

International Telecommunication Union

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**G.8031/Y.1342**

(06/2006)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA,  
DIGITAL SYSTEMS AND NETWORKS

Ethernet over Transport aspects – General aspects

SERIES Y: GLOBAL INFORMATION  
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS  
AND NEXT-GENERATION NETWORKS

Internet protocol aspects – Transport

---

## **Ethernet Protection Switching**

ITU-T Recommendation G.8031/Y.1342



ITU-T G-SERIES RECOMMENDATIONS  
TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
ETHERNET OVER TRANSPORT ASPECTS	G.8000–G.8999
<b>General aspects</b>	<b>G.8000–G.8099</b>
MPLS over Transport aspects	G.8100–G.8199
Quality and availability targets	G.8200–G.8299
ACCESS NETWORKS	G.9000–G.9999

*For further details, please refer to the list of ITU-T Recommendations.*





# **ITU-T Recommendation G.8031/Y.1342**

## **Ethernet Protection Switching**

### **Summary**

This Recommendation describes the specifics of protection switching for Ethernet VLAN signals. Included are details pertaining to ETH protection characteristics, architectures and the APS protocol. The protection scheme considered in this Recommendation is:

- VLAN-based Ethernet subnetwork connection protection with sublayer monitoring.

### **Source**

ITU-T Recommendation G.8031/Y.1342 was approved on 6 June 2006 by ITU-T Study Group 15 (2005-2008) under the ITU-T Recommendation A.8 procedure.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2007

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

## CONTENTS

	<b>Page</b>
1	Scope ..... 1
2	References..... 1
3	Definitions ..... 2
4	Abbreviations..... 4
5	Conventions ..... 5
	5.1 Representation of octets ..... 5
6	Introduction ..... 6
7	Requirements ..... 6
8	Protection characteristics ..... 7
	8.1 Monitoring methods and conditions ..... 7
9	Protection group commands ..... 8
	9.1 End-to-end commands and states ..... 8
	9.2 Local commands..... 8
10	Protection architectures ..... 9
	10.1 Unidirectional and bidirectional switching ..... 9
	10.2 Need for APS communication..... 9
	10.3 Revertive and non-revertive switching..... 9
	10.4 Provisioning mismatches..... 10
	10.5 Protection switching trigger ..... 10
	10.6 Protection switching models..... 11
11	APS Protocol ..... 16
	11.1 APS format ..... 16
	11.2 1-phase APS protocol ..... 18
	11.3 Request type ..... 20
	11.4 Protection types ..... 20
	11.5 Requested signal..... 21
	11.6 Bridged signal..... 21
	11.7 Control of bridge ..... 21
	11.8 Control of selector ..... 21
	11.9 Signal fail of the protection transport entity..... 21
	11.10 Equal priority requests..... 21
	11.11 Command acceptance and retention..... 21
	11.12 Hold-off timer..... 22
	11.13 Wait-to-restore timer ..... 22
	11.14 Exercise operation ..... 22
	11.15 Failure of protocol defects..... 23

	<b>Page</b>
Annex A – State transition tables of protection switching.....	23
A.1    State transition for 1:1 bidirectional switching with revertive mode .....	23
A.2    State transition for 1:1 bidirectional switching with non-revertive mode .....	26
A.3    State transition for 1+1 bidirectional switching with revertive mode .....	28
A.4    State transition for 1+1 bidirectional switching with non-revertive mode .....	30
A.5    State transition for 1+1 unidirectional switching with revertive mode .....	32
A.6    State transition for 1+1 unidirectional switching with non-revertive mode .....	33
Appendix I – Operation example of 1-phase APS protocol.....	34
I.1    Introduction .....	34
I.2    Example scenario.....	34
I.3    APS protocol examples .....	34
Appendix II – Interaction between Ethernet protection switching and STP.....	38
Appendix III – MIPs for protection switching environment.....	40
III.1    Introduction .....	40
III.2    Considerations .....	40
III.3    Configuration examples.....	41



# ITU-T Recommendation G.8031/Y.1342

## Ethernet Protection Switching

### 1 Scope

This Recommendation defines the APS protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC in Ethernet transport networks. All other protection schemes including point-to-multipoint and multipoint-to-multipoint are for further study.

Linear 1+1 and 1:1 protection switching architectures with unidirectional and bidirectional switching are defined in this version of the Recommendation.

The APS protocol and protection switching operation for all other Ethernet network architectures (for example ring, mesh, etc.) are for further study.

### 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- 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 Definitions**

This Recommendation uses terms defined in ITU-T Rec. G.780/Y.1351.

#### **3.1 bidirectional protection switching**

#### **3.2 unidirectional protection switching**

This Recommendation uses terms defined in ITU-T Rec. G.805:

#### **3.3 adapted information**

#### **3.4 characteristic information**

#### **3.5 link**

#### **3.6 link connection**

#### **3.7 signal degrade (SD)**

#### **3.8 signal fail (SF)**

#### **3.9 tandem connection**

#### **3.10 trail**

#### **3.11 trail termination**

This Recommendation uses terms defined in ITU-T Rec. G.806:

#### **3.12 atomic function**

#### **3.13 defect**

#### **3.14 failure**

#### **3.15 server signal fail (SSF)**

#### **3.16 trail signal fail (TSF)**

This Recommendation uses terms defined in ITU-T Rec. G.870/Y.1352:

#### **3.17 APS protocol**

##### **3.17.1 1-phase**

#### **3.18 protection class**

##### **3.18.1 individual**

##### **3.18.2 group**

##### **3.18.3 network connection protection**

##### **3.18.4 subnetwork connection protection**

###### **3.18.4.1 sublayer monitored (/S)**

###### **3.18.4.2 non-intrusive monitored**

###### **3.18.4.3 inherent monitored**

###### **3.18.4.4 test monitored (/T)**

#### **3.18.5 trail protection**

#### **3.19 switch**

- 3.20 component**
  - 3.20.1 protected domain**
  - 3.20.2 bridge**
    - 3.20.2.1 permanent bridge**
    - 3.20.2.2 selector bridge**
  - 3.20.3 selector**
    - 3.20.3.1 selective selector**
    - 3.20.3.2 merging selector**
  - 3.20.4 head end**
  - 3.20.5 tail end**
  - 3.20.6 sink node**
  - 3.20.7 source node**
  - 3.20.8 intermediate node**
- 3.21 architecture**
  - 3.21.1 1+1 protection architecture**
  - 3.21.2 1:n protection architecture**
  - 3.21.3 (1:1)<sup>n</sup> protection architecture**
- 3.22 signal**
  - 3.22.1 traffic signal**
  - 3.22.2 normal traffic signal**
  - 3.22.3 extra traffic signal**
  - 3.22.4 null signal**
- 3.23 time**
  - 3.23.1 detection time**
  - 3.23.2 hold-off time**
  - 3.23.3 wait-to-restore time**
  - 3.23.4 switching time**
- 3.24 transport entity**
  - 3.24.1 protection transport entity**
  - 3.24.2 working transport entity**
  - 3.24.3 active transport entity**
  - 3.24.4 standby transport entity**
- 3.25 protection**
- 3.26 impairment**
- 3.27 protection ratio**

This Recommendation uses terms defined in ITU-T Rec. G.809:

- 3.28 adaptation**
- 3.29 flow**
- 3.30 flow domain**
- 3.31 flow point**
- 3.32 flow termination**
- 3.33 layer network**
- 3.34 link flow**
- 3.35 network**
- 3.36 port**
- 3.37 transport**
- 3.38 transport entity**
- 3.39 termination flow point**

This Recommendation uses terms defined in ITU-T Rec. G.8010/Y.1306:

- 3.40 Ethernet characteristic information (ETH\_CI)**
- 3.41 Ethernet flow point (ETH\_FP)**
- 3.42 maintenance entity**
- 3.43 maintenance entity group**
- 3.44 maintenance entity group level**

This Recommendation uses terms defined in ITU-T Rec. G.8021/Y.1341:

- 3.45 Ethernet flow forwarding function (ETH\_FF)**

This Recommendation uses terms defined in ITU-T Rec. M.495:

- 3.46 transfer time (Tt)**

This Recommendation uses terms defined and described in ITU-T Recs G.8010/Y.1306 and Y.1731:

- 3.47 maintenance entity group end point (MEP)**

## **4 Abbreviations**

This Recommendation uses the following abbreviations:

AI	Adapted Information
APS	Automatic Protection Switching
CCM	Continuity Check Message
CI	Characteristic Information
DNR	Do Not Revert
EC	Ethernet Connection
ETH	Ethernet layer network
ETH-AIS	Ethernet Alarm Indication Signal function

ETH-APS	Ethernet Automatic Protection Switching function
ETH-CC	Ethernet Continuity Check function
EXER	Exercise
FS	Forced Switch
FT	Flow Termination
LCK	Locked
LO	Lockout for protection
LOC	Loss of Continuity
LSB	Least Significant Bit
MEP	Maintenance Entity Group End Point
MIP	Maintenance Entity Group Intermediate Point
MS	Manual Switch
MSB	Most Significant Bit
NR	No Request
OAM	Operation, Administration and Maintenance
PDU	Protocol Data Unit
PS	Protection Switching
RR	Reverse Request
RSTP	Rapid Spanning Tree Protocol
SD	Signal Degrade
SF	Signal Fail
SF-P	Signal Fail on Protection
SNC	Subnetwork Connection
SNC/I	Inherently monitored Subnetwork Connection
SNC/N	Non-intrusively monitored Subnetwork Connection
SNC/S	Sub-layer monitored Subnetwork Connection
SNC/T	Test-trail monitored Subnetwork Connection
VID	VLAN Identifier
VLAN	Virtual LAN
WTR	Wait to Restore

## **5 Conventions**

### **5.1 Representation of octets**

Octets are represented as defined in IEEE 802.1D.

When consecutive octets are used to represent a binary number, the lower octet number has the most significant value.

The bits in an octet are numbered from 1 to 8, where 1 is the least significant bit (LSB) and 8 is the most significant bit (MSB).

## 6 Introduction

This Recommendation specifies linear protection switching mechanisms to be applied to VLAN-based Ethernet networks as described in ITU-T Rec. G.8010/Y.1306. Protection switching is a fully allocated survivability mechanism. It is fully allocated in the sense that the route and bandwidth of the protection entity is reserved for a selected working entity. It provides a fast and simple survivability mechanism. It is easier for the network operator to grasp the status of the network (e.g., active network topology) with a protection switching than with other survivability mechanisms such as RSTP.

This Recommendation specifies linear 1+1 protection switching architecture and linear 1:1 protection switching architecture. The linear 1+1 protection switching architecture operates with either unidirectional or bidirectional switching. The linear 1:1 protection switching architecture operates with bidirectional switching.

In the linear 1+1 protection switching architecture, a protection transport entity is dedicated to each working transport entity. The normal traffic is copied and fed to both working and protection transport entities with a permanent bridge at the source of the protected domain. The traffic on working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made based on some predetermined criteria, such as server defect indication.

Although selection is made only at the sink of the protected domain in linear 1+1 protection switching architecture, bidirectional 1+1 protection switching needs APS coordination protocol so that selectors for both direction selects the same entity. On the other hand, unidirectional 1+1 protection switching does not need APS coordination protocol.

In the linear 1:1 protection switching architecture, the protection transport entity is dedicated to the working transport entity. However, the normal traffic is transported either on the working transport entity or on the protection transport entity using a selector bridge at the source of the protected domain. The selector at the sink of the protected domain selects the entity which carries the normal traffic. Since source and sink need to be coordinated to ensure that the selector bridge at the source and the selector at the sink select the same entity, APS coordination protocol is necessary.

## 7 Requirements

- 1) Ethernet protection switching should be applicable to Point-to-Point VLAN-based ETH SNC which provides connectivity between two ETH flow points in an ETH flow domain. VID(s) can be used to identify Point-to-Point VLAN based ETH SNC(s) within ETH links. Additional details on ETH and related atomic functions can be obtained from ITU-T Rec. G.8010/Y.1306. Other entities to be protected are for further study.
- 2) The protected domain should be configured such that 100% of the impaired working traffic should be protected for a failure on a single working entity.
- 3) Transfer time ( $T_t$ ) should be less than 50 ms.
- 4) The ETH layer connectivity of working transport entity and protection transport entity should be periodically monitored.
- 5) Subsequent to a protection switching event frames should be delivered in-order.  
NOTE – Subsequent to a protection switching event, frames may temporarily be lost or duplicated due to differential path delay.
- 6) Individual and group protection switching should be supported.

- 7) Revertive and non-revertive switching should be provided as network operator options.
- 8) A mismatch between the bridge-selector positions of the near end and the far end should be detected.
  - The bridge-selector mismatch for the local network element should be detected and reported.
  - The bridge-selector mismatch should be cleared by a network operator.
- 9) Operator requests such as lockout of protection, forced-switch and manual-switch commands should be supported.
- 10) Prioritized protection between Signal Fail (SF) and operator requests should be supported.
- 11) A provisionable "generic hold-off function" should be provided so as to delay the beginning of the protection switching action.

## **8 Protection characteristics**

### **8.1 Monitoring methods and conditions**

Protection switching will occur based on the detection of certain defects on the transport entities (working and protection) within the protected domain. How these defects are detected is the subject of the equipment Recommendations (e.g., ITU-T Rec. G.8021/Y.1341). For the purpose of the protection switching process, a transport entity within the protected domain has a condition of OK, failed (signal fail = SF), or degraded (signal degrade = SD) if applicable.

The customary monitoring methods are as follows:

**Inherent** – Inherent monitoring is based on defects detected by a trail termination function or adaptation function at the tail end. Ethernet subnetwork protection with inherent monitoring (SNC/I) is based on inherent monitoring.

**Non-intrusive** – Protection switching is triggered by a non-intrusive monitor at the tail end of the protection group. This allows protecting a segment of a trail that is not constrained by the beginning or end of the trail. Ethernet subnetwork protection with non-intrusive monitoring (SNC/N) is a linear protection based on non-intrusive monitoring. Non-intrusive monitoring may be based on monitoring of a layer or sub-layer (e.g., TCM non-intrusive monitoring).

**Sub-layer** – Ethernet subnetwork protection with sub-layer monitoring (SNC/S) is a linear protection architecture based on sub-layer monitoring. Each serial compound link connection is extended with tandem connection monitoring (TCM) or segment termination/adaptation functions to derive the fault condition status independent of the traffic signal present. For network layers supporting TCM, it is attractive to instantiate a TCM-monitored segment of a trail precisely across a protected segment so that protection switching is based only on defects within the protected segment. This has a further advantage over SNC/N in that defects that occur upstream of the protected segment will not be visible for the purpose of protection switching.

**Test Trail** – Defects are detected using extra test trail. An extra test trail is set up between source and sink of the protected domain, which includes a protection group of subnetwork connections. Ethernet subnetwork protection with test trail monitoring (SNC/T) is based on test trail monitoring that is applicable for group protection only.

The protection switching controller does not care which monitoring method is used, as long as it can be given (OK, SF, SD if applicable) information for the transport entities within the protected domain. Some monitors or network layers may not have an SD detection method. Where this is the case, there is no need to use a different APS protocol: it would simply happen that an SD would not be issued from equipment that cannot detect it. Where an APS protocol is used, the implementation

should not preclude the far end from declaring an SD over the APS protocol, even if the monitor at the near end cannot detect SD.

In this version of the Recommendation, SNC/S monitoring architecture is supported for point-to-point VLAN-based ETH SNC. Other monitoring methods such as SNC/I, SNC/N and SNC/T are for further study.

## 9 Protection group commands

### 9.1 End-to-end commands and states

This clause describes commands that apply to the protection group as a whole. When an APS protocol is present, these commands are signalled to the far end of the connection. In bidirectional switching, these commands affect the bridge and selector at both ends.

**Lockout of protection** – This command prevents a working signal from being selected from the protection transport entity. This effectively disables the protection group.

**Force switch normal traffic signal-to-protection** – Forces normal traffic signal to be selected from the protection transport entity.

**Manual switch normal traffic signal-to-protection** – In the absence of a failure of a working or protection transport entity, forces normal traffic signal to be selected from the protection transport entity.

**Wait-to-restore normal traffic signal** – In revertive operation, after the clearing of a SF (or SD if applicable) on the working transport entity, maintains normal traffic signal as selected from the protection transport entity until a Wait-to-Restore timer expires. The state will be changed to NR if the timer expires prior to any other event or command. This is used to prevent frequent operation of the selector in the case of intermittent failures.

**Exercise signal** – Exercise of the APS protocol. The signal is chosen so as not to modify the selector.

**Do-not-revert normal traffic signal** – In non-revertive operation, this is used to maintain a normal traffic signal selected from the protection transport entity.

**No request** – No Request is the state entered by the local priority under all conditions where no local protection switching requests (including wait-to-restore and do-not-revert) are active. Normal traffic signal is selected from the corresponding transport entity.

**Clear** – Clears the active near end Lockout of Protection, Forced Switch, Manual Switch, WTR state, or Exercise command.

### 9.2 Local commands

These commands apply only to the near end of the protection group. Even when an APS protocol is supported, they are not signalled to the far end.

**Freeze** – Freezes the state of the protection group. Until the freeze is cleared, additional near end commands are rejected. Condition changes and received APS information are ignored. When the Freeze command is cleared, the state of the protection group is recomputed based on the condition and received APS information.

#### Clear freeze

**Lockout normal traffic signal from protection** – Prevents normal traffic signal from being selected from the protection entity. Commands for normal traffic signal will be rejected. For normal traffic, any indication of SF (or SD if applicable) will be ignored. In bidirectional switching, remote bridge requests for normal traffic signal will still be honoured to prevent protocol failures. As a



result, a normal traffic signal must be locked out from the protection transport entity at both ends to prevent it being selected from the protection transport entity as a result of a command or failure at either end.

## **Clear lockout normal traffic signal from protection**

### **10 Protection architectures**

In the linear protection architecture defined in this version of the Recommendation, protection switching occurs at the two distinct endpoints of a point-to-point VLAN-based ETH SNC. Between these endpoints, there will be both "working" and "protection" transport entities.

For a given direction of transmission, the "head end" of the protected entity is capable of performing a bridge function, which will place a copy of a normal traffic signal onto a protection transport entity when required. The "tail end" will perform a selector function, where it is capable of selecting a normal traffic signal either from its usual working transport entity, or from a protection transport entity. In the case of bidirectional transmission, where both directions of transmission are protected, both ends of the protected entity will normally provide both bridge and selector functions.

The following architectures are possible:

**1+1** – In 1+1 architectures, a protection transport entity is employed to protect the normal traffic signal. At the head end, the bridge is permanent. Switching occurs exclusively at the tail end.

**1:1** – In 1:1 architectures, a protection transport entity is employed to protect the normal traffic signal. At the head end, the bridge is not established until a protection switch is required.

The architecture at each end of the protected domain must match.

#### **10.1 Unidirectional and bidirectional switching**

In the case of bidirectional transmission, it is possible to choose either unidirectional or bidirectional switching. With unidirectional switching, the selectors at each end are fully independent. With bidirectional switching, an attempt is made to coordinate the two ends so that both have the same bridge and selector settings, even for a unidirectional failure. Bidirectional switching always requires APS information to coordinate the two endpoints. Unidirectional switching can protect two unidirectional failures in opposite directions on different entities.

#### **10.2 Need for APS communication**

The only switching type that does NOT require APS communication is 1+1 unidirectional switching. With a permanent bridge at the head end and no need to coordinate selector positions at the two ends, the tail end selector can be operated entirely according to defects and commands received at the tail end.

Bidirectional switching always requires APS communication.

#### **10.3 Revertive and non-revertive switching**

In revertive operation, normal traffic signal is restored to the working transport entity after the condition(s) causing a switch has cleared. In the case of clearing a command (e.g., Forced Switch), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of a "Wait-to-Restore" timer, which is used to avoid chattering of selectors in the case of intermittent defects.

In non-revertive operation, normal traffic signal is allowed to remain on the protection transport entity even after a switch reason has cleared. This is generally accomplished by replacing the previous switch request with a "Do not Revert (DNR)" request, which is low priority.

1+1 protection is often provisioned as non-revertive, as the protection is fully dedicated in any case, and this avoids a second "glitch" to the normal traffic signal. There may, however, be reasons to provision this to be revertive (e.g., so that the normal traffic signal uses the "short" path except during failure conditions. Certain operator policies also dictate revertive operation even for 1+1).

1:1 protection is usually revertive. Although it is possible to define the protocol in a way that would permit non-revertive operation for 1:1 protection, however, since the working transport entity is typically more optimized (i.e., from a delay and resourcing perspective) than the protection transport entity, it is better to revert and glitch the normal traffic signal when the working transport entity is repaired.

In general, the choice of revertive/non-revertive will be the same at both ends of the protection group. However, a mismatch of this parameter does not prevent interworking; it just would be peculiar for one side to go to WTR for clearing of switches initiated from that side, while the other goes to DNR for its switches.

#### **10.4 Provisioning mismatches**

With all of the options for provisioning of protection groups, there are opportunities for mismatches between the provisioning at the two ends. These provisioning mismatches take one of several forms:

- Mismatches where proper operation is not possible.
- Mismatches where one or both sides can adapt their operation to provide a degree of interworking in spite of the mismatch.
- Mismatches that do not prevent interworking. An example is the revertive/non-revertive mismatch discussed in clauses 10.3 and 11.4.

Not all provisioning mismatches can be conveyed and detected by information passed through the APS communication. There are simply too many combinations of valid entity numbers to easily provide full visibility of all of the configuration options. What is desirable, however, is to provide visibility for the middle category, where the sides can adapt their operation to interwork in spite of the mismatch. For example, an equipment provisioned for bidirectional switching could fall back to unidirectional switching to allow interworking. An equipment provisioned for 1+1 switching with an APS communication could fall back to operate in 1+1 unidirectional switching without an APS communication. The user could still be informed of the provisioning mismatch, but a level of protection could still be provided by the equipment.

#### **10.5 Protection switching trigger**

For example, protection switching should be performed when:

- Initiated by operator control (e.g., Force Switch, Manual Switch) if it has a higher priority than any other local request or the far end request; or
- SF is declared on the active transport entity and is not declared on the standby transport entity, and the detected SF condition has a higher priority than any other local request or the far end request; or
- In the bidirectional 1+1 and 1:1 architecture, the received APS protocol requests to switch and it has a higher priority than any other local request.

Other cases are described as state transition in Annex A.

##### **10.5.1 Signal fail declaration conditions**

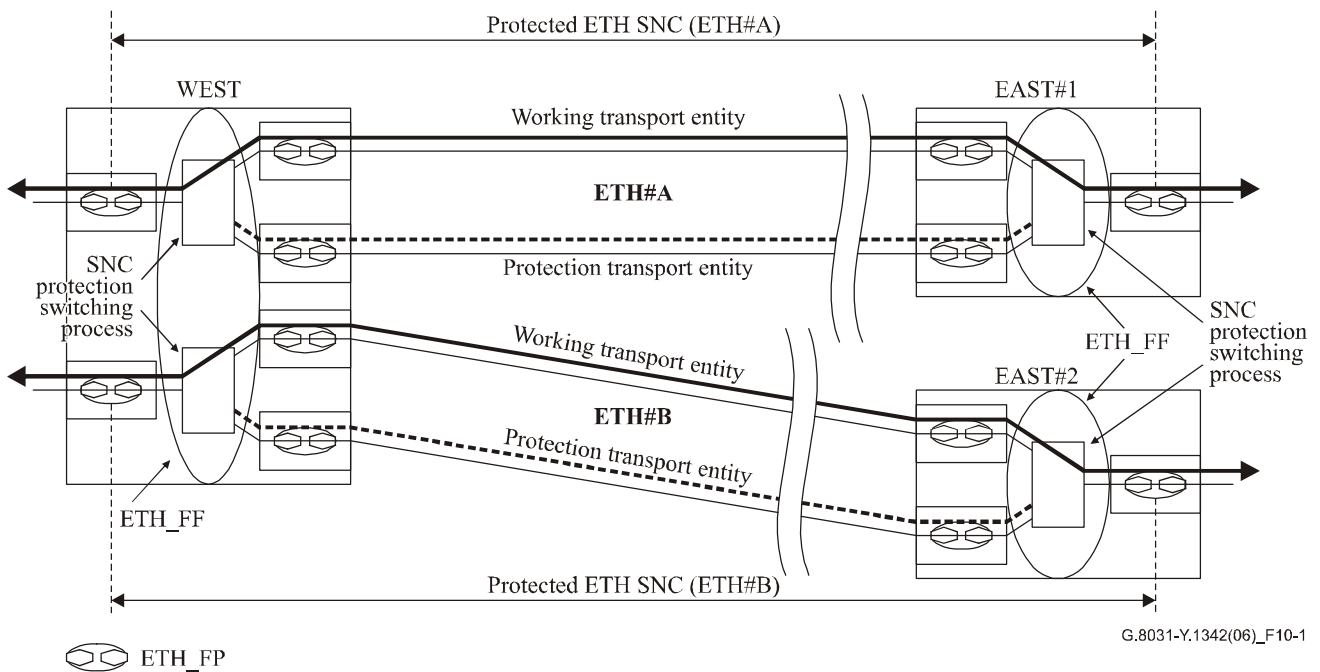
SF is declared when ETH trail signal fail condition is detected. ETH trail signal fail is specified in ITU-T Rec. G.8021/Y.1341.

## 10.6 Protection switching models

Figure 10-1 depicts an example of the VLAN based ETH SNC/S protection switching models defined in this Recommendation. Other network scenarios are permissible.

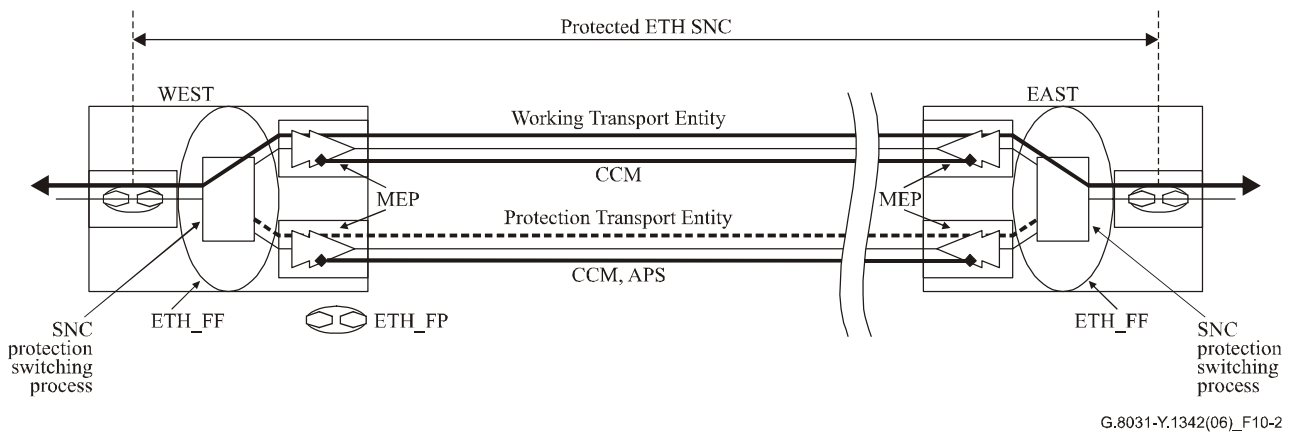
Within the ETH Flow Forwarding function (ETH\_FF) an ETH SNC protection switching process is instantiated to protect the ETH Connection (EC). When protection switching is configured for an EC, i.e., the protected ETH SNC, it is defined between two ETH Flow Points (ETH\_FPs) as depicted in Figure 10-1. Each instantiated SNC protection switching process determines the specific output ETH\_FP over which the protected ETH\_CI is transferred.

For example, in the case of 1:1 protection switching configuration, ETH\_CI for the protected ETH can be forwarded to either working or protection transport entities by the instantiated ETH SNC protection switching process within the ETH\_FF.



**Figure 10-1/G.8031/Y.1342 – ETH SNC/S protection switching architecture**

Since the protection switching mechanism requires monitoring for both working and protection transport entities, it is required that MEPs be activated for the purpose of monitoring the working and protection transport entities. Both transport entities are monitored by individually exchanging CCM defined in ITU-T Rec. Y.1731 as shown in Figure 10-2.



**Figure 10-2/G.8031/Y.1342 – MEPs in ETH SNC/S protection switching architecture**

The protection switching process also requires APS communication in order to coordinate its switching behaviour with the other end of the protected domain if the protection switching architecture is not 1+1 unidirectional protection switching. APS PDU is transmitted and received between the same MEP pair on the protection transport entity where CCM is transmitted for the monitoring.

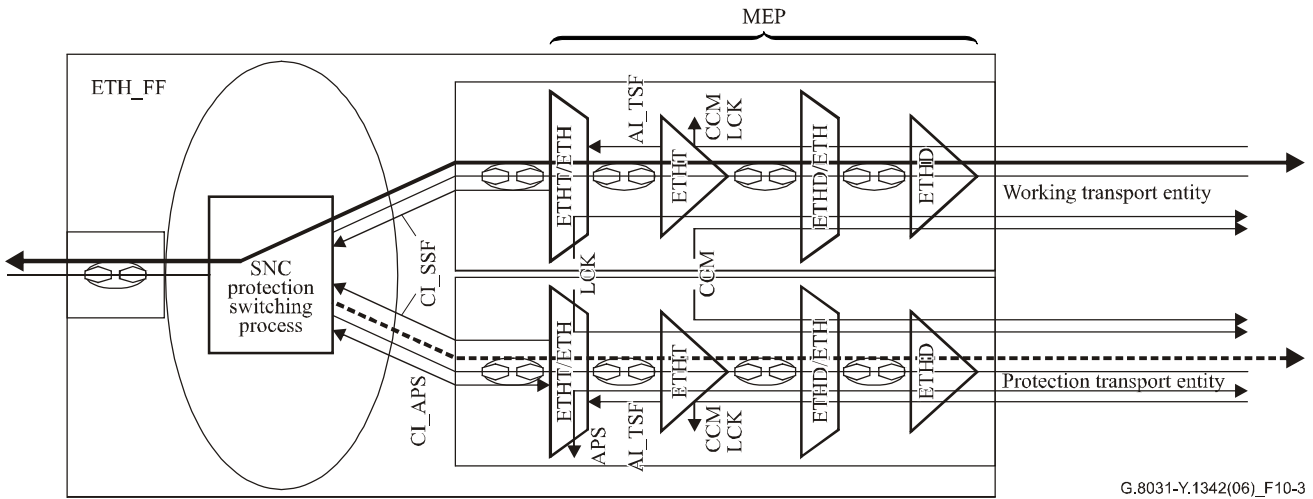
APS information and defect condition which are terminated/detected by MEP sink function can be input to the protection switching process as shown in Figure 10-3.

If an MEP detects an anomaly which contributes to a SF defect condition, it will inform the protection switching process that a failure condition has been detected. Termination of the CCM and LCK (which are defined in ITU-T Rec. Y.1731) is done by the ETH\_FT atomic function. If the ETH\_FT detects a failure condition, an AI\_TSF is signalled to the ETH(x) to ETH adaptation sink (ETH(x)/ETH\_A\_Sk) which subsequently generates a CI\_SSF. The ETH(x)/ETH adaptation function employs this CI\_SSF to notify the ETH SNC protection switching process within ETH\_FF of the signal failure condition.

The APS PDU is terminated by the ETH(x)/ETH\_A\_Sk function within the MEP. The ETH(x)/ETH\_A\_Sk function then extracts the APS specific information from the received APS PDU, and then transfers it to the ETH SNC protection switching process as the APS characteristic information (CI\_APS).

The protection switching process determines the new switching state after it receives CI\_SSF or CI\_APS, and then it determines the specific output ETH\_FP over which the protected ETH\_CI is transferred as necessary.

It is noted that the administrative state of the ETH(x)/ETH adaptation function for both working and protection transport entities shall not be locked.



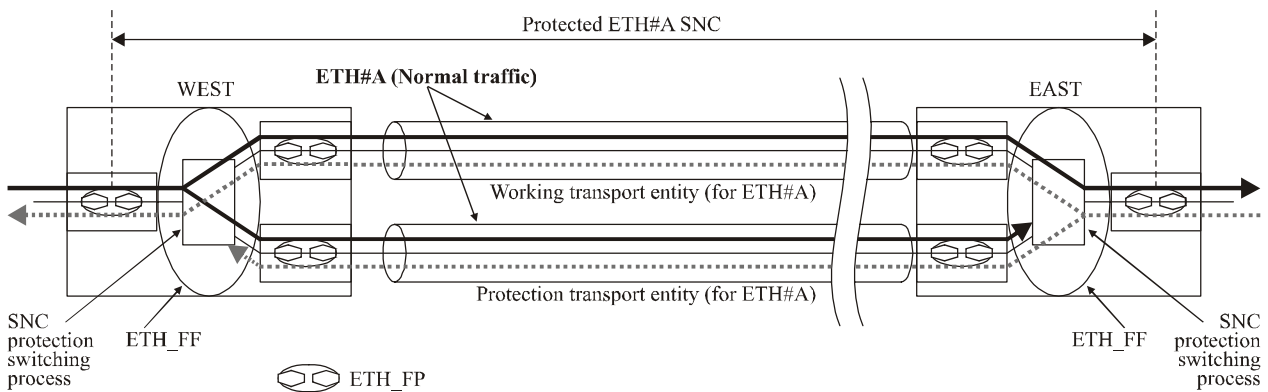
G.8031-Y.1342(06)\_F10-3

**Figure 10-3/G.8031/Y.1342 – Behaviours of both MEPs and SNC protection switching process in ETH SNC/S protection switching architecture**

SNC/S protection is not only limited to subnetwork connections; it is also possible to extend this protection mechanism to support a single link connection as well as network connections.

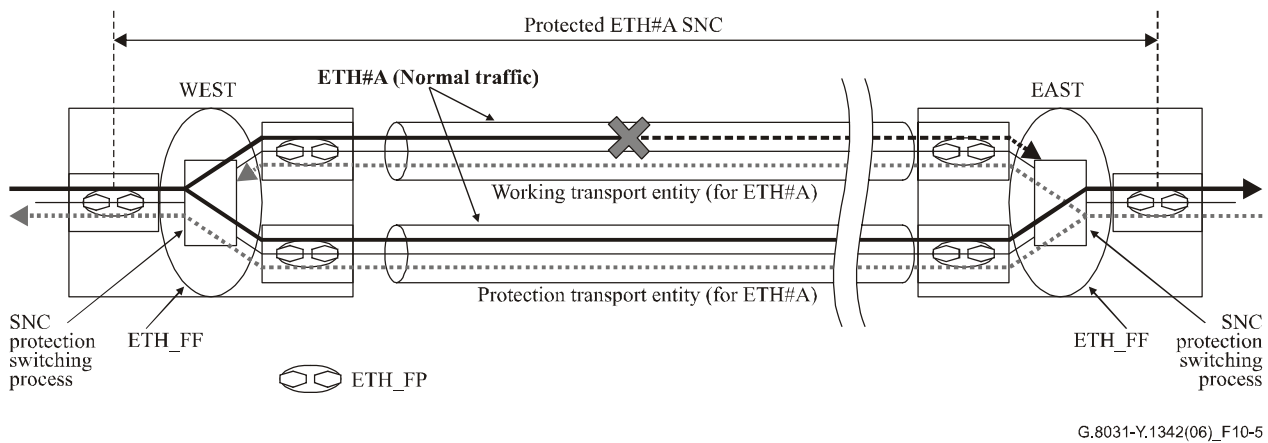
### 10.6.1 1+1 bidirectional protection switching

Figure 10-4 illustrates the 1+1 bidirectional linear protection switching architecture. The protected ETH\_CI traffic is permanently bridged to both the working transport entity and the protection transport entity. In this figure, the traffic is shown as being received via the ETH\_FF only from the working entity. Figure 10-5 illustrates a situation where a protection switching has occurred due to a signal fail condition on the working transport entity. It should be noted that both directions are switched even when a unidirectional defect occurs. For this purpose, APS coordination protocol is necessary.



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

**Figure 10-4/G.8031/Y.1342 – 1+1 bidirectional protection switching architecture**

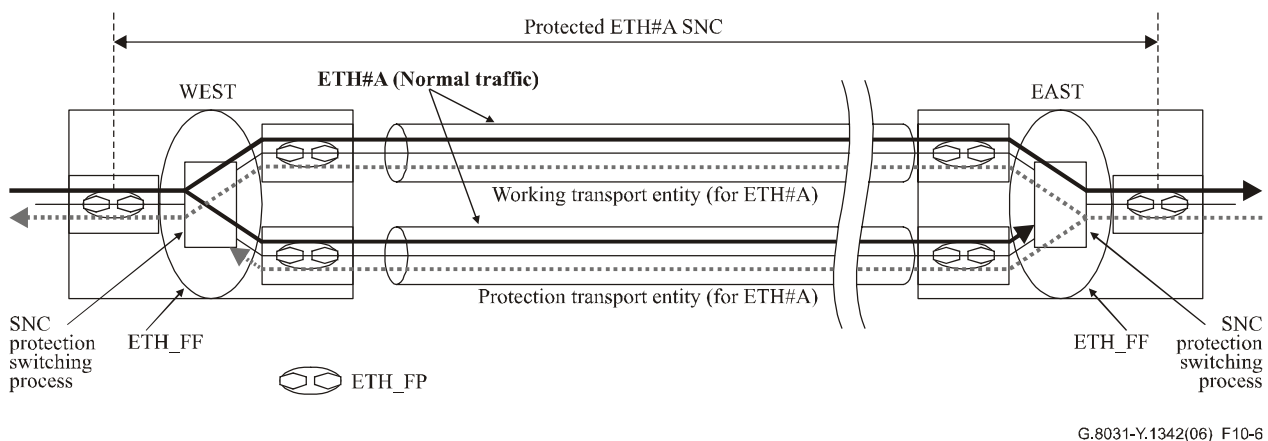


**Figure 10-5/G.8031/Y.1342 – 1+1 bidirectional protection switching architecture – Signal fail condition for working entity**

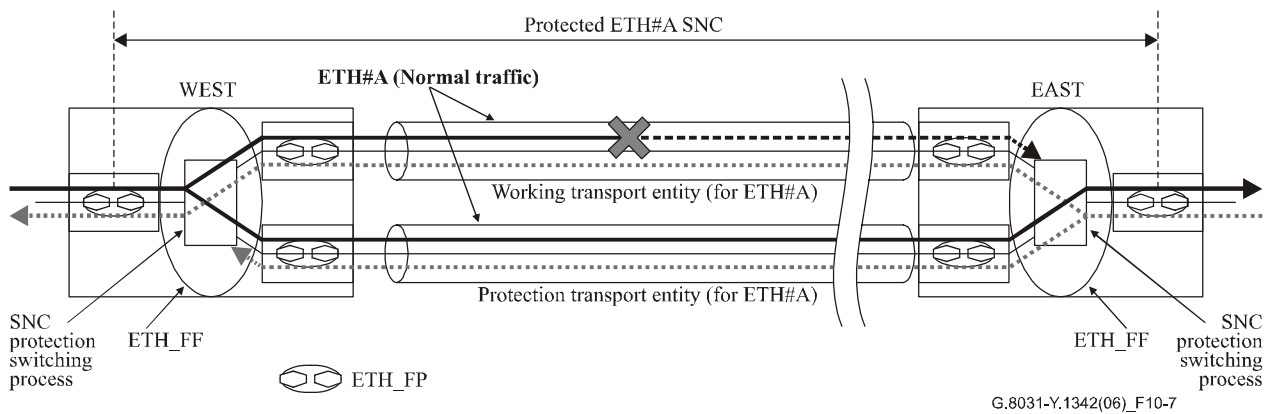
### 10.6.2 1+1 unidirectional protection switching

Figure 10-6 illustrates the 1+1 unidirectional linear protection switching architecture. The protected ETH\_CI traffic is permanently bridged to both the working transport entity and the protection transport entity. In this figure, the traffic is shown as being received via the ETH\_FF only from the working entity for both directions. Figure 10-7 illustrates a situation where a protection switching has occurred due to a signal fail condition on the working transport entity in the West-to-East direction. The normal traffic in the East-to-West direction continues to be received via the working transport entity. In unidirectional protection switching, each direction is switched independently. Selectors at the sink of the protected domain operate only based on the local information. For this purpose, APS coordination protocol is not necessary.

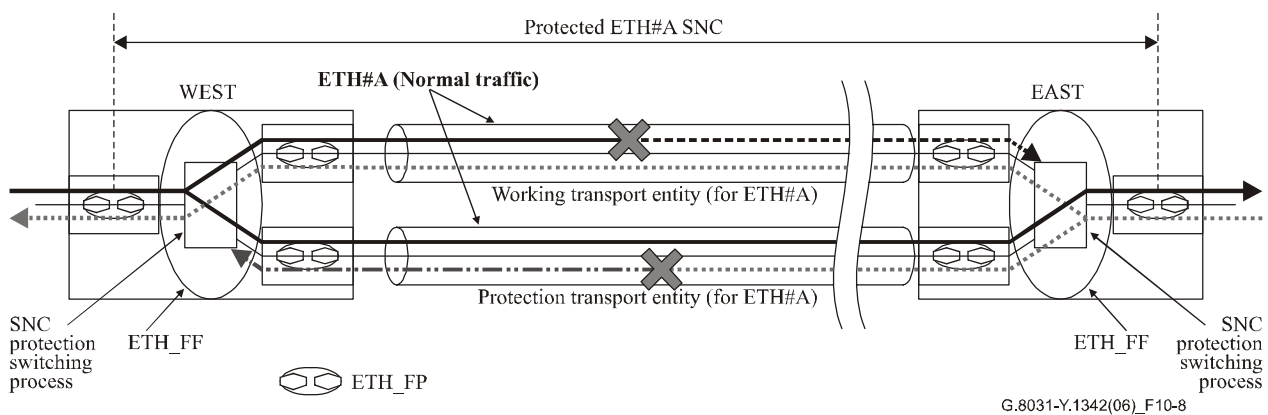
Figure 10-8 illustrates a case where signal fail condition exists on the working transport entity in the West-to-East direction and on the protection transport entity in the East-to-West direction. Unidirectional protection switching can protect this type of double defect scenarios while bidirectional protection switching cannot.



**Figure 10-6/G.8031/Y.1342 – 1+1 unidirectional protection switching architecture**



**Figure 10-7/G.8031/Y.1342 – 1+1 unidirectional protection switching architecture – Signal fail condition for working transport entity in the west-to-east direction**



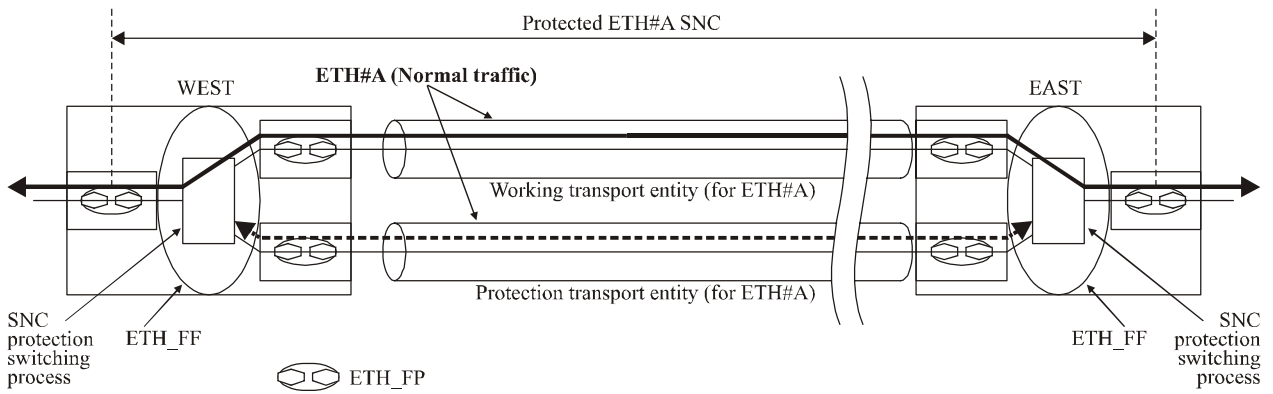
**Figure 10-8/G.8031/Y.1342 – 1+1 unidirectional protection switching architecture – Signal fail condition in both directions**

### 10.6.3 1:1 protection switching

Figure 10-9 illustrates the 1:1 linear protection switching architecture, with the normal traffic (ETH#A) being transmitted via the working transport entity. Although both the working and protection transport entities for ETH#A can be used by any other ETH traffic, the ETH SNC protection switching process only determines the specific output ETH\_FP over which the protected ETH\_CI for ETH#A is transferred if the protection switching is only established for ETH#A.

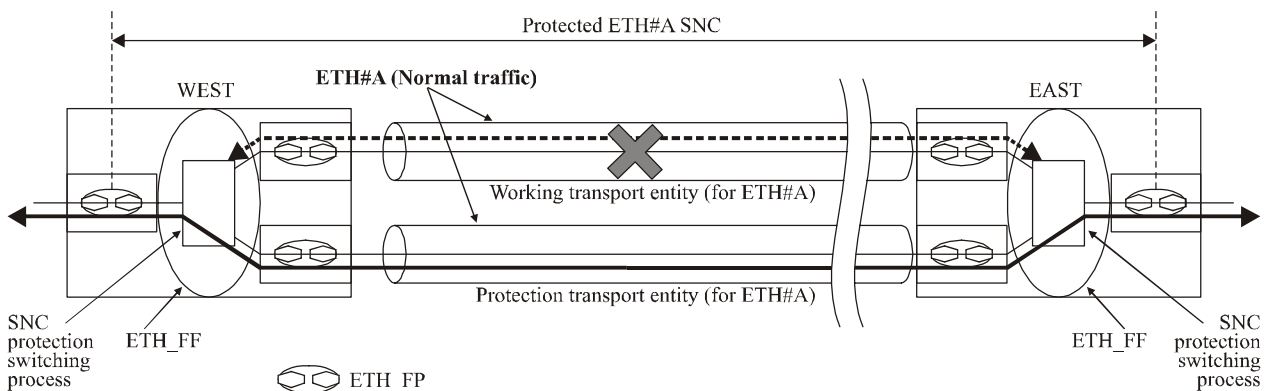
Figure 10-10 illustrates a situation where a protection switch has occurred, due to a signal fail condition on the working transport entity. At the source node, the normal traffic (ETH#A) is forwarded to the protection transport entity. At the sink node, the normal traffic (ETH#A) is received from the protection transport entity. During the protection switching operation, transient mismatch between bridge/selector positions at both ends of the protected domain is possible. However, misconnection between ETH\_CI for ETH#A and other ETH\_CI is not possible because traffic is always forwarded correctly through the ETH\_FF, based on the VID. Note that in order to achieve this forwarding behaviour, different VID must be configured on the protection transport entity for the protected ETH#A and the non-protected ETH traffic.

The forwarding of traffic according to the VID in the ETH\_FF function means that for 1:1 architectures, traffic misconnections are never possible. This greatly simplifies the functionality of the protection switching protocol, enabling a 1-phase protocol to be used, with only a single information exchange being required between both ends to complete a bidirectional switching.



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

**Figure 10-9/G.8031/Y.1342 – 1:1 protection switching architecture**



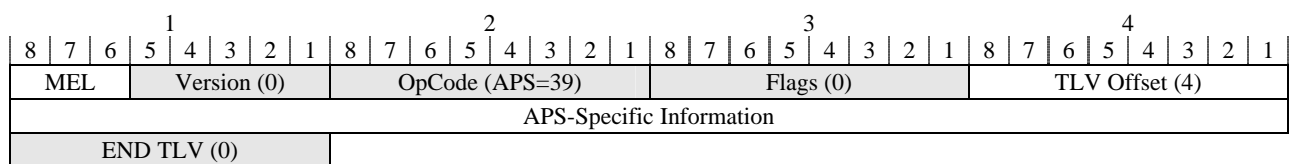
G.8031-Y.1342(06)\_F10-10

**Figure 10-10/G.8031/Y.1342 – 1:1 protection switching architecture – Signal Fail condition for working transport entity**

## 11 APS Protocol

### 11.1 APS format

APS information is carried within the APS PDU which is one of a suite of Ethernet OAM PDUs. OAM PDU formats for each type of Ethernet OAM operation are defined in ITU-T Rec. Y.1731. APS-specific information is transmitted within specific fields in the APS PDU. The APS PDU is identified by a specific Ethernet OAM OpCode. In this version of the Recommendation, 4 octets in the APS PDU are used to carry APS-specific information. This is illustrated in Figure 11-1. In addition, it should be noted that for the current version of this Recommendation, the TLV Offset field is required to be set to 0x04.



**Figure 11-1/G.8031/Y.1342 – APS PDU format**

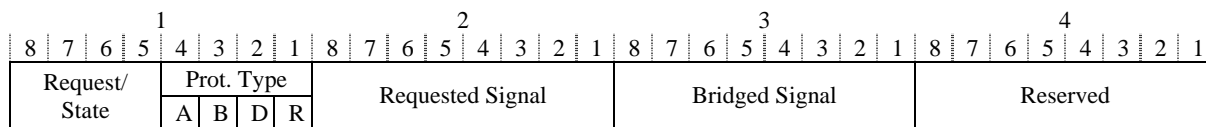


For other fields such as Version, OpCode, Flags and END TLV, the following values shall be used as defined in ITU-T Rec. Y.1731.

- **Version:** 0x00
- **OpCode:** 0x39
- **Flags:** 0x00
- **END TLV:** 0x00

In the MEL field, the MEG level of the APS PDU is inserted.

The format of the APS-specific information within each APS PDU is defined as per Figure 11-2:



**Figure 11-2/G.8031/Y.1342 – APS-specific information format**

Table 11-1 describes code points and values for APS-specific information.

**Table 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

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

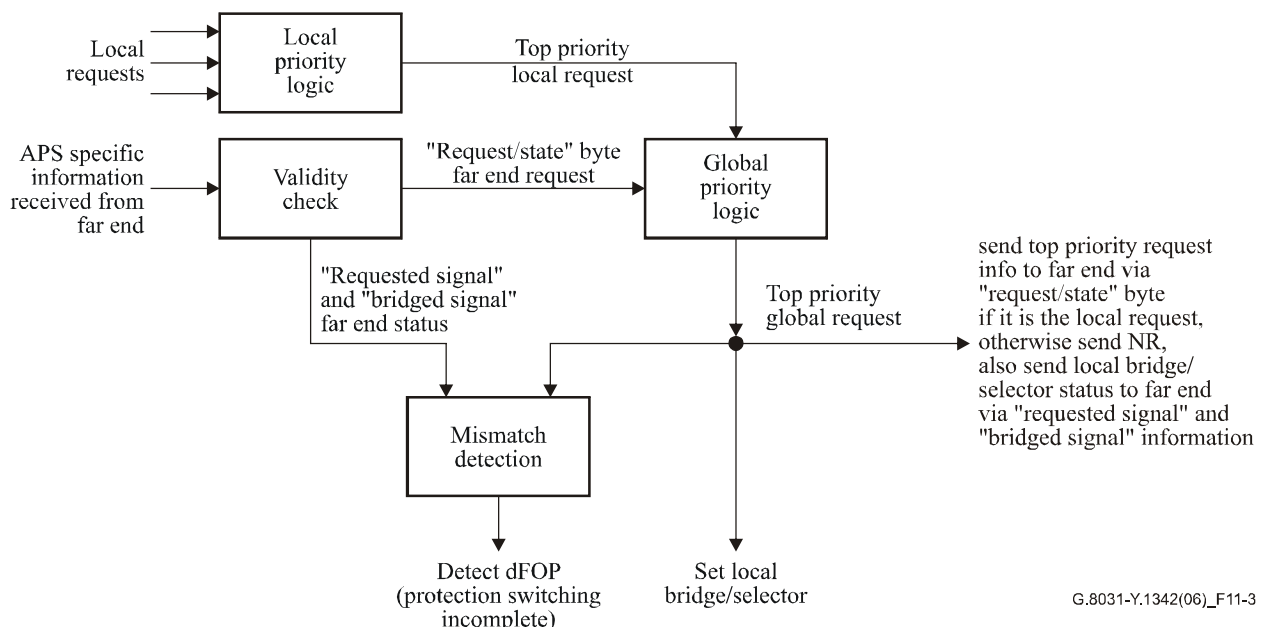
Requested Signal	0	Null Signal
	1	Normal Traffic Signal
	2-255	(Reserved for future use)
Bridged Signal	0	Null Signal
	1	Normal Traffic Signal
	2-255	(Reserved for future use)
NOTE 1 – SD is for further study.		
NOTE 2 – RR is reserved for future standardization by ITU-T.		

For the supported protection architectures described in clause 10, 1-Phase APS shall be used.

## 11.2 1-phase APS protocol

### 11.2.1 Principle of operation

Figure 11-3 illustrates the principle of the 1+1/1:1 linear protection switching algorithm. This algorithm is performed in network elements at both ends of the protected domain (locations WEST and EAST). Bidirectional switching is achieved by transmitting local switching requests to the Far End via the "Request/State" in the first octet of the APS-specific information (see Figure 11-2). The transmitted "Requested Signal" and "Bridged Signal" in the second and the third octets of the APS-specific information contain the local bridge/selector status information; a persistent mismatch between both ends may thus be detected and leads to an alarm.



**Figure 11-3/G.8031/Y.1342 – Principle of 1+1/1:1 linear protection switching algorithm**

In detail, the functionality is as follows (see Figure 11-3):

At the local network element, one or more local protection switching requests (as listed in 9.1 and 9.2) may be active. The "local priority logic" determines which of these requests is of top

priority, using the order of priority given in Table 11-1. This top priority local request information is passed on to the "global priority logic".

The local network element receives information from the network element of the far end via the APS-specific information. The received APS-specific information is subjected to a validity check (see 11.2.4). The information of the received "Request/State" information (which indicates the top priority local request of the far end) is then passed on to the "global priority logic". The "global priority logic" compares the top priority local request with the request of the received "Request/State" information (according to the order of priority of Table 11-1) to determine the top priority global request. If the top priority global request is the local request, it will be indicated in "Request/State" field, otherwise "NR" will be indicated. This request then determines the bridge/selector position (or status) of the local network element as follows:

- for 1+1 architectures, only the selector position is controlled. For 1:1 architectures, both the bridge and the selector positions are maintained to select the same position;
- if the top priority global request is a request for a working entity, the associated working traffic is bridged/switched to/from the protection entity, i.e., the associated bridge/selector of the local network element selects the protection entity. A switching request for a working entity means a request to switch from a working entity to the protection entity.

The bridge/selector status is transmitted to the far end via the "Request Signal" and "Bridged Signal" (with coding as described in Table 11-1). It is also compared with the bridge/selector status of the far end as indicated by the received "Request Signal" and "Bridged Signal". Note that the linear protection switching algorithm commences immediately every time one of the input signals (see Figure 11-3) changes, i.e., when the status of any local request changes, or when a different APS-specific information is received from the far end. The consequent actions of the algorithm are also initiated immediately, i.e., change the local bridge/selector position (if necessary), transmit a new APS-specific information (if necessary), or detect dFOP if the protection switching is not completed within a period specified in clause 11.15.

### **11.2.2 Revertive mode**

In revertive mode of operation, in conditions where working traffic is being received via the protection entity, if local protection switching requests (see Figure 11-3) have been previously active and now become inactive, a local wait-to-restore state is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted "Request/State" information and maintains the switch.

This state normally times out and becomes a no request state after the wait-to-restore timer has expired. The wait-to-restore timer is deactivated earlier if any local request of higher priority pre-empts this state.

Note that for the decision of whether or not to enter the wait-to-restore state, only local requests are considered. A switch to the protection entity may be maintained by a local wait-to-restore state or by a remote request (wait-to-restore or other) received via the "Request/State" information. Therefore, in a case where a bidirectional failure for a working entity has occurred and subsequent repair has taken place, the bidirectional reversion back to the working entity does not take place until both wait-to-restore timers at both ends have expired.

### **11.2.3 Non-revertive mode**

In non-revertive mode of operation, in conditions where working traffic is being transmitted via the protection entity, if local protection switching requests (see Figure 11-3) have been previously active and now become inactive, a local "do not revert state" is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted "Request/State" information and maintains the switch, thus preventing reversion back to the released bridge/selector position in non-revertive mode under no request conditions.

#### 11.2.4 Transmission and acceptance of APS

Traffic units which carry APS PDU are called APS frames. The APS frames are transported via the protection transport entity only, being inserted by the head end of the protected domain and extracted by the tail end of the protected domain.

A new APS frame must be transmitted immediately when a change in the transmitted status (see Figure 11-3) occurs.

The first three APS frames should be transmitted as fast as possible after the status change of the protection end point so that fast protection switching is possible even if one or two APS frames are lost or corrupted. For the fast protection switching in 50 ms, the interval of the first three APS frames is desirable to be 3.3 ms, which is the same interval as CCM frames for fast defect detection. APS frames after the first three frames should be transmitted with the interval of 5 seconds.

If no valid APS-specific information is received, the last valid received information remains applicable. In the event a signal fail condition is detected on the protection transport entity, the received APS-specific information should be evaluated.

If a protection end point receives APS-specific information from the working entity, it should ignore this information, and should detect the Failure of Protocol defect for the local network element (see 11.15).

#### 11.3 Request type

The request types that may be reflected in the APS-specific information are the "standard" types traditionally supported by protection switching for SONET and SDH. These requests reflect the highest priority condition, command, or state. In the case of unidirectional switching, this is the highest priority value determined from the near end only. In bidirectional switching, the local request will be indicated only in the case where it is as high as or higher than any request received from the far end over the APS communication, otherwise NR will be indicated. In 1-phase APS protocol, the near end will never signal Reverse Request even when the far end request has the highest priority.

#### 11.4 Protection types

The valid Protection Types are:

000x	1+1 Unidirectional, no APS communication
100x	1+1 Unidirectional w/APS communication
101x	1+1 Bidirectional w/APS communication
111x	1:1 Bidirectional w/APS communication

The values are chosen such that the default value (all zeros) matches the only type of protection that can operate without APS (1+1 Unidirectional).

Note that 010x, 001x, and 011x are invalid since 1:1 and Bidirectional require an APS communication.

If the "B" bit mismatches, the selector is released since 1:1 and 1+1 are incompatible. This will result in a defect.

Provided the "B" bit matches:

If the "A" bit mismatches, the side expecting APS will fall back to 1+1 unidirectional switching without APS communication.

If the "D" bit mismatches, the bidirectional side will fall back to unidirectional switching.

If the "R" bit mismatches, one side will clear switches to "WTR" and the other will clear to "DNR". The two sides will interwork and the traffic is protected.

## **11.5 Requested signal**

This indicates the signal that the near end requests be carried over the protection path. For NR, this is the null signal when the far end is not bridging normal traffic signal to the protection entity. When the far end is bridging normal traffic signal to the protection entity, the requested signal is the normal traffic signal for NR; for LO, this can only be the null signal. For Exercise, this can be the null signal when Exercise replaces NR or the normal traffic signal in the case where Exercise replaces DNR. For SF (or SD if applicable), this will be the normal traffic signal, or the null signal to indicate that protection has failed or has been degraded. For all other requests, this will be the normal traffic signal requested to be carried over the protection transport entity.

## **11.6 Bridged signal**

This indicates the signal that is bridged onto the protection path. For 1+1 protection, this should always indicate the normal traffic signal, accurately reflecting the permanent bridge. For 1:1 protection, this will indicate what is actually bridged to the protection entity (either the null signal, or normal traffic signal). This will generally be the bridge requested by the far end.

## **11.7 Control of bridge**

In 1+1 architectures, the normal traffic signal is permanently bridged to protection. The normal traffic signal will always be indicated in the bridged signal field of the APS information.

In 1:1 architectures, the bridge will be set to the one indicated by the "Requested Signal" field of the incoming APS information. Once the bridge has been established, this will be indicated in the "Bridged Signal" field of the outgoing APS information.

## **11.8 Control of selector**

In 1+1 unidirectional architectures (with or without APS communication), the selector is set entirely according to the highest priority local request. This is a single phase switch.

In 1+1 bidirectional architectures, the normal traffic signal will be selected from the protection entity when the outgoing "Requested Signal" indicates the normal traffic signal.

In 1:1 bidirectional architectures, normal traffic signal will be selected from the protection entity when the number appears in the outgoing "Requested Signal".

## **11.9 Signal fail of the protection transport entity**

Signal Fail on the protection transport entity is higher priority than any defect that would cause a normal traffic signal to be selected from protection. For the case an APS signal is in use, a SF-P on the protection transport entity (over which the APS signal is routed) has priority over the Forced Switch. Lockout command has higher priority than SF-P: during failure conditions, lockout status shall be kept active.

## **11.10 Equal priority requests**

In general, once a switch has been completed due to a request, it will not be overridden by another request of the same priority (first come, first served behaviour). Equal priority requests from both sides of a bidirectional protection group are both considered valid.

## **11.11 Command acceptance and retention**

The commands CLEAR, LO, FS, MS, and EXER are accepted or rejected in the context of previous commands, the condition of the working and protection entities in the protection group, and (in bidirectional switching only) the received APS information.

The CLEAR command is only valid if a near end LO, FS, MS, or EXER command is in effect, or if a WTR state is present at the near end and rejected otherwise. This command will remove the near end command or WTR state, allowing the next lower priority condition or (in bidirectional switching) APS request to be asserted.

Other commands are rejected unless they are higher priority than the previously existing command, condition, or (in bidirectional switching) APS request. If a new command is accepted, any previous, lower priority command that is overridden is forgotten. If a higher priority command overrides a lower priority condition or (in bidirectional switching) APS request, that other request will be reasserted if it still exists at the time the command is cleared.

If a command is overridden by a condition or (in bidirectional switching) APS request, that command is forgotten.

### **11.12 Hold-off timer**

In order to coordinate timing of protection switches at multiple layers or across cascaded protected domains, a hold-off timer may be required. The purpose is to allow either a server layer protection switch to have a chance to fix the problem before switching at a client layer, or to allow an upstream protected domain to switch before a downstream domain (e.g., to allow an upstream ring to switch before the downstream ring in a dual node interconnect configuration so that the switch occurs in the same ring as the failure).

Each protection group should have a provisionable hold-off timer. The suggested range of the hold-off timer is 0 to 10 seconds in steps of 100 ms (accuracy of  $\pm 5$  ms).

The operation of the hold-off timer uses the "peek twice" method specified in SDH standards. Specifically, when a new defect or more severe defect occurs (new SF (or SD if applicable)), this event will not be reported immediately to protection switching if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the hold-off timer expires, it will be checked whether a defect still exists on the trail that started the timer. If it does, that defect will be reported to protection switching. The defect need not be the same one that started the timer.

### **11.13 Wait-to-restore timer**

In revertive mode of operation, to prevent frequent operation of the protection switch due to an intermittent defect, a failed working transport entity must become fault-free. After the failed working transport entity meets this criterion, a fixed period of time shall elapse before a normal traffic signal uses it again. This period, called wait-to-restore (WTR) period, may be configured by the operator in 1 minute steps between 5 and 12 minutes; the default value is 5 minutes. A SF (or SD if applicable) condition will override the WTR.

In revertive mode of operation, when the protection is no longer requested, i.e., the failed working transport entity is no longer in SF (or SD if applicable) condition (and assuming no other requesting transport entities), a local wait-to-restore state will be activated. Since this state becomes the highest in priority, it is indicated on the APS signal (if applicable), and maintains the normal traffic signal from the previously failed working transport entity on the protection transport entity. This state shall normally time out and become a no request null signal. The wait-to-restore timer deactivates earlier when any request of higher priority pre-empts this state.

### **11.14 Exercise operation**

Exercise is a command to test if the APS communication is operating correctly. It is lower priority than any "real" switch request. It is only valid in bidirectional switching, since this is the only place where you can get a meaningful test by looking for a response.

Exercise command shall issue the command with the same requested and bridged signal numbers of the NR or DNR request that it replaces. In 1-phase APS protocol, the valid response will be an NR

with the corresponding requested and bridged signal numbers. The standard response to DNR should be DNR rather than NR. When the exercise command is cleared, it will be replaced with NR if the requested signal number is 0, and DNR for normal traffic signal number 1.

### 11.15 Failure of protocol defects

Entry and exit criteria for Failure of Protocol defects (dFOP) for APS protocol defined in this Recommendation are described in Table 11-2.

**Table 11-2/G.8031/Y.1342 – Entry/Exit criteria for dFOP**

<b>Fully incompatible provisioning (the "B" bit mismatch)</b>	
Entry criteria	Reception of three APS frames with the incompatible "B" bit value during the period of 22.5 seconds.
Exit criteria	Reception of the first APS frame with a compatible "B" bit value.
<b>Protection switching incomplete</b>	
Entry criteria	If the transmitted "Requested Signal" and received "Bridged Signal" do not match for a period of 50 ms or longer.
Exit criteria	Reception of the first APS frame which indicates the same "Bridged Signal" value with the transmitted "Requested Signal" value.
<b>Working/Protection configuration mismatch</b>	
Entry criteria	Reception of three APS frames from the working transport entity during the period of 22.5 seconds.
Exit criteria	If no APS frame is received from the working transport entity during the period of 22.5 seconds.
NOTE – 22.5 seconds enables the reception of three APS frames even if two APS frames are lost.	

If an unknown request or a request for an invalid signal number is received, it will be ignored.

## Annex A

### State transition tables of protection switching

In this annex, state transition tables for the following protection switching configurations are described.

- 1:1 bidirectional (revertive mode, non-revertive mode);
- 1+1 bidirectional (revertive mode, non-revertive mode);
- 1+1 unidirectional (revertive mode, non-revertive mode).

#### A.1 State transition for 1:1 bidirectional switching with revertive mode

##### A.1.1 Local requests

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

**Table A.1/G.8031/Y.1342 – State transition by local requests (1:1, bidirectional, revertive mode)**

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	Signal fail 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 <sup>a)</sup>	N/A	→F	N/A	→G	O	→I	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B) <sup>b)</sup> or →E	O	→F	N/A	→G	O	O	N/A
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	O	O	O	O	O	O	O	→A or →E <sup>c)</sup> →F <sup>d)</sup>	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 <sup>c)</sup>	O	N/A
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	O	O	N/A
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→C	O	O	O	N/A	→A	O	O	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

NOTE 1 – "N/A" means that the event cannot happen for the State.

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

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

<sup>a)</sup> It transits to the state E if the Signal Fail still exists after hold-off timer expires.

<sup>b)</sup> If FS is indicated in the received APS from the far end.

<sup>c)</sup> If SF is reasserted.

<sup>d)</sup> 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.

**Table A.2/G.8031/Y.1342 – State transition by far end requests (1:1, bidirectional, revertive mode)**

State		Signalled APS	Received far end request								
			k	l	m	n	o	p	q	r	s
			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]	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	(→A)	(→A) or →E <sup>a)</sup> or →F <sup>b)</sup>	(→A)
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	(→B)	N/A	→A or →E <sup>a)</sup>	N/A
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	(→C)	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
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→A	→A	→B	(→E)	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
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O
H	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→A	→A	→B	→B	→B	(→H)	O	N/A	O
I	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→A	→A	→B	→B	→B	N/A	(→I)	O	N/A

NOTE 1 – "N/A" means that the event cannot happen for the State.  
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has a lower priority.  
NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.  
<sup>a)</sup> If SF is reasserted.  
<sup>b)</sup> If SF-P is reasserted.

## 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.

**Table A.3/G.8031/Y.1342 – State transition by local requests (1:1, bidirectional, non-revertive mode)**

State		Signalled APS	Local request								
			a	b	c	d	e	f	g	h	i
			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	NR [r/b=null]	→C	→D	→E <sup>a)</sup>	N/A	→F	N/A	→G	O	→I
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B) <sup>b)</sup> or →E	N/A	→F	N/A	→G	O	O
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	O	O	O	O	O	O	O	→A or →E <sup>c)</sup> →F <sup>d)</sup>	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→H or →E <sup>c)</sup>	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]	→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	O	→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

NOTE 1 – "N/A" means that the event cannot happen for the State.

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

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

<sup>a)</sup> It transits to the state E if the Signal Fail still exists after hold-off timer expires.

<sup>b)</sup> If FS is indicated in the received APS from the far end.

<sup>c)</sup> If SF is reasserted.

<sup>d)</sup> 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.

**Table A.4/G.8031/Y.1342 – State transition by far end requests (1:1, bidirectional, non-revertive mode)**

State	Signalled APS	Received far end request										
		k	l	m	n	o	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]	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	(→A)	N/A	(→A) or →E <sup>a)</sup> or →F <sup>b)</sup>	(→A)	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	N/A	(→B)	→A or →E <sup>a)</sup>	N/A	(→B)
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	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→H)	O	O	(→H)
I	Exercise Working/Active Protection/Standby	EXER[r/b=null]	→A	→A	→B	→B	→B	(→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)	O	O	O

NOTE 1 – "N/A" means that the event cannot happen for the State.  
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has a lower priority.  
NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.  
<sup>a)</sup> If SF is reasserted.  
<sup>b)</sup> 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.

**Table A.5/G.8031/Y.1342 – State transition by local requests (1+1, bidirectional, revertive mode)**

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	Signal fail 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 <sup>a)</sup>	N/A	→F	N/A	→G	O	→I	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B) <sup>b)</sup> or →E	O	→F	N/A	→G	O	O	N/A
C	Lockout Working/Active Protection/Standby	LO [r/b= null/normal]	O	O	O	O	O	O	O	→A or →E <sup>c)</sup> →F <sup>d)</sup>	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 <sup>c)</sup>	O	N/A
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	O	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	O	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

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

**Table A.6/G.8031/Y.1342 – State transition by far end requests (1+1, bidirectional, revertive mode)**

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

NOTE 1 – "N/A" means that the event cannot happen for the State.  
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has a lower priority.  
NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.  
<sup>a)</sup> If SF is reasserted.  
<sup>b)</sup> If SF-P is reasserted.

## 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.

**Table A.7/G.8031/Y.1342 – State transition by local requests (1+1, bidirectional, non-revertive mode)**

State		Signalled APS	Local request								
			a	b	c	d	e	f	g	h	i
			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	NR [r/b=null/normal]	→C	→D	→E <sup>a)</sup>	N/A	→F	N/A	→G	O	→I
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B) <sup>b)</sup> 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 <sup>c)</sup> →F <sup>d)</sup>	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→H or →E <sup>c)</sup>	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

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

**Table A.8/G.8031/Y.1342 – State transition by far end requests (1+1 bidirectional, non-revertive mode)**

State		Signalled APS	Received far end request									
			k LO [r/b= null/normal]	l SF-P [r/b= null/normal]	m FS [r/b=normal]	n SF [r/b= /normal]	o MS [r/b=normal]	q EXER [r/b=null/normal]	r EXER [r/b=normal]	s NR [r/b=null/normal]	t NR [r/b=normal]	u DNR [r/b=normal]
A	No Request Working/Active Protection/ Standby	NR [r/b= null/normal]	(→A)	(→A)	→B	→B	→B	(→A)	N/A	(→A) or →E <sup>a)</sup> or →F <sup>b)</sup>	(→A)	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	N/A	(→B)	→A or →E <sup>a)</sup>	N/A	(→B)
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	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→A	→A	→B	→B	→B	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	O	O	N/A
J	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→J)	O	O	O

NOTE 1 – "N/A" means that the event cannot happen for the State.  
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has a lower priority.  
NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.  
<sup>a)</sup> If SF is reasserted.  
<sup>b)</sup> 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.

**Table A.9/G.8031/Y.1342 – State transition by local requests (1+1, unidirectional, revertive mode)**

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 <sup>a)</sup>	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 <sup>b)</sup> →E <sup>c)</sup>	N/A	N/A
C	Forced Switch Working/Standby Protection/Active	→B	O	O	O	→E	N/A	O	→A or →D <sup>c)</sup>	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 cannot happen for the State.  
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has a lower priority.  
<sup>a)</sup> It transits to the state D if the Signal Fail still exists after hold-off timer expires.  
<sup>b)</sup> If SF is reasserted.  
<sup>c)</sup> 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.

**Table A.10/G.8031/Y.1342 – State transition by local requests (1+1, unidirectional, non-revertive mode)**

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 <sup>a)</sup>	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 <sup>b)</sup> →E <sup>c)</sup>	N/A
C	Forced Switch Working/Standby Protection/Active	→B	O	O	O	→E	N/A	O	→G or →D <sup>b)</sup>	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 cannot happen for the State.  
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has a lower priority.  
<sup>a)</sup> It transits to the state D if the Signal Fail still exists after hold-off timer expires.  
<sup>b)</sup> If SF is reasserted.  
<sup>c)</sup> If SF-P is reasserted.

## Appendix I

### Operation example of 1-phase APS protocol

#### I.1 Introduction

Operation examples of 1-phase APS protocol (1:1, revertive and non-revertive modes) are shown here.

#### I.2 Example scenario

##### I.2.1 Revertive mode

This example assumes the scenario below.

- 1) The protected domain is operating without any defect (working entity is selected).
- 2) Then, SF (Signal Fail) occurs in the west to east direction (switches to protection entity).
- 3) Then, this defect is repaired (enters WTR state, maintains to select protection entity).
- 4) Then, WTR timer expires (switches to working entity).

##### I.2.2 Non-revertive mode

This example assumes the scenario below.

- 1) The protected domain is operating without any defect (working entity is selected).
- 2) Then, SF (Signal Fail) occurs in the west to east direction (switches to protection entity).
- 3) Then, this defect is repaired (enters DNR state, maintains to select protection entity).

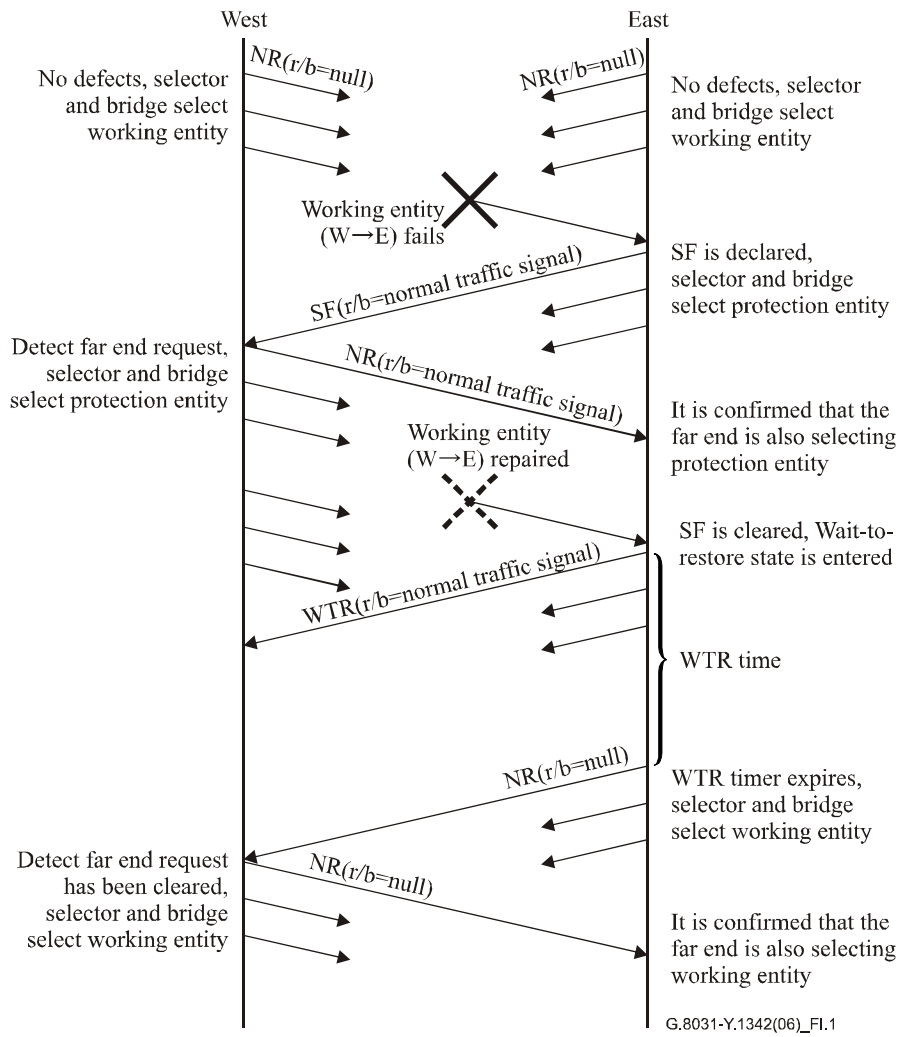
##### I.2.3 Signal fail and forced switch

This example assumes the scenario below.

- 1) SF (Signal Fail) occurs in the west to east direction (switches to protection entity).
- 2) Then, FS (Forced Switch) command is accepted at east (enters FS state).
- 3) Then, FS is cleared at east and SF is reasserted at east.

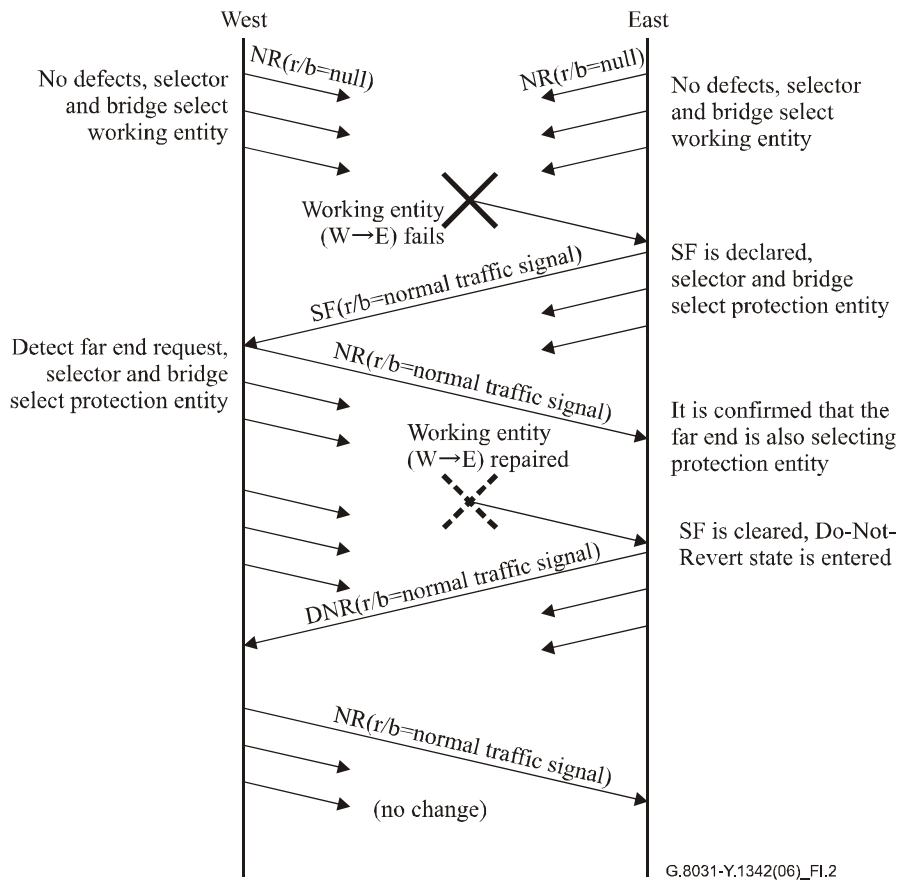
#### I.3 APS protocol examples

APS protocol examples are shown in Figure I.1 (revertive mode), Figure I.2 (non-revertive mode) and Figure I.3 (SF and FS).



DNR: Do-Not-Revert  
 NR: no request  
 r/b: requested signal/bridged signal  
 SF: signal failure  
 WTR: Wait-To-Restore  
 W→E: west to east direction

**Figure I.1/G.8031/Y.1342 – Protocol example (revertive mode)**



DNR: Do-Not-Revert  
 NR: no request  
 r/b: requested signal/bridged signal  
 SF: signal failure  
 WTR: Wait-To-Restore  
 W→E: west to east direction

**Figure I.2/G.8031/Y.1342 – Protocol example (non-revertive mode)**



## Appendix II

### Interaction between Ethernet protection switching and STP

This appendix shows that a bridge port within the protected domain must not participate in a STP domain if it is to avoid undesirable interaction between STP and Ethernet protection switching. One way to ensure this is to disable STP in the protected domain. However, domains outside of the protected domain could have STP enabled. Another way to ensure this is if the working and protection transport entities belong to two different STP domains. These two scenarios are discussed in this clause.

Figure II.1 shows the first way introduced above, the protected domain and STP domains (#1 and #2) are segmented vertically and do not overlap. Bridges #A and #B at the edge of the protected domain and STP domains interconnect the STP domains without any loop problem.

The second case mentioned above is shown in Figure II.2. STP domains (#1 and #2) are segmented horizontally, and provide two transport entities for Ethernet protection switching. Figure II.3 shows that the working and protection transport entities for Ethernet protection switching are provisioned separately within different STP domains. In this example, each VLAN and network resource would be used effectively.

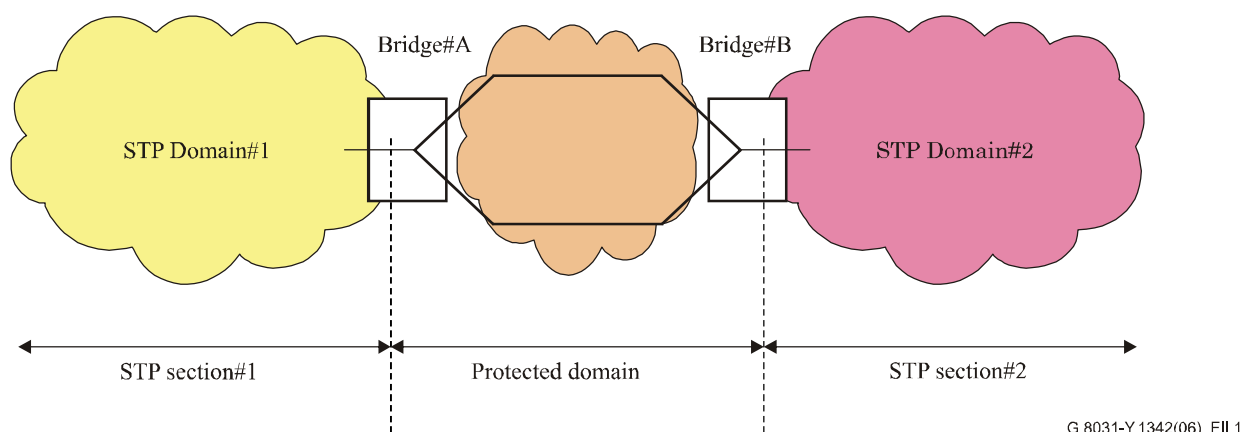
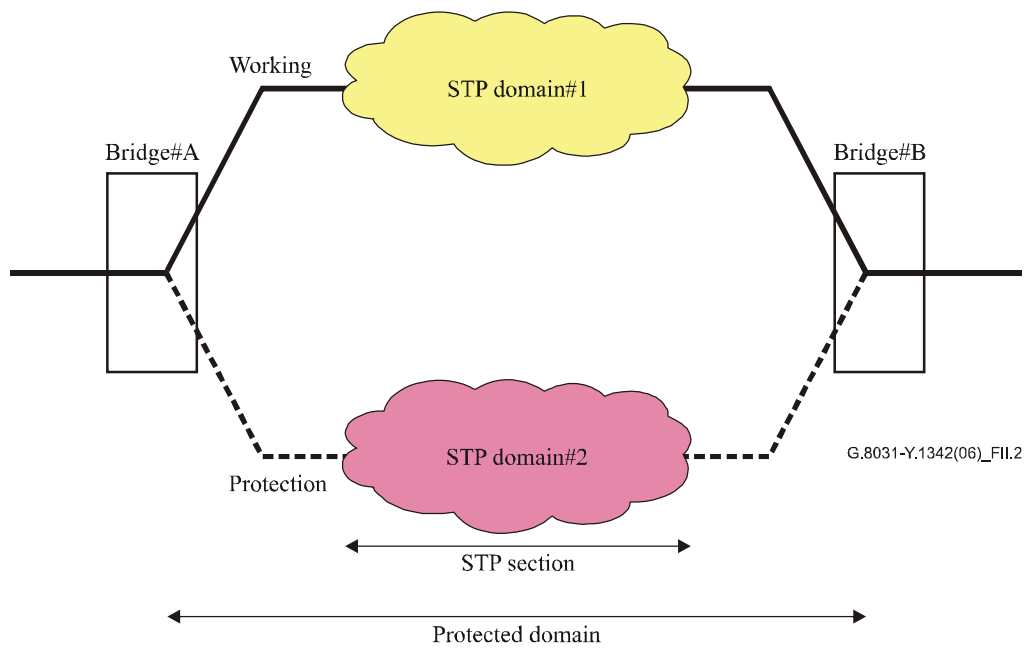
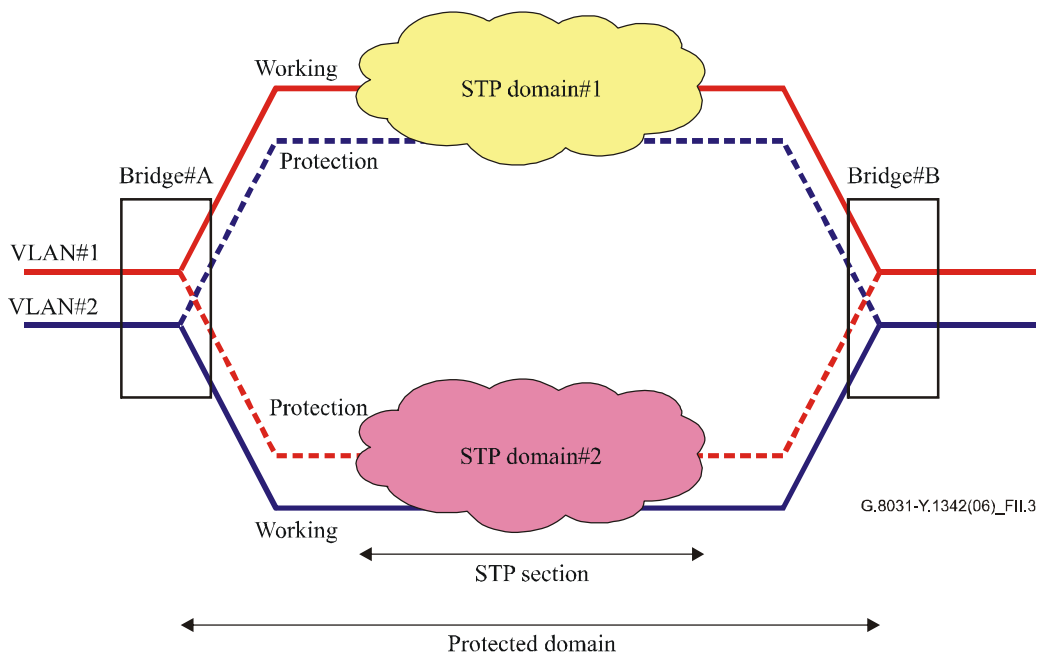


Figure II.1/G.8031/Y.1342 – No overlapping between the protected domain and STP



**Figure II.2/G.8031/Y.1342 – Overlapping between the protected domain and STP**



**Figure II.3/G.8031/Y.1342 – Overlapping between the protected domain and STP per VLAN**

## Appendix III

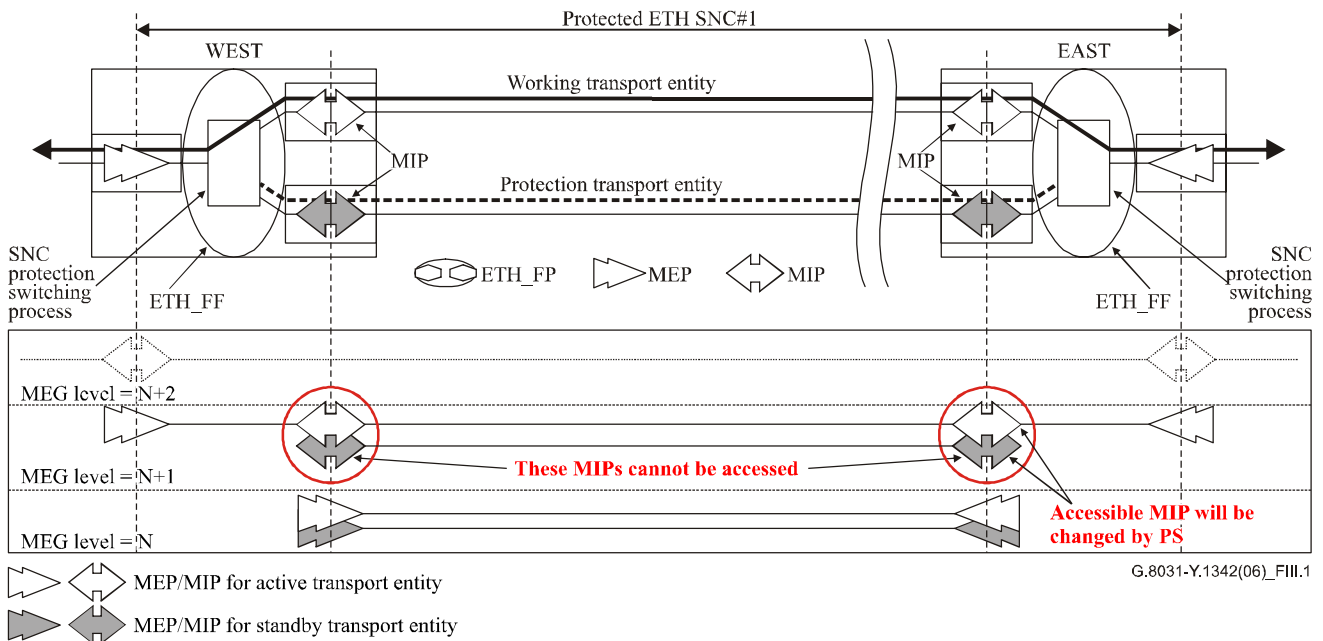
### MIPs for protection switching environment

#### III.1 Introduction

In this appendix, considerations and some configuration examples of MIPs for a protection switching environment are shown.

#### III.2 Considerations

Figure III.1 shows an example of MEPs and MIPs configuration for protection switching. In Figure III.1, two pairs of MEPs are configured to monitor both the working and protection transport entities in MEG Level N. Also in MEG Level N+1, MEPs and MIPs are configured at each port as depicted in the figure.

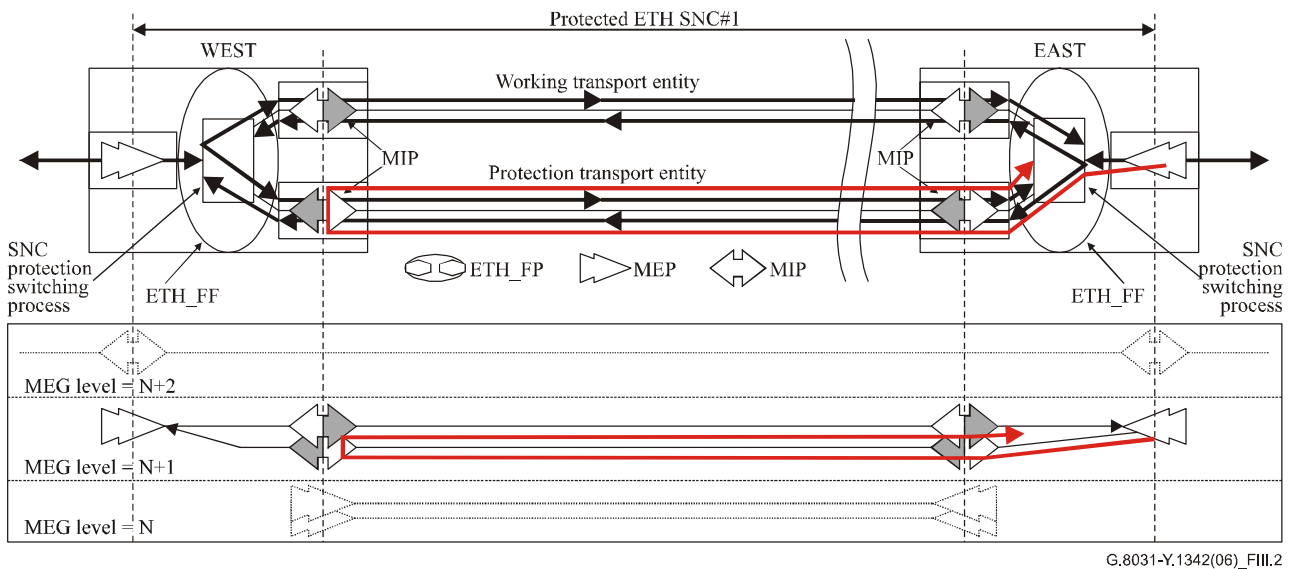


**Figure III.1/G.8031/Y.1342 – MEPs and MIPs for 1:1 bidirectional protection switching**

If 1:1 protection switching is configured, MIPs in MEG Level N+1 on the standby transport entity cannot be accessed by MEPs for the same MEG, and accessible MIPs will be changed by the protection switching. Therefore, MIPs in MEG Level N+1 shown in Figure III.1, appear to be unnecessary.

Figure III.2 shows a configuration of MEPs and MIPs for a 1+1 unidirectional protection switching environment. In this case, a request/response communication between a MEP and a MIP cannot be made correctly. Therefore, MIPs in MEG Level N+1 shown in Figure III.2 also appear to be unnecessary.





G.8031-Y.1342(06)\_FIII.2

**Figure III.2/G.8031/Y.1342 – MEPs and MIPs for 1+1 unidirectional protection switching**

As described above, configuring MIPs at anywhere inside the protected domain, for a higher MEG Level than that of MEPs which monitors both working and protection transport entities, appear to be unnecessary.

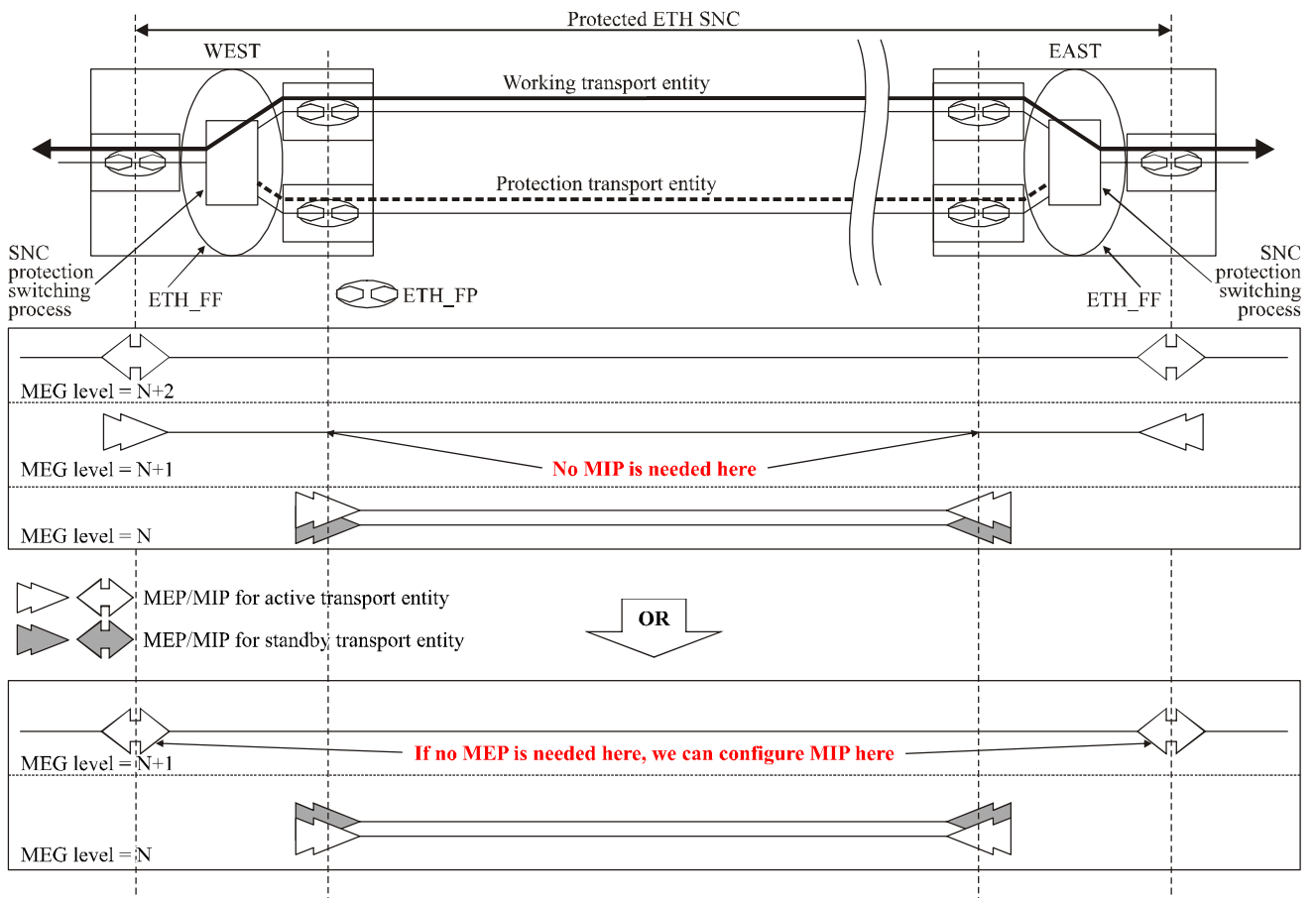
### III.3 Configuration examples

Figure III.3 shows two examples of possible MEPs and MIPs configuration.

In the first example, shown in the middle of Figure III.3, no MIPs are configured in MEG Level N+1, but MEPs are configured instead. In this case, the MEG in MEG Level N+1 represents the protected domain.

The second example is shown in the bottom of Figure III.3. In this configuration, MIPs are configured in MEG Level N+1 at the edge of the protected domain.

MEPs and MIPs shown in both examples are fully accessible because they are not configured inside the protected domain.



G.8031-Y.1342(06)\_FIII.3

**Figure III.3/G.8031/Y.1342 – Configuration examples of MEPs and MIPs for protection switching environment**

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
<b>Transport</b>	<b>Y.1300–Y.1399</b>
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

*For further details, please refer to the list of ITU-T Recommendations.*

## SERIES OF ITU-T RECOMMENDATIONS

- Series A Organization of the work of ITU-T
- Series D General tariff principles
- Series E Overall network operation, telephone service, service operation and human factors
- Series F Non-telephone telecommunication services
- Series G Transmission systems and media, digital systems and networks**
- Series H Audiovisual and multimedia systems
- Series I Integrated services digital network
- Series J Cable networks and transmission of television, sound programme and other multimedia signals
- Series K Protection against interference
- Series L Construction, installation and protection of cables and other elements of outside plant
- Series M Telecommunication management, including TMN and network maintenance
- Series N Maintenance: international sound programme and television transmission circuits
- Series O Specifications of measuring equipment
- Series P Telephone transmission quality, telephone installations, local line networks
- Series Q Switching and signalling
- Series R Telegraph transmission
- Series S Telegraph services terminal equipment
- Series T Terminals for telematic services
- Series U Telegraph switching
- Series V Data communication over the telephone network
- Series X Data networks, open system communications and security
- Series Y Global information infrastructure, Internet protocol aspects and next-generation networks**
- Series Z Languages and general software aspects for telecommunication systems