

TR-G8031

イーサネットリニアプロテクション スイッチに関する技術レポート

Technical Report on
Ethernet Linear Protection Switching

第 1 版

2009 年 4 月 23 日制定

社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

本書は、（社）情報通信技術委員会が著作権を保有しています。
内容の一部又は全部を（社）情報通信技術委員会の許諾を得ることなく複製、転載、
改変、転用及びネットワーク上での送信、配布を行うことを禁止します。

目 次

1. はじめに.....	4
2. 調査報告の概要.....	4
3. 国内の状況.....	4
4. 今後の国内標準化.....	4
5. おわりに.....	4
付録（ITU-T G.8031/Y.1342の和訳にAmendment 1 およびCorrigendum 1を反映）.....	5
Appendix I 1-フェーズ APSプロトコルの動作例.....	42
Appendix II イーサネットプロテクションスイッチとSTP間の相互作用.....	46
Appendix III プロテクションスイッチ環境のためのMIPs.....	48

1. はじめに

ITU-Tにおいても、イーサネットに関する研究・審議がさかんに行われている。また、近年、イーサネットインタフェースを用いた事業者間接続の要求が高まって来ている背景により、イーサネットレイヤネットワークに関する国内標準の整備が必要となつて来ている。TTCでは、以上の動向を踏まえ、イーサネットリニアプロテクションスイッチに関連するITU-T勧告であるG.8031/Y.1342 の調査を実施した。ただし、イーサネットに関連する技術に関しては標準化団体で活発に議論が継続されており、G.8031/Y.1342にも今後変更が加えられる可能性もあることから、今回はTTCでは標準化を見送ることとした。引き続きITU-Tにおける関連勧告の標準化状況を見極め、適切な時期に国内標準化を達成したい。

2. 調査勧告の概要

ITU-T G.8031/Y.1342 は、イーサネット VLAN 信号のリニアプロテクションスイッチを規定する勧告である。ETH リニアプロテクションスイッチの特性、アーキテクチャ、APS プロトコルに関する詳細規定が含まれる。G.8031/Y.1342 で考察されているプロテクションの仕組みは、サブレイヤモニタリングを伴う VLAN ベースのイーサネットサブネットワークコネクションリニアプロテクションである。本勧告ではリニアプロテクションとして1+1 アーキテクチャ（送信端のブリッジ機能は恒久的に行われ、切替は受信端で排他的に行われる。）

と1:1 アーキテクチャ（送信端では切り替えが必要になるまでブリッジ機能は確立されない。）がサポートされている。

3. 国内の状況

通信事業者向けイーサネットに関する研究・開発が急速に発展しつつあり、イーサネットをUNIとする通信サービスの提供がすでに行われている。今後はイーサネットNNIによる他事業者間接続が求められることが想定される。

4. 今後の国内標準化

我が国におけるイーサネットをベースとする広域LANの普及状況を考慮すると、TTC標準化を早急に実施していく必要があると判断する。

一方、イーサネットをベースとした広域LAN技術であるプロバイダバックボーンブリッジ等の標準化は現在進行中であり、今後G.8031/Y.1342にも手が入る可能性もあることから、引き続きITU-Tにおける関連勧告の標準化状況を見極めて、早急に国内標準化を達成したい。

5. おわりに

イーサネットレイヤネットワークアーキテクチャに関する国際標準であるITU-T G.8031/Y.1342の技術調査を行った。本標準の調査に基づき、国内の状況を踏まえて、国内標準化についての考え方をまとめた。本報告書が、今後のTTC標準化活動の一助となれば幸いである。

1. 適応範囲

本勧告は、APS プロトコルおよびイーサネットネットワーク上でポイント-ポイント間 VLAN の ETH SNC でのリニアプロテクションスイッチメカニズムに関して規定する。

それ以外のプロテクション構成、ポイント-マルチポイントやマルチポイント-マルチポイントは将来検討事項である。

片方向切替および双方向切替を伴うリニア 1+1 および 1:1 プロテクションスイッチングアーキテクチャが本勧告のこのバージョンで定義される。それ以外のイーサネットネットワークアーキテクチャ (たとえばリングやメッシュなど) のための APS プロトコルとプロテクションスイッチオペレーションは将来検討事項である。

2. 参考文献

以下に列挙する ITU-T 勧告その他の参照規格には、本勧告の本文内での参照によって本勧告の一部となる規定が記載されている。表示されている各版数は、本勧告の公開時点で有効であった版数を表している。勧告その他参照規格は、いずれも変更される場合がある。したがって、本勧告の使用においては、以下に列挙する勧告その他参照規格の最新版が公開されていないか確認されるようお願いする。現在有効な ITU-T 勧告の一覧は定期的に公開されている。本勧告において特定の文書を参照した場合も、その文書を単独で勧告として取り扱うものではない。

- ITU-T Recommendation G.780/Y.1351 (2004), *Terms and definitions for synchronous digital hierarchy (SDH) networks.*
- ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*
- ITU-T Recommendation G.806 (2006), *Characteristics of transport equipment – Description methodology and generic functionality.*
- ITU-T Recommendation G.808.1 (2006), *Generic protection switching – Liner trail and subnetwork protection.*
- ITU-T Recommendation G.841 (1998), *Types and characteristics of SDH network protection architectures.*
- ITU-T Recommendation G.870/Y.1352 (2004), *Terms and definitions for optical transport networks (OTN).*
- ITU-T Recommendation G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks.*
- ITU-T Recommendation G.8021/Y.1341 (2004), *Characteristics of Ethernet transport network equipment functional blocks.*
- ITU-T Recommendation M.495 (1988), *Transmission restoration and transmission route diversity: Terminology and general principles.*
- ITU-T Recommendation Y.1731 (2006), *OAM functions and mechanisms for Ethernet based networks.*

- IEEE Standard 802-2001, *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.*
- IEEE Standard 802.1D-2004, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges.*
- IEEE Standard 802.1Q-2005, *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.*

3. 定義

本勧告では G.780/Y.1351 で定義された以下の用語を用いる。

- 3.1 bidirectional protection switching: 双方向プロテクションスイッチ
- 3.2 unidirectional protection switching: 片方向プロテクションスイッチ

本勧告は G.805 で定義された以下の用語を用いる。

- 3.3 adapted information: アダプテーション情報
- 3.4 characteristic information : 特徴的情報
- 3.5 link: リンク
- 3.6 link connection: リンクコネクション
- 3.7 signal degrade (SD): 信号劣化
- 3.8 signal fail (SF): 信号断
- 3.9 tandem connection: タンデムコネクション
- 3.10 trail: トレイル
- 3.11 trail termination: トレイル終端

本勧告では G.806 で定義された以下の用語を用いる。

- 3.12 atomic function: アトミックファンクション
- 3.13 defect: 故障
- 3.14 failure: 断
- 3.15 server signal fail (SSF): サーバ信号断
- 3.16 trail signal fail (TSF): トレイル信号断

本勧告では G.870/Y.1352 で定義された以下の用語を用いる。

- 3.17 APS protocol: APS プロトコル
- 3.17.1 1-phase: 1-位相
- 3.18 Protection class : プロテクションクラス
- 3.18.1 Individual: 単一
- 3.18.2 Group: グループ
- 3.18.3 Network connection protection: ネットワークコネクションプロテクション
- 3.18.4 Subnetwork connection protection: サブネットワークコネクションプロテクション
- 3.18.4.1 Sublayer monitored (/S): サブレイヤ監視

3.18.4.2	non-intrusive monitored:	非割り込み監視
3.18.4.3	inherent monitored:	個別監視
3.18.4.4	Test monitored (/T):	テスト監視
3.18.5	Trail protection:	トレイルプロテクション
3.19	Switch:	スイッチ
3.20	Component:	コンポーネント
3.20.1	Protected domain:	保護ドメイン
3.20.2	Bridge:	ブリッジ
3.20.2.1	Permanent bridge:	パラメータブリッジ
3.20.2.2	Selector bridge:	セレクトアブリッジ
3.20.3	Selector:	セクタ
3.20.3.1	Selective selector:	選択セクタ
3.20.3.2	Merging selector:	統合セクタ
3.20.4	Head end:	ヘッドエンド
3.20.5	Tail end:	トレイルエンド
3.20.6	Sink node:	シンクノード
3.20.7	Source node:	ソースノード
3.20.8	Intermediate node:	中間ノード
3.21	Architecture:	アーキテクチャ
3.21.1	1+1 protection architecture:	1 + 1 プロテクションアーキテクチャ
3.21.2	1:n protection architecture:	1 : n プロテクションアーキテクチャ
3.21.3	(1:1)n protection architecture:	(1 : 1)n プロテクションアーキテクチャ
3.22	Signal:	信号
3.22.1	Traffic signal:	トラフィック信号
3.22.2	Normal traffic signal:	通常トラフィック信号
3.22.3	Extra traffic signal:	エクストラトラフィック信号
3.22.4	Null signal:	無効信号
3.23	Time:	時間
3.23.1	Detection time:	受信時間
3.23.2	Hold-off time:	ホールドオフ時間
3.23.3	Wait-to-restore time:	切り戻り待ち時間
3.23.4	Switching time:	切替時間
3.24	Transport entity:	トランスポートエンティティ
3.24.1	Protection transport entity:	非運用系(プロテクション)トランスポートエンティティ
3.24.2	Working transport entity:	運用系(ワーキング)トランスポートエンティティ
3.24.3	Active transport entity:	アクティブトランスポートエンティティ
3.24.4	Standby transport entity:	スタンバイトランスポートエンティティ
3.25	Protection:	プロテクション
3.26	Impairment:	損傷
3.27	Protection ratio:	プロテクション率

本勧告では G.809 で定義された用語を用いる。

3.28	adaptation:	アダプテーション
3.29	flow:	フロー
3.30	flow domain:	フロードメイン
3.31	flow point:	フローポイント
3.32	flow termination:	フロー終端
3.33	layer network:	レイヤネットワーク
3.34	link flow:	リンクフロー
3.35	network:	ネットワーク
3.36	port:	ポート
3.37	transport:	送信ポート
3.38	transport entity:	送信ポートエンティティ
3.39	termination flow point:	終端フローポイント

本勧告では G.8010/Y.1306 で定義された用語を用いる。

3.40	Ethernet characteristic information (ETH_CI):	イーサネット特徴的情報
3.41	Ethernet flow point (ETH_FP):	イーサネットフローポイント
3.42	maintenance entity:	メンテナンスエンティティ
3.43	maintenance entity group:	メンテナンスエンティティグループ
3.44	maintenance entity group level:	メンテナンスエンティティグループレベル

本勧告では G.8021/Y.1341 で定義された用語を用いる。

3.45	Ethernet flow forwarding function (ETH_FF):	イーサネットフロー転送機能
------	---	---------------

本勧告では M.495 で定義された用語を用いる。

3.46	transfer time (Tt):	切替時間
------	---------------------	------

本勧告は G.8010/Y.1306 および Y.1731 で定義された用語を用いる。

3.47	maintenance entity group end point (MEP):	メンテナンスエンティティグループエンドポイント
------	---	-------------------------

4. 略語

この勧告では、以下の略語を使用する。

AI	Adapted Information	アダプテーション情報
APS	Automatic Protection Switching	自動プロテクションスイッチ
CCM	Continuity Check Message	継続的確認メッセージ
DNR	Do Not Revert	切り戻し禁止
EC	Ethernet Connection	イーサネットコネクション
ETH	Ethernet layer network	イーサネットレイヤネットワーク
ETH-AIS	Ethernet Alarm Indication Signal function	イーサネットアラーム表示信号ファンクション
ETH-APS	Ethernet Automatic Protection Switching function	イーサネット自動プロテクションスイッチプロテクション
ETH-CC	Ethernet Continuity Check function	イーサネット継続チェックファンクション
EXER	Exercise	演習
FS	Forced Switch	強制切替
FT	Flow Termination	フロー終端
LCK	Locked	閉じ込め
LO	Lockout for protection	ロックアウトプロテクション
LOC	Loss of Continuity	継続性ロス
LSB	Least Significant Bit	最下位ビット
MEP	Maintenance Entity Group End Point	メンテナンスエンティティグループエンドポイント
MIP	Maintenance Entity Group Intermediate Point	メンテナンスエンティティグループ中間ポイント
MS	Manual Switch	手動切替
MSB	Most Significant Bit	最上位ビット
NR	No Request	要求なし
OAM	Operation, Administration and Maintenance	オペレーション、監視およびメンテナンス
PDU	Protocol Data Unit	プロトコルデータユニット
PS	Protection Switching	プロテクションスイッチ
RR	Reverse Request	切り戻し要求
RSTP	Rapid Spanning Tree Protocol	高度スパニングツリープロトコル
SD	Signal Degrade	品質劣化
SF	Signal Fail	信号断
SF-P	Signal Fail on Protection	プロテクションにおける信号断
SNC	Subnetwork Connection	サブネットワークコネクション
SNC/I	Inherently monitored Subnetwork Connection	個別監視サブネットワークコネクション
SNC/N	Non-intrusively monitored Subnetwork Connection	割り込み禁止監視サブネットワークコネクション
SNC/S	Sub-layer monitored Subnetwork Connection	サブレイヤ監視サブネットワークコネクション
SNC/T	Test-trail monitored Subnetwork Connection	テストトレイル監視サブネットワークコネクション
VID	VLAN Identifier	VLAN 識別子

VLAN	Virtual LAN	バーチャル LAN
WTR	Wait to Restore	切り戻り待ち

5. 慣例

5.1 オクテット表現

オクテットは IEEE802.1D 定義で表現している。

連続的なオクテットでバイナリー値を表現する際は、低位のオクテット値は最も重要な値となる。

オクテット内のビットには 1 から 8 までの数字が割り当てられるが、1 は最低位ビット (LSB) で 8 は最上位ビット (MSB) に振られる。

6. はじめに

本勧告は、G.8010/Y.1306 に記載された VLAN ベースのイーサネットネットワークに採用されるリニアプロテクションスイッチメカニズムを規定する。リニアプロテクションスイッチは、完全に事前に割り当てが行われる救済メカニズムである。

非運用系のエンティティのルートや帯域が、運用系エンティティにより確保されるという意味で、完全割り当てが行われる方式であるといえる。リニアプロテクションスイッチは高速でシンプルな救済メカニズムを提供する。

プロテクションスイッチを適用したネットワークは、その状態 (例えばアクティブなネットワークトポロジ) を、他の救済メカニズム (例えば RSTP など) よりも、ネットワーク運用者は簡単に把握しやすい。

本勧告はリニア 1+1 および 1:1 プロテクションスイッチのアーキテクチャを規定する。リニア 1+1 プロテクションスイッチングアーキテクチャは片方向切替、双方向切替のいずれでも運用できる。リニア 1:1 プロテクションスイッチングアーキテクチャは双方向切替により運用できる。

リニア 1+1 プロテクションアーキテクチャでは、プロテクショントランスポートエンティティは各ワーキングエンティティの占有となる。通常トラヒックは、送信側の固定ブリッジにて複製されて、ワーキングエンティティとプロテクションエンティティに入力される。ワーキング転送エンティティと、プロテクション転送エンティティのトラヒックは同時に受信端に送信される。受信端でのワーキング転送エンティティとプロテクション転送エンティティの選択は、サーバ欠陥通知など事前に決められた基準で行われる。

リニア 1+1 プロテクションスイッチングアーキテクチャでは、受信端のみにて選択が行われるが、双方向 1+1 プロテクションスイッチでは両端で同一のエンティティを選択するために APS 協調プロトコルが必要である。それに対して、片方向 1+1 プロテクションスイッチでは APS 協調プロトコルは必要としない。

リニア 1:1 プロテクションスイッチングアーキテクチャでは、非運用系 (プロテクション) エンティティは運用系 (ワーキング) エンティティに占有される。しかしながら、通常トラヒックは運用系パスか非運用系パスに送信側のセレクトブリッジにより選択されて送信される。

受信端のセクタは通常トラヒックを伝送しているエンティティを選択する。それにより、送信側と受信側のセクタが同じエンティティを選択するように送信側と受信側が協調する必要があるため、APS 協調プロトコルを必要とする。

7. ネットワーク目標

- 1) イーサネットプロテクションスイッチは 1 つの ETH フロー領域にある 2 つの ETH フローポイント間の接続を提供する ETH SNC ベースのポイント・ポイント VLAN ベース ETH SNC に適用できなくてはならない。VID(s)は、ETH リンク間のポイント・トゥ・ポイント VLAN ベース ETH SNC(s)を識別するために使

うことができる。ETHの他の細目と関連するアトミックファンクションはG.8010/Y.1306を参照のこと。
他のエンティティのプロテクションは将来検討事項である。

- 2) 保護されたドメインでは、運用系エンティティの障害により損なわれたトラフィックを100%保護するように設定されるべきである。
- 3) 切替時間(Tt)は50m秒以内である。
- 4) ETHレイヤの運用系トランスポートエンティティおよび非運用系トランスポートエンティティのETHレイヤコネクティビティは、定期的に監視すべきである。
- 5) プロテクションスイッチイベントの後は、順々にフレームを送付すべきである
注) プロテクションスイッチイベントの後、フレームはパスの相対的遅延により一時的に破棄や2重に送付されることがある。
- 6) 独立プロテクションスイッチおよびグループプロテクションスイッチをサポートすべきである。
- 7) ネットワークオペレータのオプションとして切り戻し有り切替および切り戻しなし切替をサポートすべきである。
- 8) 近端と遠端のブリッジ/セレクタの位置の不一致を検知して通知すべきである。
-ローカルネットワークエレメントのブリッジ/セレクタの位置の不一致を検知して通知すべきである。
-ブリッジ/セレクタの不一致は、ネットワークオペレータがクリアすべきである。
- 9) ロックアウト、強制切替、手動切替要求などのオペレータ要求をサポートすべきである。
- 10) シグナルフェイル(SF)とオペレータ要求の間に優先プロテクションをサポートすべきである。
- 11) プロテクションスイッチ動作開始を操作者が遅らせることができる”ジェネリックホールドオフ機能”を提供すべきである。

8. プロテクション特性

8.1 モニタ方法および状態

プロテクションスイッチはプロテクト領域内の(運用系、非運用系)トランスポートエンティティの特定の異常を検知すると動作する。これらの異常の検知方法は、機器勧告(例えば、ITU-T 勧告 G.8021/Y.1341)の主題である。プロテクションスイッチを実行するため、保護された領域内のトランスポートエンティティには、OK(正常)、SF(故障)、(適用する場合には)SD(信号劣化)の3つの状態がある。

次の慣例上のモニタ手法がある。

固有型 - 固有モニタリングは終端点のトレイル終端機能もしくはアダプテーション機能により検知する異常を基に行われる。固有モニタリングを適用するイーサネットサブネットワークプロテクション(SNC/I)は、固有モニタリングを基に行われる。

非割込み型 - プロテクショングループの終端の非割込み型モニタリングが、プロテクションスイッチの契機となる。この型は、始点および終点に制約されることのないトレイルのセグメントの保護を認める。非割込み型モニタリングを適用するイーサネットサブネットワークプロテクション (SNC/N)は、非割込み型モニタリングを基に行われる。非割込み型モニタリングはレイヤまたはサブレイヤのモニタリングを基に行われる場合もある（たとえば、TCM 非割込み型モニタリング）。

サブレイヤ型 - イーサネットサブネットワークモニタリングを適用したサブネットワークプロテクション(SNC/S)はサブレイヤモニタリングに基づくリアプロテクションアーキテクチャである。それぞれのシリアルコンパウンドリンクコネクションは、トラフィック状況とは関係なく異常状態の状況を探るために、タンデムコネクションモニタリング(TCM)もしくはセグメントターミネーション/アダプテーションにより拡張される。

TCM をサポートしているネットワークレイヤにおいては、保護されたセグメントにおける故障によってのみプロテクションスイッチがなされるように、保護されたセグメントを正しく通過するトレイルの TCM 監視されたセグメントのインスタンスを作成することは魅力的である。

SNC/S は、保護されたセグメントのアップストリームで発生する異常をプロテクションスイッチのために可視化できない SNC/N に対するさらなるアドバンテージを有する。

テストトレイル - 異常はエクストラテストトレイルを用いて検知する。サブネットワークコネクションのプロテクショングループを含む保護されたドメインのソースとシンクの間エクストラテストトレイルは設定される。テストトレイルモニタリングを適用したイーサネットサブネットワークプロテクション(SNC/T)はグループプロテクションのみに適用されるテストトレイルモニタリングを基に行われる。

プロテクションスイッチコントローラは保護されたドメインにあるトランスポートエンティティの情報 (OK、SF、(適用する場合は) SD) が与えられればいかなるモニタ手法かは頓着しない。いくつかのモニタは SD を検知できないかもしれない。しかしこれにより異なる APS を使用する必要はない。これは単純に SD を検知できない機器では SD は課題とならないのと同じである。APS プロトコル使用時に近端の SD がモニタ出来ないとしても遠端の SD を除外する必要はない。

本勧告の当該バージョンにおいては、ポイント-ポイント VLAN ベースの ETH SNC のために SNC/S モニタリングアーキテクチャがサポートされている。他のモニタ手法 SNC/I, SNC/N や SNC/T は将来検討事項である。

9. プロテクショングループコマンド

9.1 エンドエンドコマンドと状態

本セクションはプロテクショングループ全体に適用するコマンドについて記載する。APS プロトコルを適用するときには、これらのコマンドはコネクションの遠端に伝えられる。双方向スイッチの場合はこれらのコマンドは、両端のブリッジ/セレクトに影響を与える。

ロックアウト - 本コマンドは非運用系トランスポートエンティティへ運用系の信号を切替できないように

する。ロックアウトはプロテクショングループを事実上無効にする。

通常非運用トラフィック信号の強制切替 – 非運用系トランスポートエンティティから通常トラフィック信号の選択を強いる。

通常非運用トラフィック信号の手動切替 – 運用系または非運用系の障害がない限りにおいて、非運用系トランスポートエンティティから通常トラフィック信号の選択を強いる。

通常トラフィック信号切り戻り待ち時間(WTR) – 切り戻り動作で SF(SD もし有効ならば)が運用系エンティティでクリアされた場合、タイマー値が有効な間は非運用系トランスポートエンティティから選択されている通常トラフィック信号を保持する。本状態はもしタイマー値以内に他のイベントやコマンドがあった場合はノーリクエスト(NR)へ遷移する。本コマンドは、間欠障害時における頻繁なセレクトア切替を防止するのに使われる。

信号実行(Exercise Signal) – APS プロトコルの実行。本信号はセレクトアの更新をしないように選ばれる。

非切り戻り通常トラフィック信号 – 非切り戻り運用において、非運用系トラフィックエンティティから選択される通常トラフィック信号を保持するために使われる。

ノーリクエスト(NR) – ノーリクエストは、アクティブなローカルプロテクションスイッチ要求 (WTR と切り戻しなしを含む) がないすべての状況において、ローカル優先により入る状態。通常トラフィック信号は非運用系トラフィックエンティティから選択される。

クリア – 有効な、近端のロックアウト、強制切替、手動切替、WTR 状態、Exercise コマンドをクリアする。

9.2 ローカルコマンド

これらのコマンドはプロテクショングループの近端のみに適用される。APS がサポートされる場合も遠端には送信されない。

フリーズ – プロテクショングループの状態をフリーズさせる。フリーズがクリアされるまで新しい近端コマンドは拒否される。状態変化通知や受け取ったAPS情報は無視される。フリーズコマンドがクリアされたら、プロテクショングループの状態は、現在の状態と受け取ったAPS情報により再計算される。

クリアフリーズ

ロックアウト(Lockout Normal Traffic Signal from Protection) – 非運用系エンティティから通常トラフィックシグナルが選択されることを防ぐ。通常トラフィック信号のためのコマンドは拒否される。通常トラフィック信号において、SF または SD (適用時)は無視される。双方向切替において、通常トラフィック信号のリモートブリッジ要求は、プロトコル失敗を防ぐため受け付ける。結果として、非運用系トランスポートエンティティから選択中の通常トラフィック信号を各端点にて妨げるためには、通常トラフィック信号は両端で非運用トランスポートエンティティからロックアウトされなくてはならない。

クリアロックアウト(Clear lockout normal traffic signal from protection)

10. プロテクションアーキテクチャ

勧告の本版数に定義されたリニアプロテクションアーキテクチャでは、プロテクションスイッチはポイント・トゥ・ポイント VLAN ベース ETH SNC の2つの異なる終点にて行われる。これらの終点間には、「現用」と「予備」の両方のトランスポートエンティティがあることになる。

与えられた送信方向に対して、保護されたエンティティの「送信端」は、必要に応じて非運用系トランスポートエンティティに通常トラフィック信号のコピーを配置するブリッジ機能として振舞うことができる。

「受信端」は切替機能として振舞う。この切替機能は、通常の運用系トランスポートエンティティあるいは非運用系トランスポートエンティティから通常トラフィック信号を選択することができる。双方向伝送方式において、双方向のトランスポートエンティティが保護される箇所に、保護されたエンティティの両端それぞれにブリッジ機能と切替機能の両方を提供する。

以下のアーキテクチャが許容される。

1+1 - 1+1 アーキテクチャでは、非運用系トランスポートエンティティは、通常トラフィック信号を保護するために使用される。送信端のブリッジ機能は恒久的に行われる。切替は受信端で排他的に行われる。

1:1 - 1:1 アーキテクチャでは、非運用系トランスポートエンティティは、通常トラフィック信号を保護するために使用される。送信端では、プロテクションスイッチが必要になるまで、ブリッジ機能は確立されない。

1つの保護された領域内では各端点のアーキテクチャは同一のアーキテクチャでなくてはならない。

10.1 単方向切替と双方向切替

双方向伝送の場合では、単方向切替と双方向切替のいずれも選択可能である。単方向切替においては、各端のセレクトは完全に独立に動作する。双方向切替においては、片方向の故障であっても、同一のブリッジ機能と切替部設定を持つ2端点間の整合を試みる。

双方向切替においては、2端点間の整合を取るために必ず APS 情報を必要とする。単方向切替では、異なるエンティティ上の逆方向の2つの片方向故障を救済できる。

10.2 APS 通信の必要性

APS 通信を必要としない唯一の切替方法は 1+1 単方向切替である。

送信端に恒久的なブリッジを持つことと、2端点間のセレクトのポジションの整合を取る必要が無いことにより、受信端のセレクトは、異常発生に続く受信端のコマンド受信のみにより動作可能である。

双方向切替では必ず APS 通信が必要である。

10.3 切り戻り切替と非切り戻り切替

切り戻り運用においては、切替を引き起こした状態の回復後に、通常トラフィック信号は運用系トランスポートエンティティへ復帰させられる。

コマンドをクリアする場合(例えば、強制切替)には、これはただちに動作する。一般的に障害回復時は、「切り戻り待ち」時間を経過後に実施される。「切り戻り待ち」時間は、間欠故障時に切替がパタパタするのを避けるために設けられる。

非切り戻り運用においては、切替要因回復後も、通常トラフィック信号は非運用系トランスポートエンティティ上にあることが許容される。一般にこれは、先の切替要求を低優先の「切り戻し禁止 (DNR)」要求に置き換えることで実現する。

1+1 プロテクションはしばしば非切り戻り運用として設定される。これにより、どのような場合でも、保護は完全になされ、さらには通常トラヒック信号の（切り戻しに伴う）2度目の「瞬断」を回避する。しかしながら、切り戻り運用に設定する理由がある場合もある。（例えば、障害状態を除いて、正常な信号が「短い」経路を使用する。また、ある運用者の方針では、1+1 運用であってさえも切り戻し操作を必要とする。）

通常は 1:1 プロテクションは切り戻り運用される。1:1 プロテクションで非切り戻り運用を認めるようなプロトコルを定義することは可能である。しかしながら、運用系トランスポートエンティティは、遅延特性や需要予測をもとに、一般的には非運用系トランスポートエンティティよりも最適化が行われる。それは運用系トランスポートエンティティが回復された時には、通常トラヒック信号を瞬断させても（運用系へ）復旧させるほうがよいということである。

一般に、切り戻り/非切り戻り運用はプロテクショングループの両端で同じものが選択される。しかしながら、不一致となっても相互に妨げることはないが、一方が切り戻し禁止（DNR）状態に遷移するとき、もう一方が、その側から始めた切替回復のために WTR に遷移するというのは奇妙なことである。

SNC/S プロテクションスイッチングプロセスの切り戻り/非切り戻り運用は ETH_MI_PS_OperType を介して設定されなくてはならない。

10.4 プロビジョニングの誤った組合せ

プロテクショングループのすべてのオプション設定において、両端の設定が誤った組合せとなる可能性がある。これらの設定の誤った組合せは、いくつか形式のうちの 1 つを採る。

- 適切なオペレーションが可能でないところで生じる誤り
- 誤った組合せにもかかわらず、片端または両端は、ある程度の相互作用を引き起こすオペレーションに適合できるという誤り。
- 相互作用を妨げない誤り。例としては、10.3 節および 11.4 節で議論された切り戻り/非切り戻りの誤った組合せ。

すべてのプロビジョニングの誤りは、APS 通信を通して渡された情報によって、伝えられ、検出されることができるとは限らない。プロビジョニングにおいてすべてのオプションを簡易に完全に可視化するためには、有効なトランスポートエンティティ番号の組み合わせは多すぎる。しかしながら、望ましいことは中間のカテゴリーに可視化を提供することである。そこでは、誤った組合せにもかかわらず相互作用するためにそれらの操作を適合させることができる。例えば、双方向切替に設定された装置は、相互作用を許容するために、単方向切替の設定に後退することもある。APS 通信を備えた 1+1 切替に設定された装置は、APS 通信を伴わない 1+1 の単方向切替のオペレーションに後退できるだろう。使用者は今までどおりプロビジョニングの誤った組合せの通知を受けることができるかもしれないが、プロテクションレベルはそれらの装置によって今までどおりを提供される。

10.5 プロテクションスイッチトリガー

例えば、プロテクションスイッチは以下の時に行なわれるべきである。

- 他のローカル要求あるいは遠端要求より高い優先権を持っている場合、保守者の制御（例えば強制切替、手動切替）によって始められる。
- SF は動作中トランスポートエンティティに申告され、待機中トランスポートエンティティには申告されない。そして、検知された SF 条件は他のローカル要求あるいは遠端の要求より高い優先順位を持っている。
- 双方向の 1+1 や 1:1 基本概念では、受信 APS プロトコルは、切替を要求する。そして、それは他のローカル要求より高い優先順位を持っている。

他の場合は付録 A に変化状態として記述される。

10.5.1 信号劣化宣言状態

ETH 信号障害状態が検出された時、SF が申告される。ETH 信号障害状態 は、ITU-T Rec G.8021/Y.1341 で明確にされている。

10.6 プロテクションスイッチのモデル

図 10-1 に、この勧告で定義される VLAN ベースの ETH SNC/S プロテクションスイッチモデルの例を描写する。他のネットワークのシナリオは許容される。

ETH コネクション機能 (ETH_C)内では、ETH SNC プロテクションスイッチングプロセスは、ETH コネクション(EC)を保護するためにインスタンスが生成される。プロテクションスイッチが、EC(保護された ETH SNC) のために形成される場合、それは、図 10-1 の中で描写されるような 2つの ETH フロー・ポイント(ETH_FPs)間に定義される。生成された各 SNC プロテクションスイッチングプロセスは、保護された ETH_CI が転送される ETH_FP の規定出力を決定します。

例えば、1:1 プロテクションスイッチ設定の場合には、保護された ETH のための ETH_CI は、ETH_C 内に生成された ETH SNC プロテクションスイッチングプロセスによって運用系トランスポートエンティティまたは非運用系トランスポートエンティティへ転送することができます。

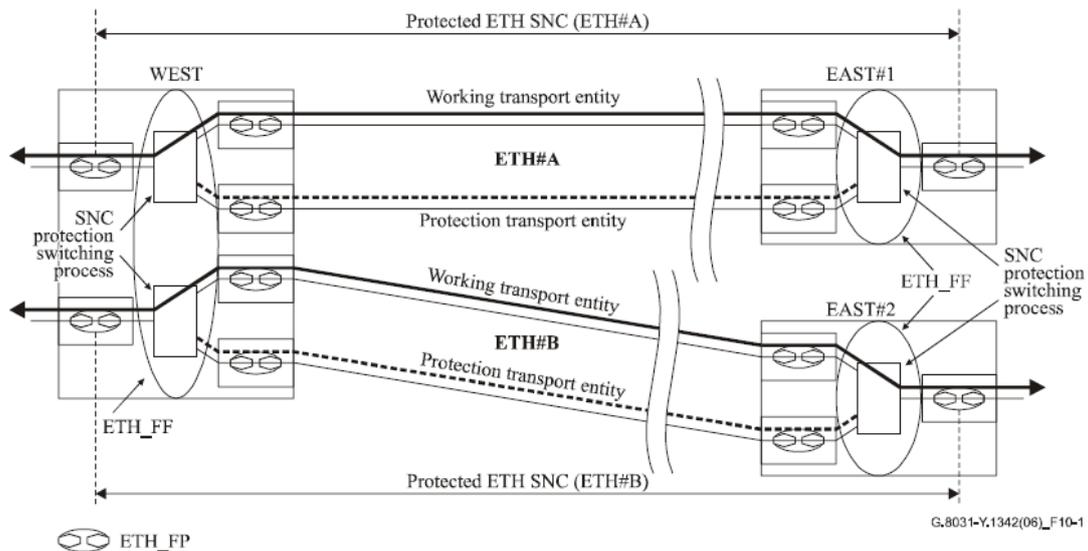


図 10-1/G.8031/Y.1342 – ETH SNC/S プロテクションスイッチングアーキテクチャ

SNC プロテクションスイッチングプロセスのための運用系と非運用系エンティティは、ETH_MI_PS WorkingPortId と ETH_MI_PS ProtectionPortId を介して構成されなくてはならない。

プロテクションスイッチのメカニズムは運用系トランスポートエンティティと非運用系トランスポートエンティティの両方の監視を必要とするので、運用系トランスポートエンティティと非運用系トランスポートエンティティを監視するために、MEP を起動することを必要とする。両方のトランスポートエンティティは、図 10-2 が示すように ITU-T Y.1731 に定義されている CCM を個々にやりとりすることにより監視される。

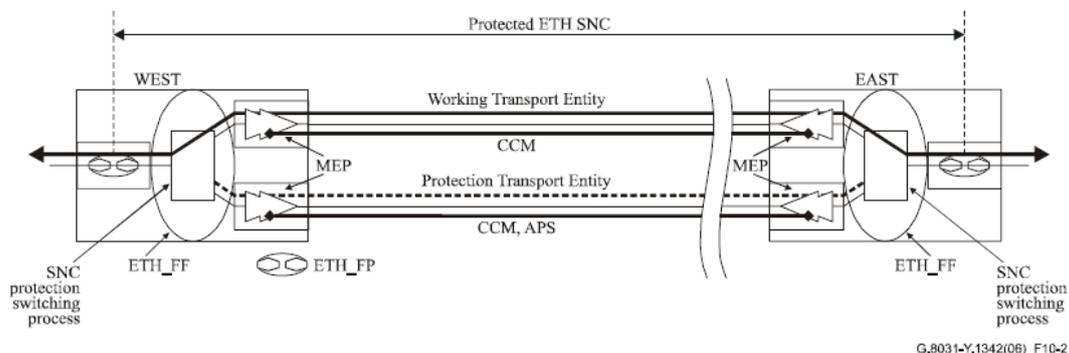


図 10-2/G.8031/Y.1342 – MEPs in ETH SNC/S プロテクションスイッチングアーキテクチャ

プロテクションスイッチの一連の動作は、プロテクションスイッチの基本概念が 1+1 の単方向のプロテクションスイッチでない場合に、保護されたドメインのもう 1 方の端の切替動作を調整させるために APS 通信を必要とする。APS PDU は、CCM が監視のために送信される非運用系トランスポートエンティティの同一 MEP ペアの間で送受信される。

MEP の sink 機能によって終端される APS 情報および検出される異常状態は、図 10-3 に示されるようにプロテクションスイッチングプロセスへ入力することができる。

MEP が SF 異常状態の原因となる異常性を検出すれば、それは障害状態が検出されたプロテクションスイッチングプロセスへ通知する。CCM および LCK (ITU-TY.1731 に定義されている) の終端は、ETH_FT アトリックファンクションによって行われる。

もし、ETH_FT が障害状態を検出する場合、ETH_AI_TSF は、ETH アダプテーションシンク (ETH(x)/ETH_A_Sk) を通って ETH(x) に伝えられる。この時に ETH(x)/ETH_A_Sk は ETH_CI_SSF を生成する。ETH(x)/ETH アダプテーション機能は、信号障害状態にある ETH_C 内の ETH SNC プロテクションスイッチングプロセスに通知するために、この ETH_CI_SSF を用いる。

APS PDU は、MEP 内の ETH(x)/ETH_A_Sk 機能によって終端される。その後、ETH(x)/ETH_A_Sk 機能は受信した APS PDU から APS 仕様情報を抽出し、次に、APS の特有の情報 (CI_APS) として ETH SNC プロテクションスイッチングプロセスにそれを転送する。

ETH_CI_SSF または ETH_CI_APS を受け取った後、プロテクションスイッチングプロセスは新しい切替状態を決定する。次に、必要に応じて保護された ETH_CI を転送する ETH_FP の規定出力を決定する。

運用系トランスポートエンティティと非運用系トランスポートエンティティの両方のための ETH(x)/ETH アダプテーション機能の管理状態は固定してはいけないことに注意すべきである。

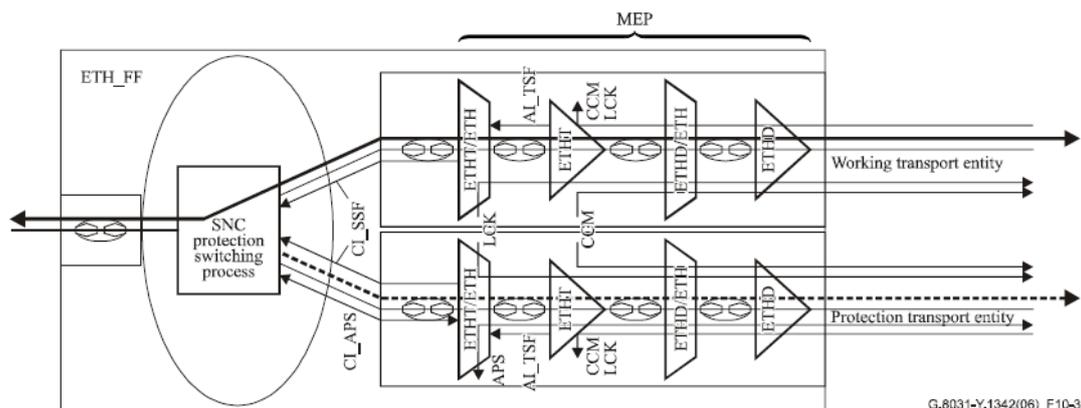


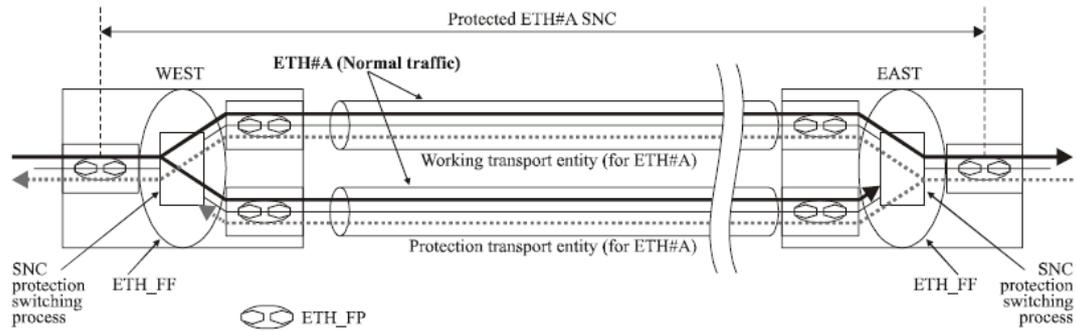
図10-3/G.8031/Y.1342 – ETH SNC/S プロテクションスイッチングアーキテクチャにおけるMEPs および SNC プロテクションスイッチングプロセスの振舞い

SNC/S プロテクションはサブネット接続のみに制限されているわけではない。ネットワーク接続と同様に単一のリンクコネクションもサポートするようにこのプロテクションメカニズムを拡張することは可能である。

10.6.1 1+1 の双方向プロテクションスイッチ

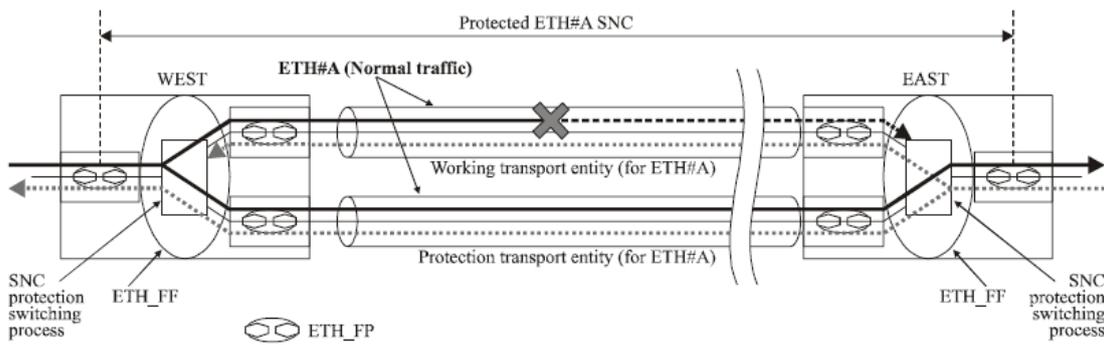
図 10-4 は 1+1 の双方向リニアプロテクションアーキテクチャを示す。保護された ETH_CI トラヒックは運用系トランスポートエンティティと非運用系トランスポートエンティティに恒久的にブリッジされる。この図では、トラヒックは、運用系トランスポートエンティティからのみ ETH_C 経由で受け取られることとして示している。

図 10-5 は、運用系トランスポートエンティティで信号障害状態が原因で発生されたプロテクションスイッチの状態を説明している。一方向で不具合が発生した時でさえ、両方向で切替られることに注意すること。この目的のために、APS 調整プロトコルは必要である。



G.8031-Y.1342(06)_F10-4

図10-4/G.8031/Y.1342 - 1+1 双方向プロテクションスイッチングアーキテクチャ



G.8031-Y.1342(06)_F10-5

図10-5/G.8031/Y.1342 - 1+1 双方向プロテクションアーキテクチャ
運用系エンティティの信号故障状態

10.6.2 1+1 の一方向のプロテクションスイッチ

図 10-6 に 1+1 の一方向リニア構成でのプロテクションスイッチングアーキテクチャを説明する。保護された ETH_CI トラフィックは運用系トランスポートエンティティと非運用系トランスポートエンティティに恒久的にブリッジされる。この図では、両方向ともトラフィックは、ETH_C 経由で運用系トランスポートエンティティからのみ受け取られることとして示している。

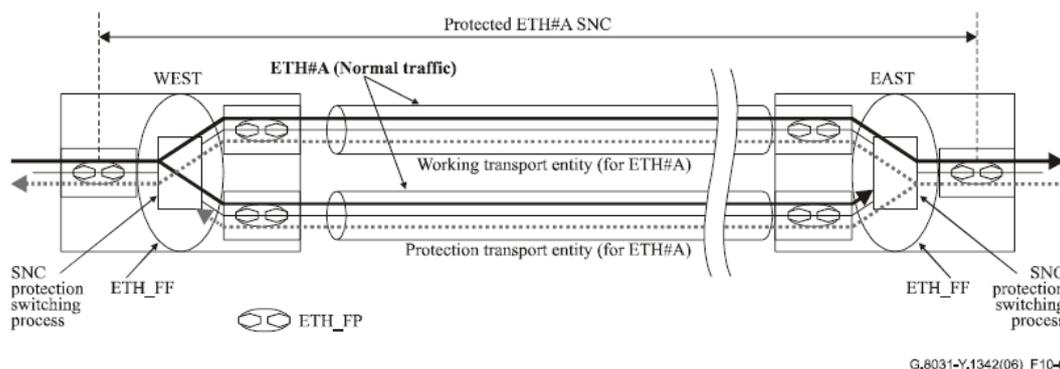


図10-6/G.8031/Y.1342 – 1+1 片方向プロテクションスイッチングアーキテクチャ

図 10-7 は、West 方向から East 方向での運用系トランスポートエンティティで信号障害状態が原因で発生されたプロテクションスイッチの状態を示している。East 方向から West 方向への通常トラフィック（データ量）は運用系トランスポートエンティティ経由で受信され続けている。片方向プロテクションスイッチでは、互いの方向はそれぞれ独立に切替えられる。保護されたドメインの受信側のセクタは、ローカル情報のみを基本として動作する。この目的のためには、APS の調整プロトコルは必要としない。

図 10-8 は West 方向から East 方向への運用系トランスポートエンティティに信号障害状態が存在した場合と、East 方向から West 方向への非運用系トランスポートエンティティに信号障害状態が存在した場合を説明する。片方向プロテクションスイッチは、双方向プロテクションスイッチでは対応できないこの種の 2 重故障シナリオでも切り替えができる。

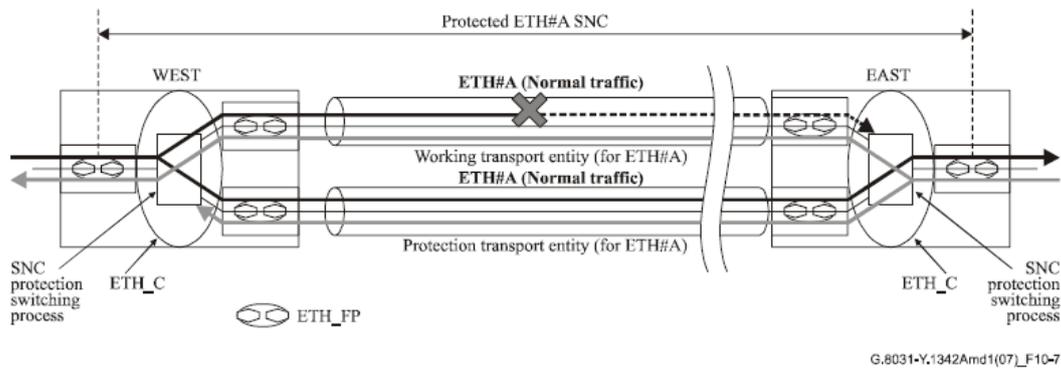


図10-7/G.8031/Y.1342 – 1+1 片方向プロテクションスイッチングアーキテクチャ –
West-to-east方向の運用系エンティティの信号故障状態

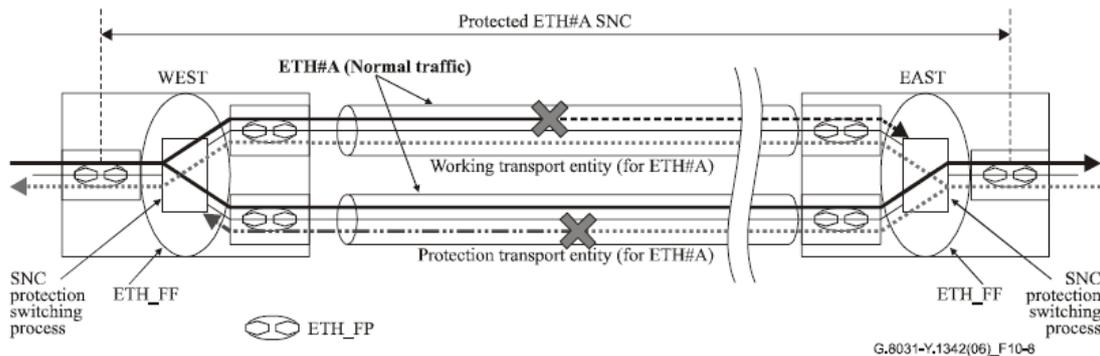


図10-8/G.8031/Y.1342 – 1+1片方向プロテクションスイッチングアーキテクチャ –
両方向の信号故障状態

10.6.3 1:1 双方向プロテクションスイッチ

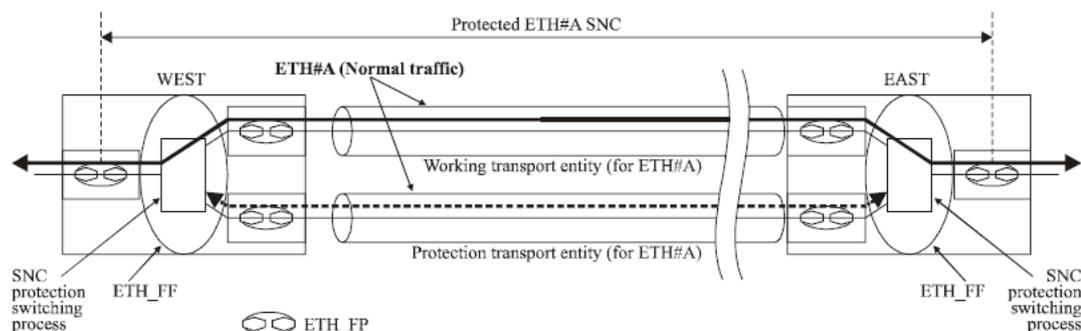
図 10-9 は通常トラヒック (ETH#A) が運用系トランスポートエンティティを經由し送信されている時の 1:1 のリニアプロテクションスイッチングアーキテクチャを説明します。ETH#A のための運用系トランスポートエンティティと非運用系トランスポートエンティティのいずれも、他の ETH トラヒックも使用可能であるが、ETH SNC プロテクションスイッチングプロセスは、プロテクションスイッチが ETH#A に対してのみのために確立されているならば、ETH#A 用の保護された ETH_CI が転送されている ETH_FP の規定出力を決定する。

図 10-10 は、運用系トランスポートエンティティの信号障害状態を理由に発生したプロテクションスイッチの場合を説明する。送信側の装置で、通常トラフィック (ETH#A)が、非運用系トランスポートエンティティへ転送される。受信側の装置で、通常トラフィック(ETH#A)は非運用系トランスポートエンティティから受信される。

プロテクションスイッチが動作中に、保護されたドメインの両端でブリッジ/切替部間で一時的な不整合は起こりえる。しかしながら、VID に基づいて、トラフィックが ETH_C を介して常に正確に転送されるので、ETH#A 用の ETH_CI と他の ETH_CI の間の誤接続は起こり得ない。

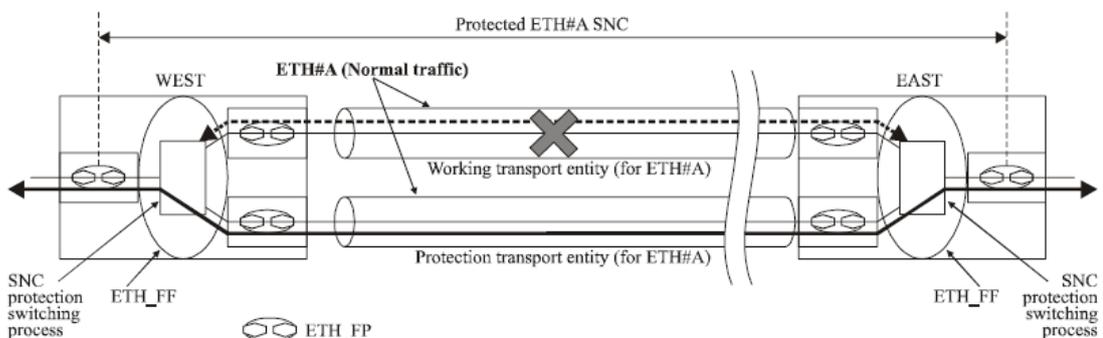
この転送動作を実現させるために、保護された ETH#A および保護されていない ETH トラフィックのために、非運用系トランスポートエンティティで異なる VID を設定しなければならないことに注意すること。

ETH_C 機能の VID によるトラフィック転送では、1:1 アーキテクチャによるトラフィック誤接続は決して起こりえない。すばらしいことに、このことは、両端間で双方向切替を完了するのに要求される 1 つの情報を交換するだけでよいことから、プロテクションスイッチングプロトコルを非常に単純化できる。すなわち 1 段階プロトコルを可能にする。



G.8031-Y.1342(06)_F10-9

図10-9/G.8031/Y.1342 – 1:1プロテクションスイッチングアーキテクチャ



G.8031-Y.1342(06)_F10-10

図10-10/G.8031/Y.1342 – 1:1プロテクションスイッチングアーキテクチャ
運用系トランスポートエンティティの信号故障状態

11 APS Protocol APS プロトコル

11.1 APS format APS フォーマット

APS 情報は、イーサネット OAM PDU セットのうちの 1 つである APS PDU によって運ばれる。イーサネット OAM オペレーションの各タイプのための OAM PDU フォーマットは、ITU-T 勧告 Y.1731 で定義されている。APS 特有情報は、APS PDU の特定フィールドの中で送信される。APS PDU は、特定のイーサネット OAM OpCode により認識される。本版の勧告において、APS PDU の 4 オクテットが、APS 特有情報を運ぶのに用いられる。これを図 11-1 に示す。さらに、この勧告の現在のバージョンでは、TLV Offset フィールドは、0x04 に設定する必要があることに留意すべきである。

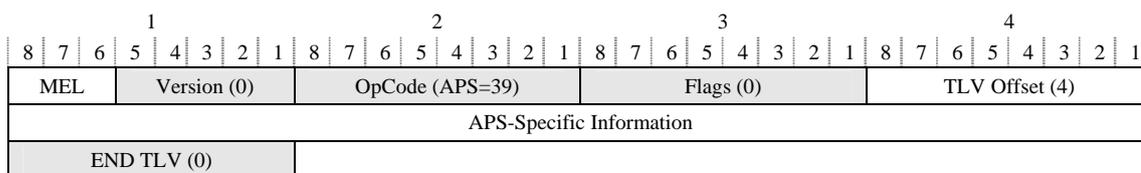


図11-1/G.8031/Y.1342 – APS PDUフォーマット

バージョン、OpCode、フラグおよび END TLV のような他のフィールドでは、ITU-T 勧告 Y.1731 で定義されるように、以下の値が使用されるべきである。

- バージョン : 0x00
- OpCode : 0x39
- フラグ : 0x00
- END TLV : 0x00

MEL フィールドでは、APS PDU の MEG レベルが挿入される。

各 APS PDU 中の APS 特有情報のフォーマットは、図 11-2 に従って定義される：

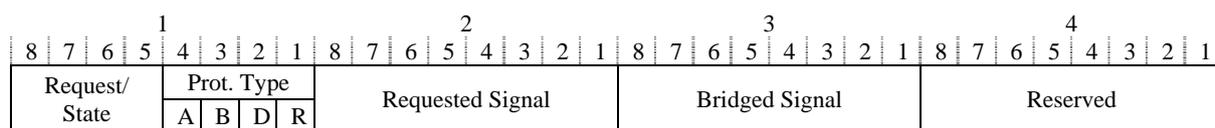


図11-2/G.8031/Y.1342 – APS特有情報のフォーマット

APS特有情報のコードポイントと値について、表11-1に記述する。

表11-1/G.8031/Y.1342 – Code points and field values
for APS-specific information

Request/State	1111	Lockout of Protection (LO)	Priority
	1110	Signal Fail for Protection (SF-P)	highest
	1101	Forced Switch (FS)	
	1011	Signal Fail for Working (SF)	
	1001	Signal Degrade (SD) (Note 1)	
	0111	Manual Switch (MS)	
	0101	Wait to Restore (WTR)	
	0100	Exercise (EXER)	
	0010	Reverse Request (RR) (Note 2)	
	0001	Do Not Revert (DNR)	
	0000	No Request (NR)	lowest
Others		Reserved for future international standardization	
Protection Type	A	0	No APS Channel
		1	APS Channel
	B	0	1+1 (Permanent Bridge)
		1	1:1 (no Permanent Bridge)
	D	0	Unidirectional switching
		1	Bidirectional switching
	R	0	Non-revertive operation
		1	Revertive operation
Requested Signal	0	Null Signal	
	1	Normal Traffic Signal	
	2-255	(Reserved for future use)	
Bridged Signal	0	Null Signal	
	1	Normal Traffic Signal	
	2-255	(Reserved for future use)	
NOTE – SD is for further study.			

第 10 章で記述されたサポートされたプロテクションアーキテクチャに対しては、1 フェーズ APS が使用されるべきである。

11.21 フェーズ APS プロトコル

11.2.1 動作原則

1+1/1:1 リニアプロテクションスイッチングアルゴリズムの原則を、図 11-3 に示す。このアルゴリズムは、保護されたドメインの両端（WEST と EAST）のネットワーク要素にて実行される。双方向切替は、APS 特有情報の最初のオクテットの「要求/状態」を介して、遠端へローカル切替要求が送信されることにより実行される（図 11-2 参照）。APS 特有情報の第 2 および第 3 のオクテットにおいて送信された"Requested Signal" および "Bridged Signal"は、ローカルのブリッジ/セクタ状態情報を含み、したがって、両端の間の持続的なミスマッチは検出されて、警報に至る。

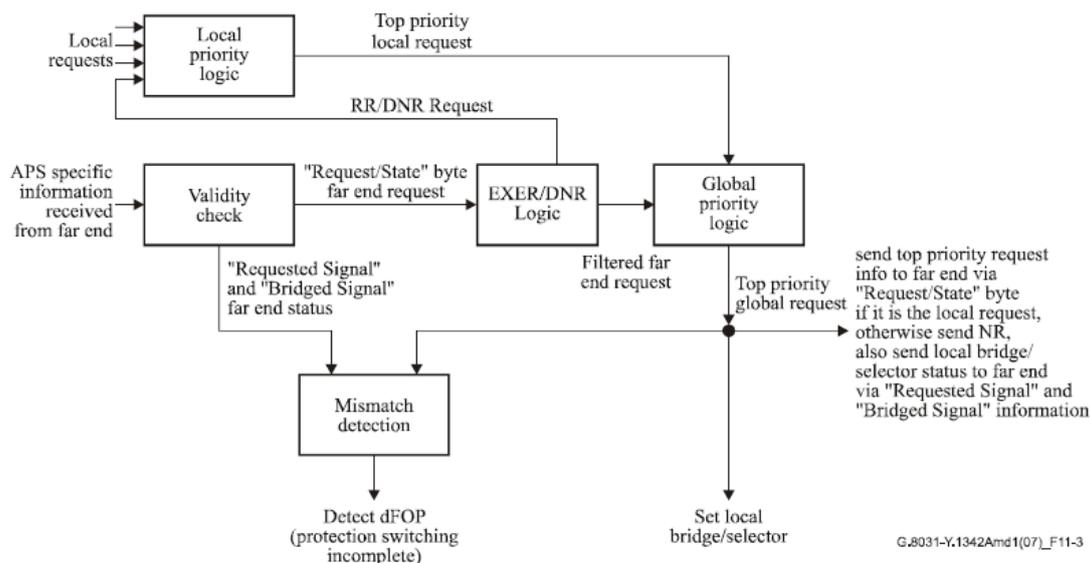


図11-3/G.8031/Y.1342 -1+1/1:1 リニアプロテクションスイッチアルゴリズムの原則

詳細における機能は以下のとおりである（図 11-3 参照）：

ローカルネットワーク要素では、（9.1 章と 9.2 章に記載したように）一つ以上のローカルプロテクションスイッチ要求が動作中になるかもしれない。「ローカルプライオリティロジック」は、表 11-1 に示す優先順序を使用して、これらの要求のうちどれが最優先事項かを決定する。この最優先のローカル要求情報は、「グローバルプライオリティロジック」に伝えられる。

ローカルネットワーク要素は、APS 特有情報を介して、遠端のネットワーク要素から情報を受信する。受信された APS 特有情報は有効性チェックを受ける（11.2.4 節参照）。受信された「要求/状態」情報（それは、遠端の最優先のローカル要求を示す）の情報は、「グローバルプライオリティロジック」に伝えられる。「グローバルプライオリティロジック」は、最優先のグローバル要求を決定するために、最優先のローカル要求と、受信された「要求/状態」情報の要求とを（表 11-1 に示す優先順序に従って）比較する。もし最優先のグローバル要求が、ローカル要求であれば、それは「要求/状態」フィールドに示される、それ以外は、「NR」が示される。そしてこの要求は、次のようなローカルネットワーク要素のブリッジ/セクタの位置（または状態）を決定する：

- 1+1 アーキテクチャでは、セクタの位置のみ制御される。1:1 アーキテクチャでは、両方のブリッジ/セクタの位置は、同じ位置を選択することで維持される；
- 最優先のグローバル要求が運用系のための要求であるならば、関連するワーキングトラヒックは、

非運用系へあるいは非運用系からブリッジあるいは切替られ、すなわち、ローカルネットワーク要素に関連するブリッジ/セクタは、非運用系を選択する。運用系に対する切替要求は、運用系から非運用系へ切替るための要求を意味する。

ブリッジ/セクタ状態は、表 11-1 に示すコードを伴って「要求信号」と「ブリッジ信号」を介して遠端に伝えられる。それは、受信された「要求信号」と「ブリッジ信号」によって示されるように遠端のブリッジ/セクタ状態とも比較される。リアプロテクションスイッチアルゴリズムは、入力信号 (図 11-3 参照) の 1 つが変更する毎に、すなわち、ローカル要求の状態が変化したり、遠端から異なった APS 特有情報を受信したりしたとき、即座に開始されることに注意すること。また、アルゴリズムの必然的な動作、すなわち、ローカルのブリッジ/セクタ位置の変更 (必要ならば)、新しい APS 特有情報の送信 (必要ならば)、または、プロテクションスイッチが 11.15 節で規定された期間内で完了しない場合には、dFOP の検出も即座に開始される。

11.2.2 切り戻りモード

切り戻りモードの動作では、ワーキングトラフィックが非運用系を経由して受信されている状態において、ローカルのプロテクションスイッチ要求 (図 11-3 参照) が以前には活性であったものが、現時点で不活性となる場合、ローカルの復旧待ち状態に入る。この状態は、現在の最優先のローカル要求を表すので、それは送信された「要求/状態」情報で示され、切替状態を維持する。

この状態は、復旧待ち状態のタイマーが切れた後、通常タイムアウトして、要求のない状態になる。よりプライオリティの高いローカルの要求が、この状態を先取りするならば、復旧待ちタイマーは前に非活性化される。

復旧待ち状態に入るかどうかの決定は、ローカル要求のみが考慮されることに注意すること。非運用系への切替は、ローカル復旧待ち状態か、「要求/状態」情報を介して受信したりリモート要求 (復旧待ちか何らかの) によって維持される。それゆえに、運用系で双方向の故障が発生し、その後の修理が行われた場合、運用系への双方向の逆戻りは、両端の両方の復旧待ちタイマーが切れるまで行われない。

11.2.3 非切り戻りモード

非切り戻りモードの動作で、ワーキングトラフィックが非運用系を介して伝送されている状態において、ローカルのプロテクションスイッチ要求 (図 11-3 参照) が以前に活性で、現在不活性となる場合、ローカルの「非切り戻り状態」に入る。この状態は、現在 最も高いプライオリティのローカル要求を意味するので、それは送信された「要求/状態」情報において示され、切替を維持し、従って、要求がない状態下の非切り戻りモードにおいて、開放されたブリッジ/セクタ位置に戻ることを防いでいる。

11.2.4 APS の送信と受理

APS PDU を運ぶトラフィック単位は、APS フレームと呼ばれる。APS フレームは、非運用系のみを介して転送され、プロテクション領域の先端によって挿入されて、プロテクション領域のトレイル端により抽出される。新しい APS フレームは、伝送された状態の変化（図 11-3 参照）が起こると即座に送信されなければならない。たとえ 1 つか、2 つの APS フレームが失われるか壊れても、高速プロテクションスイッチが可能ないように、プロテクション終端の状態変化後、できるだけ早く最初の 3 つの APS フレームが送信されなければならない。50ms の高速プロテクションスイッチのために、最初の 3 つの APS フレームの間隔は、高速故障検出のための CCM フレームと同じ間隔の 3.3ms であることが望ましい。最初の 3 つのフレーム後の APS フレームは、5 秒の間隔で送信されるべきである。

有効な APS 特有情報が受信されなかった場合、最後に受信された有効な情報が依然として適用される。非運用系伝送において信号故障状態が検出されている場合、受信した APS 特有情報は評価されるべきである。プロテクション終端点が運用系から APS 特有情報を受信する場合、この情報を無視し、ローカルネットワーク要素のプロトコル故障を検出するべきである（11.15 参照）。

11.3 要求タイプ

APS 特有情報に反映される要求タイプは、SONET や SDH のプロテクションスイッチで従来よりサポートされている「標準的な」タイプである。これらの要求は、最も高いプライオリティの状況、コマンド、または状態を反映する。片方向切替の場合、これは近端のみから決定される最も高い最優先値である。双方向切替では、APS 通信を通して遠端から受信されたどの要求よりも同じ高さか、またはより高い場合のみ、ローカル要求が示される。それ以外は NR が示される。1 フェーズ APS プロトコルでは、たとえば遠端の要求が最も高いプライオリティのときでさえ、近端は、決してリバース要求を示さない。

11.4 プロテクションタイプ

有効なプロテクションタイプは以下のとおりである：

000x1+1 片方向、APS 通信無し

100x1+1 片方向、APS 通信有り

101x1+1 双方向、APS 通信有り

111x1:1 双方向、APS 通信有り

デフォルト値（全ゼロ）は APS（1+1 片方向）なしで動作可能なプロテクションタイプのみと適合するように、値は選ばれる。

1:1 および双方向は APS 通信を必要とするので、010x、001x、011x は無効であることに注意すること。

「B」ビットが不一致の場合、1:1 と 1+1 は互換性がないので、セレクトは開放される。これは、結果として故障となる。

「B」ビットが一致で：

「A」ビットが不一致の場合、APS を予期している側は、APS 通信なしの 1+1 片方向切替に後退する。

「D」ビットが不一致の場合、双方向の側は片方向切替に後退する。

「R」ビットが不一致の場合、一方は「WTR」への切替をクリアし、他方は「DNR」への切替をクリアする。

2 つの側は相互に作用し、トラフィックはプロテクションされる。

11.5 要求信号

これは、近端の要求がプロテクションパス上で運ばれる信号を示す。遠端が非運用系エンティティに通常トラフィック信号をブリッジしていない場合は、NR に対してはヌル信号である。遠端が非運用系エンティティに通常トラフィック信号をブリッジしているとき、要求された信号は NR に対して通常トラフィック信号である；

LO にとってはヌル信号のみ可能である。エクササイズに対しては、エクササイズが NR や、エクササイズが DNR とかわる場合の通常トラヒック信号と替わるとき、これはヌル信号でありえる。SF（または、適用可能な場合の SD）に対しては、これは通常トラヒック信号か、あるいは、非運用系が故障または劣化したかを示すためのヌル信号になる。すべての他の要求に対しては、これは非運用系上で運ばれることを要求された通常トラヒック信号となる。

11.6ブリッジ信号

これは、プロテクションパスへブリッジされている信号を示す。1+1 プロテクションに対しては、これは常に通常トラヒック信号を示し、正確に永久的なブリッジを反映している。1:1 プロテクションに対しては、実際に何が（ヌル信号か通常トラヒック信号いずれか）非運用系にブリッジされるかを示す。これは、一般的に、遠端より要求されたブリッジである。

11.7ブリッジの制御

1+1 アーキテクチャでは、通常トラヒック信号は永久に非運用系にブリッジされる。通常トラヒック信号は、常に APS 情報のブリッジ信号フィールドで示される。

1:1 アーキテクチャでは、ブリッジは、入力 of APS 情報の「要求信号」フィールドによって示される一つで設定される。一旦、ブリッジが確立されたならば、これは出力される APS 情報の「ブリッジ信号」フィールドに示されることとなる。

11.8セレクトアの制御

1+1 片方向アーキテクチャ（APS 通信の有無にかかわらず）では、セレクトアは最も高いプライオリティのローカル要求に従って完全に設定されます。これは、1 フェーズスイッチである。

1+1 双方向アーキテクチャでは、出力している「要求信号」が通常トラヒック信号を示す場合、通常トラヒック信号は非運用系から選択される。

1:1 双方向アーキテクチャでは、出力している「要求信号」に数が現れる場合、通常トラヒック信号は非運用系から選択される。

11.9非運用系の信号故障

非運用系の信号故障は、非運用系から選択される通常トラヒック信号に発生するどのような故障よりも高いプライオリティである。APS 信号が使用中である場合のために、非運用系（その上に APS 信号がルートされる）上の SF-P は、強制切替えより優先される。ロックアウトコマンドは、SF-P より高いプライオリティを持つ：故障状態の間、ロックアウト状態は維持される。

11.10 イコールプライオリティ要求

一般的に、一旦、切替えが要求によって完了されているならば、それは同じプライオリティのもう一つの要求によって無効にされない（早い者勝ちのふるまい）。双方向プロテクショングループの両側からの等しいプライオリティ要求は、両方有効であると見なされる。

11.11 コマンド受理と保持

コマンド CLEAR、LO、FS、MS、EXER は、前のコマンドや、プロテクショングループの運用系および非運用系の条件や、（双方向切替においてのみ）受信した APS 情報との関係によって、受け入れられるか拒絶される。

近端の LO、FS、MS または EXER コマンドが有効であるか、あるいは、WTR 状態が近端で存在している場

合のみ CLEAR コマンドは有効であり、それ以外は拒絶される。このコマンドは近端のコマンドあるいは WTR 状態を取り除き、次に低い優先状態または（双方向切替では）アサートされた APS 要求を許容する。以前に存在するコマンド、状態または（双方向切替では）APS 要求よりも、それらが高いプライオリティでない限り、他のコマンドは拒絶される。新しいコマンドが受理されるならば、前に無効にされたどのような低いプライオリティのコマンドも忘れられる。より高いプライオリティのコマンドが、低いプライオリティの状態または（双方向切替では）APS 要求を無効にするならば、その他の要求は、そのコマンドがクリアされたときに、まだ存在するならば、再びアサートされる（有効な状態にされる）。コマンドがクリアされるときにまだ存在するならば、他の要求は再び主張されるであろう。コマンドが、状態または（双方向切替では）APS 要求によって無効にされるならば、そのコマンドは忘れられる。

11.12 ホールドオフタイマー

複数のレイヤ、またはカスケードされたプロテクションドメインを越えて、プロテクションスイッチのタイミングを調整するために、ホールドオフタイマーは必要であろう。目的は、クライアントレイヤで切り替わる前に、サーバレイヤプロテクションスイッチに問題を解決する機会を与えることを許容するためか、下流のドメインの前に、上流のプロテクションドメインに切替えることを許可するためである（例えば、二重ノード相互連結構成において、故障として同じリングで切替が発生できるように、下流のリングの前に、上流のリングに切替えることを許可するため）。

各々のプロテクショングループは、提供可能なホールドオフタイマーを持っていなければならない。ホールドオフタイマーの推奨範囲は、100ms（±5 ms の正確さ）ステップで 0～10 秒である。

ホールドオフタイマーの動作は、SDH 標準で規定された「二度覗き”peek twice”」方法を用いる。具体的には、新しい故障またはより深刻な故障が起こるとき（新しい SF（または、適用できるならば SD））、提供されたホールドタイマーの値がゼロ以外であるならば、このイベントはプロテクションスイッチに即座に通知されない。その代わりに、ホールドオフタイマーが開始される。ホールドオフタイマーが切れたとき、タイマーを始動したトレイルに故障がまだ存在するかどうかを検定される。故障がまだ存在するならば、プロテクションスイッチに故障が通知される。故障は、タイマーを始動したのと同じである必要はない。

11.13 切り戻り待ち (Wait-to-restore) タイマー

切り戻りモードの動作では、断続的な障害によるプロテクションスイッチの頻繁な動作を防ぐために、故障した運用系は、障害がなくならなければならない。故障した運用系がこの基準を満たした後、通常トラヒック信号がそれを再び使用する前に一定の期間が経過する。このタイマーは切り戻り待ち (WTR) タイマーと呼ばれ、1分のステップで5分から12分の間でオペレータにより設定されるだろう。デフォルト値は5分である。SF (あるいは適用できるならばSD) 状態は、WTRを無効にする。

切り戻りモードの動作では、プロテクションがもはや要求されないとき、すなわち、故障した運用系はもはやSF (適用できるならばSD) 状態でないとき (そして他の要求している伝送エンティティがないことを仮定すれば)、ローカルの復旧待ち状態が起動する。この状態は、最優先になるので、それはAPS信号 (適用できるならば) 上で示され、以前に故障した運用系からの通常トラヒック信号を非運用系に維持する。この状態は、通常タイムアウトし、要求のないヌル信号となる。任意の高いプライオリティがこの状態を先取りするときは、切り戻り待ちタイマーはすぐに非活性化する。

11.14 エクササイズ動作

エクササイズは、APS通信が正しく動作しているかどうかを試験するためのコマンドである。それは、任意の「本当の」切替要求よりも低いプライオリティである。これは、応答を探すことによって意味のあるテストを得ることができる唯一の場所であるので、双方向切替切えにおいてのみ有効である。

エクササイズコマンドは、それにとって代わるNRかDNR要求と同じ要求およびブリッジ信号の番号を伴うコマンドを発行する。1フェーズAPSプロトコルでは、有効な応答は、対応する要求およびブリッジ信号番号を伴うNRになるはずである。DNRへの通常の応答は、NRよりもDNRなるにちがいない。エクササイズコマンドがクリアされたとき、もし要求信号の番号が0ならばNR、通常トラヒック信号の番号が1ならばDNRと入れ替える。

11.15 プロトコル障害の失敗

この勧告で定義されたAPSプロトコルに対するプロトコル障害 (dFOP)の検出と解除失敗の条件について、表11-2で説明する。

表11-2/G.8031/Y.1342 – dFOP発生/解除条件

完全な非互換性プロビジョニング ("B"ビット不一致)	
Entry criteria	22.5秒の間、非互換性の「B」ビット値を伴う3つのAPSフレーム受信
Exit criteria	互換性を持つ「B」ビット値を伴う最初のAPSフレーム受信
プロテクションスイッチ不全	
Entry criteria	送信された「要求信号」と受信された「ブリッジ信号」が50ms以上の間一致しない場合
Exit criteria	送信された「要求信号」の値と同じ「ブリッジ信号」の値を示す最初のAPSフレームの受信
運用系/非運用系構成不一致	
Entry criteria	22.5秒の間、運用系から3つのAPSフレームを受信
Exit criteria	22.5秒の間、運用系からAPSフレームを未受信
NOTE – たとえ2つのAPSフレームが失われても、22.5秒は3つのAPSフレームの受信を可能とする。	

もし未知の要求または無効な信号番号の要求が受け取られるならば、それは無視される。

表A.1/G.8031/Y.1342 – ローカル要求による状態遷移 (1:1、双方向、切り戻りモード)

State	Signalled APS	Local request										
		a	b	c	d	e	f	g	h	i	j	
		Lockout	Forced switch	SF on working	Working recovers from SF	SF on protection	Protection recovers from SF	Manual switch	Clear	Exercise	WTR timer expires	
A	No Request Working/Active Protection/Standby	NR [r/b=null]	→C	→D	→E ^{a)}	N/A	→F	N/A	→G	N/A	→I	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B) ^{b)} or →E	O	→F	N/A	→G	N/A	O	N/A
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	O	O	O	O	O	O	O	→A or →E ^{c)} →F ^{d)}	O	N/A
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→A or →E ^{c)}	O	N/A
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	N/A	O	N/A
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→C	O	O	O	N/A	→A	O	N/A	O	N/A
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→A	O	N/A
H	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	→A
I	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	N/A
J	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→I	N/A

NOTE 1 - "N/A" means that the event is not happen for the State. However if it does happen, the event should be ignored.
 NOTE 2 - "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.
 NOTE 3 - "(→X)" represents that the state is not changed and remains the same state.
^{a)} It transits to the state E if the Signal Fail still exists after hold-off timer expires.
^{b)} If FS is indicated in the received APS from the far end.
^{c)} If SF is reasserted.
^{d)} If SF-P is reasserted.

A.1.2 Far end requests

Table A.2 shows the state transition by a far end request received by APS for the 1:1 bidirectional protection switching in revertive mode.

表A.2/G.8031/Y.1342 – 遠隔要求による状態遷移 (1:1、 双方向、 切り戻りモード)

State		Signalled APS	Received far end request									
			k	l	m	n	o	p	q	r	s	t
			LO [r/b=null]	SF-P [r/b=null]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	WTR [r/b=normal]	EXER [r/b=null]	RR [r/b=null]	NR [r/b=null]	NR [r/b=normal]
A	No Request Working/Active Protection/Standby	NR [r/b=null]	(→A)	(→A)	→B	→B	→B	N/A	(→J)	(→A)	(→A) or →E ^{a)} or →F ^{b)}	(→A)
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	(→B)	N/A	N/A	→A or →E ^{a)}	→A or →H ^{c)}
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	(→C)	O	O	O	O	O	O	O	O	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→A	(→F)	O	O	O	O	O	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O
H	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→A	→A	→B	→B	→B	(→H)	O	O	N/A	O
I	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→A	→A	→B	→B	→B	N/A	(→I)	(→I)	O	N/A
J	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→A	→A	→B	→B	→B	N/A	(→J)	→A	→A	N/A
<p>NOTE 1 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.</p> <p>NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.</p> <p>NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.</p> <p>a) If SF is reasserted.</p> <p>b) If SF-P is reasserted.</p> <p>c) If the previous local state is SF.(see Clause 11.3)</p>												

A.2 State transition for 1:1 bidirectional switching with non-revertive mode

A.2.1 Local requests

Table A.3 shows the state transition by a local request for the 1:1 bidirectional protection switching in non-revertive mode.

表A.3/G.8031/Y.1342 – ローカル要求による状態遷移 (1:1、双方向、非切り戻りモード)

State		Signalled APS	Local request								
			a	b	c	d	e	f	g	h	i
			Lockout	Forced switch	SF on working	Working recovers from SF	SF on protection	Protection recovers from SF	Manual switch	Clear	Exercise
A	No Request Working/Active Protection/Standby	NR [r/b=null]	→C	→D	→E ^{a)}	N/A	→F	N/A	→G	N/A	→I
B	No Request Working/Standby	NR [r/b=normal]	→C	→D	(→B) ^{b)} or →E	N/A	→F	N/A	→G	N/A	O
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	O	O	O	O	O	O	O	→A or →E ^{c)} →F ^{d)}	O
D	Forced Switch Working/Standby	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→H or →E ^{c)}	O
E	Signal Fail (W) Working/Standby	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→C	O	O	O	N/A	→A	O	O	O
G	Manual Switch Working/Standby	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→H	O
H	Do Not Revert Working/Standby	DNR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→J
I	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→C	→D	→E	N/A	→F	N/A	→G	→A	O
J	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→H	O
K	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→I
L	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→J

NOTE 1 - "N/A" means that the event is not expected to happen for the State. However if it does happen, the events should be ignored.
 NOTE 2 - "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.
 NOTE 3 - "(→X)" represents that the state is not changed and remains the same state.
^{a)} It transits to the state E if the Signal Fail still exists after hold-off timer expires.
^{b)} If FS is indicated in the received APS from the far end.
^{c)} If SF is reasserted.
^{d)} If SF-P is reasserted.

A.2.2 Far end requests

Table A.4 shows the state transition by a far end request received by APS for the 1:1 bidirectional protection switching in non-revertive mode.

表A.4/G.8031/Y.1342 – 遠隔要求による状態遷移 (1:1、双方向、非切り戻りモード)

State	Signalled APS	Received far end request												
		j	k	l	m	n	o	p	q	R	s	t	u	
		LO [r/b=null]	SF-P [r/b=null]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	EXER [r/b=null]	EXER [r/b=normal]	RR [r/b= null]	RR [r/b= normal]	NR [r/b=null]	NR [r/b=normal]	DNR [r/b=normal]	
A	No Request Working/Active Protection/Standby	NR [r/b=null]	(→A)	(→A)	→B	→B	→B	(→K)	N/A	(→A)	N/A	(→A) or →E ^{a)} or →F ^{b)}	(→A)	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	N/A	N/A	N/A	N/A	→A or →E ^{a)}	→H	→H
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	(→C)	O	O	O	O	O	O	O	O	O	O	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O	O	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→A	(→F)	O	O	O	O	O	O	O	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O	O	O
H	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→L)	N/A	(→H)	O	O	(→H)
I	Exercise Working/Active Protection/Standby	EXER[r/b=null]	→A	→A	→B	→B	→B	(→I)	N/A	(→I)	N/A	O	O	N/A
J	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→J)	N/A	(→J)	O	O	O
K	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→A	→A	→B	→B	→B	(→K)	N/A	→A	N/A	→A	N/A	N/A
L	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→L)	N/A	→H	N/A	N/A	→H
		NOTE 1 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the events should be ignored. NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority. NOTE 3 – "(→X)" represents that the state is not changed and remains the same state. a) If SF is reasserted. b) If SF-P is reasserted.												

A.3 State transition for 1+1 bidirectional switching with revertive mode

A.3.1 Local requests

Table A.5 shows the state transition by a local request for the 1+1 bidirectional protection switching in revertive mode.

表A.5/G.8031/Y.1342 – ローカル要求による状態遷移 (1+1、双方向、切り戻りモード)

State		Signalled APS	Local request									
			a	b	c	d	e	f	g	h	i	j
			Lockout	Forced switch	Signal fail on working	Working recovers from SF	SF on protection	Protection recovers from SF	Manual switch	Clear	Exercise	WTR timer expires
A	No Request Working/Active Protection/Standby	NR [r/b=null/normal]	→C	→D	→E ^{a)}	N/A	→F	N/A	→G	N/A	→I	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B) ^{b)} or →E	O	→F	N/A	→G	N/A	O	N/A
C	Lockout Working/Active Protection/Standby	LO [r/b= null/normal]	O	O	O	O	O	O	O	→A or →E ^{c)} →F ^{d)}	O	N/A
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→A or →E ^{c)}	O	N/A
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	N/A	O	N/A
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b= null/normal]	→C	O	O	O	N/A	→A	O	N/A	O	N/A
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→A	O	N/A
H	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	→A
I	Exercise Working/Active Protection/Standby	EXER [r/b=null/normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	N/A
L	Reverse Request Working/Active Protection/Standby	RR [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→I	N/A

NOTE 1 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.
 NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.
 NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.
^{a)} It transits to the state E if the Signal Fail still exists after hold-off timer expires.
^{b)} If FS is indicated in the received APS from the far end.
^{c)} If SF is reasserted.
^{d)} If SF-P is reasserted.

A.3.2 Far end requests

Table A.6 shows the state transition by a far end request received by APS for the 1+1 bidirectional protection switching in revertive mode.

表A.6/G.8031/Y.1342 – 遠隔要求による状態遷移 (1+1、双方向、切り戻りモード)

State	Signalled APS	Received far end request									t	
		k	l	m	n	o	p	q	r	s		
		LO [r/b= null/normal]	SF-P [r/b= null/normal]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	WTR [r/b=normal]	EXER [r/b=null/normal]	NR [r/b=null/normal]	NR [r/b=normal]		
A	No Request Working/Active Protection/Standby	NR [r/b=null/normal]	(→A)	(→A)	→B	→B	→B	N/A	(→A)	(→A)	(→A) or →E ^{a)} or →F ^{b)}	(→A)
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	(→B)	N/A	N/A	→A or →E ^{a)}	→A or →H ^{c)}
C	Lockout Working/Active Protection/Standby	LO [r/b= null/normal]	(→C)	O	O	O	O	O	O	O	O	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b= null/normal]	→A	(→F)	O	O	O	O	O	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O
H	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→A	→A	→B	→B	→B	(→H)	O	O	N/A	O
I	Exercise Working/Active Protection/Standby	EXER [r/b=null/normal]	→A	→A	→B	→B	→B	N/A	(→I)	(→I)	O	N/A
J	Reverse Request Working/Active Protection/Standby	RR [r=null, b=normal]	→A	→A	→B	→B	→B	N/A	(→J)	→A	→A	N/A

NOTE 1 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.
NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.
^{a)} If SF is reasserted.
^{b)} If SF-P is reasserted.
^{c)} If the previous local state is SF (see Clause 11.3)

A.4 State transition for 1+1 bidirectional switching with non-revertive mode

A.4.1 Local requests

Table A.7 shows the state transition by a local request for the 1+1 bidirectional protection switching in non-revertive mode.

表A.7/G.8031/Y.1342 – ローカル要求による状態遷移（1+1、双方向、非切り戻りモード）

State		Signalled APS	Local request								
			a	b	c	d	e	f	g	h	i
			Lockout	Forced switch	SF on working	Working recovers from SF	SF on protection	Protection recovers from SF	Manual switch	Clear	Exercise
A	No Request Working/Active Protection/Standby	NR [r/b=null/normal]	→C	→D	→E ^{a)}	N/A	→F	N/A	→G	O	→I
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B) ^{b)} or →E	N/A	→F	N/A	→G	O	O
C	Lockout Working/Active Protection/Standby	LO [r/b= null/normal]	O	O	O	O	O	O	O	→A or →E ^{c)} →F ^{d)}	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→H or →E ^{c)}	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b= null/normal]	→C	O	O	O	N/A	→A	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→H	O
H	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→J
I	Exercise Working/Active Protection/Standby	EXER [r/b=null/normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O
J	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→H	O
K	Reverse Request Working/Active Protection/Standby	RR [r/b=null/normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→I
L	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→J

NOTE 1 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.
NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.
^{a)} It transits to the state E if the Signal Fail still exists after hold-off timer expires.
^{b)} If FS is indicated in the received APS from the far end.
^{c)} If SF is reasserted.
^{d)} If SF-P is reasserted.

A.4.2 Far end requests

Table A.8 shows the state transition by a far end request received by APS for the 1+1 bidirectional protection switching in non-revertive mode.

表A.8/G.8031/Y.1342 – 遠隔要求による状態遷移 (1+1 双方向、非切り戻りモード)

State	Signalled APS	Received far end request												
		j	k	l	m	n	o	p	q	r	s	t	u	
		LO [r/b= null/normal]	SF-P [r/b= null/normal]	FS [r/b=normal]	SF [r/b= /normal]	MS [r/b=normal]	EXER [r/b=null/normal]	EXER [r/b=normal]	RR [r=null, b=normal]	RR [r/b= normal]	NR [r/b=null/normal]	NR [r/b=normal]	DNR [r/b=normal]	
A	No Request Working/Active Protection/Standby	NR [r/b= null/normal]	(→A)	(→A)	→B	→B	→B	→K	N/A	(→A)	N/A	(→A) or →E ^{a)} or →F ^{b)}	(→A)	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	N/A	N/A	N/A	N/A	→A or →E ^{a)}	→H	→H
C	Lockout Working/Active Protection/Standby	LO [r/b= null/normal]	(→C)	O	O	O	O	O	O	O	O	O	O	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O	O	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b= null/normal]	→A	(→F)	O	O	O	O	O	O	O	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O	O	O
H	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→A	→A	→B	→B	→B	N/A	→L	N/A	(→H)	O	O	(→H)
I	Exercise Working/Active Protection/Standby	EXER [r/b= null/normal]	→A	→A	→B	→B	→B	(→I)	N/A	(→I)	N/A	O	N/A	N/A
J	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→J)	N/A	(→J)	N/A	O	O
			→A	→A	→B	→B	→B	(→K)	N/A	→A	N/A	→A	N/A	N/A
			→A	→A	→B	→B	→B	N/A	(→L)	N/A	→H	N/A	N/A	→H

NOTE 1 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.

^{a)} If SF is reasserted.

^{b)} If SF-P is reasserted.

A.5 State transition for 1+1 unidirectional switching with revertive mode

A.5.1 Local requests

Table A.9 shows the state transition by a local request for the 1+1 unidirectional protection switching in revertive mode.

表A.9/G.8031/Y.1342 – ローカル要求による状態遷移 (1+1、片方向、切り戻モード)

State		Local request									
		a	b	c	d	e	f	g	h	i	j
		Lockout	Forced switch	Signal fail on working	Working recovers from SF	Signal fail on protection	Protection recovers from SF	Manual switch	Clear	Exercise	WTR timer expired
A	No Request Working/Active Protection/Standby	→B	→C	→D ^{a)}	N/A	→E	N/A	→F	O	N/A	N/A
B	Lockout Working/Active Protection/Standby	O	O	O	O	O	O	O	→A or →D ^{b)} →E ^{c)}	N/A	N/A
C	Forced Switch Working/Standby Protection/Active	→B	O	O	O	→E	N/A	O	→A or →D ^{c)}	N/A	N/A
D	Signal Fail (W) Working/Standby Protection/Active	→B	→C	N/A	→G	→E	N/A	O	O	N/A	N/A
E	Signal Fail (P) Working/Active Protection/Standby	→B	O	O	O	N/A	→A	O	O	N/A	N/A
F	Manual Switch Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	O	→A	N/A	N/A
G	Wait to Restore Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	→F	→A	N/A	→A

NOTE 1 - "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.
 NOTE 2 - "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

^{a)} It transits to the state D if the Signal Fail still exists after hold-off timer expires.
^{b)} If SF is reasserted.
^{c)} If SF-P is reasserted.

A.6 State transition for 1+1 unidirectional switching with non-revertive mode

A.6.1 Local Requests

Table A.10 shows the state transition by a local request for the 1+1 unidirectional protection switching in non-revertive mode.

表A.10/G.8031/Y.1342 – ローカル要求による状態遷移 (1+1、片方向、非切り戻りモード)

State		Local request								
		a	b	c	d	e	f	g	i	j
		Lockout	Forced switch	Signal fail on working	Working recovers from SF	Signal fail on protection	Protection recovers from SF	Manual switch	Clear	Exercise
A	No Request Working/Active Protection/Standby	→B	→C	→D ^{a)}	N/A	→E	N/A	→F	O	N/A
B	Lockout Working/Active Protection/Standby	O	O	O	O	O	O	O	→A or →D ^{b)} →E ^{c)}	N/A
C	Forced Switch Working/Standby Protection/Active	→B	O	O	O	→E	N/A	O	→G or →D ^{b)}	N/A
D	Signal Fail (W) Working/Standby Protection/Active	→B	→C	N/A	→G	→E	N/A	O	O	N/A
E	Signal Fail (P) Working/Active Protection/Standby	→B	O	O	O	N/A	→A	O	O	N/A
F	Manual Switch Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	O	→G	N/A
G	Do Not Revert Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	→F	O	N/A

NOTE 1 - "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 - "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

a) It transits to the state D if the Signal Fail still exists after hold-off timer expires.

b) If SF is reasserted.

c) If SF-P is reasserted.

Appendix I

1-フェーズ APSプロトコルの動作例

1.1 はじめに

ここでは、1-フェーズ APS プロトコル(1:1 での切り戻し、または非切り戻りモード)の動作例を示す。

1.2 動作シナリオ例

1.2.1 切り戻りモード

この例は以下の動作シナリオを仮定する。

1. 保護されたドメインは障害の無い状態で動作している（運用系エンティティを選択中）。
2. このとき、SF（信号故障）が WEST から EAST 方向において発生する（非運用系エンティティに切替）。
3. その後、障害が復旧する（WTR 状態に移行し非運用系エンティティ選択状態が維持される）。
4. その後、WTR 時間が経過する（運用系エンティティに切り戻る）。

1.2.2 非切り戻りモード

この例は以下の動作シナリオを仮定する。

1. プロテクションドメインは障害の無い状態で動作している（運用系エンティティを選択中）。
2. このとき、SF（信号故障）が WEST から EAST 方向において発生する（非運用系エンティティに切替）。
3. その後、障害が復旧する（DNR 状態に移行し非運用系エンティティ選択状態が維持される）。

1.2.3 信号故障と強制切替

この例は以下の動作シナリオを仮定する。

1. SF（信号故障）が WEST から EAST 方向において発生する（非運用系エンティティに切替）。
2. その後、FS（強制切替）コマンドが EAST 側にて受信される（FS 状態に移行する）。
3. その後、FS（強制切替）が EAST 側にて解除され、SF が EAST において再度検出される。

I.3 APS プロトコルの例

APS プロトコルの例を図 I.1(切り戻りモード)、図 I.2(非切り戻りモード)、図 I.3 (SF と FS) に示す。

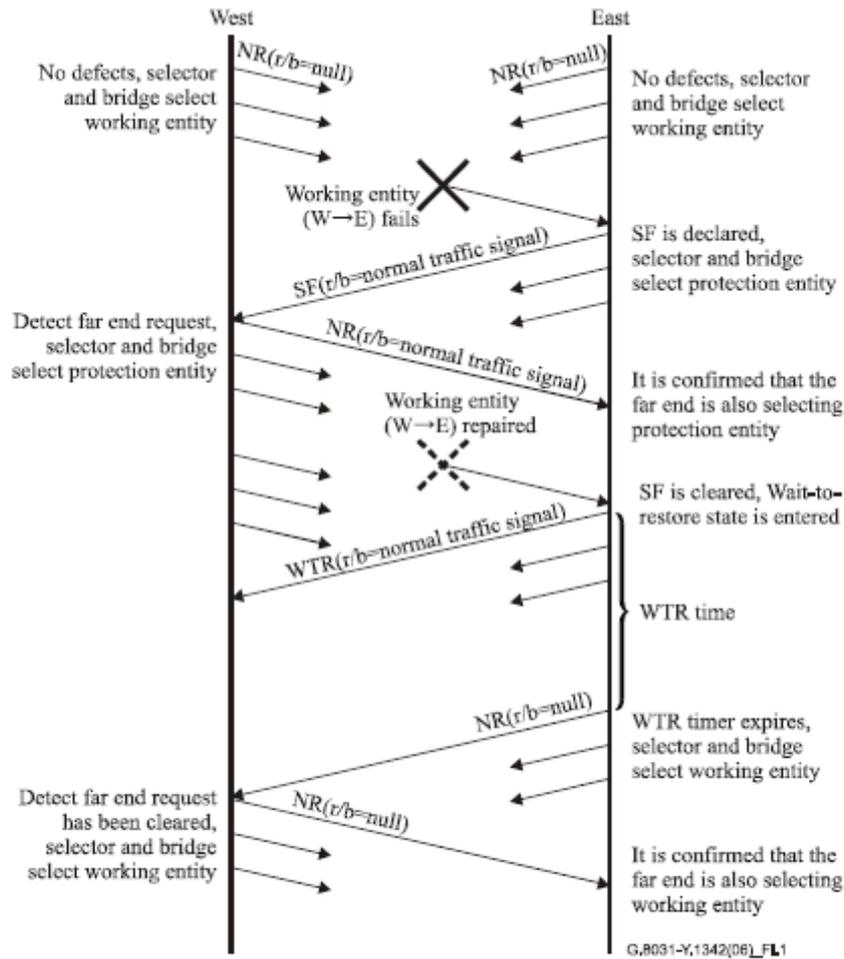


図 I.1/G.8031/Y.1342 - プロトコル例(切り戻りモード)

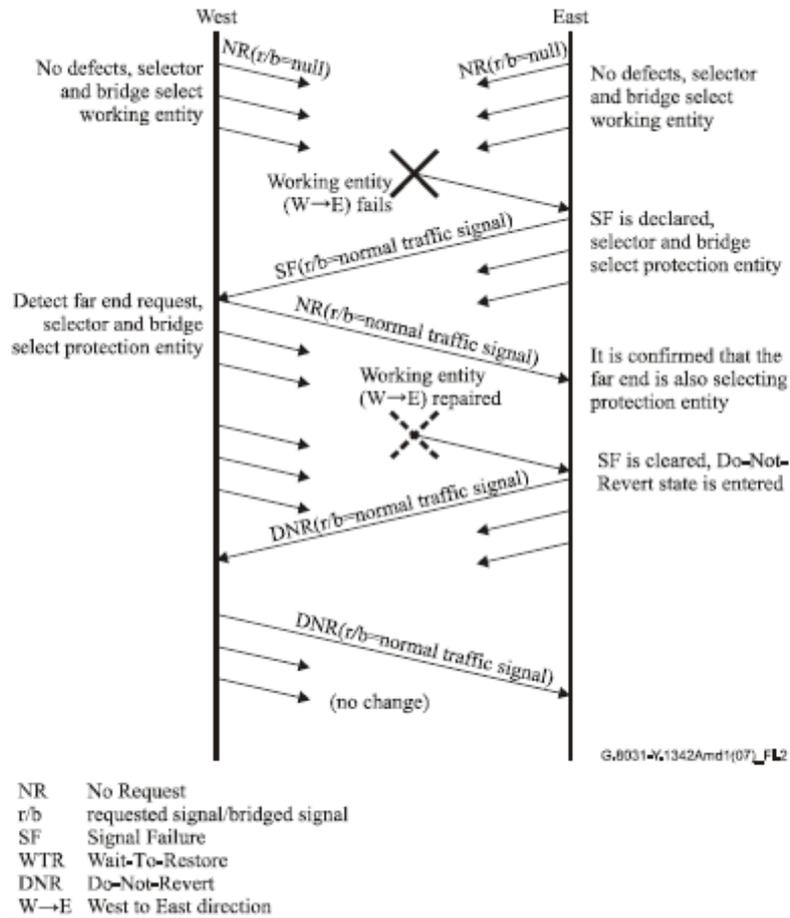


図 I.2/G.8031/Y.1342 - プロトコル例(非切り戻りモード)

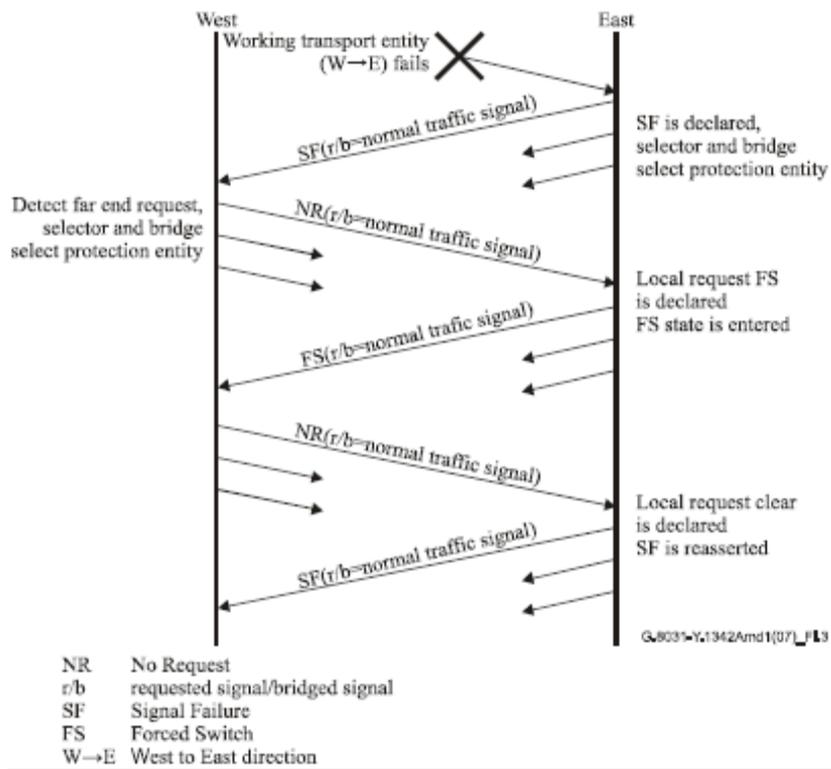


図 I.3/G.8031/Y.1342 - プロトコル例(SF と FS)

Appendix II

イーサネットプロテクションスイッチとSTP間の相互作用

ここでは、STP とイーサネットプロテクションスイッチの間における不要な相互作用を回避するために、プロテクションドメイン内のブリッジポートが、STP ドメインに参加してはいけないことを示す。これを回避する1つの方法は、プロテクションドメイン内のSTPを無効にすることである。しかし、プロテクションドメインの外にあるドメインはSTPが有効に設定されると考えられる。もう1つ方法は、ワーキングとプロテクションの転送エンティティが異なるSTPドメインに属することである。これらの2つのシナリオは、次のセクションで議論する。

図 II.1 は上述の1つ目の方法を示している。つまり、プロテクションドメインとSTPドメイン(#1と#2)が縦に区切られており重複していない。プロテクションドメインとSTPドメインの端に位置するブリッジ#Aと#Bは、ループ問題の無い状態においてSTPドメイン間で相互接続される。

上述の二つ目のケースは図 II.2 に示される。STPドメイン(#1と#2)は横に区切られており、イーサネットプロテクションスイッチのための二つの伝送エンティティを提供する。図 II.3 はイーサネットプロテクションスイッチのための二つの伝送エンティティが、異なるSTPドメイン内で独立して配備されている。この例では、それぞれのVLANとネットワークリソースが、有効に利用されるだろう。

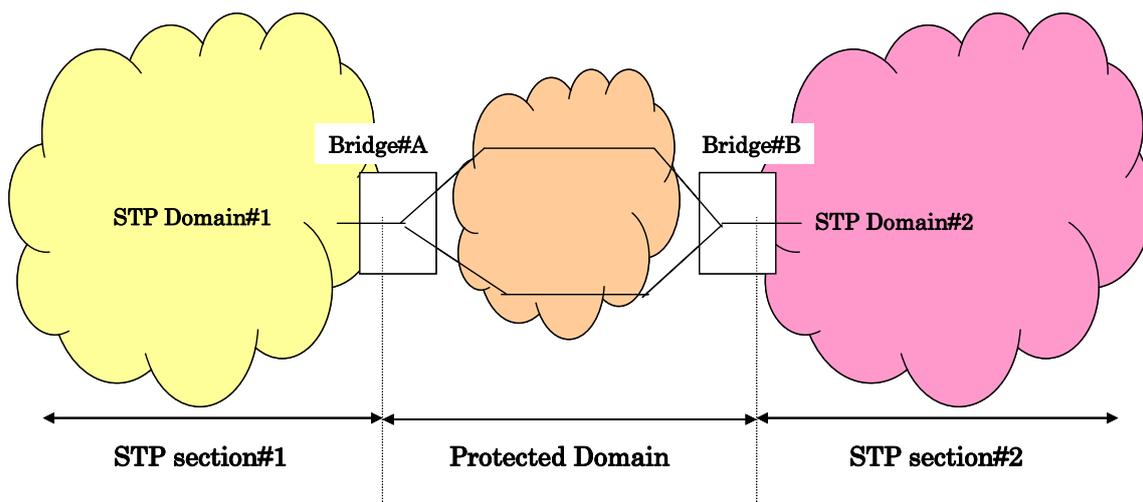


図 II.1/G.8031/Y.1342 –プロテクションドメインとSTPドメイン間で重複が無いケース

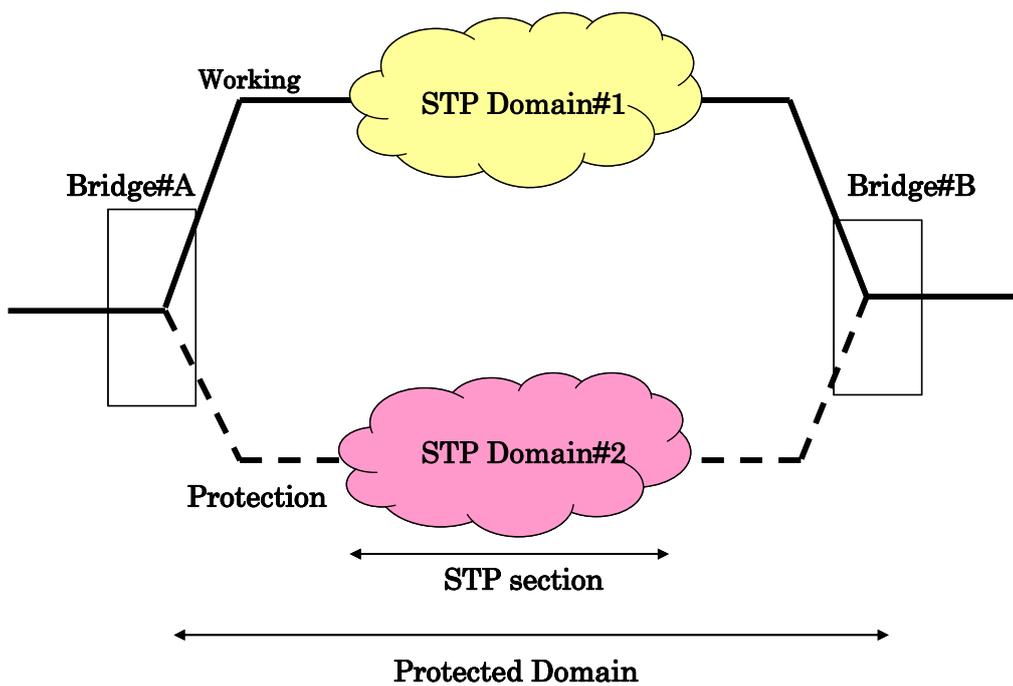


図 II.2/G.8031/Y.1342 -プロテクションドメインと STP ドメイン間で重複が有るケース

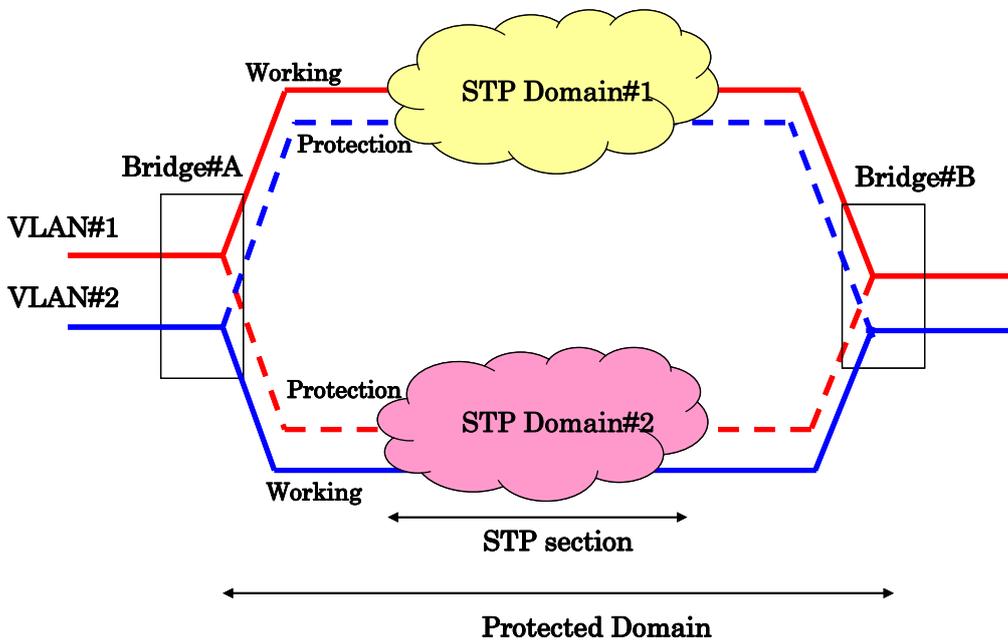


図 II.3/G.8031/Y.1342 -VLAN ごとにプロテクションドメインと STP ドメイン間で重複が有るケース

Appendix III
 プロテクションスイッチ環境のためのMIPs

III.1 はじめに

この付録では、プロテクションスイッチ環境のための MIPs の構成例と考察を示す。

III.2 考察

図 III.1 はプロテクションスイッチのための MEPs と MIPs 構成の例を示している。図 III.1 において、MEPs の 2 つのペアはワーキングとプロテクションの両方の伝送エンティティを MEG レベル N で監視するために構成されている。MEG レベル N+1 も同様に MEPs と MIPs がそれぞれのポートにおいて図のように構成される。

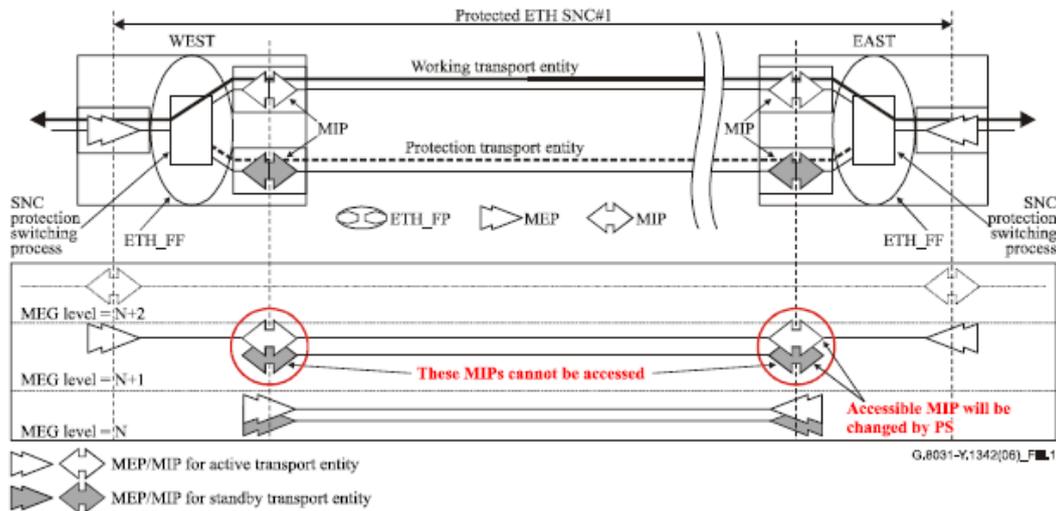


図 III.1/G.8031/Y.1342- 1:1 双方向プロテクションスイッチのための MEPs と MIPs

もし、1:1 プロテクションスイッチが構成される場合、待機側の伝送エンティティにおける MEG レベル N+1 の MIPs は、同一の MEG に対して MEPs によってアクセスすることはできない。そして、アクセス可能な MIPs はプロテクションスイッチによって切り替わるだろう。そのため、図 III.1 に示される MEG レベル N+1 の MIPs は不要であることが分かる。

図 III.2 は 1+1 片方向プロテクションスイッチ環境のための MEPs と MIPs の構成を示している。このケースでは、MEP と MIP 間の要求/応答の通信を正しく行うことができない。そのため、図 III.2 に示される MEG レベル N+1 の MIPs は不要であることが分かる。

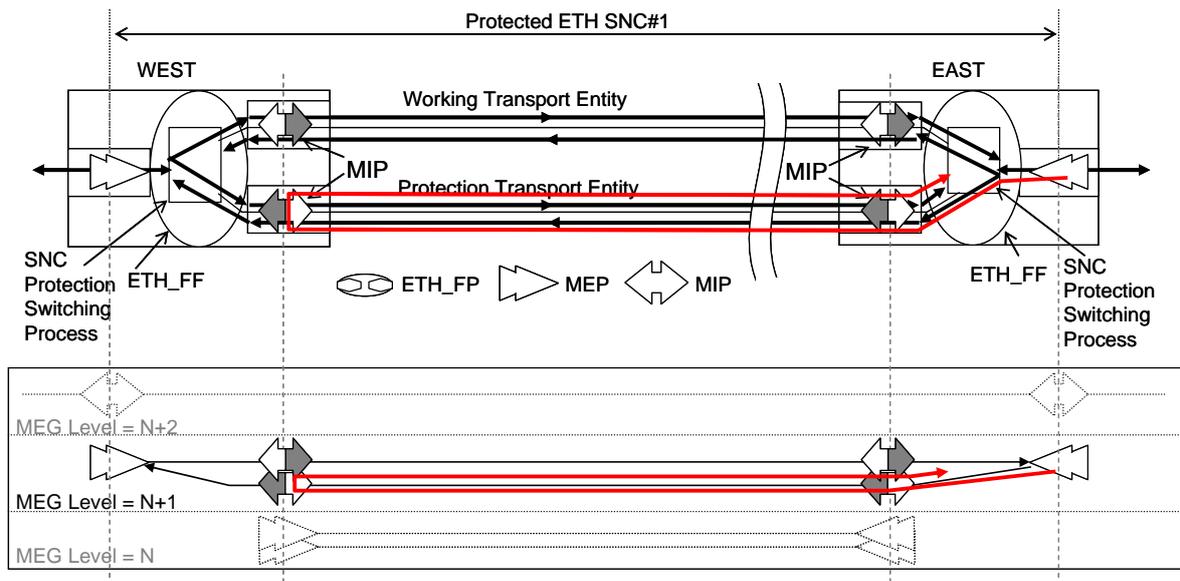


図 III.2/G.8031/Y.1342 -1+1 片方向プロテクションスイッチのための MEPs と MIPs

上述のように、ワーキングとプロテクション両方の伝送エンティティを監視する MEPs のそれよりも高次の MEG レベルに対して、プロテクションドメイン内のどこに MIPs を構成しても不要であることが分かる。

III.3 構成例

図 III.3 は有効な MEPs と MIPs 構成の例を示す。図 III.3 の中段にある最初の例は、MEG レベル N+1 において MIPs は構成されないが、MEPs が変わりに構成される。このケースでは、MEG レベル N+1 の MEG はプロテクションドメインを表す。

図 III.3 の下段に二つ目の例が示されている。この構成では、MIPs はプロテクションドメインの端点において MEG レベル N+1 内で構成される。

両例で示される MEPs と MIPs は、それぞれが同じプロテクションドメイン内で構成されないため、アクセス可能である。

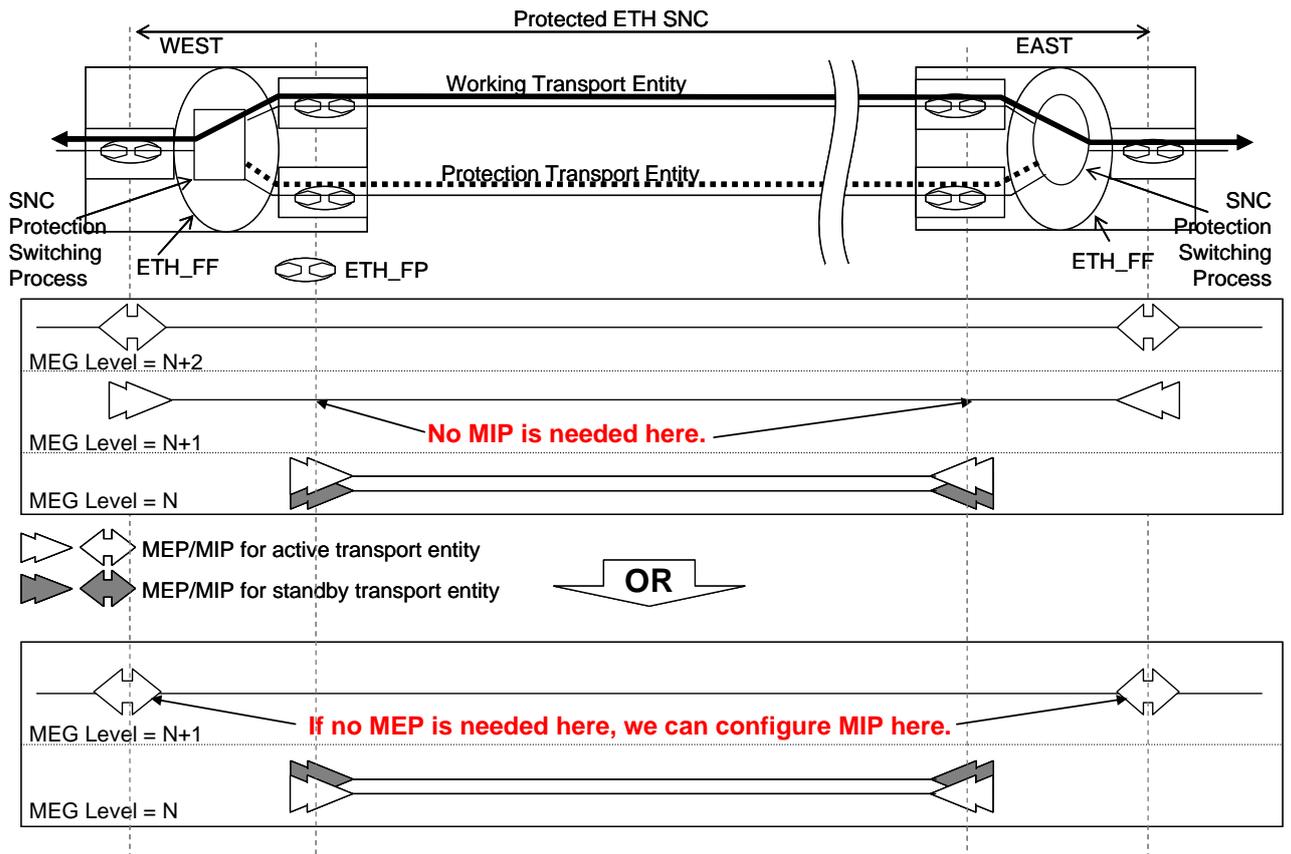


図 III.3/G.8031/Y.1342- プロテクション構成環境のための MEPs と MIPs の構成例