PIL 障害回復方式実装仕様案　(Ver. 2.0)

PIL 標準化 WG 編
2005 年 11 月 30 日版

最終印刷日時：2008/04/10 午後 2 時 11 分

目次

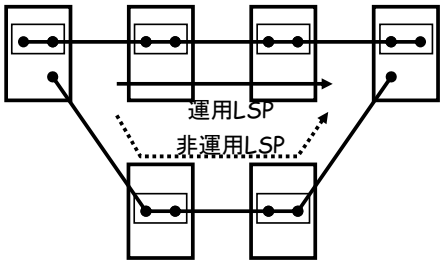
1. はじめに

障害回復は通信網の信頼性を高める上で必須の技術である。Multi-Protocol Label Switching (MPLS)のフレームワークにおいては Fast ReRoute (FRR)と呼ばれる技術が RFC 化（RFC4090）され、商用網への適用も進んでいる。同様に、MPLS を拡張した GMPLS を用いた網においても、信頼性を高める技術の開発が必要と判断され、従来回線網で用いられてきたプロテクション技術や、検討はされたが実際には応用例が少なかったリストレーション技術を GMPLS 技術の中に取り込まれるに至った。しかしながら、IETF での標準化の作業は一旦終結したものの、当該技術の実装や、ISOCORE、UNH（University of New Hampshire）等における異ベンダ間相互接続検証はこれからである。本 IA の目的はドラフトでは記述が不十分な部分を補い、実装可能な細かいレベルの仕様を制定することでマルチベンダ相互接続性を実証する点にある。結果として IETF での標準化作業をリードし、本分野での PIL 参加組織のプレゼンスを高めると共に、商用網における GMPLS 技術の適用が進展することが期待できる。
本 IA によって合意された障害回復仕様の一部は技術検証 WG での検証を行い、PIL としての相互接続試験のアイテムとする。また、本 IA で対象とするデータプレーンは主として SDH、Lambda とする。

2. 定義

2.1. リストレーションとプロテクション

- プロテクション
  - 平時は非運用LSPのXCTも設定しておく。
  - 非運用LSPを運用に切り替える場合にXCT設定のためのシグナリングは不要。



- リストレーション
  - 平時は非運用LSPのXCTは設定しておかない。
  - 非運用LSPは他の非運用のLSPをリソース(ラベル、帯域)を共有することが可能。
  - 非運用LSPを運用に切り替える場合にXCT設定のためのシグナリングが必要。

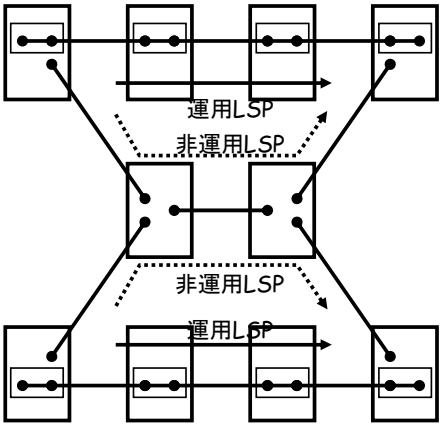


図 2-1 プロテクションとリストレーション

2.1.1. プロテクション機能概要

プロテクションは、GMPLS がサポートする障害回復(リカバリ)の一形態である。
一般に、LSP のプロビジョニングを段階分けすると、下記 3 フェーズに分けることが出来る。

(1) 経路計算
(2) シグナリング
(3) クロスコネクト設定

(1),(2)は、C-Plane 内に閉じた LSP 確立動作であるが、(3)は D-Plane も含めた LSP 確立動作である。
障害回復(Recovery)の中には、リストレーション(Restoration)とプロテクション(Protection)という 2 つのカテゴリがあるが、これらの違いは予備 LSP を提供する際のタイミングと提供方法の差分による。
本節が対象とするプロテクションには、以下の特徴がある。

① 保護対象である現用 LSP の運用時、これを保護する予備 LSP については、経路計算が完了している。
② 現用 LSP の運用時、予備 LSP に対するシグナリングが完了している。
③ 現用 LSP の運用時、予備 LSP に対するクロスコネクトが完了している。
④ 予備 LSP を構成するリソースの一部又は全部を複数の現用 LSP 間で共有することを許容しない。
⑤ LSP の切替(Switchover)制御を D-Plane で行う形態を許容する。

本節が対象として記述するプロテクションについては、Extra-Traffic の観点から以下の 2 種類がある。

- 1+1 Protection ; 現用運用中に、予備に Extra-Traffic を流さない。
- 1:1 Protection ; 現用運用中に、予備に Extra-Traffic を流すことを許容する。

1+1 Protection については、切替時に送受信端ノードでの連携の要否により、更に 2 種類の形態が存在する。

- 1+1 Uni-directional Protection ; 受信端ノード単独で切替実行
- 1+1 Bi-directional Protection ; 送受信端ノードで連携して切替実行

又、本 IA は 2005 年 11 月 30 日時点でのプロテクション関連の最新版 IETF ドラフトである

「draft-ietf-ccamp-gmpls-recovery-e2e-signaling-03」を参照している。ここで述べられているリカバリ形態との対応を含め、上記三形態のプロテクションの相違点を表 2-1に示す。

表 2-1　1+1(uni/bi)と 1:1 Protection の特徴

項番	比較項目	1+1 Uni-directional Protection	1+1 Bi-directional Protection	1:N Protection
1	予備 LSP の経路計算	現用 LSP の運用中に完了		
2	予備 LSP のシグナリング	現用 LSP の運用中に完了		
3	予備 LSP のクロスコネクト	現用 LSP の運用中に完了		
4	予備 LSP リソースの共有	許容しない		
5	LSP 切替制御	D-Plane での切替制御を許容		
6	Extra-Traffic	現用運用中でも許容しない		現用運用中に予備へ Extra-Traffic を流すことを許容
7	切替時の送受端ノード連携	受端単独	送受端で連携	送受端で連携
	e2e-signaling-03 との対応	・ 1+1 Unidirectional Protection	・ 1+1 Bi-directional Protection	・ 1:N Protection with Extra-Traffic

ては、将来的な拡張機能の扱いとし、規定しない。

この為、本 IA の以降の節では主に現用 LSP/予備 LSP プロビジョニングの為のシグナリング、及び通知シグナリングを中心に規定を行う。

リカバリ処理上、上記の比較項目も含め、シグナリング及びルーティングにおける機能要件を以下に整理する。

【RSVP シグナリング】

RSVP シグナリングは、LSP のプロビジョニング・起動に使用され、リカバリ処理上、求められる機能要件は以下の通りである。

(a) 現用/予備 LSP のうち何れを使用するかを識別する機能
(b) 非運用中の予備 LSP のクロスコネクト状態を識別する機能
(c) 障害発生時に、C-Plane での切替制御シグナリングの要否を識別する機能
(d) 現用 LSP から見た切替先の予備 LSP、予備 LSP から見た切替元の現用 LSP を関連付ける機能
(e) 予備 LSP 上の各ノードに、現用 LSP の明示ルートを把握させる機能
(f) リカバリ種別を識別する機能
(g) 非運用中の LSP の警報を抑止する機能
(h) 現用/予備 LSP 切替を強制的に禁止させる機能

上記機能要件を満足する為に、GMPLS では、リカバリ関連のシグナリング用として以下のオブジェクトが定義されている。

- PROTECTION object (Class-Num=37 / C-Type=2)
- PRIMARY PATH ROUTE object (Class-Num=TBA / C-Type=1)[略称：PPRO]
- ADMIN_STATUS object (Class-Num=196 / C-Type=1)
- ASSOCIATION object (Class-Num=198 / C-Type=1)

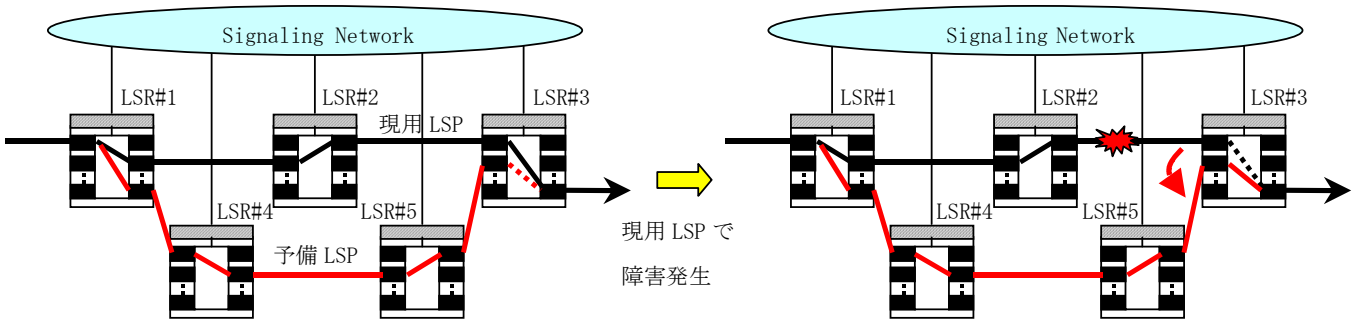
表 2-2に上記 RSVP シグナリングの各オブジェクト中で定義されているフィールドとリカバリ処理上の機能要件との対応一覧を示す。

表 2-2　RSVP シグナリング中のフィールドとリカバリ処理上の機能要件との対応一覧

項番	オブジェクト名	メッセージ	フィールド名	データ長	対応する機能要件	概要
1-1	PROTECTION	・PATH ・RESV	Secondary bit (S bit)	1 bit	(b)	0:クロスコネクト実施 1:クロスコネクト未実施
1-2			Protecting bit (P bit)	1 bit	(a)	0:現用 1:予備
1-3			Notification bit (N bit)	1 bit	(c)	0:切替制御シグナリングを C-Plane で実施する 1:切替制御シグナリングを C-Plane で実施しない
1-4			LSP Flags	6 bit	(f)	0x00;保護無 0x01;(Full) Re-routing 0x02;1:1 Rerouting(Extra-Traffic 無) 0x04;1:1 Protection(Extra-Traffic 有) 0x08;1+1 Uni-directional Protection) 0x10;1+1 Bi-directional Protection)
2-1	PRIMARY PATH ROUTE	・PATH	Subobjects	可変長	(e)	primary protected LSP の RECORD ROUTE オブジェクトの抜粋
3-1	ADMIN_STATUS	・PATH ・RESV	Administratively Down(A bit)	1 bit	(g)	0; Administratively up 1; Administratively down
3-2			Lock Out(L bit)	1 bit	(h)	0; Normal 1; Lock Out
4-1	ASSOCIATION	・PATH	Association ID	16 bit	(d)	Protected 側;Protecting LSP ID Protecting 側;Protected LSP ID
4-2			Association Source IPv4	32 bit	(d)	Protected 側 ;Protecting LSP の Source IPv4 アドレス Protecting 側 ;Protected LSP の Source IPv4 アドレス

プロテクション種別名	S bit	P bit	N bit	LSP Flags	Association ID	PPRO
1+1 Unidirectional Protection	0	1	1	0x08	protected LSP ID	-
1+1 Bi-directional Protection	0	1	1	0x10	protected LSP ID	-
1:N Protection	0	1	1	0x04	protected LSP ID	-

図 2-2に 1+1 Unidirectional Protection の概念図を示す。
図 2-3に 1+1 Bi-directional Protection の概念図を示す。
図 2-4に 1:N Protection の概念図を示す。



〈現用 LSP 運用中〉

予備 LSP は、

・受信端ノードでのみクロスコネクト未完了

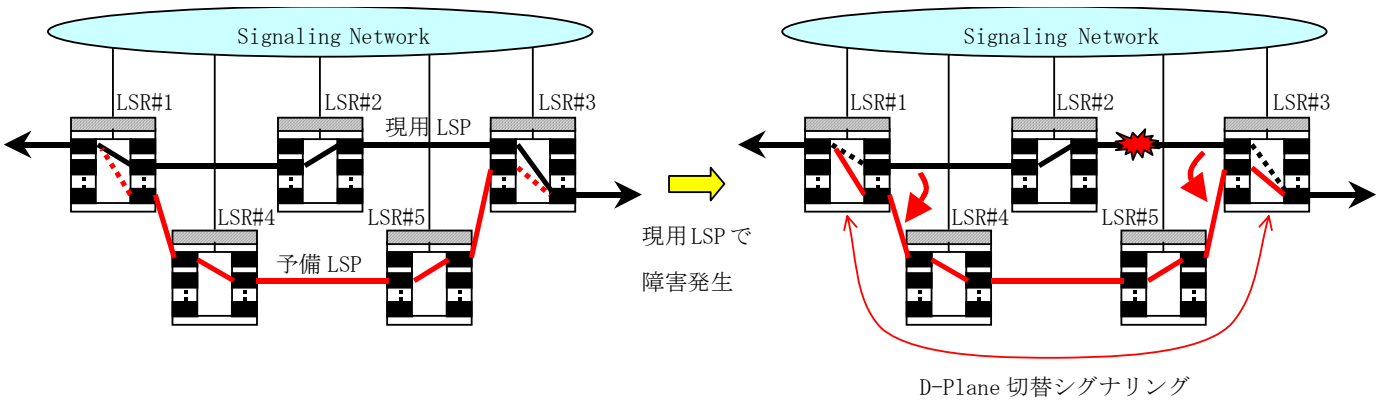
・送信端ノード及び中間ノードではクロスコネクト完了

〈予備 LSP 運用〉

現用 LSP の障害発生を検出し、

・受信端ノードで予備 LSP のクロスコネクト(切替)を実行

図 2-2　1+1 Unidirectional Protection 概念図



〈現用 LSP 運用中〉

予備 LSP は、

・送受信端ノードでクロスコネクト未完了

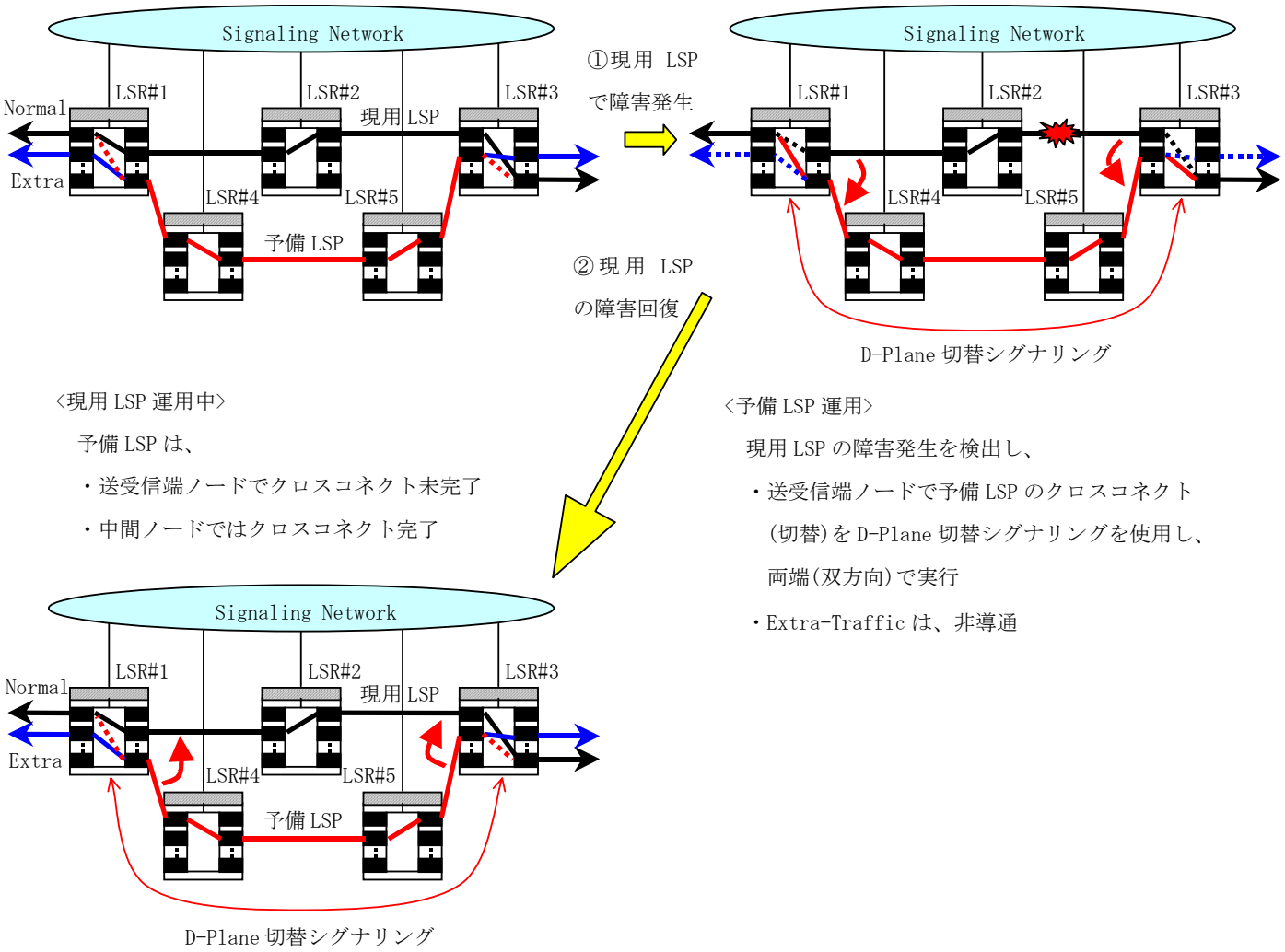
・中間ノードではクロスコネクト完了

〈予備 LSP 運用〉

現用 LSP の障害発生を検出し、

・送受信端ノードで予備 LSP のクロスコネクト(切替)を D-Plane 切替シグナリングを使用し、両端(双方向)で実行

図 2-3　1+1 Bi-directional Protection 概念図



〈現用 LSP 運用中〉

予備 LSP は、

・送受信端ノードでクロスコネクト未完了

・中間ノードではクロスコネクト完了

〈予備 LSP 運用〉

現用 LSP の障害発生を検出し、

・送受信端ノードで予備 LSP のクロスコネクト(切替)を D-Plane 切替シグナリングを使用し、両端(双方向)で実行

・Extra-Traffic は、非導通

〈現用 LSP 運用へ切戻し〉

現用 LSP の障害回復を検出し、

・送受信端ノードで予備 LSP のクロスコネクト(切戻し)を D-Plane 切戻しシグナリングを使用し、両端(双方向)で実行

・Extra-Traffic は、再度導通

〈凡例〉

現用(Normal Traffic)　予備(Normal Traffic)　Extra Traffic

(※) 尚、この他のシンボルの説明は図 4.1.3 の〈凡例〉を参照のこと

図 2-4　1:N Protection 概念図

【ルーティング】

リカバリ上、ルーティングが果たす役割は、現用/予備 LSP のルート計算を行う際に、各経路が使用するリソースがリスク管理上重ならない様にする Shared Risk Link Group(SRLG)情報の広告である。SRLG sub-TLV は、Link TLV(Type=2)に含まれ

る。
ルート計算上、現用/予備 LSP を構成するリソースは、各々完全に独立な SRLG に含まれるべきである。

又、現在、現用/予備 LSP をクライアントに対し、「特別な FA」として見せる方式も検討されている。この場合にもルーティングの機能を使用し、FA の広告を行う。詳細については、4章を参照のこと。

2.1.2. リストレーション機能概要

リストレーションは、GMPLS がサポートする障害回復(リカバリ)の一形態である。
本節が対象とするリストレーションには、以下の特徴がある。

① 保護対象である現用 LSP の運用時、これを保護する予備 LSP の経路計算が完了していない状態であることを許容する。
② 現用 LSP の運用時、予備 LSP に対するシグナリングが完了していない状態であることを許容する。
③ 現用 LSP の運用時、予備 LSP に対するクロスコネクトが完了していない状態を許容する。
④ 予備 LSP を構成するリソースの一部又は全部を複数の現用 LSP 間で共有することを許容する。
⑤ LSP の切替(Switch over)制御は、必ず C-Plane で行う。

本節が対象として記述するリストレーションとしては、上記①～⑤の許容範囲に応じて、以下の二種類が有る。

・ 事前予約型リストレーション
・ ダイナミック型リストレーション

又、本 IA は 2005 年 11 月 30 日時点でのリストレーション関連の最新版 IETF ドラフトである「draft-ietf-ccamp-gmpls-recovery-e2e-signaling-03」を参照している。ここで述べられているリカバリ形態との対応を含め、上記二形態のリストレーションの相違点を表 2-4に示す。

表 2-4　事前予約型とダイナミック型リストレーションの特徴

項番	比較項目	事前予約型	ダイナミック型
1	予備 LSP の経路計算	現用 LSP の運用中に完了	現用 LPS の運用中に未完了であることを許容
2	予備 LSP のシグナリング	現用 LSP の運用中に完了	現用 LPS の運用中に未完了であることを許容
3	予備 LSP のクロスコネクト	現用 LPS の運用中に未完了であることを許容	現用 LPS の運用中に未完了であることを許容
4	予備 LSP リソースの共有	・Shared Mesh Restoration の場合許容 ・1:1 Restoration の場合は許容しない	許容
5	LSP 切替制御	C-Plane	C-Plane
	e2e-signaling-03 との対応	・Re-routing without Extra-Traffic	・(Full) LSP Re-routing

②-2　ラベル割当まで完了

実装上、上記の二形態を想定することが可能である。ある一つの LSP で、LSP を構成するノードがサポートする形態の混在を許容する。

リカバリ処理上、上記の比較項目も含め、シグナリングにおける機能要件を以下に整理する。
ルーティングにおける機能要件については、プロテクションの場合と同様である。2.1.1節を参照のこと。

【RSVP シグナリング】
RSVP シグナリングは、LSP のプロビジョニング・起動に使用され、リカバリ処理上、求められる機能要件は2.1.1節で示した(a)～(f)と同様である。

これらの機能要件を満足する為に、規定されているシグナリング用のオブジェクトは、リストレーションの場合と同様、以下の通りである。

・ PROTECTION object (Class-Num=37 / C-Type=2)
・ PRIMARY PATH ROUTE object (Class-Num=TBA / C-Type=1)[略称：PPRO]
・ ADMIN_STATUS object (Class-Num=196 / C-Type=1)
・ASSOCIATION object (Class-Num=198 / C-Type=1)

上記 RSVP シグナリングの各オブジェクト中で定義されているフィールドとリカバリ処理上の機能要件との対応一覧については、表 2-2を参照のこと。

表 2-2に示す各フィールドの中で、LSP プロビジョニング直後(現用 LSP を運用している状態)に、「リストレーション」各方式において予備 LSP が取る値の一覧を表 2-5に示す。(動的な値は各節を参照のこと)

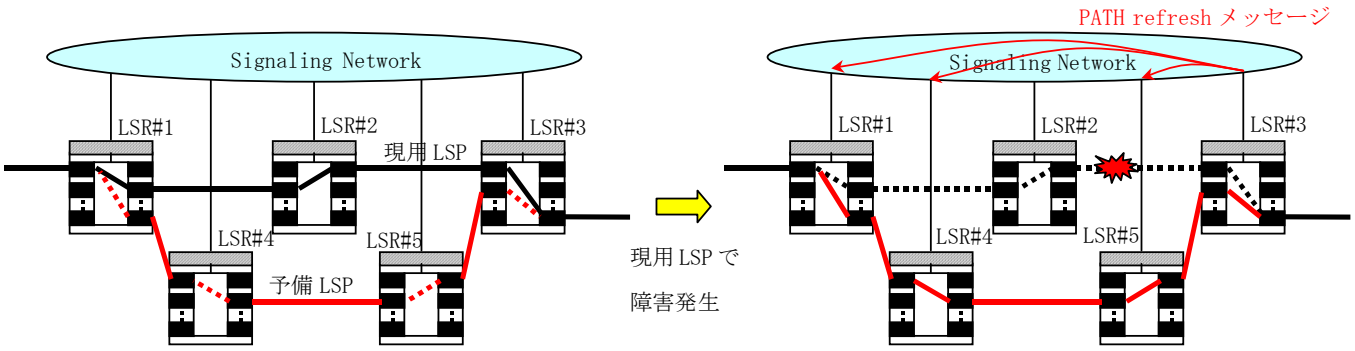
表 2-5 各リストレーション種別の予備 LSP が LSP プロビジョニング直後に取る各リカバリ関連フィールド値

リストレーション種別名	S bit	P bit	N bit	LSP Flags	Association ID	PPRO
Shared Mesh Restoration	1	1	0	0x02	protected LSP ID	有
1:1 Restoration	1	1	0	0x02	protected LSP ID	無

(*1)表 2-2(2-1 項)概要欄の説明を参照のこと。
(*2)(Full) LSP Re-routing(ダイナミック型)については、予備 LSP は存在せず、各フィールド値は比較の為に意味のあると思われるもののみを示した現用 LSP のものである。

有り)である点であることが分かる。また、Shared Mesh Restoration と 1:1 Restoration は PPRO の有無で区別する。

図 2-5に 1:1 Restoration の概念図を示す。
図 2-6に Shared Mesh Restoration の概念図を示す。
図 2-7に(Full) LSP Re-routing の概念図を示す。



〈現用 LSP 運用中〉

予備 LSP は、

・経路計算完了

・シグナリング完了

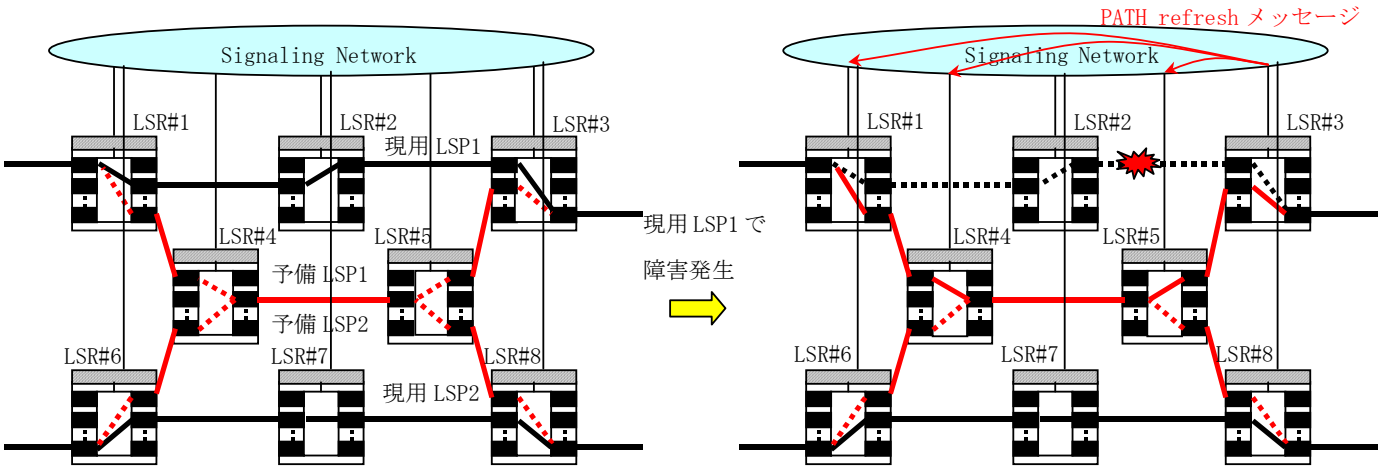
・クロスコネクト未完了

〈予備 LSP 運用〉

現用 LSP の障害発生を検出し、

・C-Plane のシグナリングにより、予備 LSP のクロスコネクトを設定

図 2-5 1:1 Restoration 概念図



〈現用 LSP1, 2 運用中〉

予備 LSP1, 2 は、

・経路計算完了

・シグナリング完了

・クロスコネクト未完了

予備 LSP1, 2 は LSR#4～#5 間でリソースを共有

〈予備 LSP1 運用〉

現用 LSP1 の障害発生を検出し、

・C-Plane のシグナリングにより、予備 LSP1 の

クロスコネクトを設定

・現用 LSP2, 予備 LSP2 は変化無し

現用 LSP1, 2 同時故障時は、何れか一方救済不可

図 2-6　Shared Mesh Restoration 概念図

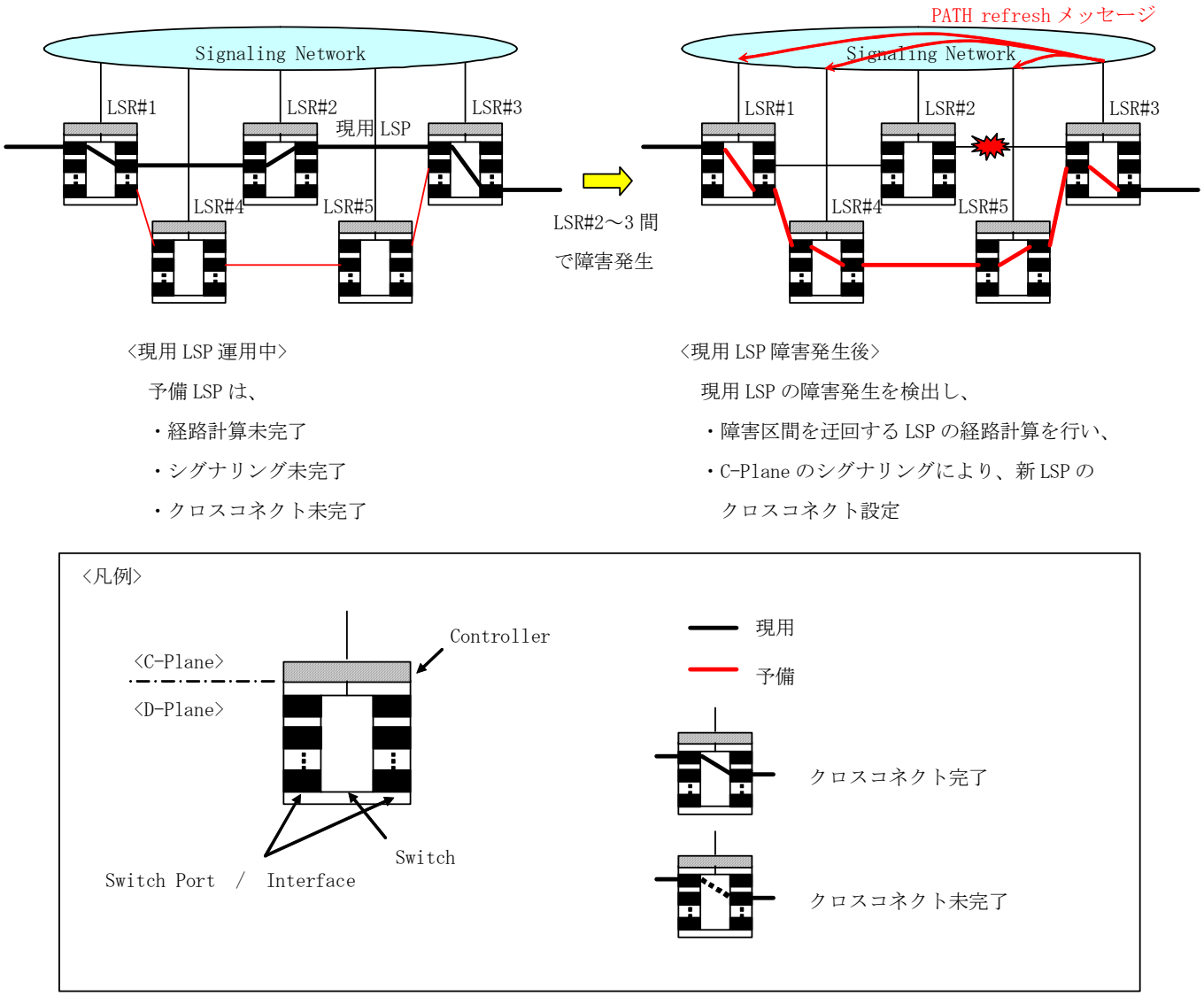


図 2-7 (Full) LSP Re-routing 概念図

尚、リストレーションの二形態のうち、本 IA では事前予約型の規定のみ行い、ダイナミック型の規定は行わない。

事前予約型リストレーションは、現用 LSP プロビジョニングと同時に、予備 LSP についても C-Plane 内に閉じた設定は完了している

事前予約型リストレーションの特徴をここで再整理すると、以下の様になる。
(1) 予備 LSP 経路計算 → 現用 LSP の運用時に完了
(2) 予備 LSP シグナリング → 現用 LSP の運用時に完了
(3) 予備 LSP クロスコネクト → 現用 LSP の運用時に未完了
(4) LSP 切替制御 → C-Plane で実施

又、事前予約型リストレーションは、その予備 LSP リソースの共有という観点から、以下の 2 種類に分類することが出来る。

① 1:1 Restoration ：予備 LSP リソースを複数の現用 LSP 間で共有しない
② Shared Mesh Restoration ：予備 LSP リソースを複数の現用 LSP 間で共有する

更に、予備 LSP シグナリングをどこまで行うかにより、ネットワークとしての共有率、LSP の耐障害性、及び障害回復

時間の点で差分が有る。表 2-6に、予備 LSP シグナリングレベルに応じた各項目での方式比較一覧を示す。

表 2-6　予備 LSP シグナリングレベルに応じた方式比較一覧

比較項目	ラベル予約まで ⟷ 帯域予約まで
共有率	低い → 高い
耐障害性	低い → 高い
回復時間	速い → 遅い

又、Extra-Traffic には、下記の二種類が考えられる。

・予備 LSP の端点以外の全部を使用する形態(Extra-Traffic 用 LSP の為のシグナリングが不要)
・予備 LSP のリソースの一部を使用する形態(Extra-Traffic 用 LSP の為のシグナリングが必要)

リストレーションでは、このうち両方の形態をサポートする。

2.2. LSP 二重化と切替動作

LSP を二重化することにより、GMPLS ネットワークにおいて高信頼性を実現することが出来る。
高信頼化されたトンネルは対応する現用 LSP と予備 LSP とからなる。図 2-8にトンネルと LSP の関係を示した。ノード A と B 間にトンネルを設定し、その構成要素として現用 LSP と予備 LSP を設定する。
プロテクションの場合には現用 LSP と予備 LSP は実際にネットワーク内に設定される。図 2-9にコネクションとクロスコネクションの状態について示した。プロテクションにおいては関連する全てのコネクション、クロスコネクションが運用状態にあり、他の LSP が利用することは出来ない状態である。Ingress もしくは Egress にて 2 分岐されたトラフィックは現用と予備の両方の LSP を用いて転送され、対抗側の Egress もしくは Ingress にて選択される。選択されている運用系に障害が発生した場合には、予備系を運用系にすることで障害を回復することが可能である。
リストレーションの場合には、現用 LSP は実際に設定されるが、予備 LSP のクロスコネクションは実際には設定されない。図 2-10にコネクションとクロスコネクションの状態について示した。現用系は Ingress-Core1-Core2-Egress を通過する経路、予備系は Ingress-Core3-Core4-Egress を通過する経路に割り当てられている。現用系は全てのコネクション、クロスコネクションが運用状態にあり、トラフィックの伝送に供されることが可能である。予備系は、全てのクロスコネクションが非運用状態にあることが必須である。一方で、コネクションは必ずしも非運用である必要はない、したがって、リストレーションにおいても予備経路を計算すること(routed 状態)、予備帯域を確保すること(reserved 状態)、ラベルを割り当てた状態(assigned 状態)、などの操作は行っても良いことになる。現用系に障害が発生した場合には、全てのコネクション、クロスコネクションを運用状態にし、トラフィックを予備系によって伝送することで障害回復を行うこととする。自動切替、コマンド切替によって、現用/予備、運用/非運用の状態が変化することがわかる。[recovery-e2e]に記述されている Protection Object 内の S(Secondary)-bit、P(Protecting)-bit を用いて状態を記述する場合について説明する。表 2-7に示すとおり、S-bit が 1 の場合の LSP は予備且つクロスコネクションは実施しない、0 の場合は現用を表す。P-bit は、1 の場合には LSP は予備系、0 の場合には現用系であることを表す。表 2-8は切替による S-bit、P-bit の変化を示した([recovery-e2e]を参考に作成)。
プロテクション、リストレーションいずれの場合においても、障害が起きた現用系が修理され再び運用系として供することが出来るようになった場合に、予備系運用の状態から、再び現用系運用状態に復帰するよう切り戻しする。切り戻し操作はオプションとし、必ずしも実装の必要はないが、あった方が運用上は望ましい。
LSP を二重化する場合、Call と Connection の分離の観点から、トンネル ID と 2 つの LSP-ID は独立に割り当てることとする。例えば、トンネル(ID:X)の二重化を一度解除し、再び予備 LSP を設定した場合には始めの予備 LSP の ID と再設定後の予備 LSP の ID は一致しなくても良い。また、他の例としては、切り戻しの無いリストレーションによって現用 LSP が予備 LSP に切り替わった後に、元の現用 LSP が解除された場合には、今までの予備 LSP の ID を現用 LSP の ID として用いても良く、予備 LSP は新規に設定されるので、新しい予備 LSP の ID は全く新規のものを割り当てることも可能である。

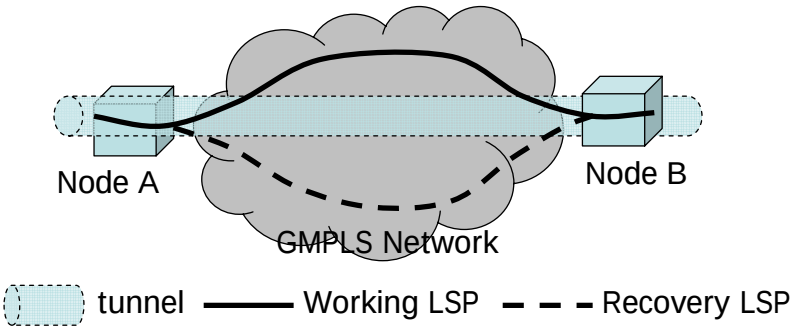


図 2-8　トンネルと現用/予備 LSP の関係

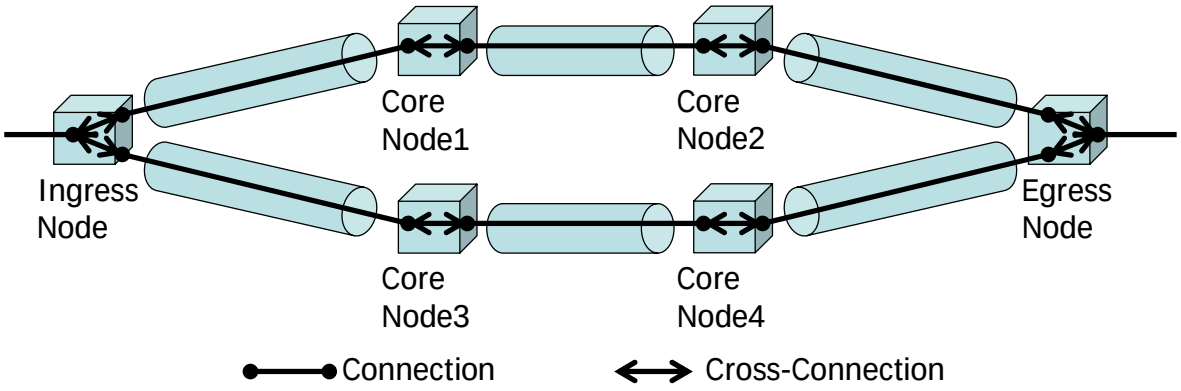


図 2-9　プロテクションの設定状態

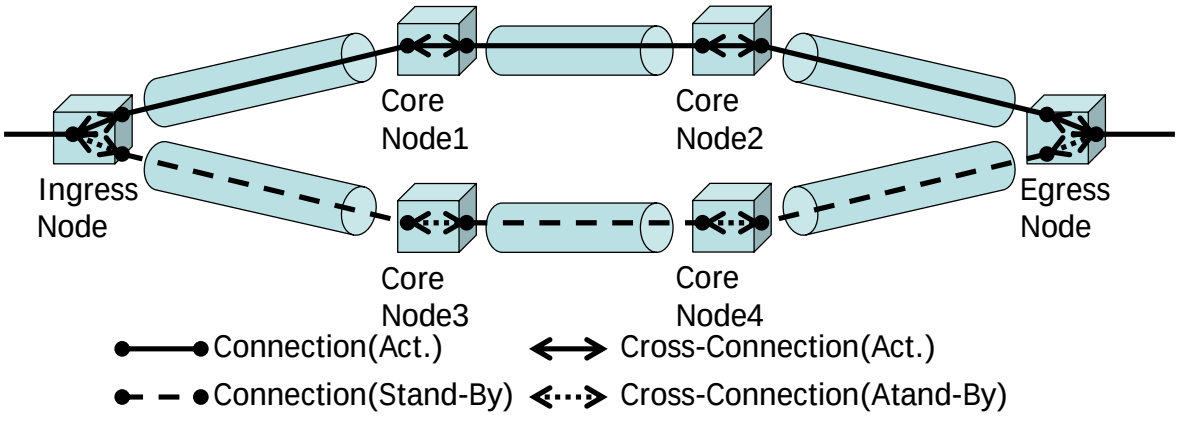


図 2-10リストレーションの設定状態

表 2-7　S-bit，P-bit，O-bit の定義

	値	意味
S-bit	0	クロスコネクション設定
	1	クロスコネクション未設定
P-bit	0	現用
	1	予備
O-bit	0	予備 LSP 運用状態以外
	1	予備 LSP 運用状態

表 2-8　切替方式と S-bit、P-bit の関係

切替方式	状態	現用/予備	LSP (Protection Type) Flags	S-bit	P-bit	O-bit
1+1 Bi-directional Protection	切替前	現用	0x10	0	0	0
		予備	0x10	0	1	0
	切替後	現用	0x10	0	0	0
		予備	0x10	0	1	1
1+1 Unidirectional Protection	切替前	現用	0x08	0	0	0
		予備	0x08	0	1	0
	切替後	現用	0x08	0	0	0
		予備	0x08	0	1	1
1:1 Protection with Extra-Traffic (Path and bandwidth protection)	切替前	現用	0x04	0	0	0
		予備	0x04	0	1	0
	切替後	現用	0x04	0	0	0
		予備	0x04	0	1	1
1:1 Re-Routing without Extra-Traffic (Path protection only)	切替前	現用	0x02	0	0	0
		予備	0x02	1	1	0
	切替後	現用	0x02	0	0	0
		予備	0x02	0	1	1
Shared Mesh	切替前	現用	0x02	0	0	0
		予備	0x02	1	1	0
	切替後	現用	0x02	0	0	0
		予備	0x02	0	1	0
Full Re-routing		現用	0x01	0	0	0

【参考】
(draft-ietf-ccamp-gmpls-recovery-e2e-signaling-03.txt、14 章、protection object より抜粋)

The format of the PROTECTION Object (Class-Num = 37, C-Type = 2 by IANA) is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Length             | Class-Num(37) | C-Type (2)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|S|P|N|O|  Reserved | LSP Flags |     Reserved      | Link Flags|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Secondary (S): 1 bit

When set to 1, this bit indicates that the requested LSP is a secondary LSP. When set to 0 (default), it indicates that the requested LSP is a primary LSP.

Protecting (P): 1 bit

When set to 1, this bit indicates that the requested LSP is a protecting LSP. When set to 0 (default), it indicates that the requested LSP is a working LSP. The combination, S set to 1 with P set to 0 is not valid.

Notification (N): 1 bit

When set to 1, this bit indicates that the control plane message exchange is only used for notification during protection switching. When set to 0 (default), it indicates that the control plane message exchanges are used for protection switching purposes. The N bit is only applicable

when the LSP Protection Type Flag is set to either 0x04 (1:N Protection with Extra-Traffic), or 0x08 (1+1 Unidirectional Protection) or 0x10 (1+1 Bi-directional Protection). The N bit MUST be set to 0 in any other case.

Operational (O): 1 bit

When set to 1, this bit indicates that the protecting LSP is carrying the normal traffic after protection switching. The O bit is only applicable when the P bit is set to 1 and the LSP Protection Type Flag is set to either 0x04 (1:N Protection with Extra-Traffic), or 0x08 (1+1 Unidirectional Protection) or 0x10 (1+1 Bi-directional Protection). The O bit MUST be set to 0 in any other case.

参考文献

[recovery-e2e] draft-ietf-ccamp-gmpls-recovery-e2e-signaling-03.txt

2.3. 用語・略語集

○ 運用(active)と非運用(stand-by)
運用：現在使用中(クライアントのデータが流れていて、障害が起きた場合にクライア ントに影響が出る状態)
非運用：運用に対する待機状態

○ 現用(working)と予備(recovery)
現用：通常運用時に供されるもの
予備：現用の障害回復に用いられるもの

○ protection と restoration
Protection:1+1,1:n,ring protection を指す。ただし、本 IA では ring protection は対 象外。
中間ノードのクロスコネクション設定が不要な場合
Restoration:(主に mesh ネットワークで、)現用 LSP 障害後に予備が確立される障害回復方式。
中間ノードのクロスコネクション設定が必要な場合
＃中間形態については本 IA のスコープ外とする。

○ スパン、セグメント、E2E
スパン：たとえば SDH における M セクション、直近の 2 ノード間の経路
セグメント：複数のスパンの連結
E2E：LSP の Ingress から Egress までのセグメント

○ extra トラフィック
他のトラフィック予備を用いて伝達されるトラフィック。
切替時に現用を通るトラフィックに取って代わられる。
本 IA では、protection と restoration での区別は特に無し。

○ グローバルリペア(global repair)とローカルリペア(local repair)
グローバルリペア：パス端切替
ローカルリペア：障害端切替

○ full span restoration, partially span restoration, full LSP restoration
full span restoration:あるスパンで障害が発生した場合に、そのスパンに収容され ている LSP を全て救済
partially span restoration:あるスパンで障害が発生した場合に、そのスパンに収容 されている LSP の一部を救済
full LSP restoration: LSP の initiator が障害箇所を迂回して救済する。その際にも との中継ノードを再び通ってもよい。

○ LSP の状態

経路だけ計算した状態:routed
帯域を予約した状態:(label-)reserved
ラベルを割り当てた状態:(label-)assigned
スイッチを設定した状態:cross-connected

○TE-Link と FA
TE Link = {基本 TE Link、FA}
TE Link: ルーティングプロトコルでの広告の対象となるリンク
FA: LSP を TE Link として広告したもの
FA-LSP: FA の実体である LSP
基本 TE Link: FA ではない TE Link。レイヤによって、ファイバ、bundled ファイバ、波長、タイムスロット等が基本 TE Link になり得る。

3. RSVP シグナリング

3.1. 事前予約型リストレーションシグナリング

3.1.1. シグナリングシーケンス

3.1.1.1. 現用 LSP、予備 LSP の設定

現用 LSP（LSP0）、予備 LSP（LSP1）の設定シーケンスを図 3-1に示す。

- LSP0 と LSP1 とで、SESSION Object は同じ値を、LSP ID は異なる値を用いる。
- PROTECTION Object、ASSOCIATION Object は次のように設定する。
  LSP Flags = 0x02
  【LSP0】
  P=0, S=0
  Association ID = "LSP1 の LSP ID"
  【LSP1】
  P=1, S=1
  Association ID = "LSP0 の LSP ID"
- Shared Mesh Restoration の予備 LSP を設定する場合は、PATH メッセージに PRIMARY_PATH_ROUTE Object を含める。PRIMARY_PATH_ROUTE Object には、対応する現用 LSP の経路を入れる。それ以外の場合は、PRIMARY_PATH_ROUTE Object を含めない。
- ADMIN_STATUS Object は optional とする。ADMIN_STATUS がない場合は全ての値を 0 として扱う。ADMIN_STATUS Object がある場合、A-bit は次のように設定する。
  【LSP0、LSP1】
  - 1 往復目: A= 1 （こうすることにより、LSP 設定中の障害の誤検出を防ぐことができる）
  - 2 往復目以降: A=0
- RESVCONF メッセージは optional とする（Egress ノードはこのメッセージの到着をトリガとしてユーザトラフィックを流し始めることができる）。
- LSP の状態は、各メッセージにより次のように変化する。
  【LSP0】
  - PATH: Routed→Reserved
  - RESV: Reserved→Connected
  【LSP1】
  - PATH: Routed→Reserved
  - RESV: Reserved→Reserved or Assigned
- LSP0、LSP1 ともに、refresh を行う。

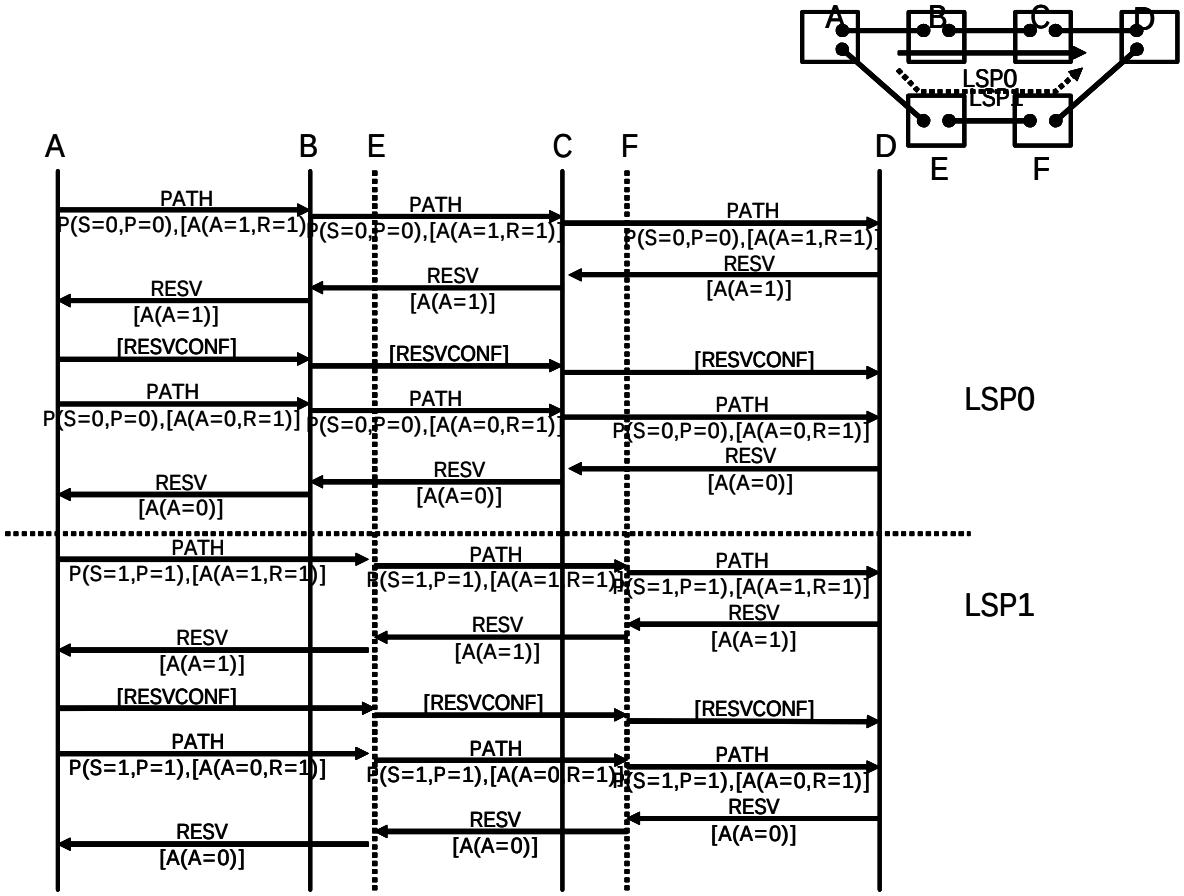


図 3-1　1:1/Shared Mesh Restoration での現用／予備 LSP 設定シグナリングシーケンス

3.1.1.2.障害切替

現用 LSP に障害が発生すると、障害通知が Ingress ノードに送られる（5 章参照）。Ingress ノードは障害が通知された現用 LSP に対応する予備 LSP の状態を Reserved または Assigned から Connected に変更（以後、この操作を activation と呼ぶ）した後、現用 LSP のトラフィックを予備 LSP に切り替える。このときのシグナリングシーケンスを図 3-2に示す。

- LSP1（予備 LSP）の PATH メッセージでは、S-bit を 1 から 0 に変更する。これにより LSP1 上のノードは、このシグナリングが通常の refresh ではなく activation であることを知り、この LSP を activate する。
- LSP0（現用 LSP）の PATH メッセージでは、どのビットも変更しない（それまで通り refresh を続ける）。

- ADMIN_STATUS Object は optional とする。ADMIN_STATUS がない場合は、全ての値を 0 として扱う。ADMIN_STATUS Object がある場合、A-bit は次のように設定する。

  【LSP0】

  A=0 または A=1（障害検出を制御プレーンに伝えたくない場合に A=1 とする等の使い方が可能）

  【LSP1】

  - 障害検出後 1 往復目: A= 1　（こうすることにより、activation 中の障害の誤検出を防ぐことができる）
  - 2 往復目以降: A=0

- 障害切替により、LSP0, LSP1 の状態は次のように変化する。

  【LSP0】

  Connected のまま

  【LSP1】

  Reserved or Assigned→Connected

- 障害切替後も、LSP0, LSP1 の refresh を継続する。制御チャネルの障害などにより refresh を行えない場合は、RFC3473 の 9 章に記載の手順に従って、soft state を維持する。

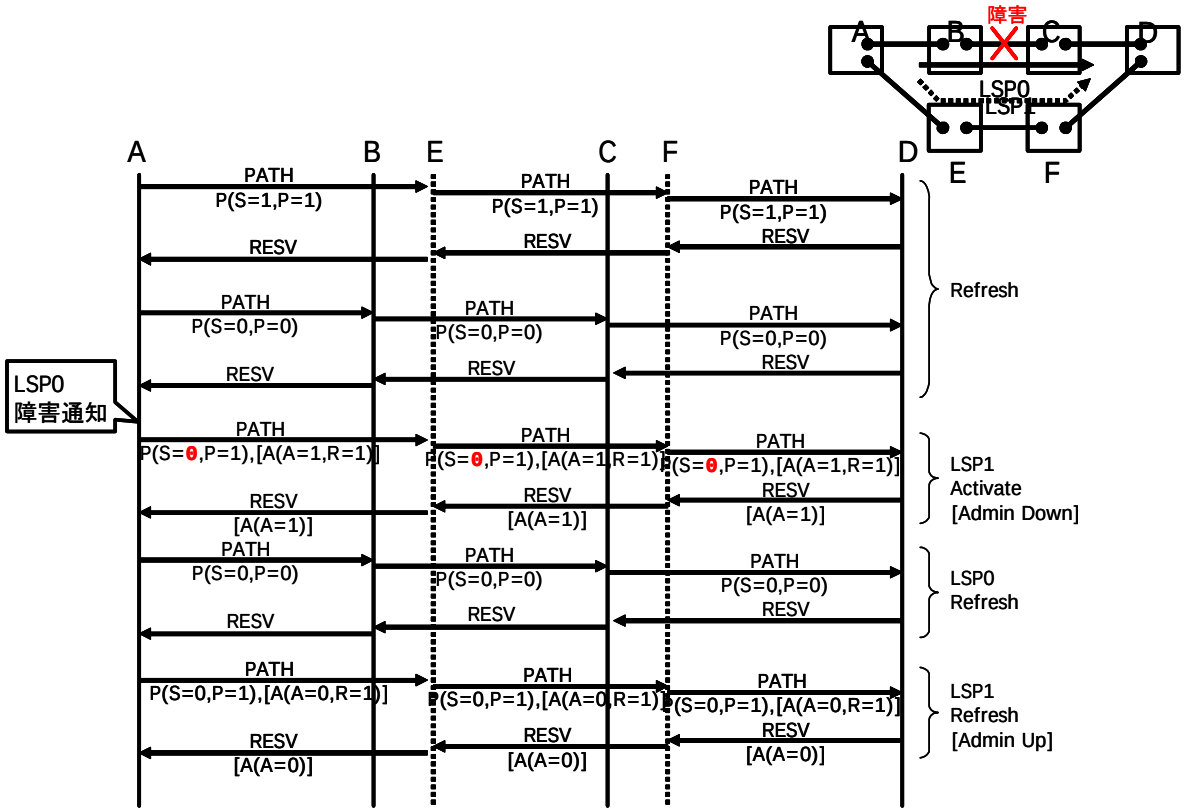


図 3-2　1:1/Shared Mesh Restoration での障害切替シグナリングシーケンス

3.1.1.3.切り戻し

1:1/Shared Mesh Restoration で障害切替の後、現用 LSP が復旧すると切り戻しを行うことができる。切り戻しは現用 LSP の障害回復通知をトリガとして自動で行うこともできるし、手動で行うこともできる。切り戻しでは、先ず、予備 LSP のトラフィックを現用 LSP に切り替え、次に予備 LSP の状態を Connected から Reserved または Assigned に変更する（以後、この操作を de-activation と呼ぶ）。トラフィックを現用 LSP に切り替える際に、中断を最小限に抑えるため、bridge&select（上流でトラフィックを現用 LSP と予備 LSP の両方に流した後に下流で現用 LSP に切り替える）を行う。このときのシグナリングシーケンスを図 3-3に示す。

- LSP0 が復旧すると、ノード A は LSP1 の A→D 方向のトラフィックを LSP0 にも流すようにスイッチを切り替えた後（bridge）、Error Code/Sub Code が"Notify Error/LSP Recovered"で ACK_Desired フラグを立てた NOTIFY メッセージをノード D に送る。これを受けたノード D は、LSP1 から受け取っていた A-D 方向のトラフィックを LSP0 から受け取るようにスイッチを切り替え（select）、また、LSP1 の D→A 方向のトラフィックを LSP0 にも流すようにスイッチを切り替える（bridge）。続いてノード D は ACK_Desired フラグを立てた NOTIFY ACK をノード A に返す。これを受けたノード A は、A→D 方向のトラフィックを LSP0 だけに流すようにスイッチを切り替え（bridge 解除）、また、LSP1 から受け取っていた D→A 方向のトラフィックを LSP0 から受け取るようにスイッチを切り替え（select）、NOTIFY ACK をノード D に返す。これを受けたノード D は、D→A 方向のトラフィックを LSP0 だけに流すようにスイッチを切り替える（bridge 解除）。以上の後、S=1 とした PATH/RESV メッセージにより LSP1 を de-activate する。
- 切り戻しにより、LSP0, LSP1 の状態は次のように変化する。
  【LSP0】
  Connected のまま
  【LSP1】
  Connected→Reserved or Assigned
- LSP0, LSP1 ともに、refresh を行う。

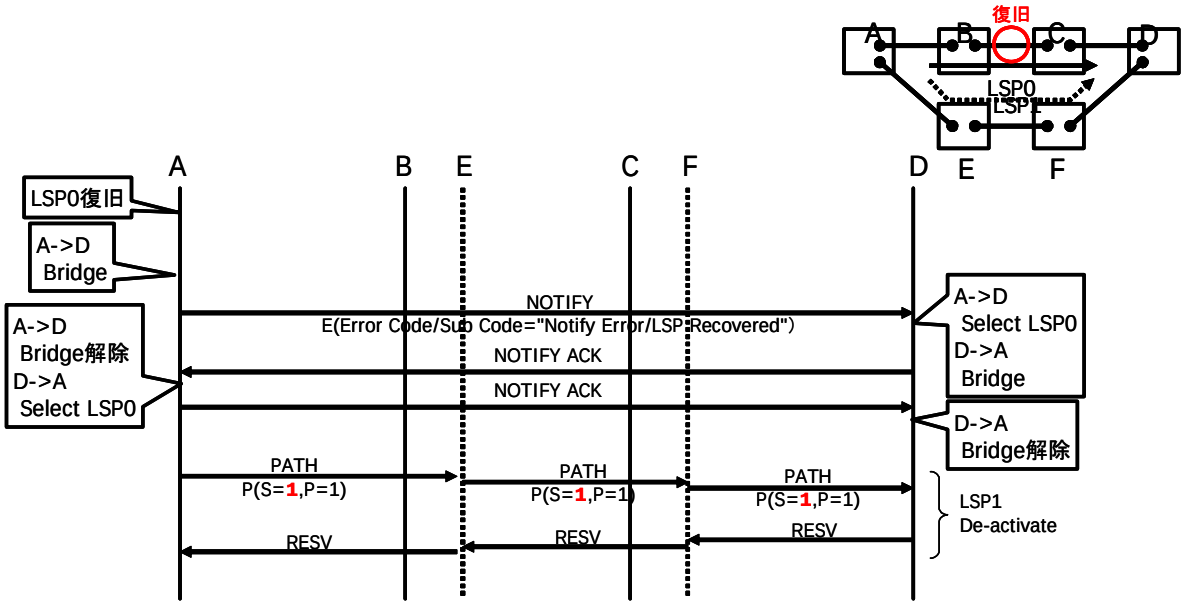


図 3-3　1:1/Shared Mesh Restoration での切り戻しシグナリングシーケンス

3.1.1.4.現用 LSP 解放

切り戻しを行わない場合、障害切替の後、現用 LSP（LSP0）を解放しても良い。このときのシグナリングシーケンスは、通常の LSP 解放（削除）シーケンスと同じ。

3.1.1.5.Forced Switch

LSP0 のトラフィックを LSP1 に切り替える場合: 障害切替のシーケンスと同じ
LSP1 のトラフィックを LSP0 に切り替える場合: 切り戻しのシーケンスと同じ

3.1.1.6.Manual Switch

LSP0 のトラフィックを LSP1 に切り替える場合: 障害切替のシーケンスと同じ
LSP1 のトラフィックを LSP0 に切り替える場合: 切り戻しのシーケンスと同じ

3.1.1.7.ロックアウト、ロックアウト解除

ロックアウトされた LSP では、自動切替も手動切替も禁止される。ロックアウトとロックアウト解除のシグナリングシーケンスを図 3-4に示す。PATH/RESV メッセージにおいて ADMIN_STATUS Object の L-bit を 1 とすることにより、ロックアウトを行い、L-bit を 0 とすることによりロックアウト解除を行う。障害切替後、自動切り戻しを防ぐために、現用 LSP または予備 LSP をロックアウトしても良い。その場合、切り戻しを行うためにはロックアウトを解除する。

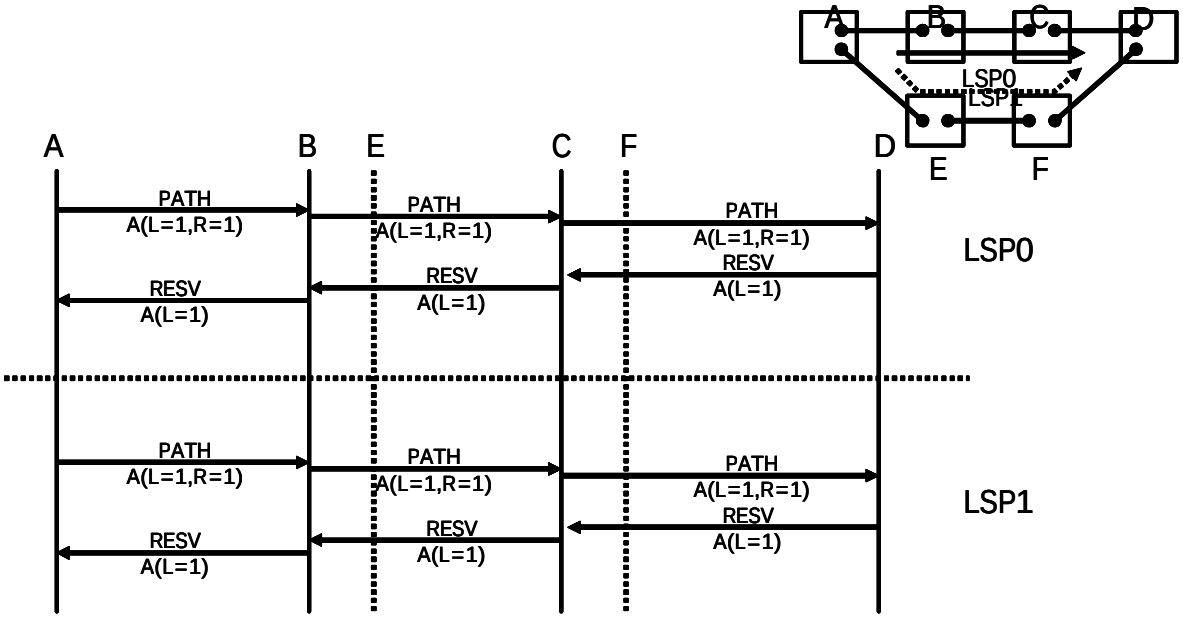


図 3-4　ロックアウトシグナリングシーケンス

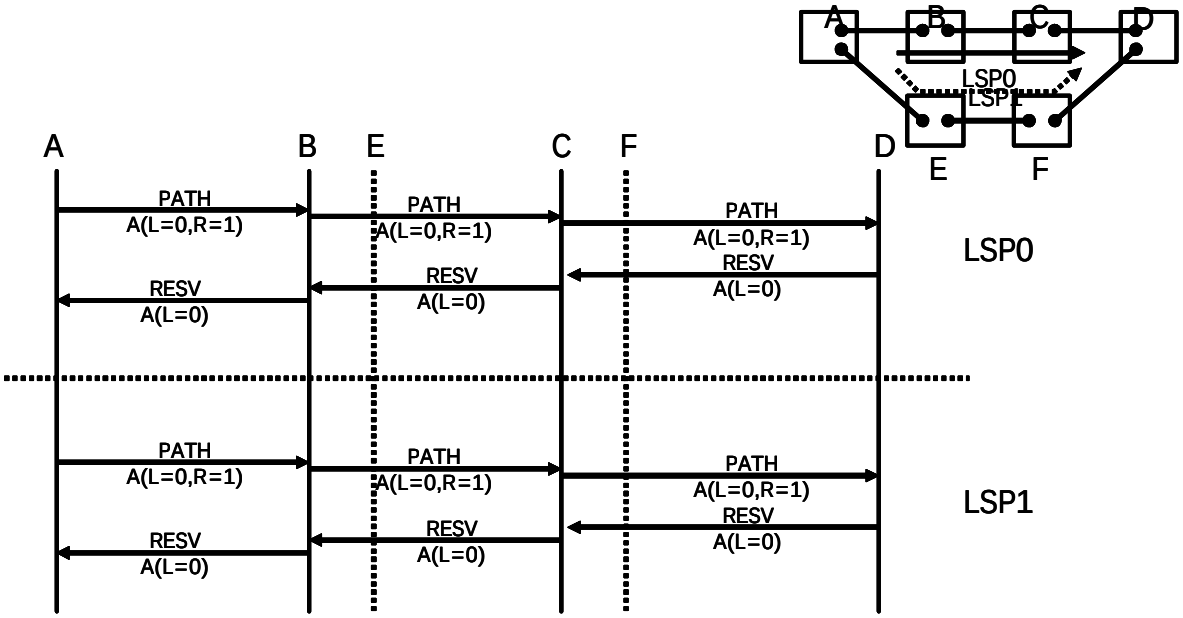


図 3-5　ロックアウト解除シグナリングシーケンス

3.1.2. メッセージ処理

3.1.2.1.Ingress Node のメッセージ処理

障害通知を受けたあとの，Ingress Node での Message 処理を図 3-6に示す。

Ingress Node

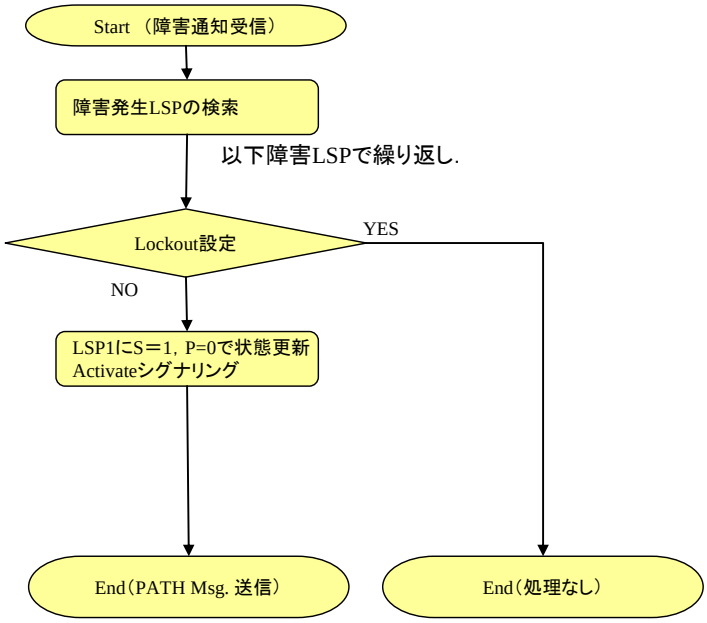


図 3-6 Ingress Node での Message 処理

3.1.2.2.Transit/Egress Node のメッセージ処理

Transit/Egress Node でのメッセージの種類には、

- 新規メッセージ： 新規 LSP を設定するためのメッセージ。
- Refresh メッセージ： RSVP の Soft State Session を維持するためのリフレッシュメッセージ。
- 変更メッセージ： 以前に受信したメッセージからパラメータが変化したメッセージ。GMPLS による傷害回復では、この変更メッセージを使って LSP の状態変更を行うことにより、LSP の切替/切戻しをする。

以下に、RSVP-TE Path/Resv メッセージを受信した各ノードでの処理フローを示す。

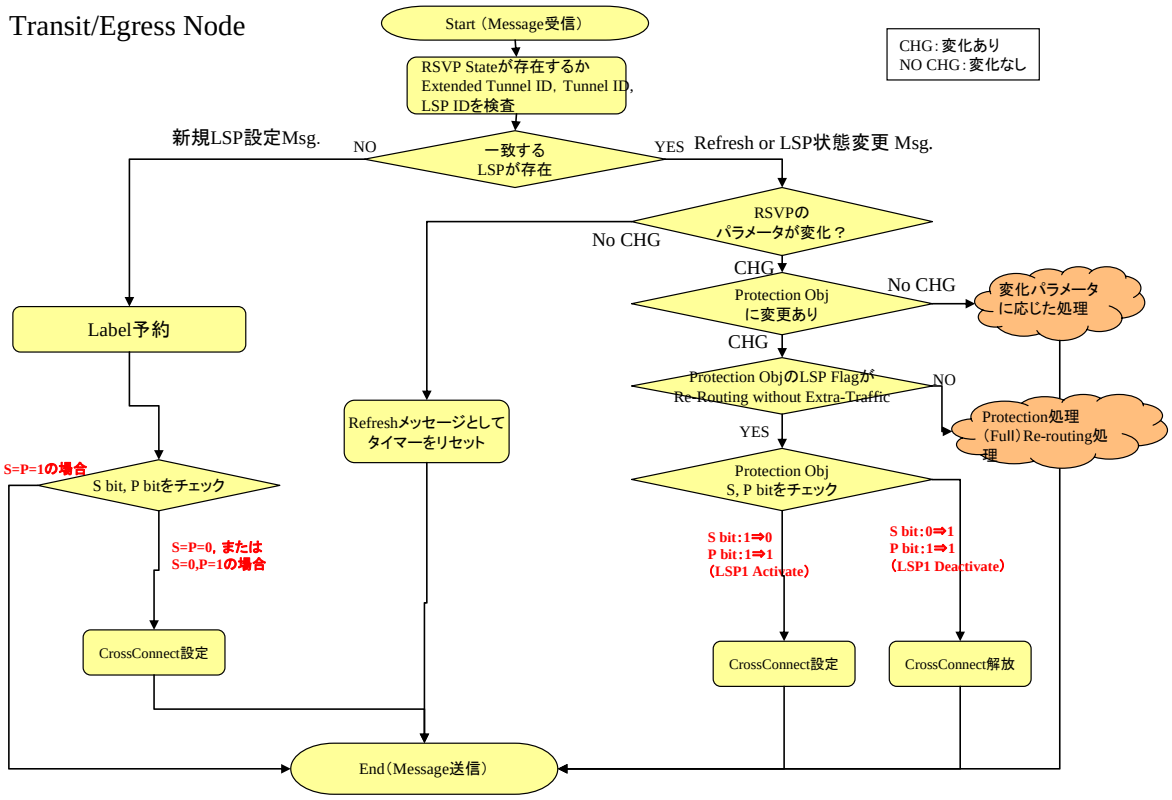


図 3-7　Message 処理フロー

NOTE：cross-connect 設定は，PATH/RESV Msg.のいずれのタイミングで実施してもよい．RESV のタイミングは PATH Msg.で受信した Protection Obj の S/P bit を参照して，cross-connect 設定を行う．

3.1.3. メッセージフォーマット

以下に，PATH, RESV, Notify メッセージのフォーマットを記す．障害回復に関する以外は技術検証 WG で使用しているパラメータを記述する。

【注】

- 相互接続性を高めるため，Refresh/切替/切戻メッセージを送信する際には，設定のときに使用した Object は必ず含める．
- Option flag は，PIL 障害回復 IA での選択肢であり，RFC とは連動しない．Option Object は，送信時に含める必要はないが，転送および受信ができなければならない

【PATH メッセージ】

Object	Class	CType	Option	Parameter/Sub-Object	Value	備考
RSVP Header	なし	なし		RSVP Version	1	IP alert Option は設定しない
				Flag	0x00	
				Message Type	1（Path）	
				Message Checksum	チェックサム値	
				Sending TTL	1 以上	
				Message Length	Path Msg. 長	
SESSION	1	7		Destination Address	Destination の Node ID	
				Tunnel ID	1 以上の値	
				Extended Tunnel ID	Source の Router ID	
RSVP HOP	3	3		Neighbor Address	C-Plane の Router ID	
				LIH	C-Plane の IF ID	
				IF_INDEX TLV - IPv4 Address - Interface－ID	 D-Plane の Node ID D-Plane の IF ID	
TIME VALUE	5	1		Refresh Interval	30000 msec（参考値）	
LABEL REQUEST	19	4		LSP Encoding Type	8 ; Lambda（参考値）	
				Switching Type	150 ; LSC（参考値）	
				G-PID	31 ; POS（参考値）	
PROTECTION	37	??		S, P, N bit	Protection Restoration 動作に従う（3.1 章）	
				LSP flag	0x02 （ 1:1 Rerouting without Extra Traffic）	
				Link flag	0x02（Unprotected）（参考値）	
ASSOCIATION	198			Association Type	0x01（Recovery）	
				Association ID	関連付ける LSP ID	
SESSION ATTRIBUTE	207	7	O	Setup Priority	3（参考値）	
				Holding Priority	4（参考値）	
				Flag	0x00（参考値）	
				Name	任意	
NOTIFY REQUEST	195	1	O	IPv4 Notify Address	Node ID	
ADMIN_STATUS	196	1	O	R, T, A, D	R: Reflect T: Testing A: Administratively Down D: Deletion in progress	R：応答を期待 T：規定なし A：Admin Down D: Graceful Deletion
EXPLICIT ROUTE	20	1		ERO Unnumbered Link - Router ID - Interface ID	(Next Hop) D-Plane の Node ID D-Plane の IF ID	
SENDER TEMPLATE	11	7		Sender IPv4 Address	Source Node ID	
				LSP ID	1 以上の値	
SENDER TSPEC	12	1		Token Bucket Rate	0	
				Token Bucket Size	0	
				Peak Data Rate	19440000 （参考値）	
				Maximum Policed Unit	0	
				Maximum Packet Size	9180（参考値）	
UPSTREAM LABEL	35	2		Generalized Label	Label 値	Bi-directional LSP の場合
LSP_TUNNEL_IF_ID	227? 193	1	O	Router ID	Message を送るノードの Node ID	
				Interface ID	論理 IF に割り振るインターフェース値．1 以上	既存 IF に使われていない番号
PRIMARY PATH ROUTE	??	1		ERO Unnumbered Link - Router ID - Interface ID	現用 LSP の D-Plane の Node ID D-Plane の IF ID	1 : 1 Re-routing without Extra Traffic かつ予備 LSP の設

						定にのみ含める.

【RESV メッセージ】

Object	Class	C-Type	Option	Sub-Object	パラメータ	備考
RSVP Header				RSVP Version	1	
				Flag	0x00	
				Message Type	2（Resv）	
				Message Checksum	チェックサム値	
				Sending TTL	1 以上	
				Message Length	Resv Msg. 長	
SESSION	1	7				PATH と同じ
RSVP HOP	3	3				PATH の値をコピーすること
TIME VALUE	5	1				PATH と同じ
RESV CONF	8	15	O	Receiver Address	Node ID	
NOTIFY REQUEST			O			
ADMIN STATUS			O			PATH と同じ
LSP_TUNNEL_IF_ID	227? 193	1	O			PATH と同じ
STYLE	8	1		Flag	0x00	
				Style	0x0a(Fixed Style)	
FLOW SPEC	9	2		Token Bucket Rate	0	
				Token Bucket Size	0	
				Peak Data Rate	19440000（参考値）	
				Maximum Policed Unit	0	
				Maximum Packet Size	9180（参考値）	
FILTER SPEC	10	7		Sender IPv4 Address	Source Node ID	
				LSP ID	1 以上	
LABEL	16	2		Generalized Label	ラベル値	

【Notify メッセージ（障害通知、切り戻し、1+1 Protection における切替での End-End 通信用途)】

Object	Class	C-Type	Option	Sub-Object	パラメータ	備考
RSVP Header				RSVP Version	1	
				Flag	0x00	
				Message Type	2（Resv）	
				Message Checksum	チェックサム値	
				Sending TTL	1 以上	
				Message Length	Notify Msg. 長	
Message ID	23	1		Message ID	ノードユニーク値	必須 Object Ack Desired
ERROR SPEC	6	3		IPv4 Error Node Address	Node ID	
				Flag		
				Error Code	Working Path Failure	
				Error Value	Reversion Request/Response	
				IF_INDEX - IPv4 Address - Interface－ID	 D-Plane の Node ID D-Plane の IF ID	
SESSION	1	7				PATH と同じ
SENDER TEMPLATE	11	7				PATH と同じ
SENDER TSPEC	12	1				PATH と同じ
SESSION	1	7				PATH と同じ
FLOW SPEC	9	2				PATH と同じ
FILTER SPEC	10	7				PATH と同じ

3.2. プロテクションシグナリング

対象とするプロテクションの方式は下記とする。定義は、[E2E]を参照のこと。

1+1 Unidirectional Protection
1+1 Bi-directional Protection
1:1 Protection with Extra-Traffic

ingress ノードは、現用 LSP と予備 LSP をそれぞれ設定する必要がある。現用 LSP、予備 LSP どちらを最初に設定しても、同時に設定しても構わない。

現用 LSP と予備 LSP のルートは node/link/SRLG disjoint なルートである必要がある。

3.2.1. 現用 LSP 設定

(1) シグナリングシーケンス

シーケンスを図 3-8, 図 3-9に示す。図 3-8は、ResvConf メッセージおよび ADMIN_STATUS を使わないシーケンスであり、図 3-9は、Option として、ResvConf メッセージおよび ADMIN_STATUS を使うシーケンスである。シーケンスは例であり、必ずしもメッセージの送信順序は図中に示す順序でなくともよい。例えば，パス設定の順序は現用 LSP(LSP0)、予備 LSP(LSP1)のどちらが先に実行されてもよく、同時でもよい。

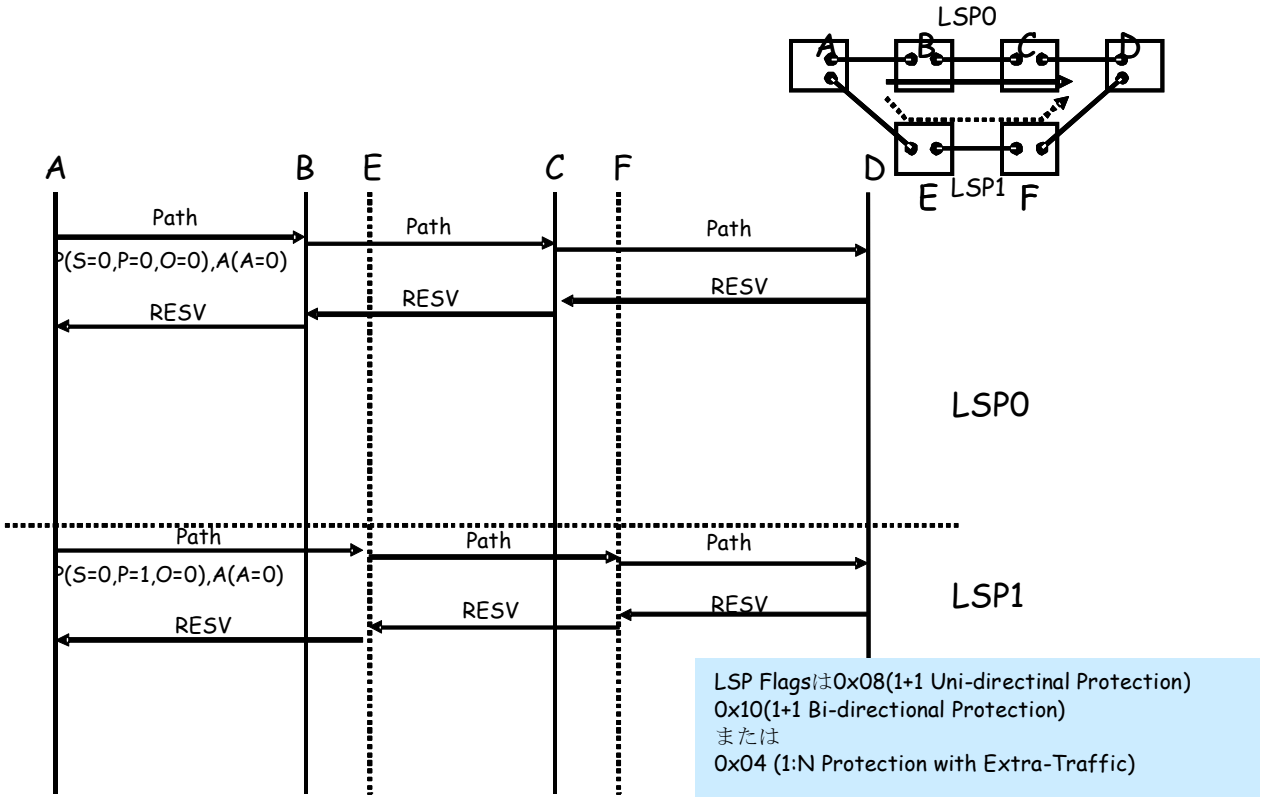


図 3-8 1+1 Unidirectional Protection、1+1 Bi-directional Protection、または 1:1 Protection with Extra-Traffic のシグナリングシーケンス(ResvConf と ADMIN_STATUS をサポートしない場合)

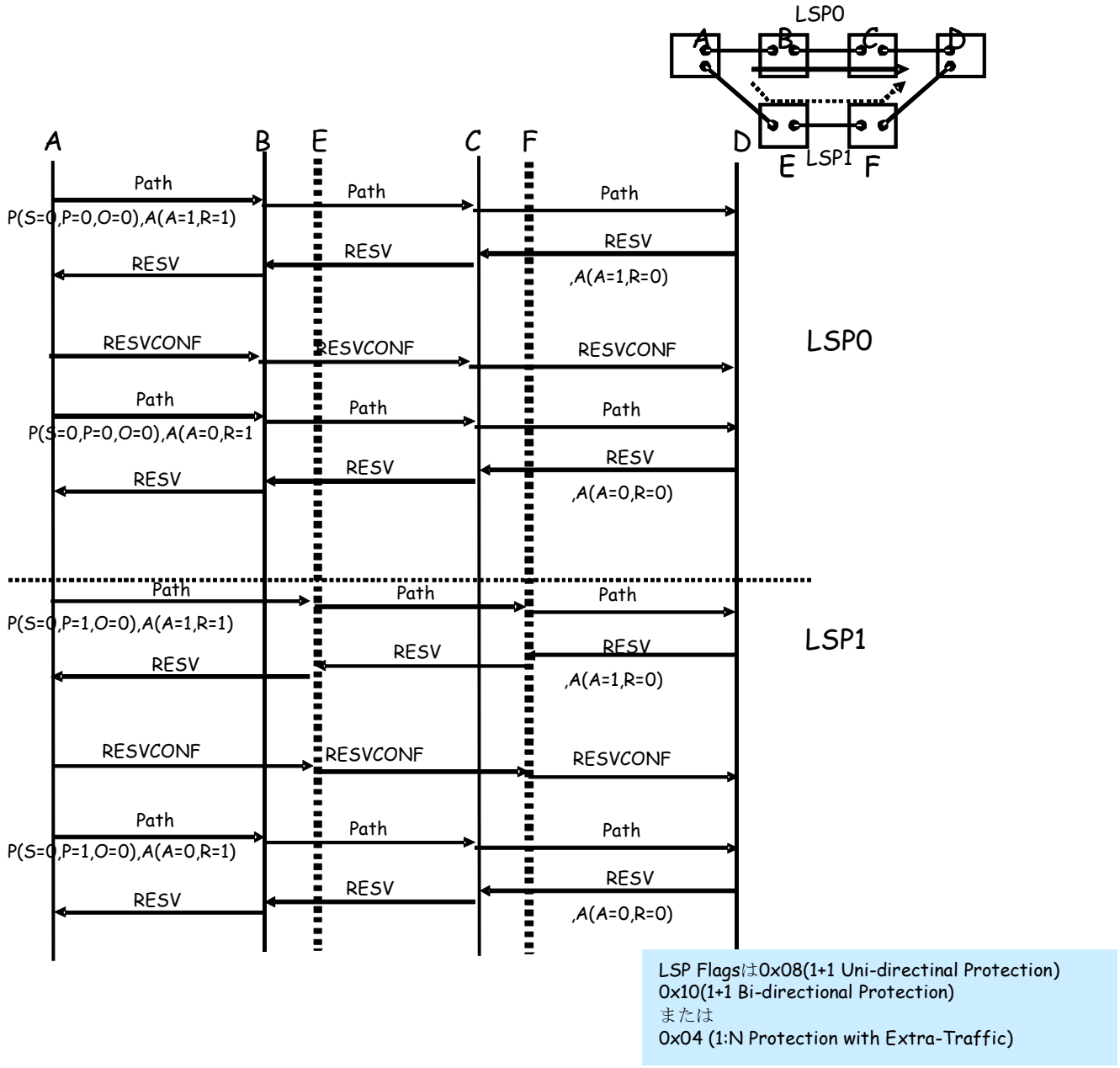


図 3-9　1+1 Unidirectional Protection、1+1 Bi-directional Protection、または 1:1 Protection with Extra-Traffic のシグナリングシーケンス(Option の手順として、ResvConf と ADMIN_STATUS をサポートする場合)

(2)　オブジェクトの内容、パラメータの指定

下記にパス設定時のメッセージに関して、プロテクションに関わる主要なオブジェクトの内容を示す。RSVP の各メッセージの詳細な定義(BNF、TLV ビットアサイン)は、[RFC3473]を参照のこと。

Path メッセージには、[E2E]で定義された PROTECTION Object, ASSOCIATION object を含める。

現用 LSP と予備 LSP の SESSION object は同じ値を設定する。SENDER_TEMPLATE object または FILTER_SPEC object の LSP ID は異なる値とする。

ingress ノード、egress ノードは、Notify Request を Path、Resv メッセージに含める。ただし、切替を D-plane で実施する場合(N ビット=1)において、D-plane において障害検出することとし、障害通知も不要な場合は、Notify Request は必須ではない。

Path メッセージ

オブジェクト	フィールド/Sub object	値	備考
SESSION	Destination address	egress ノード IP アドレス	
	Tunnel ID	予備 LSP と同一で、tunnel を識別するユニークな値	

	Extended Tunnel ID	ingress ノードの IP アドレス	
SENDER TEMPLATE	Sender IPv4 address	ingress ノードの IP アドレス	
	Sender LSP ID	tunnel 内でユニークな値。予備 LSP と異なる値とする。	
PROTECTION	Secondary (S)	0	[E2E]の定義を参照
	Protecting (P)	0	
	Notification (N)	0 または 1	本 IA では 1 の場合のみ規定
	Operational (O)	0	
	LSP (Protection Type) Flags	下記のいずれか 0x04(1:N Protection with Extra-Traffic) 0x08(1+1 Unidirectional Protection) 0x10(1+1 Bi-directional Protection)	
	Link Flags	規定上の任意の値 (RFC3471 参照)	
NOTIFY_REQUEST	IPv4 Notify Node Address	ingress ノードの IP アドレス	通知が必要の場合のみ本オブジェクトを使用
ADMIN_STATUS	Reflect (R)		必要に応じて本オブジェクトを使用(プロテクション手順には関係なし)
	Testing (T)		
	Administratively down (A)		
	Deletion in progress (D)		
ASSOCIATION	Association Type	1	Recovery (R)
	Association ID	予備 LSP の LSP ID の値	
	Association Source	ingress ノードの IP アドレス	

Resv メッセージ

オブジェクト	フィールド/Sub object	値	備考
NOTIFY_REQUEST	IPv4 Notify Node Address	egress ノードの IP アドレス	通知が必要の場合のみ本オブジェクトを使用
ADMIN_STATUS	Reflect (R)	0	必要に応じて本オブジェクトを使用(プロテクション手順には関係なし)
	Testing (T)	受信 Path メッセージと同じ値をコピー	
	Administratively down (A)		
	Deletion in progress (D)		

(3) Ingress、Intermediate、Egress 毎のメッセージ処理

(a) Ingress ノードでの処理

ingress ノードは、現用 LSP のルートを計算し、上記値の Object と決定したルートを ERO(Explicit Route Object)に含めて Path メッセージを送信する。Path 送信時には upstream の label を割り当て、Resv 受信後、cross-connect 設定は完了した状態にある。

1+1 Protection の場合、Resv 受信後、ingress ノードは、トラフィックを現用 LSP(LSP0)に転送する。bi-directional LSP の場合、逆方向(upstream)のトラフィックについて、現用 LSP(LSP0)からトラフィックを受信するように選択する。

1:1 Protection の場合、Resv 受信後、ingress ノードは、トラフィックを現用 LSP(LSP0)にのみ転送する。bi-directional LSP の場合、逆方向(upstream)のトラフィックについて、現用 LSP(LSP0)からトラフィックを受信するように選択する。

(b) Intermediate ノードでの処理

Path 送信、Resv 送信時それぞれ upstream/downstream の label を割り当て、Resv 送信時には、cross-connect 設定は完了した状態にある。

(c) Egress ノードでの処理

Resv 送信時 downstream の label を割り当て、Resv 送信時には、cross-connect 設定は完了した状態にある。

1+1 Protection の場合、egress ノードは、現用 LSP(LSP0)からトラフィックを受信するように選択する。bi-directional LSP の場合、逆方向(upstream)のトラフィックについて、トラフィックを現用 LSP(LSP0)に転送する。

1:1 Protection の場合、Resv 受信後、egress ノードは、現用 LSP(LSP0)からトラフィックを受信する。bi-directional LSP の場合、逆方向のトラフィックについて、トラフィックを現用 LSP にのみ転送する。

3.2.2. 予備 LSP 設定

(1) シグナリングシーケンス

シーケンスは3.2.1で示した図 3-8、図 3-9を参照のこと。

(2) オブジェクトの内容、パラメータの指定

下記に LSP 設定時のメッセージに関して、プロテクションに関わる主要なオブジェクトの内容を示す。SESSION Object と SENDER_TEMPLATE の IPv4 (or IPv6) tunnel sender address は、現用 LSP と同じ値を設定する。これにより現用と予備のペアが識別できる。SENDER_TEMPLATE/FILTER_SPEC object の LSP ID は、現用 LSP と予備 LSP で異なる値を使用する。

Path メッセージ

オブジェクト	フィールド/Sub object	値	備考
SESSION	Destination address	egress ノード IP アドレス	
	Tunnel ID	現用 LSP と同一で、tunnel を識別するユニークな値	
	Extended Tunnel ID	ingress ノードの IP アドレス	
SENDER TEMPLATE	Sender IPv4 address	ingress ノードの IP アドレス	
	Sender LSP ID	tunnel 内でユニークな値。現用 LSP と異なる値とする。	
PROTECTION	Secondary (S)	0	[E2E]の定義を参照
	Protecting (P)	1	
	Notification (N)	0 または 1	本 IA では 1 の場合のみ規定
	Operational (O)	0	
	LSP (Protection Type) Flags	下記のいずれか 0x04(1:N1 Protection with Extra-Traffic) 0x08(1+1 Unidirectional Protection) 0x10(1+1 Bi-directional Protection)	
	Link Flags	規定上の任意の値 (RFC3471 参照)	
NOTIFY_REQUEST	IPv4 Notify Node Address	ingress ノードの IP アドレス	通知が必要の場合のみ本オブジェクトを使用
ADMIN_STATUS	Reflect (R)		必要に応じて本オブジェクトを使用(プロテクション手順には関係なし)
	Testing (T)		
	Administratively down (A)		
	Deletion in progress (D)		
ASSOCIATION	Association Type	1	Recovery (R)
	Association ID	現用 LSP の LSP ID の値	
	Association Source	ingress ノードの IP アドレス	

Resv メッセージ

オブジェクト	フィールド/Sub object	値	備考
NOTIFY_REQUEST	IPv4 Notify Node Address	egress ノードの IP アドレス	通知が必要の場合のみ本オブジェクトを使用
ADMIN_STATUS	Reflect (R)	0	必要に応じて本オブジェクトを使用(プロテクション手順には関係なし)
	Testing (T)	受信 Path メッセージと同じ値をコピー	
	Administratively down (A)		
	Deletion in progress (D)		

(3)　Ingress、Intermediate、Egress 毎のメッセージ処理

(a) Ingress ノードでの処理

ingress ノードは、予備 LSP のルートを決定する。予備 LSP のルートは、現用 LSP のルートと link/node/SRLG disjoint なルートとする。上記値の Object と決定したルートを ERO に含めて Path メッセージを送信する。Path 送信時には upstream の label を割り当てる。

1+1 Protection の場合、Resv 受信後、ingress ノードは、トラフィックを予備 LSP(LSP1)にもコピーして転送する。

(b) Intermediate ノードでの処理

Path 送信、Resv 送信時それぞれ upstream/downstream の label を割り当て、Resv 送信時には、cross-connect 設定は完了した状態にある。

(b) Egress ノードでの処理

Resv 送信時 downstream の label を割り当てる。

1+1 Protection で bi-directional LSP の場合、逆方向(upstream)のトラフィックについて、トラフィックを予備 LSP(LSP1)にもコピーして転送する。

3.2.3. 切替

本 IA では、D-plane 上の手順で切替を実施することを前提とする。例として、OTN ベースの Lambda Switch LSP の場合、G.873.1 で定義されている linear protection(ODU の APS channel)の仕組みを使うことが可能である。

SDH では、G.841 に MSP(K1/K2 バイト) 、VC trail(K3/K4。プロトコル未定義)の規定がある。

C-plane での切替(N ビットが 0）の手順は、本 IA の対象外とする。概要は、[E2E]を参照のこと。

以下では、D-plane 上の手順で切替を実施することを前提として、シグナリング状態の変化について示す。

(1)　シグナリングシーケンス

シーケンスを図 3-10に示す。シーケンスは例であり、シグナリング状態更新の順序は現用 LSP(LSP0)、予備 LSP(LSP1)のどちらが先に実行されてもよく、同時でもよい。

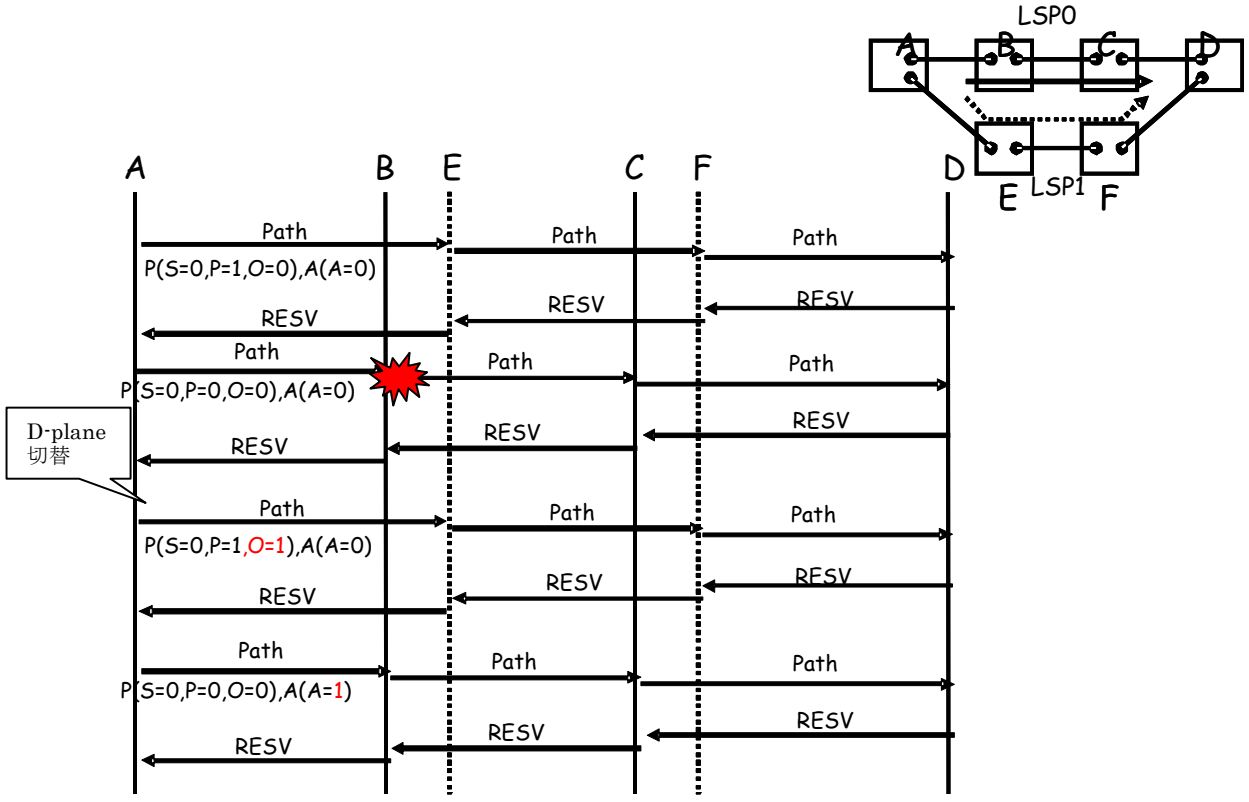


図 3-10　1+1 Unidirectional Protection、1+1 Bi-directional Protection、または 1:1 Protection with Extra-Traffic のシグナリングシーケンス(障害監視抑止のために現用 LSP の A ビットを 1 に設定する手順は Optional)

(2)　オブジェクトの内容、パラメータの指定

現用 LSP、予備 LSP のシグナリング状態は、切替完了後、ingress/egress ノードが理解していれば、どちらが運用なのかを知ることはできるので、現用 LSP(LSP0)については変わらず、予備 LSP(LSP1)の O ビットのみが 0 から 1 に変化する。Intermediate ノードでは、障害監視を考えて、どの LSP が運用なのかを知る必要がある。しかし、D plane の切替手順を Intermediate ノードが理解していれば、どちらが運用なのかを知ることはできるので、O ビットの値を変更せずとも問題ない。

また、障害監視を抑止するため、切替前に運用中であった LSP（本例では LSP0） の ADMIN_STATUS の A ビットを 1 に設定しても良い(Optional)。障害が回復すれば、任意の時点で 0 に戻してよい。

(3) Ingress、Intermediate、Egress 毎のメッセージ処理

bridge/select の変更が LSP の両端のノードで行われ、label の割り当て状態の変更はなく、Intermediate ノードにおいて cross-connect 状態は変更されない。

(a) Ingress ノードでの処理

1+1 Protection で bi-directional の場合、逆方向(upstream)のトラフィックについて、トラフィックを現用 LSP(LSP0)から受信していたが、切替後は、予備 LSP(LSP1)から受信するようになる。

1:1 Protection の場合、ingress ノードは、予備 LSP(LSP1)にトラフィックを送信するようになる。bi-directional の場合、逆方向(upstream)のトラフィックについて、予備 LSP(LSP1)からトラフィックを受信するようになる。

(b) Intermediate ノードでの処理

cross-connect 状態は変更されない。

(c) Egress ノードでの処理

1+1 Protection の場合、egress ノードにてトラフィックを現用 LSP(LSP0)から受信していたが、切替後は、予備 LSP(LSP1)から受信するようになる。

1:1 Protection の場合、egress ノードは、予備 LSP(LSP1)からトラフィックを受信するようになる。bi-directional の場合、逆方向(upstream)のトラフィックについて、予備 LSP(LSP1)にトラフィックを送信するようになる。

3.2.4. 切り戻し動作

本 IA では、切替動作と同様に、D-plane 上の手順で切リ戻しを実施することを前提とする。切り戻しについても、切替動作と同様に、例として、G.873.1 で定義されている OTN linear protection(ODU の APS channel)や、G.841 の SDH MSP(K1/K2 バイト)を適用可能である。

C-plane での切替(N ビットが 0）の手順は、本 IA の対象外とする。概要は、[E2E]を参照のこと。

以下では、D-plane 上の手順で切替を実施することを前提として、シグナリング状態の変化について示す。

(1)　シグナリングシーケンス

シーケンスを図 3-11に示す。シグナリング状態更新の順序は現用 LSP(LSP0)、予備 LSP(LSP1)のどちらが先に実行されてもよく、同時でもよい。

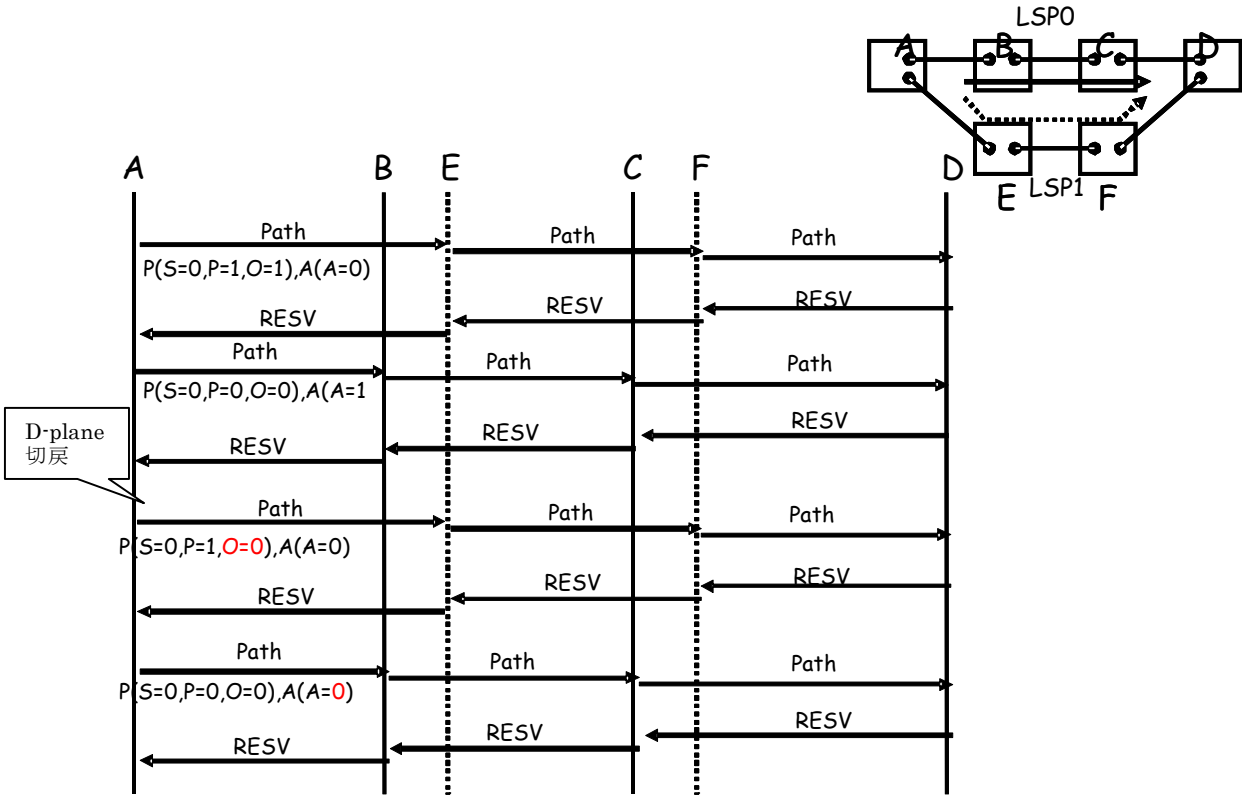


図 3-11　1+1 Unidirectional Protection、1+1 Bi-directional Protection、または 1:1 Protection with Extra-Traffic のシグナリングシーケンス(障害監視抑止を実施していたために現用 LSP の A ビットを 1 に設定しており、0 に変更する手順は Optional)

(2)　オブジェクトの内容、パラメータの指定

現用 LSP、予備 LSP のシグナリング状態は、切替完了後、予備 LSP の O ビットの値が変化する。すなわち、切り戻し前に運用中であった予備 LSP（LSP1）の O ビットは 1 から 0 になる. 障害監視を抑止するため、切り戻し前に故障中であった LSP 0　の ADMIN_STATUS の A ビットは 1 に設定されているが、切り戻し後は、0 に設定する

(3)　Ingress、Intermediate、Egress 毎のメッセージ処理

bridge/select の変更が LSP の両端のノードで行われ、label の割り当て状態の変更はなく、Intermediate ノードにおいて cross-connect 状態は変更されない。

(a) Ingress ノードでの処理

1+1 Protection で bi-directional の場合、逆方向(upstream)のトラフィックについて、トラフィックを予備 LSP（LSP1）から受信していたが、切替後は、現用 LSP（LSP0）から受信するようになる。

1:1 Protection の場合、ingress ノードは、現用 LSP（LSP0）にトラフィックを送信するようになる。bi-directional の場合、逆方向(upstream)のトラフィックについて、現用 LSP（LSP0）からトラフィックを受信するようになる。

(b) Intermediate ノードでの処理

cross-connect 状態は変更されない。

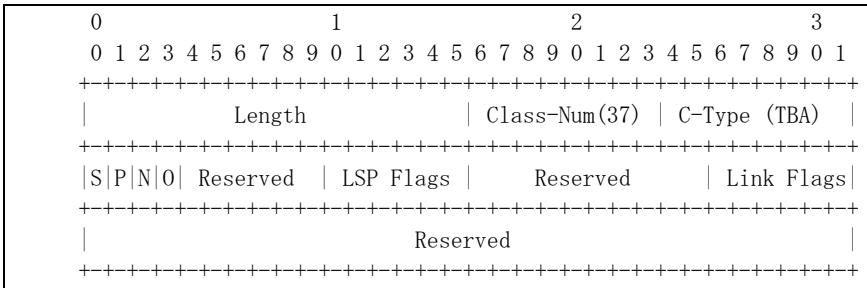
(c) Egress ノードでの処理

1+1 Protection の場合、トラフィックを予備 LSP（LSP1）から受信していたが、切替後は、現用 LSP（LSP0）から受信するようになる。

1:1 Protection の場合、現用 LSP（LSP0）からトラフィックを受信するようになる。bi-directional の場合、逆方向(upstream)のトラフィックについて、現用 LSP（LSP0）にトラフィックを送信するようになる。

3.3. オブジェクト

3.3.1. （Extended） protection object



Secondary (S): 1 bit
When set to 1, this bit indicates that the requested LSP is a secondary LSP. When set to 0 (default), it indicates that the requested LSP is a primary LSP.

Protecting (P): 1 bit
When set to 1, this bit indicates that the requested LSP is a protecting LSP. When set to 0 (default), it indicates that the requested LSP is a working LSP. The combination, S set to 1 with P set to 0 is not valid.

Notification (N): 1 bit
When set to 1, this bit indicates that the control plane message exchange is only used for notification during protection switching. When set to 0 (default), it indicates that the control plane message exchanges are used for protection switching purposes. The N bit is only applicable when the LSP Protection Type Flag is set to either 0x04 (1:N Protection with Extra-Traffic), or 0x08 (1+1 Unidirectional Protection) or 0x10 (1+1 Bi-directional Protection). The N bit MUST be set to 0 in any other case.

Operational (O): 1 bit
When set to 1, this bit indicates that the protecting LSP is carrying the normal traffic after protection switching. The O bit is only applicable when the P bit is set to 1 and the LSP Protection Type Flag is set to either 0x04 (1:N Protection with Extra-Traffic), or 0x08 (1+1 Unidirectional Protection)or 0x10 (1+1 Bi-directional Protection). The O bit MUST be set to 0 in any other case.

Reserved: 5 bits
This field is reserved. It MUST be set to zero on transmission and MUST be ignored on receipt. These bits SHOULD be passed through unmodified by transit nodes.

LSP (Protection Type) Flags: 6 bits
Indicates the desired end-to-end LSP recovery type. A value of 0 implies that the LSP is "Unprotected". Only one value SHOULD be set at a time. The following values are defined. All other values are reserved.

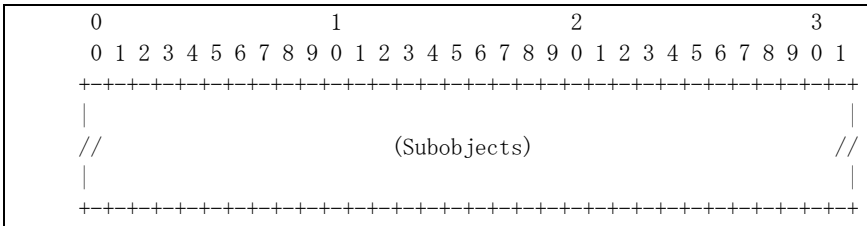
0x00	Unprotected
0x01	(Full) Re-routing
0x02	Re-routing without Extra-Traffic
0x04	1:N Protection with Extra-Traffic
0x08	1+1 Unidirectional Protection
0x10	1+1 Bi-directional Protection

Reserved: 10 bits
This field is reserved. It MUST be set to zero on transmission and MUST be ignored on receipt. These bits SHOULD be passed through unmodified by transit nodes.

Link Flags: 6 bits
Indicates the desired link protection type (see [RFC3471]).

Reserved field: 32 bits
Encoding of this field is detailed in [SEGREC].

3.3.2. PRIMARY PATH ROUTE Object



The contents of a PRIMARY_PATH_ROUTE object are a series of variable-length data items called subobjects (see Section 15.3).

To signal a secondary protecting LSP, the Path message MAY include one or multiple PRIMARY_PATH_ROUTE objects, where each object is meaningful. The latter is useful when a given secondary protecting LSP must be link/node/SRLG disjoint from more than one primary LSP (i.e. is protecting more than one primary LSP).

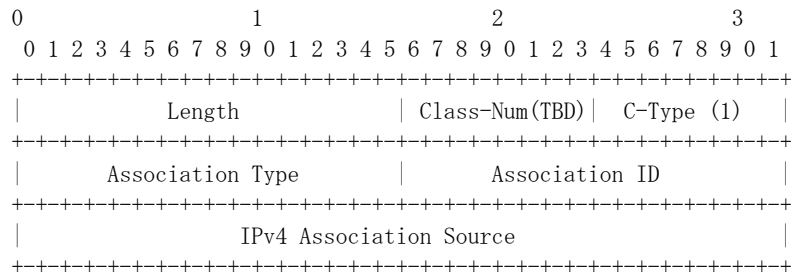
Sub-Objects:

The following subobjects are currently defined for the PRIMARY PATH ROUTE object:

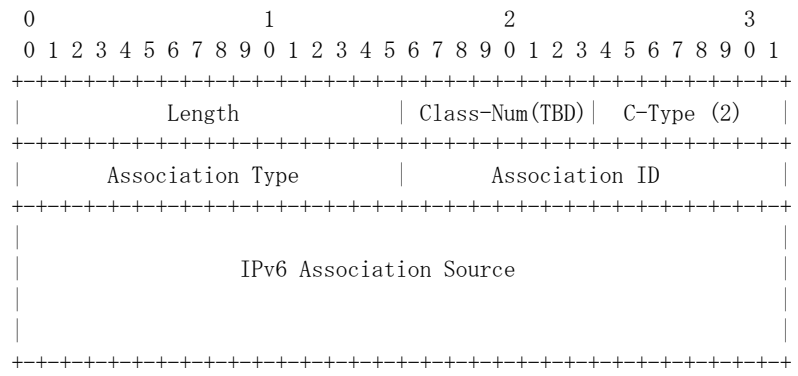
- Sub-Type 1: IPv4 Address (see [RFC 3209])
- Sub-Type 2: IPv6 Address (see [RFC 3209])
- Sub-Type 3: Label (see [RFC-3473])
- Sub-Type 4: Unnumbered Interface (see [RFC-3477])

3.3.3. ASSOCIATION Object

IPv4 ASSOCIATION object:



IPv6 ASSOCIATION object:



Association Type: 16 bits

Indicates the type of association being identified. Note that this value is considered when determining association. The following are values defined in this document.

Value	Type
0	Reserved
1	Recovery (R)

Association ID: 16 bits

A value assigned by the LSP Ingress. When combined with the Association Type and Association Source, this value uniquely identifies an association.

Association Source: 4 or 16 bytes

An IPv4 or IPv6 address, respectively, that is associated to the node that originated the association.

3.3.4. Protection Obj の S, P, O-bit の定義

- S ビット
  LSP の設定において D-Plane の cross-connect を設定するかどうかを示す。
  0： cross-connect 設定
  ・1： cross-connect 設定しない

- P ビット：
  LSP の現用/予備を示す．現用/予備は障害発生の有無にかかわらず，（名称変更がない限り）固定である．
  0： 現用 LSP
  1： 予備 LSP

- O ビット：
  以下の Protection の予備 LSP（P=1）が，障害に発生のため、使用（運用）されているかどうかを示す．
  0x04 1:N Protection with Extra-Traffic
  0x08 1+1 Unidirectional Protection
  0x10 1+1 Bi-directional Protection

  0：非運用
  1：運用

4. ルーティング

4.1. ルーティング基本概要

4.1.1. 障害回復のための拡張

OSPF-TE、GMPLS 拡張のために追加さえた OSPF の Sub-TLV のうち、障害回復に関係の深い Sub-TLV を以下に示す[OSPF-TE, GMPLS-OSPF, SHARABLE-OSPF]。

表 4-1

Sub-TLV Type	長さ	名前
1	1	Link type [OSPF-TE]
5	4	Traffic engineering metric [OSPF-TE]
6	4	Maximum bandwidth [OSPF-TE]
7	4	Maximum reservable bandwidth [OSPF-TE]
8	32	Unreserved bandwidth [OSPF-TE]
11	8	Link Local/Remote Identifiers [GMPLS-OSPF]
14	4	Link Protection Type [GMPLS-OSPF]
15	variable	Interface Switching Capability Descriptor [GMPLS-OSPF]
17	variable	Shared Risk Link Group [GMPLS-OSPF]
TBD	variable	Sharable Bandwidth [SHARABLE-OSPF]

各 Sub-TLV の一般的利用方法を以下に示す。

Link type
リンクのタイプ(Point-to-point, Multi-access)を表す[OSPF-TE]。

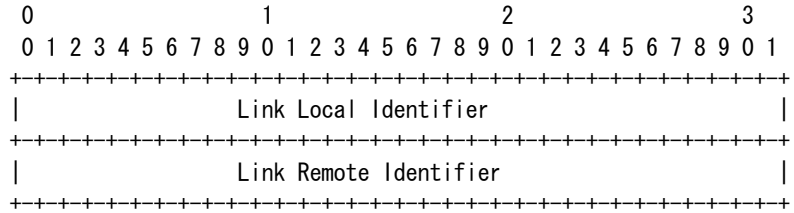
Traffic engineering metric
トラフィックエンジニアリングに用いられるリンクのメトリックである、通常の OSPF のメトリック情報とは異なる[OSPF-TE]。

Maximum bandwidth
そのリンクで可能利用な最大帯域を表す[OSPF-TE]。

Maximum reservable bandwidth
そのリンクで予約利用な最大帯域を表す[OSPF-TE]。

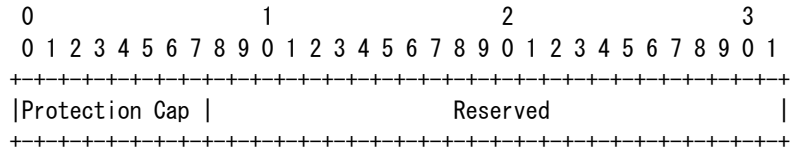
Unreserved bandwidth
０～７の各優先順位レベルで、そのリンクの未予約状態の帯域を表す [OSPF-TE]。

Link Local/Remote Identifiers
Unnumbered 型のインターフェースを識別情報である。
リンクのローカル側とリモート側のペアを広告する。フォーマットを以下に示す[GMPLS-OSPF]。



Link Protection Type

リンクのプロテクション種別を識別するのに利用される。フォーマットを以下に示す[GMPLS-OSPF]。



第一オクテットの” Protection Cap”は、以下に示す Protection 種別を表す。

0x01 Extra Traffic
0x02 Unprotected
0x04 Shared
0x08 Dedicated 1:1
0x10 Dedicated 1+1
0x20 Enhanced
0x40 Reserved
0x80 Reserved

Shared Risk Link Group (SRLG)
障害時に、その障害が影響する複数のリンクの集合を識別するのに用いられる。フォーマットを以下に示す[GMPLS-OSPF]。

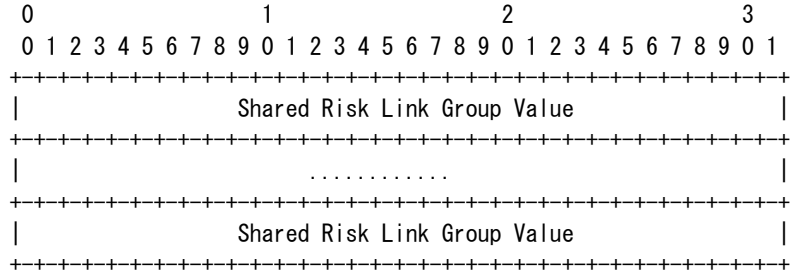


図 4-1

Interface Switching Capability Descriptor
インタフェースの種別、LSP が利用可能な帯域等の情報の広告に利用される。フォーマットを以下に示す[GMPLS-OSPF]。

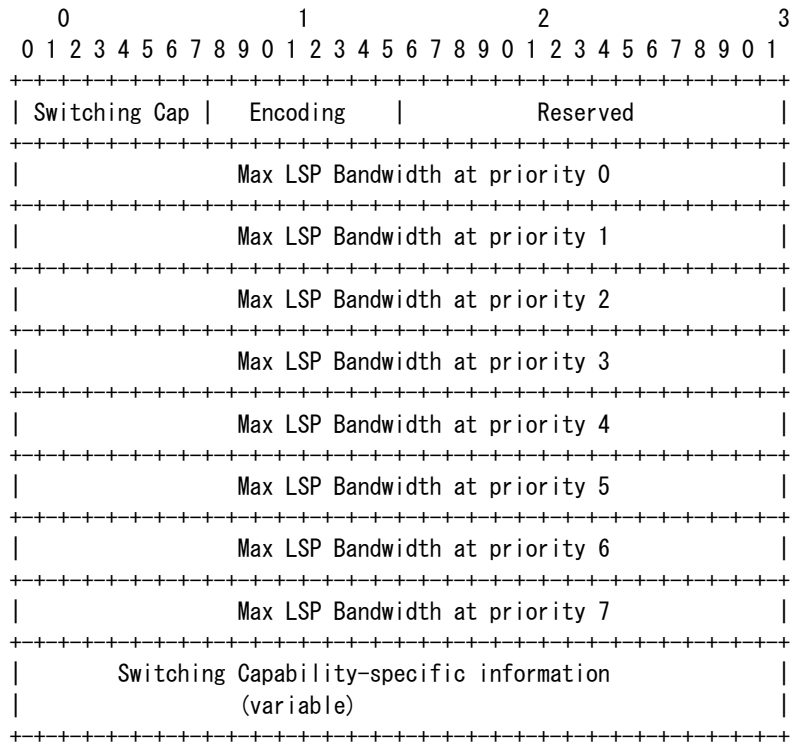
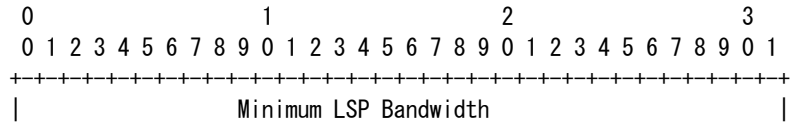


図 4-2

Switching capability が SONET/SDH の場合は、さらに以下に示すフィールドが追加され、最小帯域の利用等に用いられる[GMPLS-OSPF]。



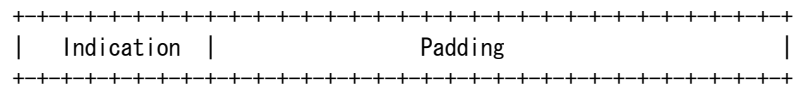


図 4-3

Sharable Bandwidth
共有可能な帯域の広告に用いられる。フォーマットを以下に示す[SHARABLE-OSPF]。

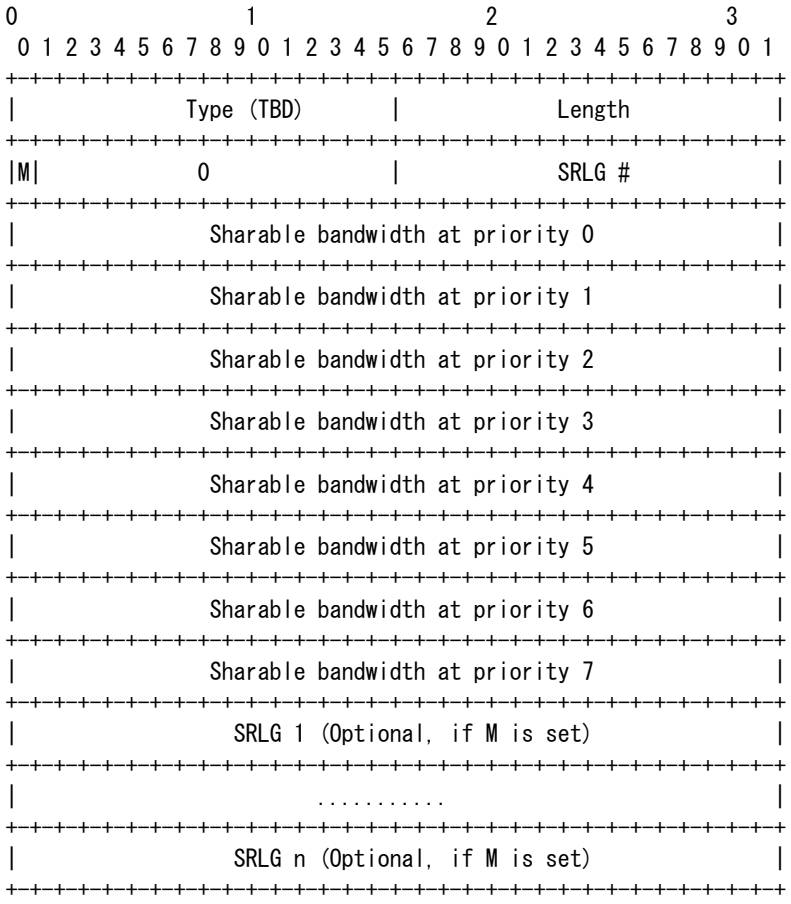


図 4-4

Forwarding adjacency
FA の属性
OSPF で広告される FA の Sub-TLV のうち、障害回復に関係の深い Sub-TLV の一般的利用方法を以下に示す。

Link type
FA の Link type は、point-to-pint となる[LSP-HIER]。

Traffic engineering metric
FA の Ingress に設定がない場合、メトリックの値は FA-LSP パスのメトリックから 1 引いた値が設定される[LSP-HIER]。

Maximum bandwidth
FA の Ingress に設定がない場合、FA の帯域の値は FA-LSP パスの値が設定される[LSP-HIER]。

Maximum reservable bandwidth
FA の最大予約可能帯域の初期値は、FA-LSP の帯域が設定される[LSP-HIER]。

Unreserved bandwidth
FA の未予約帯域の初期値は、FA-LSP の帯域が設定される[LSP-HIER]。

Link Local/Remote Identifiers
LSP を設定する際、LSP の Ingress がローカルの Link Identifier を割当、RSVP の PATH メッセージ中の LSP_TUNNEL_INTERFACE_ID により、パス中の各ノードに通知する。LSP の Egress は LSP_TUNNEL_INTERFACE_ID が含まれる PATH メッセージを受信すると、FA のリモート側の Link Identifier を割り当て、応答する RESV メッセージにより通知する。FA 中の Link Local/Remote Identifiers は上記手順で割当られた値が広告される [RFC3477]。

Link Protection Type
FA のプロテクション種別を表す。詳細は 6 章を参照。

SRLG
FA-LSP パスを形成する TE-Link 中の SRLG の集合が FA の SRLG として広告される[LSP-HIER]。
二重化された LSP を FA で広告する場合の SRLG については、6 章を参照。

Interface Switching Capability Descriptor
FA の Interface Switching Capability Descriptor は、FA-LSP パスの最初のリンクの値が設定される。Interface Switching Capability Descriptor が TDM の場合、FA-LSP パス中の Minimum LSP Bandwidth のうち、最大のものが FA に設定される。

Sharable Bandwidth
FA の共有可能帯域は、FA-LSP の共有可能帯域が設定される。

【Note】　FA の属性について
Protection type
- Local/remote link identifier
- Interface switching capability
- Maximum bandwidth
- Maximum reservable bandwidth：全体の割当
- Maximum LSP bandwidth　(Residual bandwidth)：全体の残余
- Maximum sharable bandwidth：予備の割当
- Residual sharable bandwidth：予備の残余
- Maximum extra bandwidth：Extra の割当
- Residual extra bandwidth：Extra の残余

4.2.　障害回復のための FA 利用方法
障害回復のために利用される FA 中の各 OSPF の Sub-TLV については、二重化された LSP については 6 章を、Extra トラヒックについては 7 章を参照。

4.3.　FA と LSP の管理
LSP の二重化を行う場合、これらの LSP は 1 本の FA として広告される。FA は非番号とする。FA と LSP に関する識別子を表 4-2に示す。
同一 FA を構成する LSP は同一の Tunnel ID が割り当てられる。LSP は LSP-ID により識別される。

表 4-2　FA と LSP に関する識別子

	属性	説明
FA	Link local identifier	自ノードが払い出す Link identifier
	Link remote identifier	対向ノードが払い出す Link identifier
LSP	IPv4 Tunnel end point address	Egress 側の Router ID を指定する。
	Tunnel ID（Session Obj）	RSVP でセッションを識別するために用いる。ここで、セッションと FA は同じものを指す。
	Extended Tunnel ID（Session Obj）	RSVP でセッションを識別するために用いる。ここで、セッションと FA は同じものを指す。セッション識別を Ingress-Egress 間で限定するために、Ingress の Router ID を指定してもよい。通常は All ‘0’。
	LSP ID（Sender Template Obj 又は Filter Spec Obj）	セッション（FA）を構成する LSP を識別するために用いる。起点ノードでユニークな値を割り当てる。
	Interface ID (LSP TUNNEL INTERFACE ID Obj)	自ノードおよび対向ノードが払い出す Link identifier を交換するために用いられる。Path メッセージには Ingress ノードが払い出したものを、Resv メッセージには Egress ノードが払い出したものを搭載する。RSVP で交換されると OSPF で FA を広告する際に Link Local/Remote identifier として広告される。

Link identifier
FA は非番号とする。双方向 LSP の場合、FA は発側ノードがそれぞれ広告する。FA の Link identifier はそれぞれ自ノード側が払い出す。自分が発側となる FA については Local の Link identifier を払い出す。自分が着側となる FA については Remote の Link identifier を払い出す。
図 4-5ではノード A とノード D の間に二重化の LSP を設定した例を示す。ノード A はノード A からノード D への方向の FA を広告し、ノード D はノード D からノード A への方向の FA を広告する。ノード A 側の Link identifier はノード A が払い出す（図 4-5では X とする）。ノード D 側の Link identifier はノード D が払い出す（図 4-5では Y とする）。ノード A とノード D は Link identifier の交換を RSVP-TE を用いて行う[RFC3473,RFC3477]。ノード A は Path メッセージに LSP_TUNNEL_INTERFACE_ID オブジェクトを搭載し、自ノードのルーターID を RouterID フィールドに、払い出した Link identifier（ここでは X）を Interface ID に設定し、送信する。ノード D は Path メッセージを受信すると、ノード A が払い出した Link identifier が X であることを認識する。次にノード D は Resv メッセージに LSP_TUNNEL_INTERFACE_ID オブジェクトを搭載し、自ノードのルーターID を RouterID フィールドに、払い出した Link identifier（ここでは Y）を Interface ID に設定し、送信する。ノード A は Resv メッセージを受信すると、ノード D が払い出した Link identifier が Y であることを認識する。このようにしてノード A とノード D はそれぞれが払い出した Link identifier を交換する。この後、ノード A とノード D はそれぞれ FA を広告する。ノード A はノード A から D 方向の FA を、ノード D はノード D からノード A 方向の FA を、それぞれ広告する。

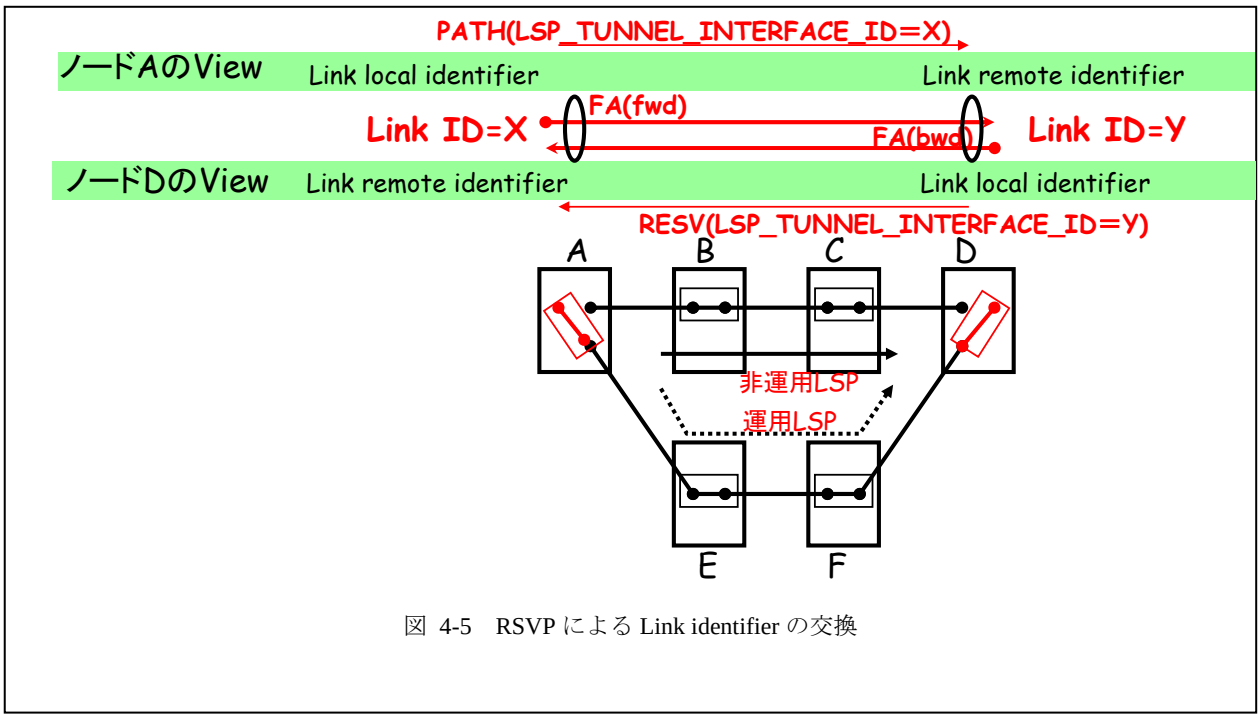


図 4-5　RSVP による Link identifier の交換

Protection type
LSP を FA として広告する際の Protection type は LSP の Protection type（PROTECTION Obj の LSP Flags）によって決まる[E2E]。
表 4-3に PROTECTION Obj の LSP Flags と FA の Protection type の関係を示す。

表 4-3 LSP の PROTECTION Obj の LSP Flags と FA の Protection type の関係

LSP（PROTECTION Obj の LSP Flags）	FA（Protection type）
0x00 Unprotected	0x02 Unprotected
0x01 (Full) Re-routing	NA
0x02 1:1 Re-routing without Extra-Traffic	0x04 Shared
TBD 1:1 Re-routing with Extra-Traffic	0x04 Shared
0x04 1:1 Protection with Extra-Traffic	0x08 Dedicated 1:1
0x08 1+1 Unidirectional Protection	0x10 Dedicated 1+1
0x10 1+1 Bi-directional Protection	0x10 Dedicated 1+1

Dedicated 1+1
Dedicated 1+1 の場合の FA の広告を図 4-6に示す。

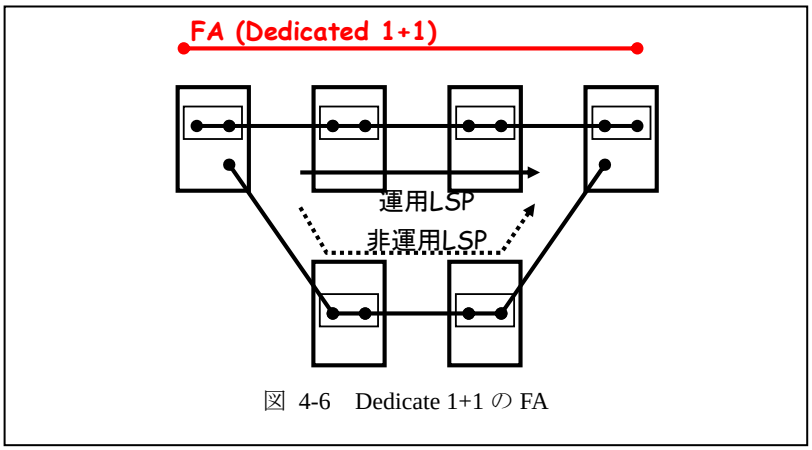


図 4-6　Dedicate 1+1 の FA

Dedicated 1:1
Dedicated 1:1 の場合の FA の広告を図 4-7に示す。

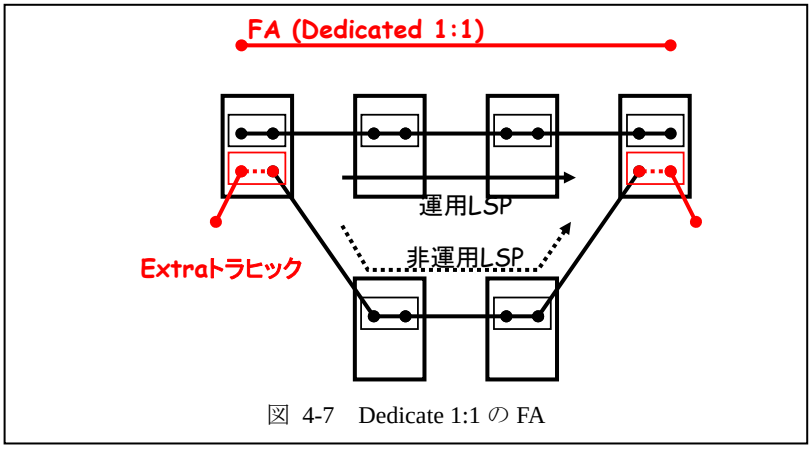


図 4-7　Dedicate 1:1 の FA

Shared
Shared の場合の FA の広告を図 4-8に示す。

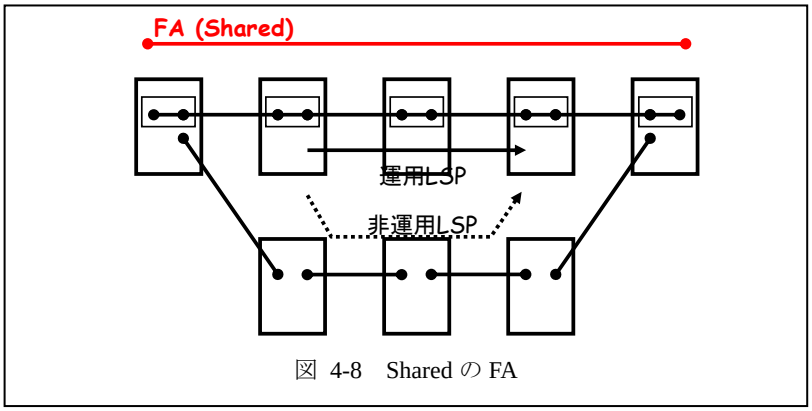


図 4-8　Shared の FA

Unprotected
Unprotected の場合の FA の広告を図 4-9に示す。

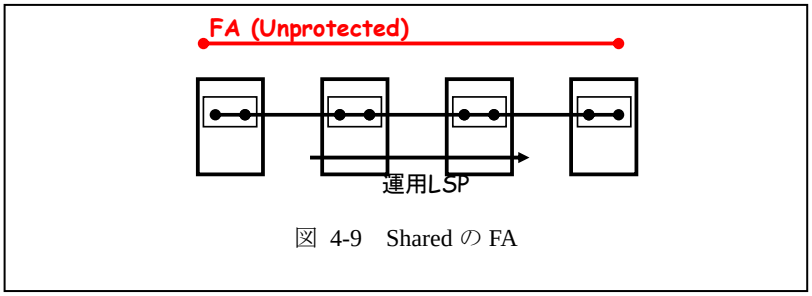


図 4-9　Shared の FA

SRLG
LSP の SRLG は LSP を構成する TE リンクから構成される。
二重化 LSP を FA として広告する場合の SRLG は FA を構成する LSP とは独立に割り当てられる。
一重化 LSP を FA として広告する場合の SRLG は LSP の SRLG を用いる。
図 4-10はノード A とノード D の間に二重化の LSP を設定し、それを FA として広告する場合の例である。0 系の LSP の SRLG は通過する TE リンクの SRLG の和集合の{1,2,3}である。一方 1 系の LSP の SRLG は通過する TE リンクの SRLG の和集合の{4,5,6}である。これらをまとめて FA として広告する際に、FA の SRLG は新たに払い出し、{100}を広告する。

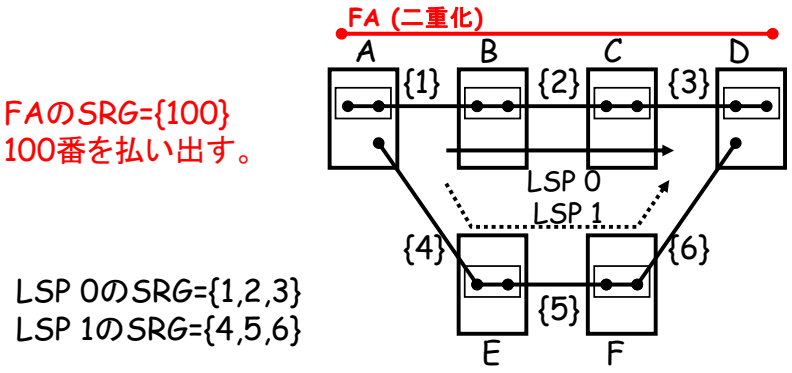


図 4-10 SRLG

[RFC3477] Signalling Unnumbered Links in Resource ReSerVation Protocol -Traffic Engineering (RSVP-TE), 1/03
[RFC3473] Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions, RFC3473, 1/03
[E2E] RSVP-TE Extensions in support of End-to-End GMPLS-based Recovery < draft-ietf-ccamp-gmpls-recovery-e2e-signaling-03.txt>, 5/03

5. 障害通知

5.1. リストレーションにおける障害通知

(1) 障害回復のためのステップ

障害が発生してからどのようにそれを回復させるかについて述べる。図 5-1に障害回復のためのステップを示す。

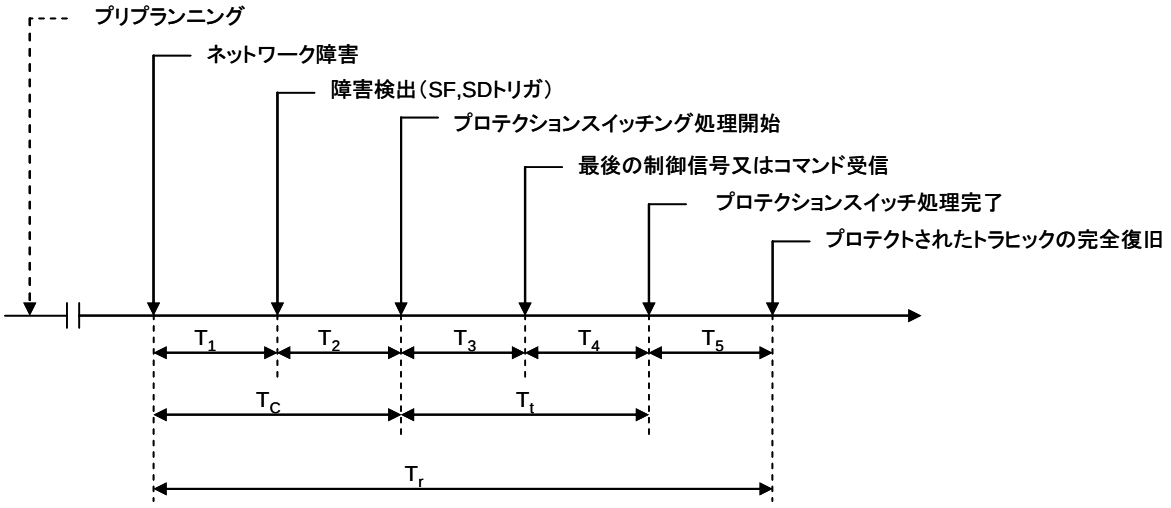


図 5-1

以下に各ステップの詳細を述べる。

【プリプランニング】

管理システムにおいて、予めある障害を想定し予備 LSP 経路を設計する。

【T1：障害検出時間(detection time)】

障害を検出するまでの時間間隔。障害箇所の隣接ノードは、光チャネルの入力断や閾値以上のビット誤りから障害(SD, SF)を検出する。

【T2：ホールドオフ時間(hold-off time)】

障害を検出したノードが障害回復プロセスを開始するまでの待ち時間。データプレーンにおける下位のレイヤが障害回復を行う場合、T2 はその上位のレイヤで障害回復を行うかどうかを判断する起動タイマーとしての役割も持つ。

【T3：障害通知時間(protection switching operation time)】

プロテクションスイッチを実行するために必要となる制御信号の転送及びその処理時間

【T4：プロテクション経路切替時間(protection switching transfer time】

全てのプロテクションスイッチを切り替えるための時間

【T5：復旧時間(recovery time)】

復旧処理された主信号が、障害を起こす前の通信状態になるまでの時間。各ノードで設定されたプロテクションパスの接続性を検証するため、あらかじめ定義されている光チャネルのパストレース用のバイトなどを利用する。

【Tc：障害確認時間(confirmation time)】

ネットワーク障害発生から SF や SD の検出を完了するまでの時間：Tc = T1 + T2

【Tt：転送時間(transfer time)】

プロテクションスイッチ切替開始から完了までの時間：Tt = T3 + T4

【Tr：障害回復時間(protected traffic restoration time)】

障害発生からトラヒックの完全な復旧までの時間。Tr = T1 + T2 + T3 + T4 + T5 = Tc + Tt + T5

ダイナミック型リストレーションの場合、障害を回避するルート計算を行う時間を必要とする。その行う時間は、ダイナミック型リストレーションを行う方式によって異なる。パス端切替の場合はパス端ノードでルーティングを行うため、T3 と T4 の間に当てはまる。一方障害端で普及を行うような場合、障害端でルートを計算するので、その計算時間は T2 と T3 の間に当てはまる。

ITU-T 勧告 G.841 では、エクストラトラヒックが流れていないなどのある条件下における SDH ネットワークにおけるプロテクション切替時間を規定しており、それが 50ms と定められている。フォトニック IP ネットワークにおいも、既存 SONET / SDH ネットワークを置き換えることを想定すると、同等の切替時間を保証する必要があるかもしれない。

すなわち、障害回復のための要求時間を Tr(例えば 50ms)と仮定すると、Tr を保証するには

$$T1 + T2 + T3 + T4 + T5 \leqq Tr$$

を満たさなければならない。

(2) 障害検出方式

GMPLS コントロールプレーンを用いた障害検出方式として、以下に示す２つの方式が考えられる。ハードウェアによる障害検出が基本であるが、制御ノード障害やハードウェアにより障害検出が使えない場合などを考慮すると、GMPLS コントロ

ールプレーン上で障害を検出する手法は必須である。ハードウェアにより障害検出方式に関しては、5.2節を参照のこと。

方式１：RSVP Hello メッセージを用いる方式
RSVP Hello は、隣接ノードへの到達性を検証することが可能である。特に RSVP Hello はノード間の障害検出に有効である。ノードはある間隔毎に隣接ノードへ Hello Request を送信する。もし隣接ノードで Hello が走っていたならば、Hello Ack を返す。もし４回連続して Ack メッセージを受け取らなかった場合は(Cisco 仕様)、もしくは間違ったメッセージを受け取ったならば、ノードは隣接ノードがダウンしたものと判断する。
以下の２つの設定パラメータがある。

- Hello インターバル(ip rsvp signalling hello refresh interval command)(default 200 ミリ秒(Cisco 仕様))
- 隣接ノードがダウンと判定する ack の送信回数(ip rsvp signalling hello refresh misses command)(default 4 回)

方式２：LMP Hello メッセージを用いる方式[LMP]
LMP は LMP Hello を持ち高速に障害を検出できる機能を持っている。一度制御チャネルが確立すると、隣接ノードとの接続性を維持するために Hello プロトコルが使用される。パラメータは、Config Message でやり取りされる。ノードが ConfigAck メッセージを送信/受信すると、Hello メッセージ通信を開始する。Hello メッセージは HelloInterval 毎に送信される。HelloDeadInterval までに Hello メッセージを受信しなかった場合は、制御チャネルがダウンしたと認識する。
障害検出に関し、以下の２つの設定パラメータがある。

- HelloInterval (default 150ms)
- HelloDeadInterval (default 500ms: 少なくとも HelloInterval の 3 倍以上の値を取ること)

(3) 障害箇所の特定
基本的にはハードウェアによる障害箇所の特定(localization)を行うことを基本とする。しかしながら全光ネットワークのような場合、光断による障害警報が光パス上で多重に発生する可能性がある。LMP ではそのような障害箇所を特定するために、ChannelStatus メッセージを用いて行えるようになっている。ChannelStatus メッセージは、単一データチャネル障害、多重データチャネル障害、全 TE リンク障害に使用できる。
データリンク障害を検出した下流ノード(データフローの意味での下流)は、上流隣接に対して(すべての障害データリンクの通知をまとめて)、ChannelStatus メッセージを送信する。ChannelStatus メッセージを受信した上流ノードは、ChannelStatus メッセージを受信したことを示す ChannelStatusAck メッセージを下流ノードに対して送信しなければならない(MUST)。上流ノードは、(ingress 側を含めて)その障害が対応する LSP(s)でも障害が検出されるかどうかを確認するために、障害の関連付けを行うべきである。例えば、上流ノードの入力チャネル上または内部的に障害が検出されなかった場合、上流ノードは障害位置を特定できるだろう。いったん障害位置が特定されると、上流ノードはチャネルが障害か正常化を示す ChannelStatus メッセージを下流ノードに送信すべきである。（SHOULD）もし ChannelStatus メッセージは下流ノードで受信されないならば、問題のチャネルのために ChannelStatusRequest メッセージを送るべきである。（SHOULD）いったん障害が特定されらならば、スパンもしくはパスプロテクション/レストレーション手順を始めるために、シグナリングプロトコルを使うことが出来る。
TE リンクのすべてのデータリンクが障害した場合、上流ノードは障害 TE リンク内のそれぞれのデータリンクの障害を通知すること無しに、TE リンク障害を通知できる(MAY)。これを行う場合は、CHANNEL_STATUS オブジェクト内にインターフェース ID を一つも含めずに TE リンクを指定して、ChannelStatus メッセージを送信することにより通知できる。

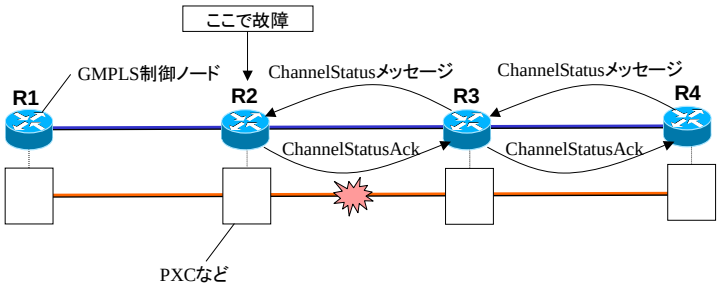


図 5-2 障害箇所の特定(localization)

(4) 障害通知方式
GMPLS コントロールプレーンを用いた障害通知方式として、以下に示す４つの方式が考えられる。ハードウェアによる障害通知も考えられるが、マルチリージョン、マルチドメインや非 OTN ネットワークを考慮すると、GMPLS コントロールプレーン上で障害を通知する手法は必須である。ハードウェアにより障害通知方式に関しては、5.2.3 節を参照のこと。
またデータプレーンが自動化された Protection Switching 能力を提供する場合(例として、ITU-T G.841 Recommendation 参照)、Notification (N) bit が Protection Object に定義される。これは、コントロールプレーンもしくはデータプレーンを介する Protection シグナリングと区別するためである。

方式１：RSVP-TE Path Error メッセージを用いる方式

本方式は、RSVP-TE の Path Error メッセージを障害通知に使用するものである。MPLS Fast Reroute(FRR)では、Path Error を障害通知として使用している。GMPLS においても同様な方式が適用できる(図 5-3参照)。つまり障害発生時に、通常 Resv Tear メッセージが上流下流に流れるが、MPLS FRR ではその替わりに Path Error メッセージを上流に流し、下流のパス端(R4)では refresh メッセージを待つ。上流のパス端(R1)では、Path Error を契機にリカバリ動作を開始する(MPLS FRR では PLR が動作を開始すると共に、パス端 R1 が Path Error を契機に現用 LSP の再最適化を行っても良い仕様となっている)。

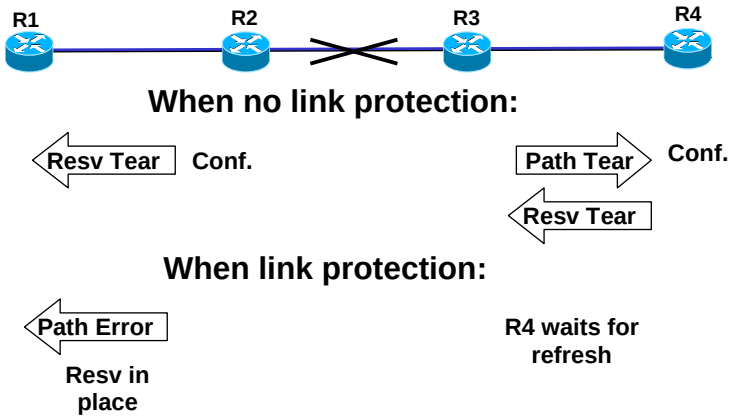


図 5-3 Path Error を使用した障害通知

方式２：RSVP-TE Notify メッセージを用いる方式

GMPLS シグナリングプロトコルでは、Notify Message と呼ぶ機能がサポートされている。Notify Message は隣接でない現用 LSP 上のノードに直接 LSP の状況を通知できる機能である。この Notify Message の拡張により、プロテクションパスを中継するノードに対し、切替指示を行うことができる。中継ノードに通知する必要がなければ、標準の Notify メッセージを使用することができる。本方式の利点として、ラベル情報を管理しているシグナリングプロトコルが障害通知を行うため、実装し易いという点が挙げられる。欠点として、例えばファイバ断など一つの障害で生じる、複数の障害通知（例えば波長毎の）通知が必要になるため高速な障害回復向きではない。

方式３：OSPF flooding を用いる方式(独自方式)

OSPF / IS-IS では flooding を用いて制御情報をネットワーク全体に通知している。このレイヤ３の flooding の仕組みをベースとすることにより、障害情報を通知できるようになる。具体的には OSPF の Opaque LSA を用い、Opaque LSA に障害箇所情報を明記してネットワーク中に Flooding を行う。Opaque LSA で障害を通知されたノードは、その障害に対応した障害回復の動作を取る。

この方式の利点としては、一つの障害から生じる多くの障害情報を、一回の flooding 操作で通知できる点が挙げられる。欠点として現状の OSPF における flooding 処理は重く、例えば SONET/SDH ネットワークで規定されている 50ms のプロテクション時間は満たせない可能性が大きい。

方式４：障害通知専用 flooding 方式(独自方式)

一般に flooding は障害通知メッセージ数を削減させる点で有力な方式である。したがってデータプレーンに近いレイヤで flooding を行うことにより、高速に障害情報を通知することが可能となる。以下にその概要を示す。

①スタートアップ時にノード間の隣接関係を取る
②Hello メッセージなどを用い接続性を確保する
③FaultNotify と FaultNotifyAck という２種類のメッセージを規定する
④FaultNotify メッセージ中には、障害箇所の情報およびシーケンス番号を格納する。

これら機能は、新たな障害通知のためのプロトコルを規定して実現するのが最良であるが、IETF の sub IP エリアで標準化中の LMP(Link Management Protocol)などのプロトコルに実装することも考えられる。本方式は従来の flooding 機能を障害通知に特化させた方式であり、標準化という課題はあるものの、コントロールプレーンを用いて高速に障害を通知する方式としては、現実的な方式と考えられる。

図 5-4に、flooding を用いた障害通知方式の概略を示す。データプレーンで発生した障害は、データプレーン内のノードにて検出され、コントロールプレーンに通知される。コントロールプレーン内のコントローラは、その障害情報を flooding を用いてネットワーク内に通知する。障害通知メッセージを受け取ったコントロールプレーンのコントローラは障害情報に該当していたならば、データプレーンのノードの設定をアクティブにする。特にエッジノードでは現用系から予備系へとパスを切り替える。

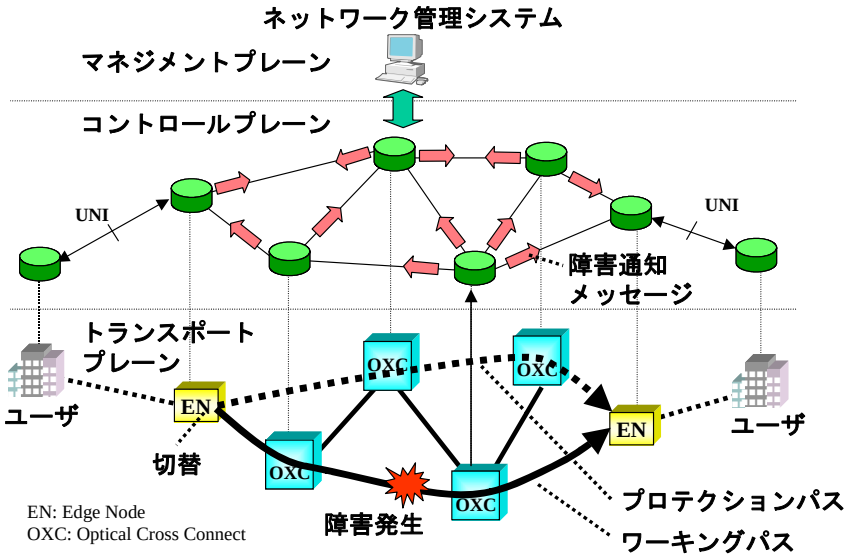


図 5-4　flooding を用いた障害通知方式

以下の表に各通知方式の通知箇所(ingress, egress, 中継)への適用判定を示す。

表 5-1　障害通知のまとめ

	Ingress に障害通知	Egress に障害通知	中継ノードに通知	備考
方式１：Path Error	○	メッセージを規定すれば可能	×	中継ノードの active 化は RSVP を用いる
方式２：Notify	○	○	メッセージ拡張が必要	中継ノードの active 化は RSVP を用いる
方式３：OSPF 拡張	○	○	○	独自方式
方式４：専用 flooding	○	○	○	独自方式

上述したようにコントロールプレーンを用いた障害通知に関しては、様々な方式が考えられるが、本 IA においては、IETF で標準化が進められている GMPLS Notify メッセージを用いた障害通知を用いることを基本とする。以下 Notify メッセージの詳細を示す。

(5) Notify メッセージを用いた障害通知手順

(5-1) 動作手順

e2e recovery において障害通知は、単に障害を通知する場合と、障害通知を行いプロテクションスイッチの切り替えを伴う場合の 2 種類がある。Protection オブジェクトの N ビットが 0 に設定されている場合、プロテクション動作をトリガし、1 に設定されている場合は CP のみの通知となる。

○障害通知のみの場合（1+1 Unidirectional Protection の場合）

1:N Protection with Extra-Traffic、1+1 Unidirectional Protection 又は 1+1 Bi-directional Protection の場合、Protection オブジェクトの N ビットは 1 に設定可能でありそれ以外の場合は、N ビットは 0 に設定しなければならない。

N ビットが 1 である場合は、障害通知によりプロテクションスイッチをトリガしない。

図 5-5 においてノード 1 －ノード 4 間に 1+1 Unidirectional Protection の現用 LSP0、予備 LSP1 を設定し、ノード 2 で障害が発生した場合、Egress 側のノード 4 で LSP0 の障害を検出し、正常なトラヒックを転送している LSP1 側に切り替えられる。Unidirectional の場合は、この様に方向ごとに独立に切替が行われる。

プロテクションスイッチの切り替え後、障害 LSP0 に対し PathErr メッセージを生成する時は、RROR_SPEC オブジェクトの Path_State_Removed フラグを設定しない。（RECOMMEND）

プロテクションスイッチが完了し、PathErr メッセージを受信した場合、LSP1 では O ビットを 1 に設定し Protecting LSP が通常トラヒックを転送している事をしめす。（SHOULD）LSP0 では ADMIN_STATUS オブジェクトの A ビットを設定しても良い。

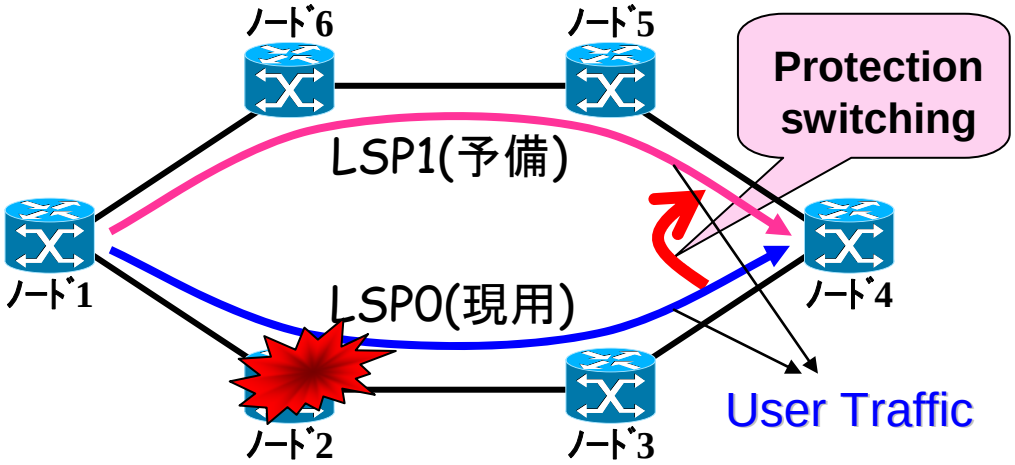


図 5-5　1+1 Unidirectional Protection 図

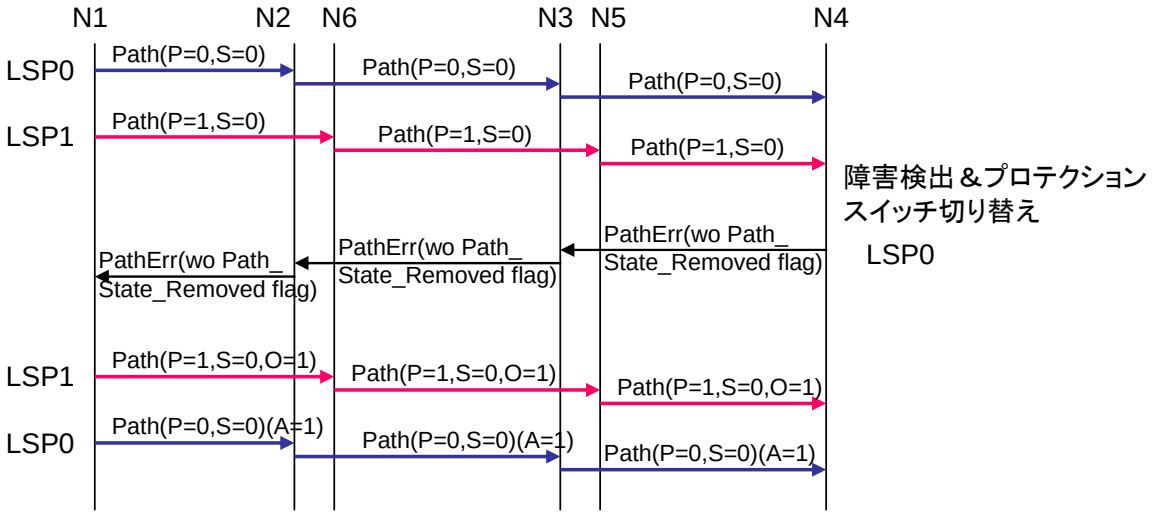


図 5-6 1+1 Unidirectional Protection シーケンス図

○プロテクションスイッチ制御を伴う場合（1+1 Bidirectional Protection の場合）

１. Egress ノードが現用 LSP0 の障害（又は現用 LSP0 の信号性能劣化）を検出又は、<upstream/downstream session list>内に SESSION を含み（IF_ID）_ERROR_SPEC オブジェクト内に新しい error code/sub-code “Notify Error/LSP Locally Failed”を含む Notify メッセージを受信したとき、予備側 LSP の受信を開始（プロテクションスイッチ切替）しなければならない。（MUST）即ち、障害を検出した中間ノードで障害を通知する場合、<upstream/downstream session list>内に SESSION を含み（IF_ID）_ERROR_SPEC オブジェクト内に新しい error code/sub-code “Notify Error/LSP Locally Failed”を含む Notify メッセージを生成しなければならない。

Notify メッセージを受信するノードは同一障害に対し複数の Notify メッセージを受信する場合があることより、障害状態の LSP を認識後 Notify メッセージの競合を解決するため Notify メッセージ内の<sender descriptor>又は<flow descriptor>を用いる事が必要となる。

プロテクションスイッチ切り替えを行ったノードは現用 LSP0 が障害であることを示す新しい error code/sub-code “Notify Error/LSP Failed”(Switchover Request)を持ち、MESSAGE_ID オブジェクトを含む Notify メッセージを他の終点ノードに信頼できる方法で送らなければならない。本 Notify メッセージは受信者にメッセージの確認の送信を要求するために MESSAGE_ID オブジェクト内に ACK_Desired フラグを設定して送らなければならない。

本（Switchover Request）Notify メッセージは IF_ID ERROR_SPEC オブジェクトを使用して障害リンクや関連情報の識別子を送ることが出来る。（MAY）この場合、Notify メッセージの ERROT_SPEC オブジェクトは IF_ID ERROR_SPEC オブジェクトに置き換えられるか、PathErr/ResvErr メッセージで送ることができる。

２．(Switchover request)Notify メッセージを受信した場合、そのエンドノードは予備 LSP から受信を開始しなければならない。（MUST）

本エンドノードは他のエンドノードへ MESSAGE_ID オブジェクトと（Switchover Request）Notify メッセージを受信確認のための MESSAGE_ID_ACK オブジェクトを含む(Switchover response)Notify メッセージを信頼できる方法で送らなければならない。
（Switchover response）Notify メッセージは IF_ID ERROR_SPEC オブジェクトを使用し障害リンクや関連情報の識別子を送っても良い。（MAY）
(Switchover response)Notify メッセージ受信時、エンドノードはその受信を確認するため他のエンドノードへ Ack メッセージを送らなければならない。（MUST）

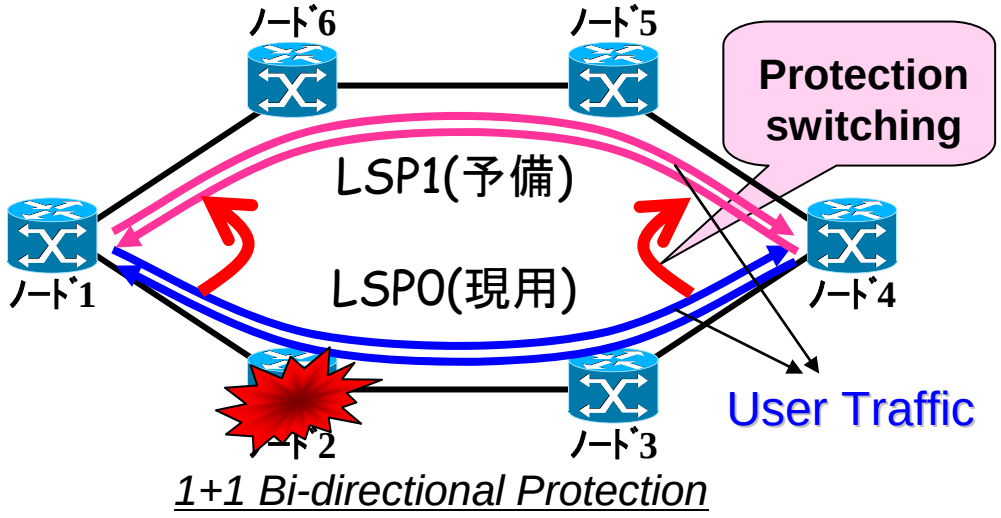


図 5-7　1+1 Bi-directional Protection 図

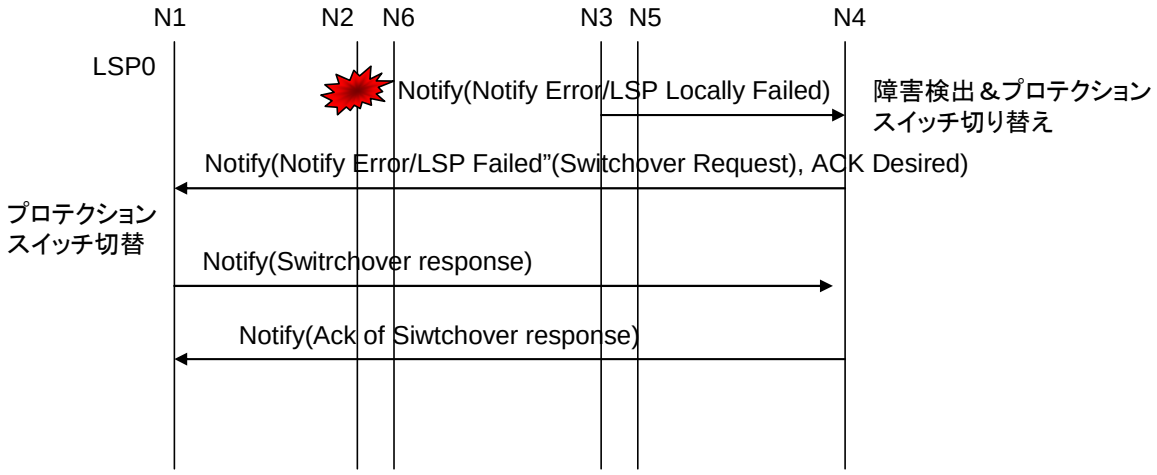


図 5-8　1+1 Bi-directional Protection シーケンス図

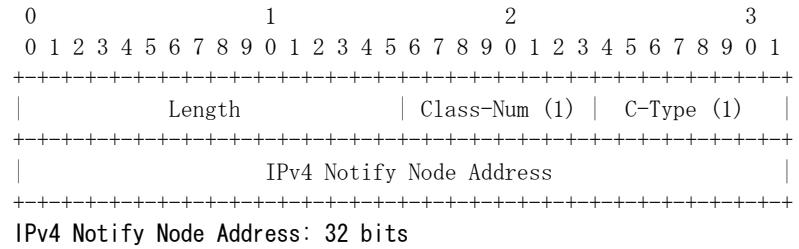
中間ノードが GMPLS RSVP-TE シグナリング能力を持つ場合、障害と隣接する各ノードは LSP の始点や終点のどちらか又は両方に直接 Notify メッセージを生成するかもしれない。（MAY）それゆえ、これらの LSP を終端している（データプレーンから LSP 障害を検出するかもしれない）ノードは上記手順の繰り返しを防ぐため正しく関係付けるためのメカニズムや、同じセッションに対応した複数 Notify メッセージの廃棄メカニズムの提供が期待される。さらに、障害 LSP について PathErr メッセージの生成時に ERROR_SPEC オブジェクトの Path_State_Removed フラグを設定しない。（RECOMMENDED）

プロテクションスイッチが完了し(ステップ 2)、PathErr メッセージを受信後、信号をどちらから受信しているか LSP を見失わないため、予備側 LSP1 は O-bit を設定してシグナリングしなければならない。（SHOULD）前の現用 LSP0 は ADMIN_STATUS オブジェクトの A-bit を設定してシグナリングしてもよい。（MAY）

N ビットが設定されている場合、エンドーエンドでの Switchover request/response はコントロールプレーンのみで使用され、データプレーンへのアクションをトリガしない。

(5-2) 使用されるオブジェクト[RFC3473]
(5-2-1) Notify Request Objects
Notify Request オブジェクトは、Path あるいは Resv メッセージの中で運ばれる。Notify Request クラス番号は 195 である

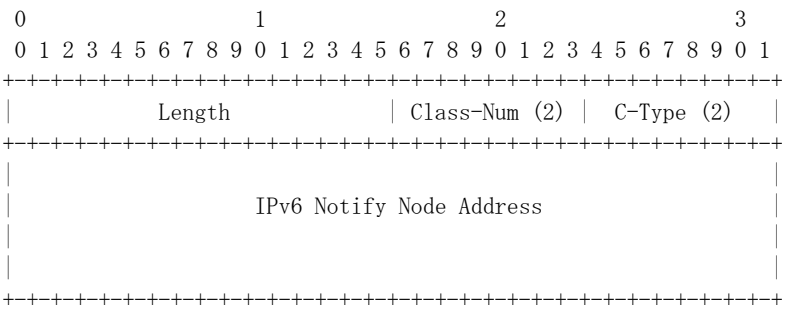
(11bbbbbb の形)。Notify Request のフォーマットは：
IPv4 Notify Request Object



IPv4 Notify Node Address: 32 bits

上記ノードアドレスは、エラーメッセージを生成する時に、通知されるべきノードの IP アドレスを示す。

IPv6 Notify Request Object



IPv6 Notify Node Address: 16 bytes

上記ノードアドレスは、エラーメッセージを生成する時に、通知されるべきノードの IP アドレスを示す。

もしメッセージが複数の Notify Request オブジェクトを含んでいるなら、最初のオブジェクトのみが意味を持つ。残りの Notify Request オブジェクトは無視されるかも知れず(MAY)、伝播されるべきではない(SHOULD NOT)。

Notify_Request オブジェクトは、LSP 障害が通知されるべきノードのアドレスを示すために Path あるいは Resv メッセージの中に挿入されるかもしれない。以前に触れたように、通知は上流方向及び下流方向の両方から要求されるかもしれない。上流方向への通知は、対応する Path メッセージの中に Notify Request オブジェクトを含めることにより示される。下流方向への通知は、対応する Resv メッセージの中に Notify Request オブジェクトを含めることにより示される。

Notify Request オブジェクトを含んでいるメッセージを受信したノードは、対応するステートブロックの中に Notify Node アドレスをストアすべきである。(SHOULD) もしノードが通過ノードなら、それはまた出力される Path あるいは Resv メッセージの中に Notify Request オブジェクトを含めるべきである。(SHOULD) 出力される Notify Node アドレスは、ローカルポリシによりアップデートされるかもしれない。(MAY)

Notify_Request オブジェクトが含まれることは、Notify メッセージが生成されることを保証しないことに注意。

(5-2-2) Notify メッセージ

Notify メッセージは、LSP に関するイベントを隣接ではないノードの通知するためのメカニズムを提供する。Notify メッセージは通常、Notify Request メッセージが受信された後でのみ生成される。Notify メッセージは、直接上流側あるいは下流側に隣接しているノード以外のノードに宛てて通知できること、及び一般的な通知メカニズムであることが既に定義されているエラーメッセージ(つまり、PathErr 及び ResvErr メッセージ)とは異なる。Notify メッセージは既存のエラーメッセージを置き換えない。Notify メッセージは、以下のいずれかの方法で送られる;(a) [RFC2205]の中の ResvConf 処理と同じように、non-target ノードは target ノードに対する Notify メッセージを単にフォワードするだけで通常に送られる; (b) target IP アドレスと同じ destination アドレスを持つ新しい IP ヘッダでカプセル化されて送られる。トランスミッションメカニズムによらず、自分があて先ではない Notify メッセージを受信したノードは、target に向けてメッセージを変更しないでフォワードする。

Notify メッセージの信頼性のある配達をサポートするために、Notify メッセージの受信を確認するための Ack メッセージ[RFC2961]が利用される。信頼性のある RSVP メッセージ配達に関する詳細は、[RFC2961]を参照。

必要な情報

Notify メッセージは、一般的な通知メッセージである。IP destination アドレスは、意図された受信ノードの IP アドレスにセットされる。Notify メッセージはルータアラートオプション無しで送られる。一つの Notify メッセージは、上流と下流の両方のそれぞれのリストされたセッションとともに送られる通知を含んでいるかもしれない。

Notify メッセージは、メッセージタイプ 21 である。Notify メッセージのフォーマットは以下のとおりである:

```
<Notify message>::= <Common Header> [<INTEGRITY>]
                    [ [<MESSAGE_ID_ACK> | <MESSAGE_ID_NACK>] ... ]
                    [ <MESSAGE_ID> ]
                    <ERROR_SPEC> <notify session list>

<notify session list>::= [ <notify session list> ]
                          <upstream notify session> |
                          <downstream notify session>

<upstream notify session>::= <SESSION> [ <ADMIN_STATUS> ]
                             [<POLICY_DATA>...]
                             <sender descriptor>

<downstream notify session> ::= <SESSION> [<POLICY_DATA>...]
                                <flow descriptor list>
```

ERROR_SPEC オブジェクトはエラーを示しており、エラーを検出したノードあるいは障害となったリンクいずれかの IP アドレスを含んでいる。ERROR_SPEC の定義は[RFC2205]を参照。MESSAGE_ID 及び関連するオブジェクトは、[RFC2961]の中で定義されており、リフレッシュリダクションがサポートされているときに利用される。

- 手順

Notify メッセージは、最も一般的には PathErr あるいは ResvErr メッセージの生成をトリガするエラーを検出したノードで生成される。もし PathErr メッセージが生成され対応する Path メッセージの中で Notification Request オブジェクトが受信されていたら、記録されていたノードに宛てた Notify メッセージが生成されるべきである(SHOULD)。もし ResvErr メッセージが生成されて対応する Resv メッセージの中で Notification Request オブジェクトが受信されていたら、記録されていたノードに宛てた Notify メッセージが生成されるべきである(SHOULD)。前に触れたように、一つのエラーが上流と下流方向の両方に向けた Notify メッセージを生成するかもしれない。Notify メッセージは適切な Notify Request オブジェクトが受信されていない時には生成されてはならない(MUST NOT)。

Notify メッセージを生成する時、ノードは同じ Notify ノードに対して送られる通知を結合しようと試み、一つの Notify メッセージの中に同じ ERROR_SPEC を共有しようと試みる。どの情報が結合されることができるかをノードが判断する手段は、インプリメンテーション依存である。インプリメンテーションはイベント、タイマベースのもの、あるいはその他のアプローチを用いるかもしれない。もしタイマベースのアプローチをとるなら、インプリメンテーションはどれだけの間の通知が結合されるのかをユーザが設定することを可能にすべきである(SHOULD)。タイマベースのアプローチをとるとき、デフォルトの "notification interval" 1ms が利用されるべきである(SHOULD)。Notify メッセージは、[RFC2961]の中で定義された信頼性のあるメッセージ配達メカニズムを利用して配達されるべきである(SHOULD)。Notify メッセージを受信した場合、Notify ノードは対応する Ack メッセージを送るべきである。（SHOULD）

5.2. プロテクションにおける障害通知

障害通知に関し、データプレーンが自動化された Protection Switching 能力を提供する場合(例として、ITU-T G.841 Recommendation 参照)、Notification (N) bit が Protection Object に定義される。これは、コントロールプレーンもしくはデータプレーンを介する Protection シグナリングと区別するためである。

この節では主にデータプレーンでの障害通知に関して述べる。プロテクションに関してもコントロールプレーンでの障害通知が使用できるが、コントロールプレーンでの障害通知に関しては、5.1節を参照のこと。

光レイヤ(OTN)における障害通知方式[G.709]

図 5-5に OTN のレイヤ構造を示す。

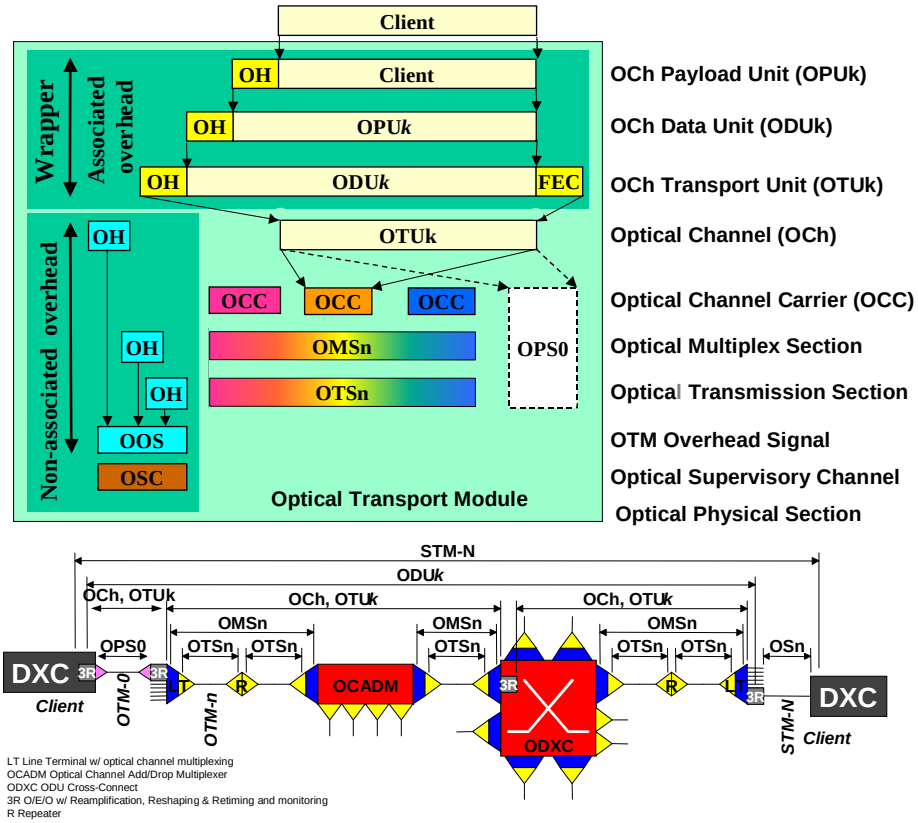


図 5-5 OTN のレイヤ構造

図 5-6に OTN メンテナンス信号を示す。基本的には下位レイヤから上位レイヤへとメンテナンス信号が伝搬されていく。OTN では主信号の方向と同じ方向に障害を通知することを FDI(Forward Defect Indication) / AIS(Alarm Indication Signal)と言う。図を見ると分かるように OMS-OCh への警報情報を FDI、それ以上のレイヤを AIS と呼ぶ。さらに FDI には FDI-P と FDI-O に分かれる。OMSn-FDI-P は、Payload の状態を用いて障害を通知する方式で、OMSn-FDI-O は OMS の Overhead を用いて障害を通知する方式である。PMI(Payload Missing Indication)は、OMS の上流でのソースにおいて、OCCp(OCC with full functionality Payload)に信号が全く含まれていないことを示すために下流に送られる信号である。つまり下流のノードはこの PMI 信号を見ることによって上流の障害を知ることができる。AIS はいわば電気処理を行うレイヤでの障害通知であり、OTUk 以上のレイヤでの障害通知機能である。ODUk から上位へは各レイヤ(SONET/SDH, ATM, MPLS など)へメンテナンス信号がインターワーキングされていく。

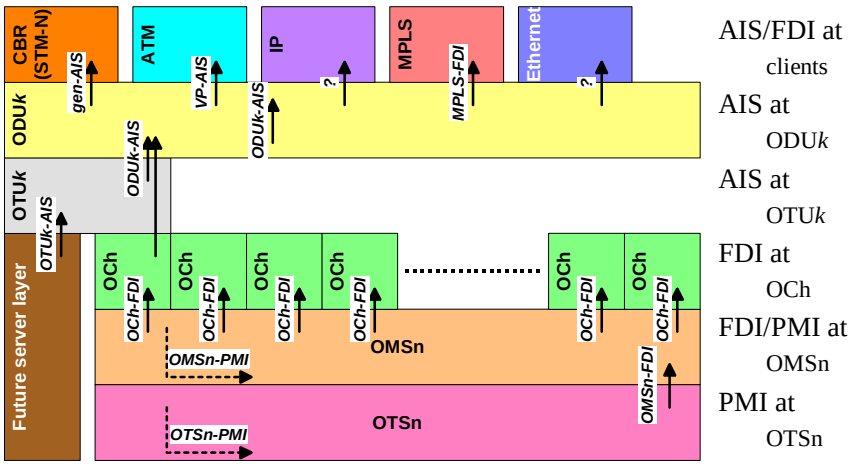


図 5-6 OTN メンテナンス信号(前方通知)

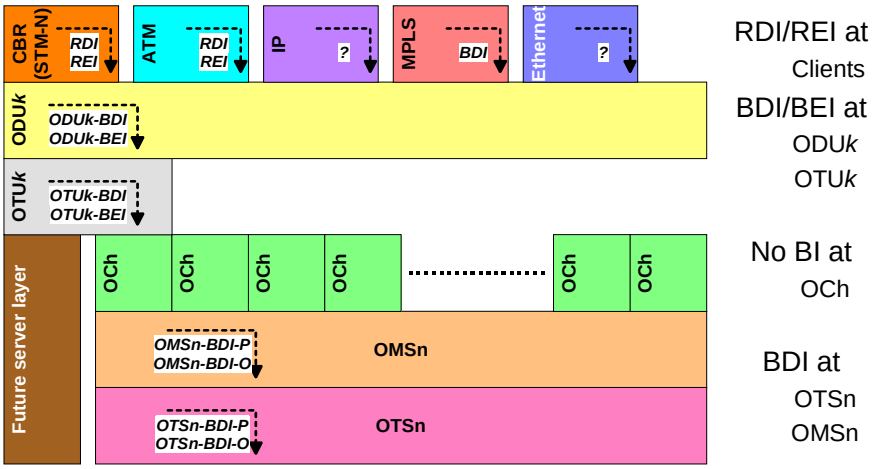


図 5-7　OTN メンテナンス信号(後方通知)

光レイヤでこのメンテナンス信号を用いてリカバリを行う場合は、Och レイヤの信号をトリガーにリカバリ動作を行う。光レイヤ(ODUk 以下)に限定すると、障害発生時の前方通知時に OCh レイヤでの前方通知又は ODUk レイヤの終端点で ODUk－AIS として障害通知が行われ、遠端の ODKk 終端点で ingress ノードへの後方通知がなされる。これは ODUk が光信号を終端しているエンドーエンドで流すことができるためである。

(2) ハードウェアによる障害検出・障害通知のまとめ

SONET/SDH に関しては ITU-T 勧告 G.783 を参照のこと。MPLS に関しては ITU-T 勧告 Y.1711/Y.1720 を参照のこと。以上述べた方式を以下の表にまとめる。

表 5-2　ハードウェアによる障害検出・通知方式

オーバヘッドレイヤ	障害検出	障害通知	備考
OTS Layer OMS Layer OCh Layer		前節参照	G.709
SONET RS Section	セクションオーバヘッドの A1,A2(フレーム同期)、B1(誤り監視)で検出可能		
SONET MS Section	セクションオーバヘッドの B2(誤り監視)、LOS(Loss of Signal)で検出可能	セクションオーバヘッドの K1, K2 バイトで通知。信号障害･信号劣化の事象に対して優先順位が付けられている。	G.783
SONET Path layer	パスオーバヘッドの J1(導通監視), B3(誤り監視)で検出可能	パスオーバヘッドの K3,K4 で切替制御、G1 で対局警報が行える	
MPLS	MPLS OAM パケットを使用可能。Connectivity Verification で通信正常性をチェック可能。	MPLS OAM パケットを使用可能。FDI, BDI を指定可能。	Y.1711 / Y.1720
Ethernet	MEF や ITU-T において、Mac レベル OAM の検討が開始	MEF や ITU-T において、Mac レベル OAM の検討が開始	

(3) LMP-WDM[RFC4209]を用いた OLS(Optical Line System)との障害通知

LMP-WDM では従来の LMP を拡張し、ノードーOLS 間で LMP を走らせることにより、LMP の機能を使用できるようにしたものである(図 5-8参照)。OLS とは、WDM のような光伝送装置や、SONET/SDH や Ether ポートを持つ機器、のことを指す。主な機能としては、LMP と同様に、Control channel management, Link property correlation, Link verification, Fault management の４つの機能がある。

LMP-WDM では、LinkSummary の機能として、ビットエラー率の評価、OLS で既にプロテクションがサポートされているかどうか、トータルスパン長などをノードと OLS の間でやり取りが可能である。また Fault management の機能として、障害検出、位置特定、障害通知も LMP と同様に行えるようになっている。また ChannelStatus メッセージを使用し、障害をスパン上の装置に通知することが可能である。

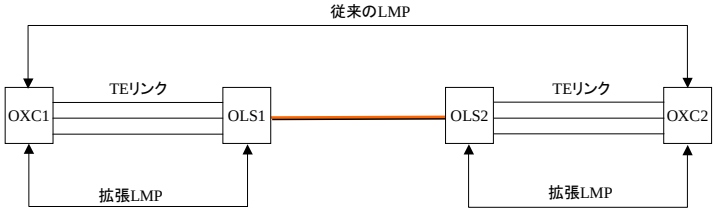


図 5-8　拡張 LMP モデル

参考文献

[G.808.1] ITU-T Draft Recommendation G.808.1, “GENERIC PROTECTION SWITCHING - LINEAR TRAIL AND SUBNETWORK PROTECTION”
[RFC4204] RFC4204, “Link Management Protocol (LMP)”,　October 2005.
[RFC3473] RFC3473, “Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions”, January 2003.
[G.709] ITU-T Recommendation G.709
[RFC4209] RFC4209, “Link Management Protocol (LMP) for Dense Wavelength Division Multiplexing (DWDM) Optical Line Systems”, , October 2005.

6. ルーティングとシグナリングの連携動作

6.1. 機能概要

LSP の二重化は Ingress と Egress のノード間に 2 本の LSP を設定することにより実現する。このとき、2 本の LSP を 0 系と 1 系と呼ぶこととする。
0 系および 1 系の LSP のそれぞれの経路は Ingress ノードにおいて計算する。経路はトラヒックエンジニアリングデータベース（TED）を用いて計算する。TED はルーティングプロトコル OSPF により広告される FA から構成される。
Ingress ノードにおいて計算された 0 系と 1 系の LSP の経路は、Ingress ノードがシグナリングプロトコル RSVP を用いて 0 系と 1 系の LSP を設定する際に、Path メッセージの ERO に搭載される。0 系と 1 系の LSP が実際に設定された経路は RRO を用いて収集される。
LSP を設定する際に LSP が通過する途中ノードでは必要なリソースの予約を行う。途中ノード間の TE リンクのリソース状態が変化すると、TE リンクは FA として OSPF を用いて再広告される。このとき広告される FA には、その時点での TE リンクの属性が搭載される。
設定された LSP そのものを FA として OSPF により広告することが可能である。設定された LSP を FA として広告することで複数階層の LSP のルーティングが可能となる。
経路の計算
0 系および 1 系の LSP のそれぞれの経路は Ingress ノードにおいて計算する。経路はトラヒックエンジニアリングデータベース（TED）を用いて計算する。TED は GMPLS 拡張された OSPF-TE[GMPLS-OSPF]により広告される FA から構成される。0 系および 1 系の LSP のそれぞれの経路は互いに SRLG-Disjoint になるように計算することも可能であり、また Shared mesh リストレーションの場合には、予備帯域の共有と復旧性能を考慮して計算することも可能である。予備帯域がどの LSP のバックアップに割り当てられるかを通知するため PRIMARY PATH ROUTE オブジェクトを用いる[E2E]。このオブジェクトは現用の LSP が通過する経路情報を運ぶために用いられる。

6.2. シグナリング

Ingress ノードにおいて計算された 0 系と 1 系の LSP の経路は、Ingress ノードが GMPLS 拡張された RSVP-TE[RFC3473]シグナリング手順を用いて 0 系と 1 系の LSP を設定する際に、Path メッセージの ERO に搭載される[RFC3209]。ERO に搭載された経路情報に従って 0 系と 1 系の LSP が設定される。0 系と 1 系の LSP が実際に設定された経路は RRO を用いて収集される。
Ingress ノードが Path メッセージの RRO に自分の IP アドレスを搭載し送信する。途中ノードが RRO が搭載された Path メッセージを受信すると自分の IP アドレスを順次 RRO スタックの上に搭載しながら次のホップへ送信する。このように RRO が搭載された PATH メッセージは Egress ノードまで届けられる。Egress ノードが RRO が搭載された Path メッセージを受信すると RESV メッセージに RRO を搭載して Path メッセージとは反対方向に送信する。このとき Egress ノードは RESV メッセージの RRO に自分の IP アドレスを搭載し送信する。

6.3. リソースの管理

LSP を設定する際に LSP が通過する途中ノードでは必要なリソースの予約を行う。途中ノードと隣接ノード間の TE リンクのリソースを予約する。このため TE リンクのリソースの状態が変化する。TE リンクのリソース状態が変化すると、TE リンクは FA として再度広告される。このとき広告される FA には、その時点での TE リンクの属性が搭載される。TE リンクのリソース状態が変化するたびに FA を広告すると OSPF のパケット量が多くなるため、FA を広告する頻度は制御可能であるべきである。また、リソース状態の変化率を元に FA の広告を行うべきである。

6.4. FA としての広告

設定された LSP そのものを FA として広告することが可能である。FA は GMPLS 拡張された OSPF-TE[GMPLS-OSPF]により広告される。

[GMPLS-OSPF] OSPF Extensions in Support of Generalized MPLS <draft-ietf-ccamp-ospf-gmpls-extensions-09.txt>, 12/02
[RFC3473] Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions, RFC3473, 1/03
[RFC3209] RSVP-TE: Extensions to RSVP for LSP Tunnels, RFC3209, 12/01
[E2E] RSVP-TE Extensions in support of End-to-End GMPLS-based Recovery < draft-ietf-ccamp-gmpls-recovery-e2e-signaling-03.txt>, 5/03

7. Extra トラヒック LSP

本 IA では、[E2E]で定義された shared mesh restoration の方式を拡張して、shared mesh restoration に適用する extra traffic のための LSP 設定を提案する。この LSP を extra LSP と呼ぶこととする。また、1:1 protection に適用する extra traffic についても定義と用法を整理する。

7.1. extra traffic の定義

それぞれの Protection type における extra traffic と LSP、リソース管理の関係を定義する。

7.1.1. shared mesh restoration

[E2E]で定義された shared mesh restoration においては、extra traffic はサポートしておらず、予備 LSP に割り当てられた帯域は、障害が無い状態では、いずれのトラフィックも転送していない未使用の状態にある。本 IA では、ネットワークのリソースをより有効利用するため、shared mesh restoration に適用する extra traffic のための LSP 設定を提案する．このためのシグナリング仕様が，[E2E]に一部反映された．

本方式での extra traffic は、1:1 protection のように、特定の予備 LSP と同一のルートである必要はない。複数の、任意の予備 LSP に割り当てられた帯域を使って extra traffic を運ぶ LSP（本 IA では、extra LSP と定義する)の設定を必要とする。図 7-1は、extra LSP の例である。①、②は、あるトラフィックを保護するための 1 対の現用 LSP と予備 LSP である。③および④は、extra LSP であり、それぞれ異なる extra traffic を転送している。③の extra LSP は、ノード E-F 間のリンクにおいて、予備 LSP②に割り当てられた帯域を使用している。④の extra LSP は、ノード F-G 間のリンクにおいて、予備 LSP②に割り当てられた帯域を使用している。

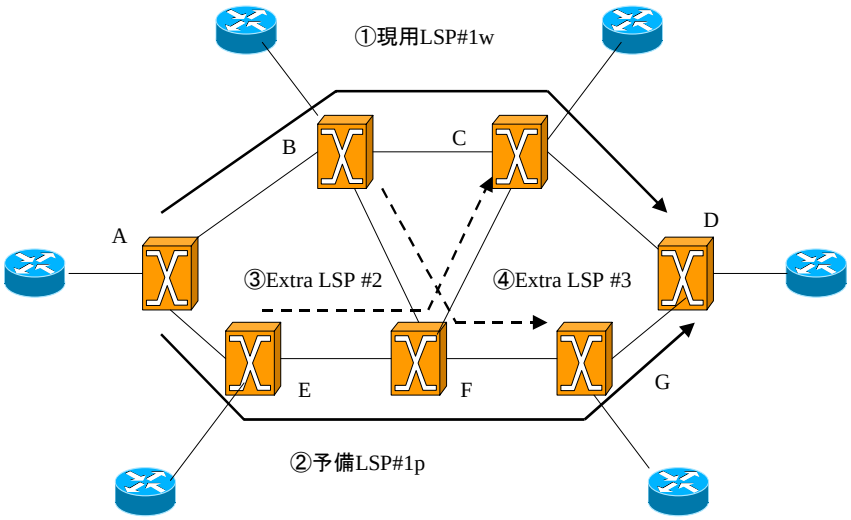


図 7-1　shared mesh restoration における extra LSP

図 7-2は、図 7-1における①(現用 LSP#1w)、②(予備 LSP#1p)、③(Extra LSP #2)の cross-connect 設定内容を示している。

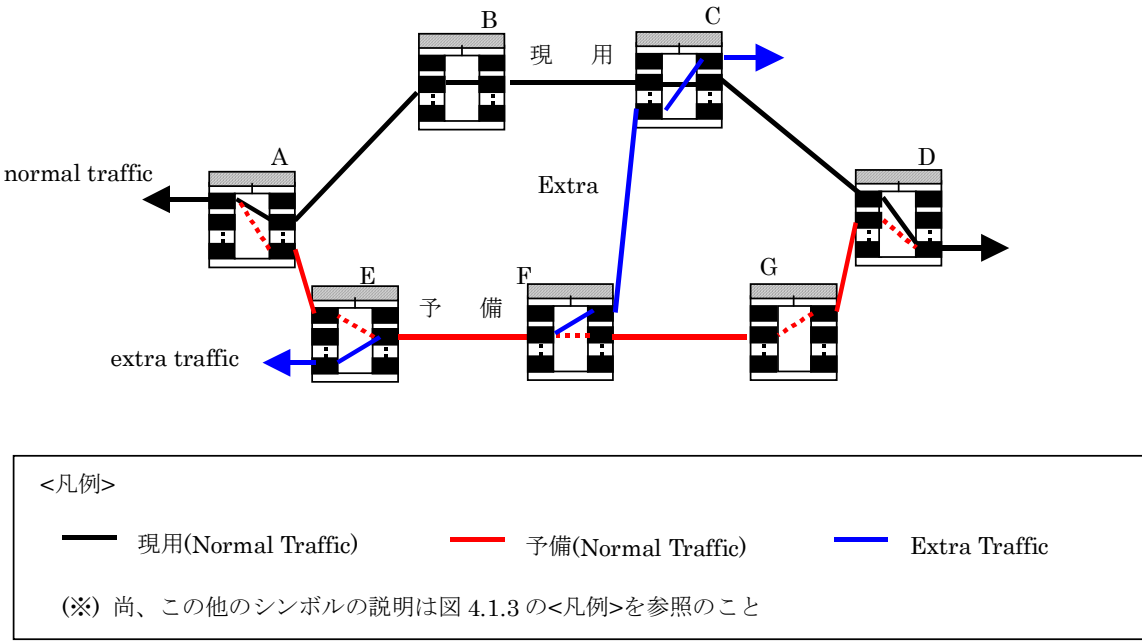


図 7-2　shared mesh restoration における extra LSP の cross-connect 設定

extra LSP は、任意の予備 LSP に割り当てられた帯域または未使用の帯域を使用する。すなわち、未使用の帯域(unreserved bandwidth)は、extra LSP に割り当て可能であり、予備に割り当てられた帯域(protecting bandwidth)は、extra LSP に割り当て可能である。

extra LSP は，[E2E]に基づき，予備 LSP より priority の低い LSP として実現することが可能である．protecting bandwidth の扱いも[E2E]に従う．すなわち，予備 LSP の(holding) priority より低い holding priority の LSP に対しては，protecting bandwidth が割当て可能である．

なお、、1:1 protection の予備 LSP に割当てられた帯域を使うことはできない。

7.1.2. 1:1 protection with extra traffic

extra traffic は、特定の予備 LSP と同じルート、リソース(帯域等)を使用して転送される。

extra traffic のためのシグナリング、ルーティングは行わない。

図 xxx は、extra traffic、現用 LSP、予備 LSP の cross-connect 状態を示す。extra traffic の入口ポート、出口ポートは、プロテクションで保護される normal traffic の入口、出口ポートとは異なる。extra traffic のためのシグナリングは行わないため、ingress ノードは、egress ノードに extra traffic の出口のポートを指定することができなくなり、extra traffic の用途が限られる。このため、予備 LSP を protection type = extra traffic とした FA-LSP として広告する利用方法が考えられる。

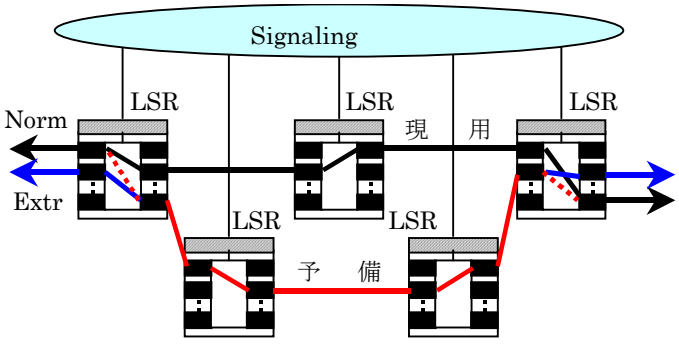


図 7-3　1:1 protection における extra traffic の cross-connect 設定

7.2.　シグナリング

7.2.1. shared mesh restoration

extra traffic を運ぶ LSP を設定する。SESSION、SENDER_TEMPLATE の値は、いずれの現用、予備 LSP とも無関係の値であ

り、設定される LSP は、独立した LSP である。

[E2E]に基づき extra LSP は，予備 LSP より priority の低い LSP として設定する。すなわち，extra LSP の holding priority を，予備 LSP の holding priority より低い priority(値としては大きい)でシグナリングする．なお，setup priority は，予備 LSP の holding priority 以下でなければならない（そうでなければ，予備 LSP が切断されてしまう）．

この時，シグナリングの各処理ノードでは，予備 LSP に割当てた protecting bandwidth を extra LSP に割当てることが出来る．

7.2.2. 1:1 protection with extra traffic

シグナリングは行わない。予備 LSP を設定した時点で、LSP の両端のノードは、予備 LSP 上に extra traffic を転送/受信することができる。

7.3. ルーティング

7.3.1. shared mesh restoration

[E2E]に基づき，予備 LSP に割当てた protecting bandwidth は，priority の低い帯域として extra LSP に割当て可能であり，広告可能である．すなわち，予備 LSP の holding priority より低い（値としては大きい）priority の帯域は，予備 LSP が確立しても減じない．予備 LSP 確立時は，その holding priority と同じ priority の帯域のみが減じられ，(それ以外の priority は変更なしのまま)Unreserved bandwidth, Max LSP bandwidth が広告される

7.3.2. 1:1 protection with extra traffic

extra traffic に使用可能な帯域の広告は行わない。

予備 LSP を TE link として広告する(FA-LSP とする)際は、protection type は"extra traffic"となる。

7.4. 切替

切替発生時、誤接続を防ぐ(現用トラフィックが extra トラフィックの LSP に流れ込まないようにする、またはその逆)ため、cross-connect 状態を適切なタイミングで変更する必要がある。

7.4.1. shared mesh restoration

予備 LSP の activation 時，誤って，各ノードで extra LSP のトラフィックを予備 LSP に流したり，その逆が発生しないように cross-connect 状態を適切に解除，設定する必要がある．例えば，予備 LSP の ingress ノードで，activation の Path 送信時に，cross-connect 設定（受信トラフィックの選択）をすると，extra LSP のトラフィックが ingress ノードに流れ込んでしまう。このための規定が，[E2E]の“8.3 Signaling Secondary LSPs”，“10. LSP Preemption”に示されている．

例えば，Path メッセージの転送時に，extra LSP の cross-connect 状態を解除し，Resv の転送時に予備 LSP の cross-connect 状態を設定すれば，誤接続を防止することが出来る．このために，Resv が activation であることを refresh の場合と区別するために PROTECTION object を含める．

また、切替により extra traffic を運ぶ LSP の D-plane は切断されるため、予備 LSP 上で extra LSP を提供している各ノードは，Path State Removed flag 付きの PathErr と，PathTear を extra LSP に関して送信し，C-plane の状態も解放する。PathErr の Error Code は"Policy Control failure/Hard Pre-empted"とする。更に，extra LSP の切断時の警報通知を抑止するため，cross-connect の解除前に，ADMIN_STATUS を使うことが出来る．

Extra traffic を運ぶ LSP は切断されるため､切り戻しが発生しても extra traffic を運ぶサービスは復元されない｡再度､extra traffic のための LSP を設定する必要がある。

7.4.2. 1:1 protection with extra traffic

[E2E] に書かれている手順で切替を実施する。

7.5. 切り戻し

7.5.1. shared mesh restoration

切り戻し時、Extra LSP の復元は行わない。

7.5.2. 1:1 protection with extra traffic

[E2E] に書かれている手順で切替を実施する。

8. 外部コマンド

障害回復に関する外部コマンドとして、以下の 3 コマンドを実装すること。

- ロックアウト(Lock Out)

自動切替、主導切替のどちらの切替動作を禁止。

- 強制切替(Forced Switch)

ロックアウト状態でなく、切替先の状態に関わらず運用系を非運用系に切り替えること。

- マニュアル切替(Manual Switch)

ロックアウト状態でなく、切替先が正常である場合、もしくは切替可能である場合に運用系を非運用系に切り替えること。

プロテクションと切り戻しを行う場合のリストレーションにおける状態遷移を図 8-1に示す。ロックアウト状態では自動切替、コマンド切替による状態遷移を禁止する。ロックアウト状態はロックアウト解除コマンドによってのみ解除可能とする。

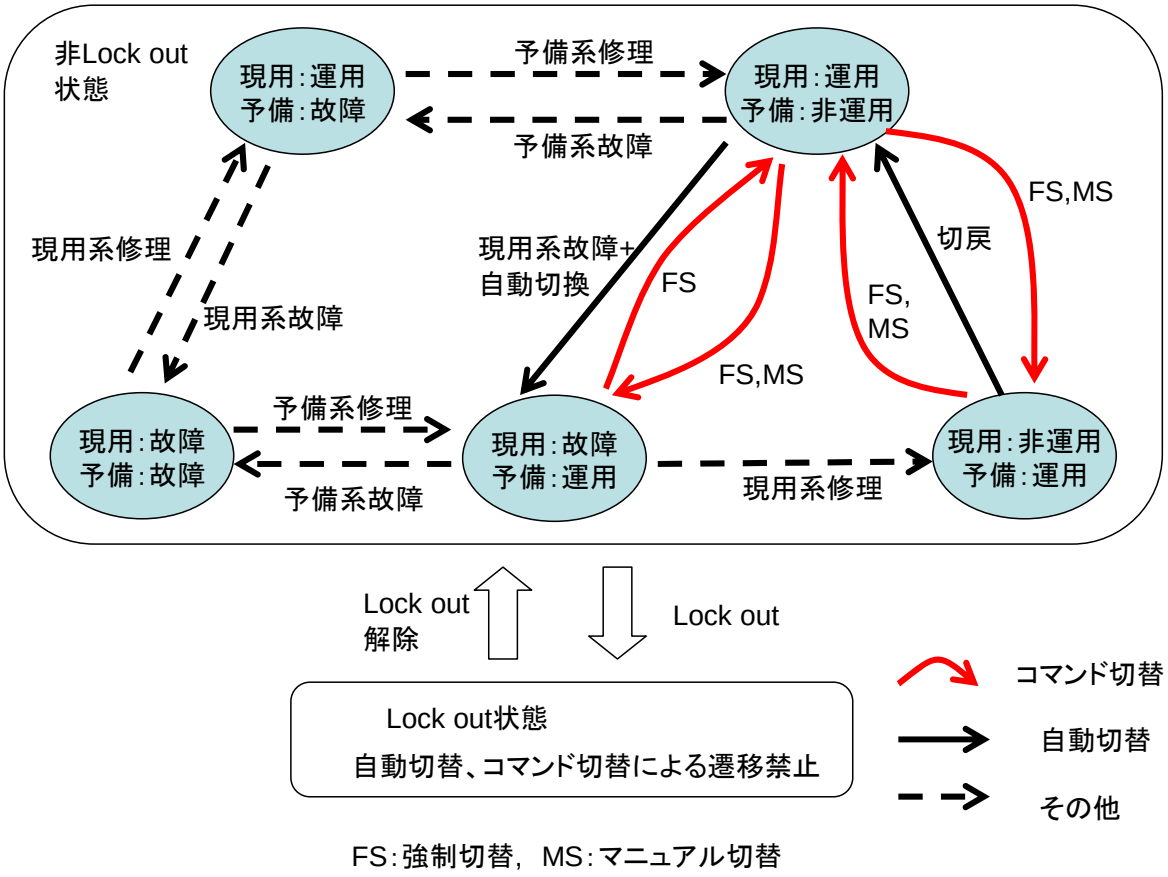


図 8-1 プロテクションと切り戻しのあるリストレーションの状態遷移

図 8-2に切り戻しの無い場合のリストレーションの状態遷移を示す。切り戻しのないリストレーションでは、障害回復動作後、予備系を現用系として運用するため、名称変更動作が必要である。また、元の現用系のリソースは解放される必要がある。新しい予備系は新しい現用系に対して再設定される。

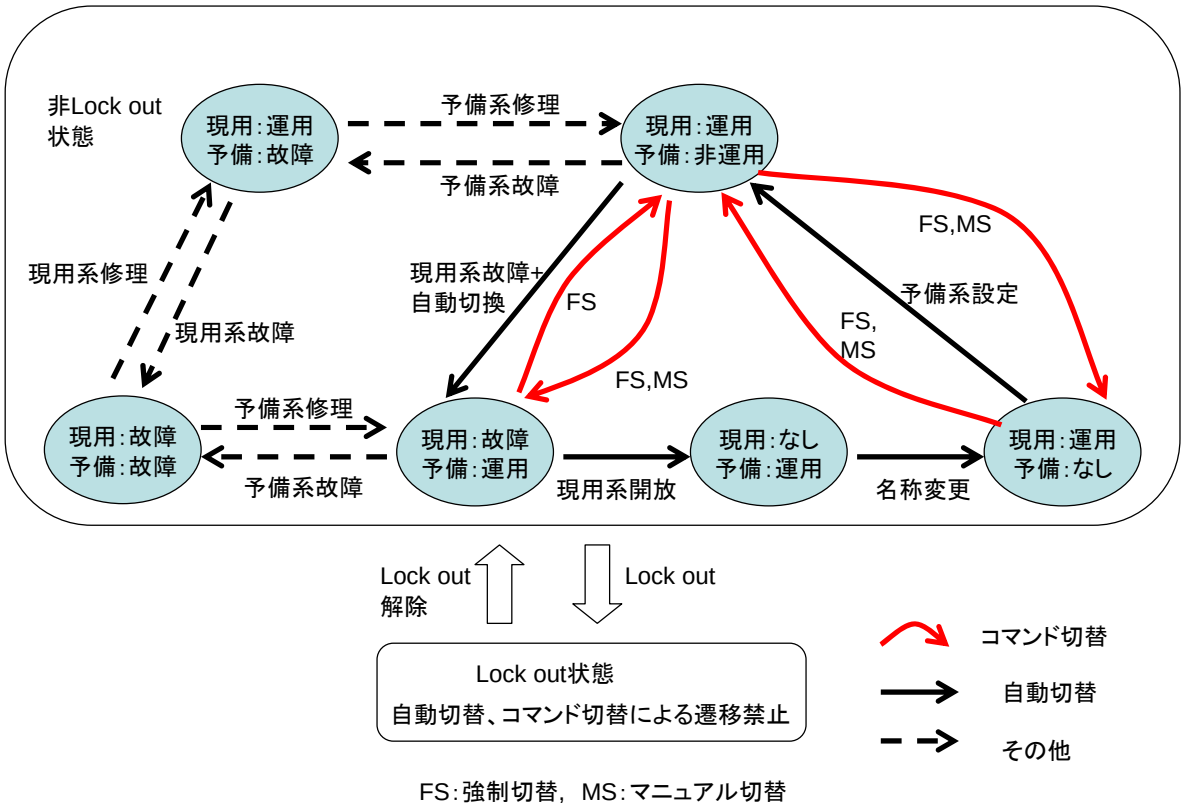


図 8-2　切り戻しのないリストレーションの状態遷移例

9. 参考文献

- RSVP-TE Extensions in support of End-to-End GMPLS-based Recovery <draft-ietf-ccamp-gmpls-recovery-e2e-signaling-03.txt >
- Generalized MPLS Recovery Functional Specification < draft-ietf-ccamp-gmpls-recovery-functional-04.txt >
- Recovery (Protection and Restoration) Terminology for GMPLS <draft-ietf-ccamp-gmpls-recovery-terminology-06.txt>
- Analysis of Generalized MPLS-based Recovery Mechanisms (including Protection and Restoration) < draft-ietf-ccamp-gmpls-recovery-analysis-05.txt >
- Optical Network Failure Recovery Requirements <draft-czezowski-optical-recovery-reqs-01.txt>
- Fault Notification Protocol for GMPLS-Based Recovery <draft-rabbat-fault-notification-protocol-02.txt>
- RSVP extensions for GMPLS restoration signaling <draft-shimano-imajuku-gmpls-restoration-00.txt>
- Extensions to LMP for Flooding-based Fault Notification <draft-soumiya-lmp-fault-notification-ext-00.txt>
- Extensions to RSVP-TE for Supporting Multiple Protection and Restoration Types <draft-suemura-gmpls-restoration-signaling-00.txt>s
- Protection of Hierarchical LSPs <draft-suemura-protection-hierarchy-00.txt>
- Extensions to OSPF-TE for supporting shared mesh restoration <draft-yagyu-gmpls-shared-restoration-routing-00.txt>

10. 本ドキュメントについて

10.1. 著者

日本電気　末村　剛彦
日本電気　西岡　到
富士通研究所　宗宮　利夫
富士通研究所　加納　慎也
富士通研究所　宮崎　啓二
古河電気工業　武藤　大
三菱電機　妹尾　尚一郎
三菱電機　堀内　栄一
日立コミュニケーションテクノロジー　野木　啓生
日立製作所　片岡　健二
日本電信電話　塩本　公平
日本電信電話　島野　勝弘
日本電信電話　今宿　亙

10.2. 改版履歴

2003 年 6 月 4 日　0.7 版　(各社の原稿を集約)
2003 年 6 月 13 日　0.9 版　(6 月 10 日、PIL 標準化 WG での意見交換の結果を反映)
2003 年 6 月 18 日　0.92 版　(6 月 19 日の打ち合わせに向け改版)
2003 年 7 月 1 日　0.95 版　(佐久会合の内容を反映)
2003 年 9 月 16 日　1.0 版
2005 年 11 月 30 日　2.0 版　（最新の Internet Draft に合わせて改版）