

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.873.1

(10/2017)

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

Digital networks – Optical transport networks

Optical transport network: Linear protection

Recommendation ITU-T G.873.1



International
Telecommunication
Union

Documents
Document Sharing Hub

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 AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
General aspects	G.800–G.809
Design objectives for digital networks	G.810–G.819
Synchronization, quality and availability targets	G.820–G.829
Network capabilities and functions	G.830–G.839
SDH network characteristics	G.840–G.849
Management of transport network	G.850–G.859
SDH radio and satellite systems integration	G.860–G.869
Optical transport networks	G.870–G.879
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA 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
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

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



Recommendation ITU-T G.873.1

Optical transport network: Linear protection

Summary

Recommendation ITU-T G.873.1 defines the automatic protection switching (APS) protocol and protection switching operation for the linear protection schemes for the optical transport network at the optical data unit k (ODUk) level. Protection schemes considered in this Recommendation are:

- ODUk subnetwork connection protection with inherent monitoring (1+1, 1:n);
- ODUk subnetwork connection protection with non-intrusive monitoring (1+1);
- ODUk subnetwork connection protection with sublayer monitoring (1+1, 1:n).
- ODUk compound link subnetwork connection group protection with inherent monitoring (1+1, 1:1).

In addition, client-related protection architectures are described.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.873.1	2003-03-29	15	11.1002/1000/6306
2.0	ITU-T G.873.1	2006-03-29	15	11.1002/1000/8762
3.0	ITU-T G.873.1	2011-07-22	15	11.1002/1000/11120
3.1	ITU-T G.873.1 (2011) Amd. 1	2012-10-29	15	11.1002/1000/11790
4.0	ITU-T G.873.1	2014-05-14	15	11.1002/1000/12181
4.1	ITU-T G.873.1 (2014) Amd. 1	2014-12-05	15	11.1002/1000/12368
5.0	ITU-T G.873.1	2017-10-07	15	11.1002/1000/13302

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2017

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

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Protection characteristics	4
	6.1 Monitoring methods and conditions	4
	6.2 Protection switching performance	6
7	Protection group commands	6
	7.1 End-to-end commands and states	6
	7.2 Local commands.....	7
8	Protection architectures	8
	8.1 Unidirectional and bidirectional switching	8
	8.2 Need for an APS/PCC channel.....	9
	8.3 Revertive and non-revertive switching.....	9
	8.4 Provisioning mismatches.....	9
	8.5 Overview of protection architectures for OTN linear protection	10
9	APS protocol.....	11
	9.1 APS channel format.....	11
	9.2 Transmission and acceptance of APS protocol	12
	9.3 Request type	13
	9.4 Protection types	14
	9.5 Requested signal.....	14
	9.6 Bridged signal.....	15
	9.7 Control of bridge	15
	9.8 Control of selector	15
	9.9 Signal Fail of the protection entity	15
	9.10 Equal priority requests.....	15
	9.11 Command acceptance and retention.....	16
	9.12 Hold-off timer.....	16
	9.13 Exercise operation	16
	9.14 APS channel alarming	17



	Page
9.15 SF persistency timer	17
Appendix I – Examples of operation	18
I.1 1+1 unidirectional switching	18
I.2 1+1 bidirectional switching	18
I.3 1:n bidirectional switching	19
I.4 Exercise command operation	20
Appendix II – ODUk client protection	23
II.1 Overview over protection architectures of OTN linear client protection.....	23
II.2 Model of client SNC/Nc protection architecture of OTN linear client protection.....	23
II.3 Model of client SNC/I protection architectures of OTN linear client protection.....	24
Appendix III – Media layer protection	27
III.1 Overview of media layer protection	27
III.2 Media layer protection types	27
Bibliography.....	32

Recommendation ITU-T G.873.1

Optical transport network: Linear protection

1 Scope

This Recommendation defines the automatic protection switching (APS) protocol and protection switching operation for the linear protection schemes for the optical transport network (OTN) at the optical data unit k (ODUk) level. These schemes are based on the generic linear protection specifications in [ITU-T G.808.1]. Linear protection schemes considered in this Recommendation are:

- ODUk subnetwork connection protection with inherent monitoring (1+1, 1:n);
- ODUk subnetwork connection protection with non-intrusive monitoring (1+1);
- ODUk subnetwork connection protection with sublayer monitoring (1+1, 1:n);
- ODUk compound link subnetwork connection group protection with inherent monitoring (1+1, 1:1).

In addition, client-related protection architectures are described.

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 G.709] | Recommendation ITU-T G.709/Y.1331 (2016), <i>Interfaces for the optical transport network</i> . |
| [ITU-T G.798] | Recommendation ITU-T G.798 (2017), <i>Characteristics of optical transport network hierarchy equipment functional blocks</i> . |
| [ITU-T G.798.1] | Recommendation ITU-T G.798.1 (2013), <i>Types and characteristics of optical transport network equipment</i> . |
| [ITU-T G.806] | Recommendation ITU-T G.806 (2012), <i>Characteristics of transport equipment – Description methodology and generic functionality</i> . |
| [ITU-T G.808] | Recommendation ITU-T G.808 (2016), <i>Terms and definitions for network protection and restoration</i> . |
| [ITU-T G.808.1] | Recommendation ITU-T G.808.1 (2014), <i>Generic protection switching – Linear trail and subnetwork protection</i> . |

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

Terms defined in [ITU-T G.808]:

- APS channel;

- extra traffic signal;
- head-end;
- normal traffic signal;
- null signal;
- protection communication channel;
- protection group;
- signal;
- tail-end.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AIS	Alarm Indication Signal
APS	Automatic Protection Switching
CBR	Constant Bit Rate signal
CL_SNCG/I	Compound Link Subnetwork Connection Group protection with Inherent monitoring
CSF	Client Signal Fail
DNR	Do Not Revert
ETC3	Ethernet Coding 1000BASE-X
EXER	Exercise
FDI	Forward Defect Indication
FS	Forced Switch
HO	Higher Order
LCK	Locked defect
LO	Lower Order
LoP	Lockout for Protection
MFAS	Multiframe Alignment Signal
MS	Manual Switch
NIM	Non-Intrusive Monitor
NR	No Request
OCI	Open Connection Indication
ODU[i]j_A	ODUkP to ODU[i]j Adaptation function
ODU[i]j_A_SK	ODUkP to ODU[i]j Adaptation Sink function
ODUj-21_A	ODUj payload type 21 Adaptation function
ODUk	Optical Data Unit k
ODUk_A	Optical Data Unit Adaptation of rate K

ODUk_A_Sk	ODUk Adaptation Sink function
ODUk[i]j	ODUj[i] Optical Data Unit of level j or i (i is optional; $i < j$)
ODUkP	Optical Data Unit of level k, Path
ODUkT	Optical Data Unit of level k, Tandem connection sub-layer
OPU	Optical Payload Unit
OTN	Optical Transport Network
OTUk	Optical Transport Unit k
OTUkV	Functionally standardized Optical Transport Unit k
OTUk[V]	OTUk or OTUkV
PCC	Protection Communication Channel
PMOH	Path Monitoring Overhead
RR	Reverse Request
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SF	Signal Fail
SMOH	Section Monitoring Overhead
SNC	Subnetwork Connection
SNC/I	Subnetwork Connection with Inherent monitoring
SNC/Nc	Subnetwork Connection with Non-intrusive monitoring of Client signal fail
SNC/Ne	Subnetwork Connection with Non-intrusive end-to-end monitoring
SNC/Ns	Subnetwork Connection with Non-intrusive Sublayer monitoring
SNC/S	Subnetwork Connection with Sub-layer monitoring
SSD	Server Signal Degraded
SSF	Server Signal Fail
TCM	Tandem Connection Monitoring
TCMOH	Tandem Connection Monitoring Overhead
TSD	Trail Signal Degraded
TSF	Trail Signal Fail
TTI	Trail Trace Identifier
WTR	Wait-to-Restore

5 Conventions

None.

6 Protection characteristics

6.1 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 G.806] and [ITU-T G.798]). For the purpose of the protection switching controller, an entity within the protected domain has a condition of no defect = OK, degraded (signal degrade = SD), or failed (signal fail = SF).

The customary monitoring methods are specified in clauses 11.2 and 11.3 of [ITU-T G.808.1] and in clause 14.1 of [ITU-T G.798] and are supported in the OTN as follows:

Inherent – Protection switching is triggered by defects detected at the ODUk link connection (e.g., server layer trail and server/ODUk adaptation function). The trail termination sink of an (OTUk[V] or ODUkP) server layer provides the test signal fail (TSF)- and test signal degraded (TSD)-based SF and SD protection switching criteria via the OTUk[V]/ODUk_A, ODUkP/ODU[i]j_A, or ODUkP/ODUj-21_A functions (as SSF and SSD). No defect detection is performed on the ODUk or ODU[i]j or ODUj signals themselves. It can be used for individual and for compound link group protection (CL_SNCG/I).

NOTE 1 – In contrast to SDH SNC/I, ODUk SNC/I can stretch only a single link connection, as the FDI/AIS defect resulting from further upstream server layer defects is not detected in the server/ODUk adaptation function. The limitation to a single server layer trail for SNC/I protection is given by the use of signal degrade (SD) as protection switching criteria. SD is only available from the OTUk[V] or HO ODUk trail that is locally terminated and not from further upstream OTUk[V] or HO ODUk trails. Furthermore, FDI/AIS, which provides information about defects in upstream OTUk[V] or HO ODUk trails, is not detected in the OTUk[V]/ODUk_A_Sk or ODUkP/ODU[i]j_A_Sk. For details of the atomic functions for TSF TSD forwarding for the subnetwork connection (SNC) protection on LO ODU refer to [ITU-T G.798].

Figure 6-1 shows an OTUk or OTUkV monitored ODUk SNC/I protection configuration.

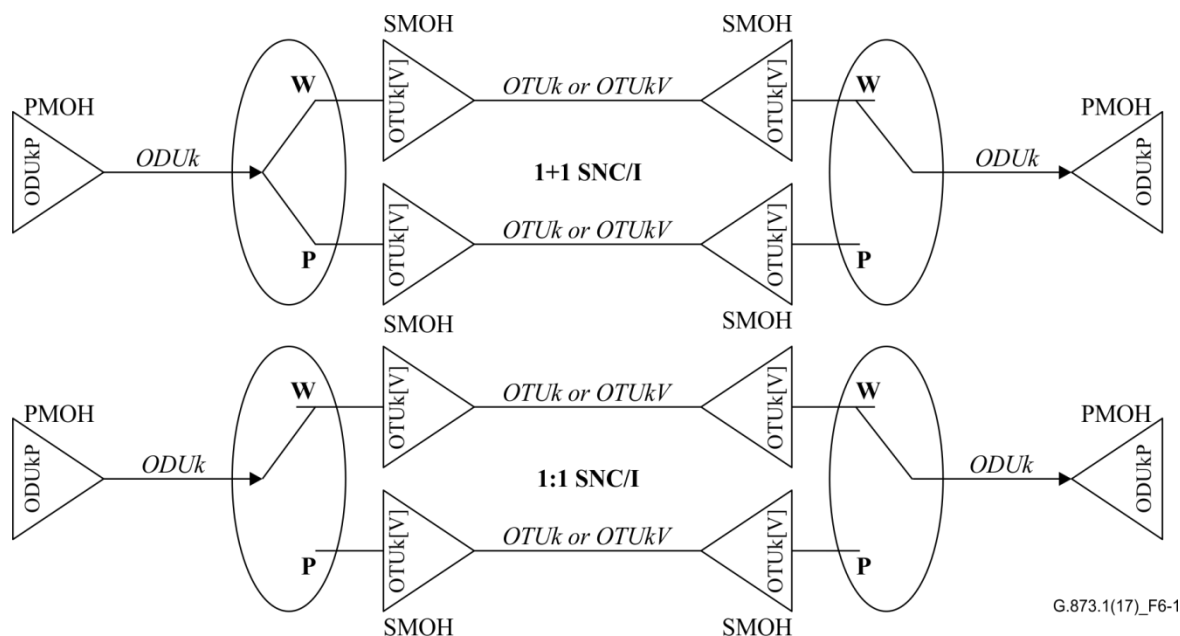


Figure 6-1 – OTUk or OTUkV monitored ODUk SNC/I protection configuration

Figure 6-2 shows a server ODUk monitored ODU[i]j/ODUj SNC/I protection configuration.

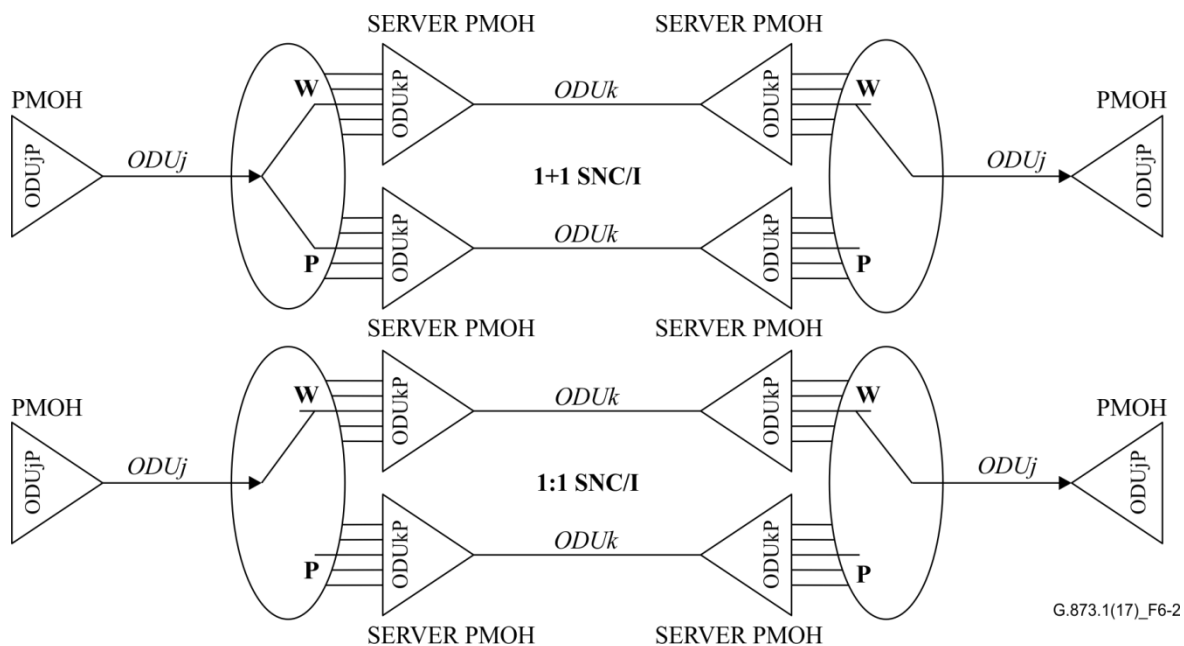


Figure 6-2 – Server ODUk monitored ODU[i]j/ODUj SNC/I protection configuration

Non-intrusive – Protection switching is triggered by a non-intrusive monitor of the ODUkP trail or ODUkT sub-layer trail at the tail-end of the protection group.

NOTE 2 – For a SNC/N protection the criteria according to [ITU-T G.798] are taken. This ensures that ODUk-AIS as well a Locked or open connection indication (OCI) condition is contributing to switch criteria of an ODU SNC/N protection. For details refer to clause 14.2 of [ITU-T G.798].

Figure 6-3 shows an ODUkP non-intrusively monitored ODUk SNC/Ne configuration and an ODUkT monitored ODUk SNC/Ns protection configuration.

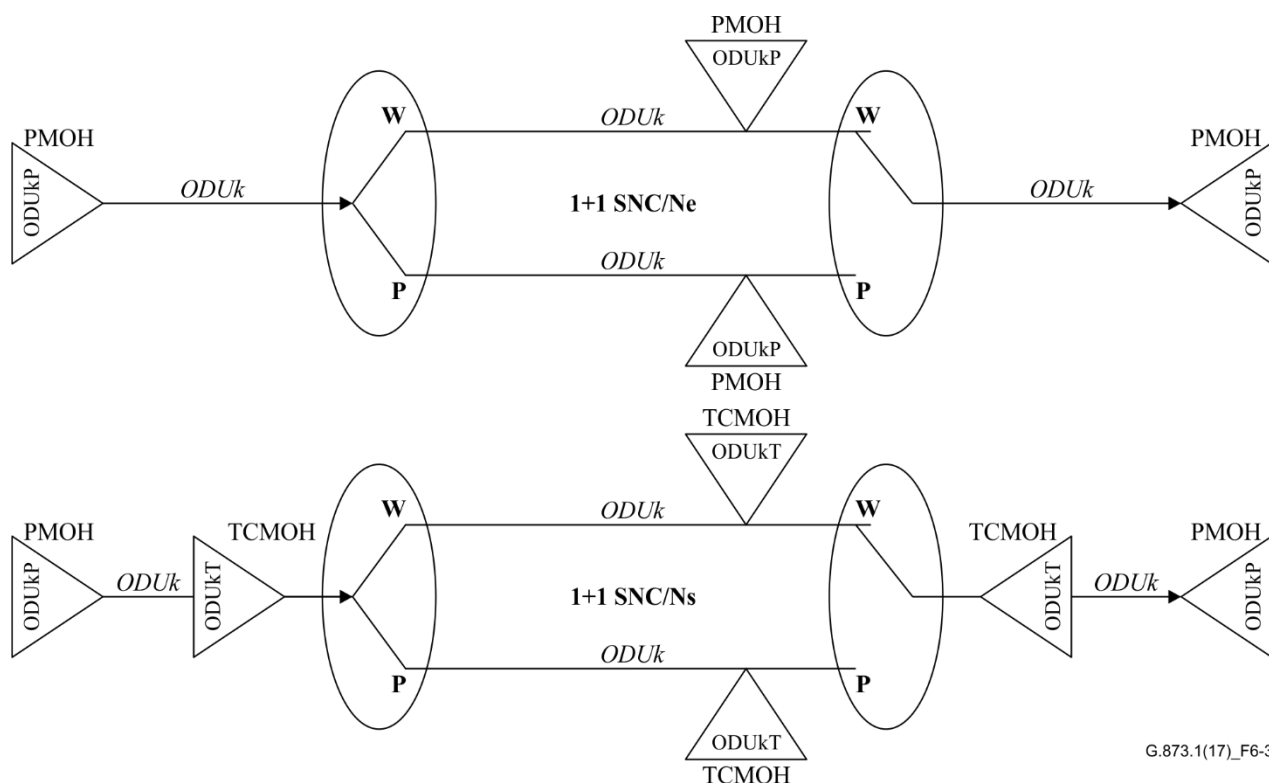


Figure 6-3 – ODUkP non-intrusively monitored ODUk SNC/Ne and ODUkT monitored ODUk SNC/Ns protection configurations

Sublayer – Protection switching is triggered by defects detected at the ODUkT sublayer trail (TCM). An ODUkT sublayer trail is established for each working and protection entity. Protection switching is therefore triggered only on defects of the protected domain. Figure 6-4 shows an ODUkT monitored SNC/S protection configuration.

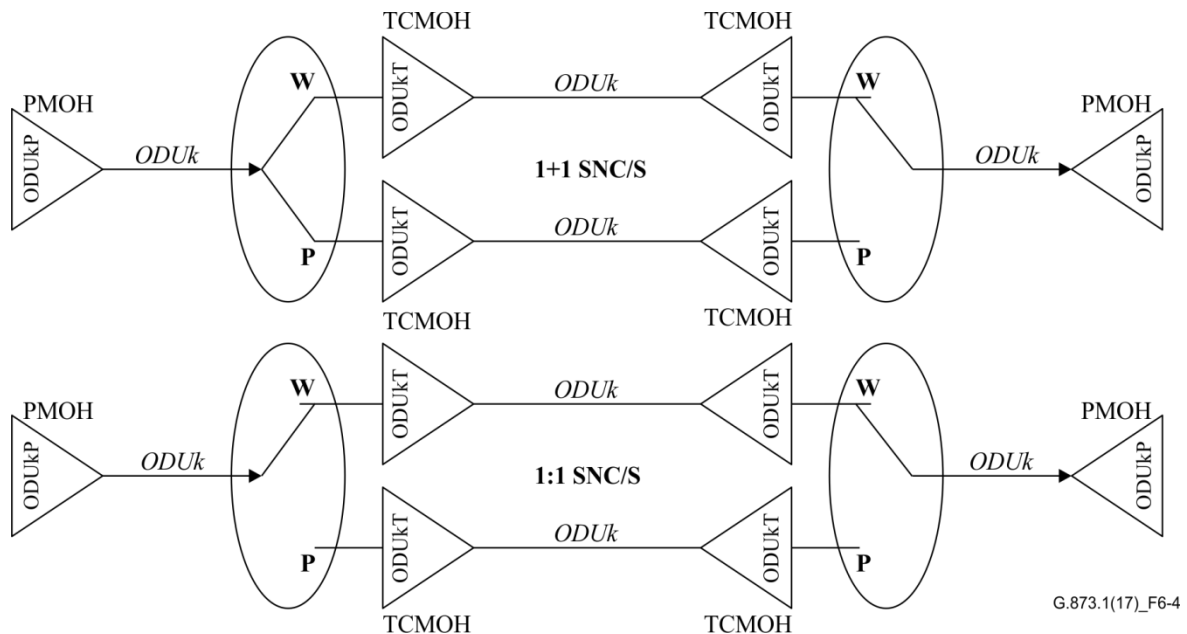


Figure 6-4 – ODUkT monitored SNC/S protection configuration

The protection switching controller does not care which monitoring method is used, as long as it can be given (OK, SD, SF) 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 that the far end declares an SD over the APS channel, even if the monitor at the near-end cannot detect SD.

NOTE 3 – In accordance with [ITU-T G.709], for sublayer monitoring, nesting and cascading are the default operational configurations. Overlapping is an additional configuration for testing purposes only. Overlapped monitored connections must be operated in a non-intrusive mode and not used for protection. Maintenance signals ODUk-AIS and ODUk-LCK must not be generated for overlapped monitored connections. For the case where one of the endpoints in an overlapping monitored connection is located inside a SNC protected domain while the other endpoint is located outside the protected domain, the SNC protection should be forced to working when the endpoint of the overlapping monitored connection is located on the working connection and forced to protection when the endpoint is located on the protection connection.

6.2 Protection switching performance

The transfer time T_t , as defined in clause 13 of [ITU-T G.808.1], shall not exceed 50 ms for a protection span length that does not exceed 1200 km.

7 Protection group commands

7.1 End-to-end commands and states

This clause describes commands that apply to the protection group as a whole. When an APS 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.