Revertiveモード	必要	必要
非Revertiveモード	必要	不要

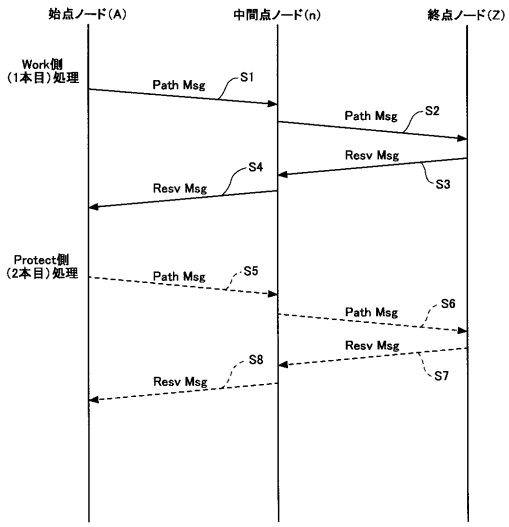
【図２】

メッセージのフォーマット例を示す図



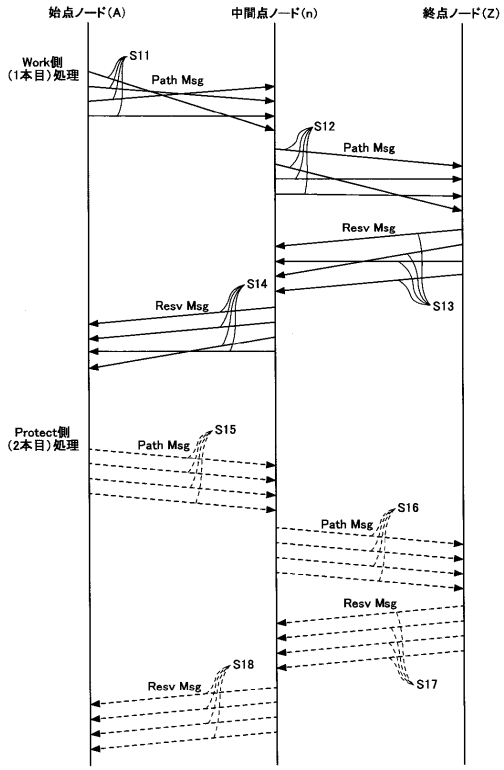
【図３】

従来の逐次式による
１＋１プロテクトパス構築の処理例を示すシーケンス図（その１）



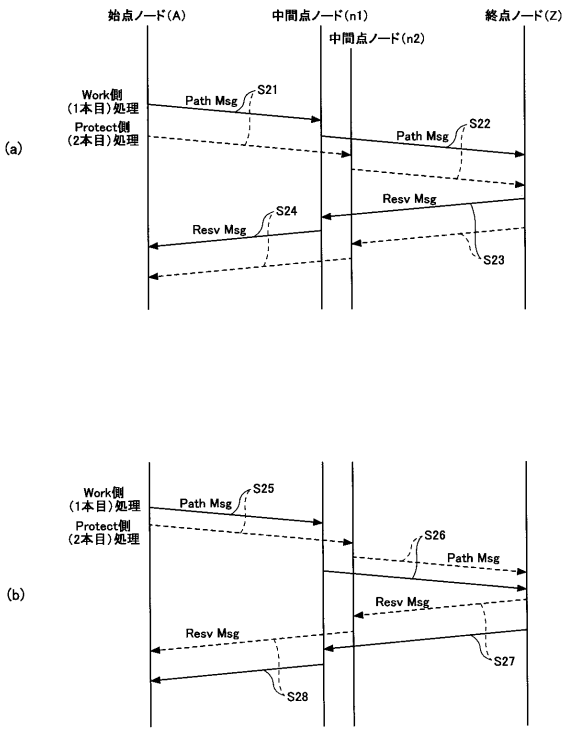
【図４】

従来の逐次式による
１＋１プロテクトパス構築の処理例を示すシーケンス図（その２）



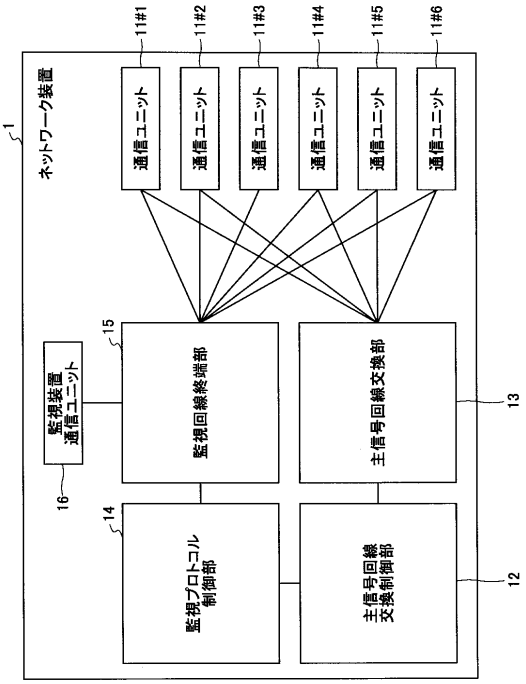
【図５】

従来の同時設定式による
１＋１プロテクトパス構築の処理例を示すシーケンス図



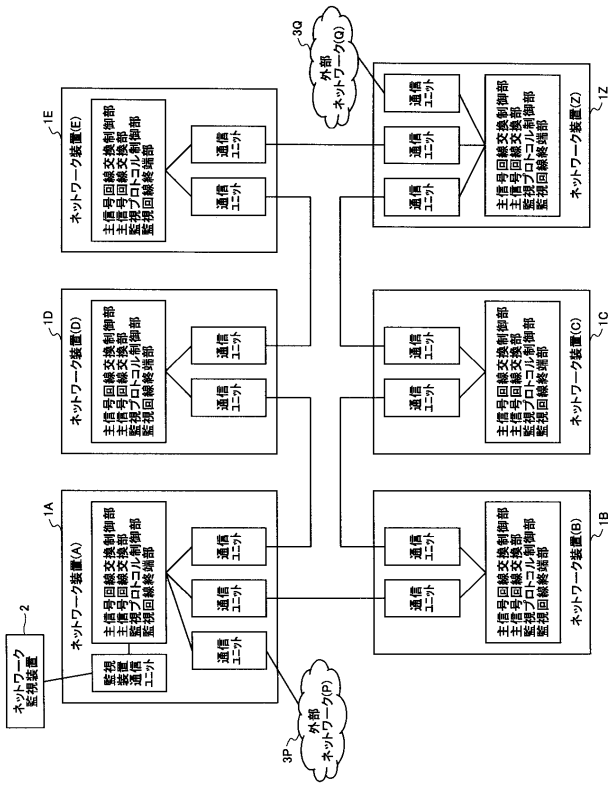
【図６】

本発明の一実施形態にかかるネットワーク装置の構成例を示す図



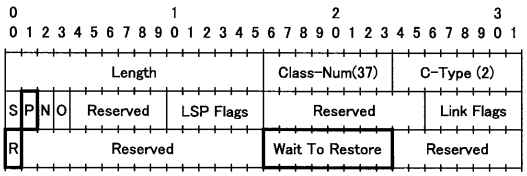
【図７】

複数のネットワーク装置を用いたネットワークの例を示す図



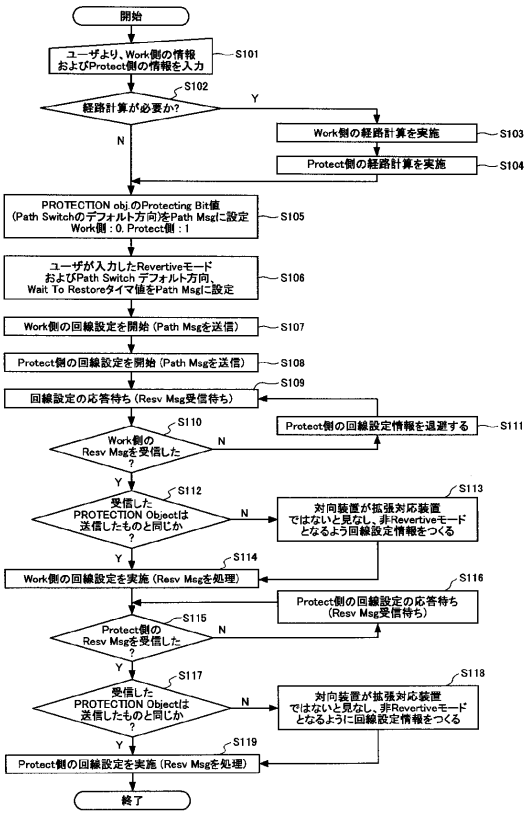
【図８】

プロテクションオブジェクトのフォーマット例を示す図



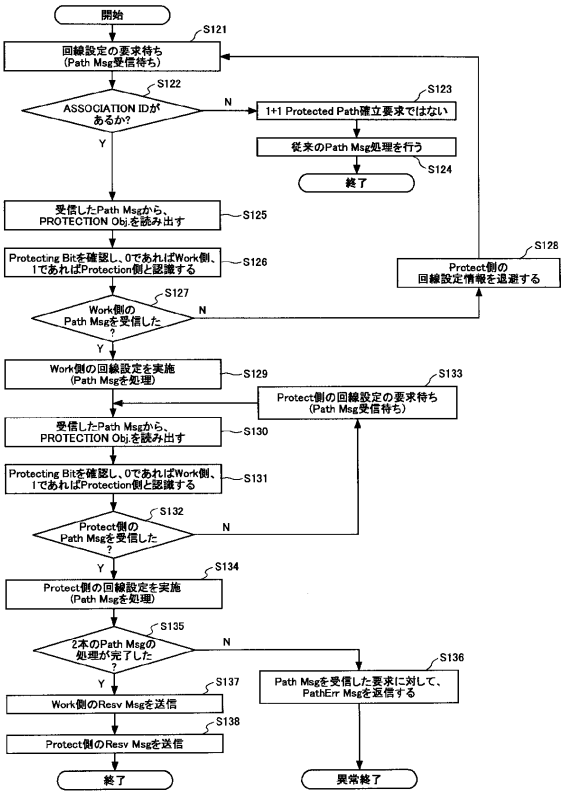
【図９】

始点ノードの処理例を示すフローチャート



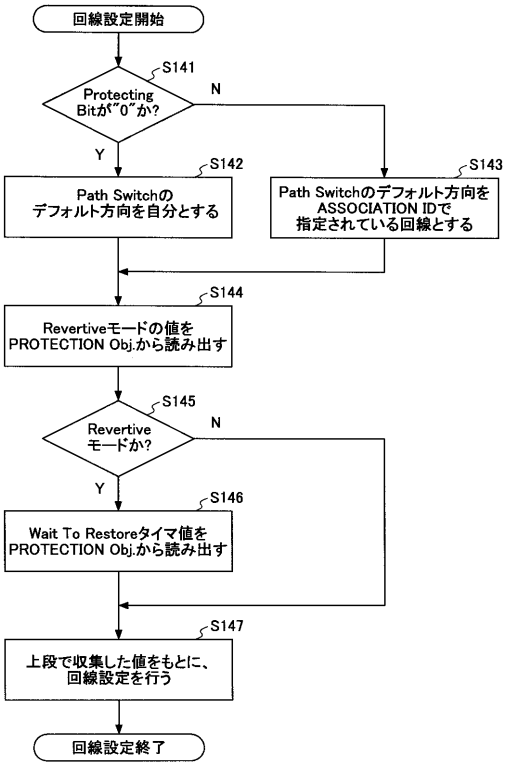
【図１０】

終点ノードの処理例を示すフローチャート



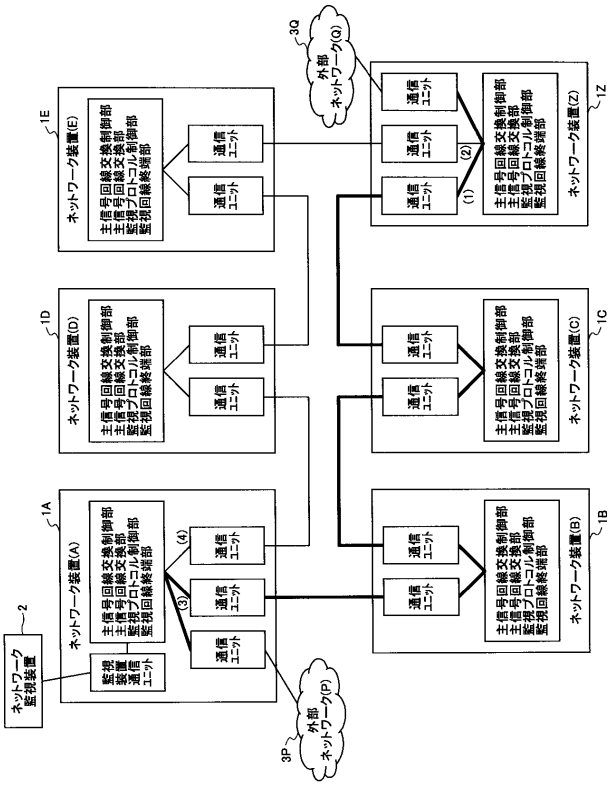
【図１１】

回線設定ロジックの例を示すフローチャート



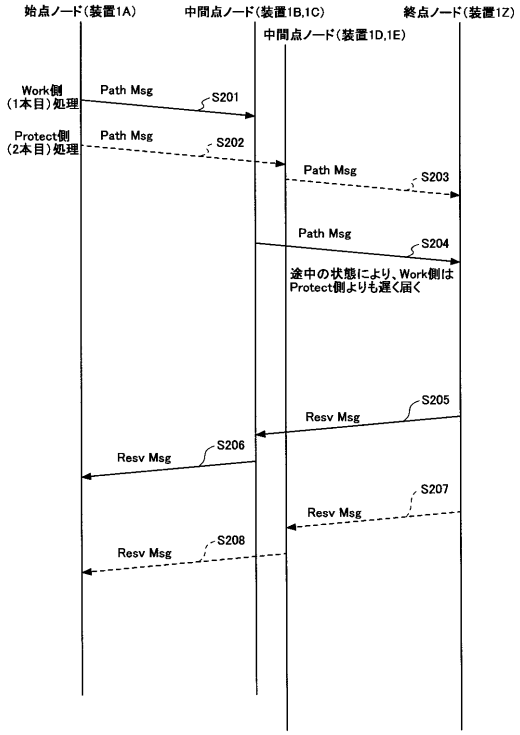
【図１２】

ネットワーク上の回線設定の例を示す図



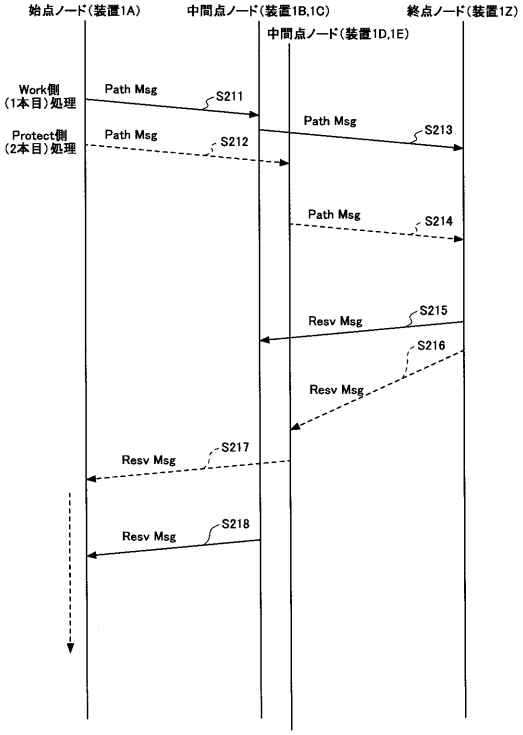
【図１３】

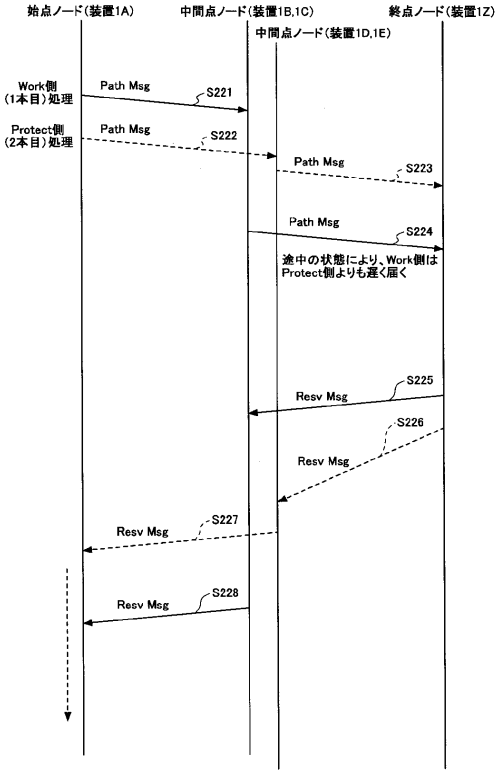
実施形態の処理例を示すシーケンス図(その1)



【図１４】

実施形態の処理例を示すシーケンス図(その2)



【図１５】

実施形態の処理例を示すシーケンス図(その3)