International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.873.3

(09/2017)

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

Digital networks – Optical transport networks

Optical transport network – Shared mesh protection

Recommendation ITU-T G.873.3

ITU-T

ITU International Telecommunication Union

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.873.3

Optical transport network – Shared mesh protection

Summary

Recommendation ITU-T G.873.3 defines the protection switching operation and associated protocol for shared mesh protection at the optical data unit (ODU) layer.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.873.3	2017-09-22	15	11.1002/1000/13303

Keywords

Optical transport network, OTN protection, shared mesh protection.

* 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/.

Table of Contents

Recommendation ITU-T G.873.3

Optical transport network – Shared mesh protection

1 Scope

This Recommendation defines the protection switching operation and associated protocol for shared mesh protection at the optical data unit (ODU) layer. The ODU shared mesh protection (SMP) mechanism is based on the generic shared mesh protection architecture defined in [ITU-T G.808.3]. The SMP mechanism uses pre-computed protection paths that are pre-configured into the network elements. These protection paths are activated when necessary via data plane protocol operations. This Recommendation focuses on the activation of the protection paths and the information that the network elements must maintain in order to support the activation of protection paths. The details of how the pre-computation of protection paths is done and how the information about the protection paths is configured into the network elements are outside the scope of this Recommendation. The encoding of the automatic protection switching (APS) protocol into the APS/PCC bytes is outside the scope of this Recommendation. The use of this mechanism with ODUflex that are capable of being resized is 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 G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks.*

[ITU-T G.806] Recommendation ITU-T G.806 (2012), *Characteristics of transport equipment – Description methodology and generic functionality.*

[ITU-T G.808] Recommendation ITU-T G.808 (2016), *Terms and definitions for network protection and restoration.*

[ITU-T G.808.3] Recommendation ITU-T G.808.3 (2012), *Generic protection switching – Shared mesh protection.*

[ITU-T G.873.1] Recommendation ITU-T G.873.1 (2017), *Optical transport network: Linear protection.*

[ITU-T G.873.2] Recommendation ITU-T G.873.2 (2015), *ODUk shared ring protection.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Terms related to protection architecture and components

3.1.1.1 bridge: [ITU-T G.808]

3.1.1.2 intermediate node: [ITU-T G.808]

3.1.1.3 link: [ITU-T G.805]

3.1.1.4 protection transport entity: [ITU-T G.808]

3.1.1.5 revertive (protection) operation: [ITU-T G.808]

3.1.1.6 selector: [ITU-T G.808]

3.1.1.7 shared mesh protection: [ITU-T G.808.3]

3.1.1.8 transport entity: [ITU-T G.805]

3.1.1.9 working transport entity: [ITU-T G.808]

3.1.2 Terms related to fault conditions

3.1.2.1 signal degrade (SD): [ITU-T G.806]

3.1.2.2 signal fail (SF): [ITU-T G.806]

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 ODU SMP domain: A subnetwork in which ODU SMP is used to provide protection.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APS	Automatic Protection Switching
BER	Bit Error Ratio
HO	High Order
LO	Low Order
NMS	Network Management System
ODU	Optical Data Unit
ODUT	ODU Tandem Connection
OPU	Optical Payload Unit
PCC	Protection Communication Channel
P_ID	Protection transport entity Identifier
SD	Signal Degrade
SF	Signal Fail
SMP	Shared Mesh Protection
SNC	Subnetwork Connection
TCM	Tandem Connection Monitoring
W_ID	Working transport entity Identifier

5 Conventions

Within figures and text in this Recommendation, the following conventions are used:

– A-H and squares are used to identify nodes in a network.

– Triangles are used to identify tandem connection monitoring endpoints.

– W1, W2, ..., Wn are used to identify working transport entities.
– P1, P2, ..., Pn are used to identify protection transport entities corresponding to the working paths.
– Solid lines are used to identify all working transport entities, as well as protection transport entities that are active.
– Dashed lines are used to identify protection transport entities that are not active.

For the purpose of identifying high order (HO) and low order (LO) ODU layers, the suffixes k and j are used, respectively, as well as ODUkT and ODUjT.

6 Protection characteristics

An overview of shared mesh protection (SMP) can be found in [ITU-T G.808.3].

ODU SMP provides a shared mesh protection scheme for the ODU layer network based on the principles of [ITU-T G.808.3]. It operates on either an end-to-end ODU path or ODU tandem connection.

The SMP mechanism is based on pre-computed protection transport entities that are pre-configured into the network elements. Pre-configuring but not activating the protection transport entities allows the link connections in a protection transport entity to be shared by multiple working transport entities. Protection transport entities are activated in response to network failures or operator's commands by means of a protocol that operates in the data plane. Because link connections within a protection transport entity may be shared, SMP is always revertive.

In ODU SMP, a working transport entity may have one or more protection transport entities. A link connection within a protection transport entity may provide protection for one or more working transport entities. The allocation of shared resources between various protection transport entities is accomplished via the control plane or network management system (NMS) configuration.

An ODU SMP domain may be either concatenated or nested with other ODU SMP domains or with other ODU protection schemes, such as linear subnetwork connection (SNC) protection [ITU-T G.873.1] or shared ring protection [ITU-T G.873.2].

ODU SMP includes mechanisms for establishing the link connections during protection transport entity activation, including, when needed, configuration of the multiplexing structure of high order ODU server layer trails used by the protection transport entities. The information necessary to determine whether a high order ODU should be terminated and how to configure the multiplex structure (in the case where the high order ODU is terminated) is part of the information that is pre-configured into the network elements or communicated via SMP messages. The multiplex structure may be viewed as being undefined at the time of the pre-configuration of the protection transport entity. The ODU SMP mechanism will modify the multiplex structure of the server trail as part of the process of activating a protection transport entity when it is necessary to do so.

7 Protection architectures

Generic network models of SMP are described in [ITU-T G.808.3].

A node can be the endpoint of the ODU SMP domain for a number of normal traffic signals (N1, N2, N3) and it will provide ODU tandem connection monitoring (TCM) endpoints for their working transport entities (W1, W2, W3), as illustrated by the solid ODU tandem connection (ODUT) termination and adaptation functions. It will also provide potential ODU TCM endpoints for their protection transport entities (P1, P2, P3), as shown in Figure 7-1, by the dashed ODUT termination and adaptation functions.

A node can also be an intermediate point of the ODU SMP domain for a number of working and protection transport entities, e.g., W4, P5. A working transport entity may be protected by multiple protection transport entities (e.g., W1 is protected by P1 and P1'). Figure 7-1 shows the functional model for an ODU SMP node.

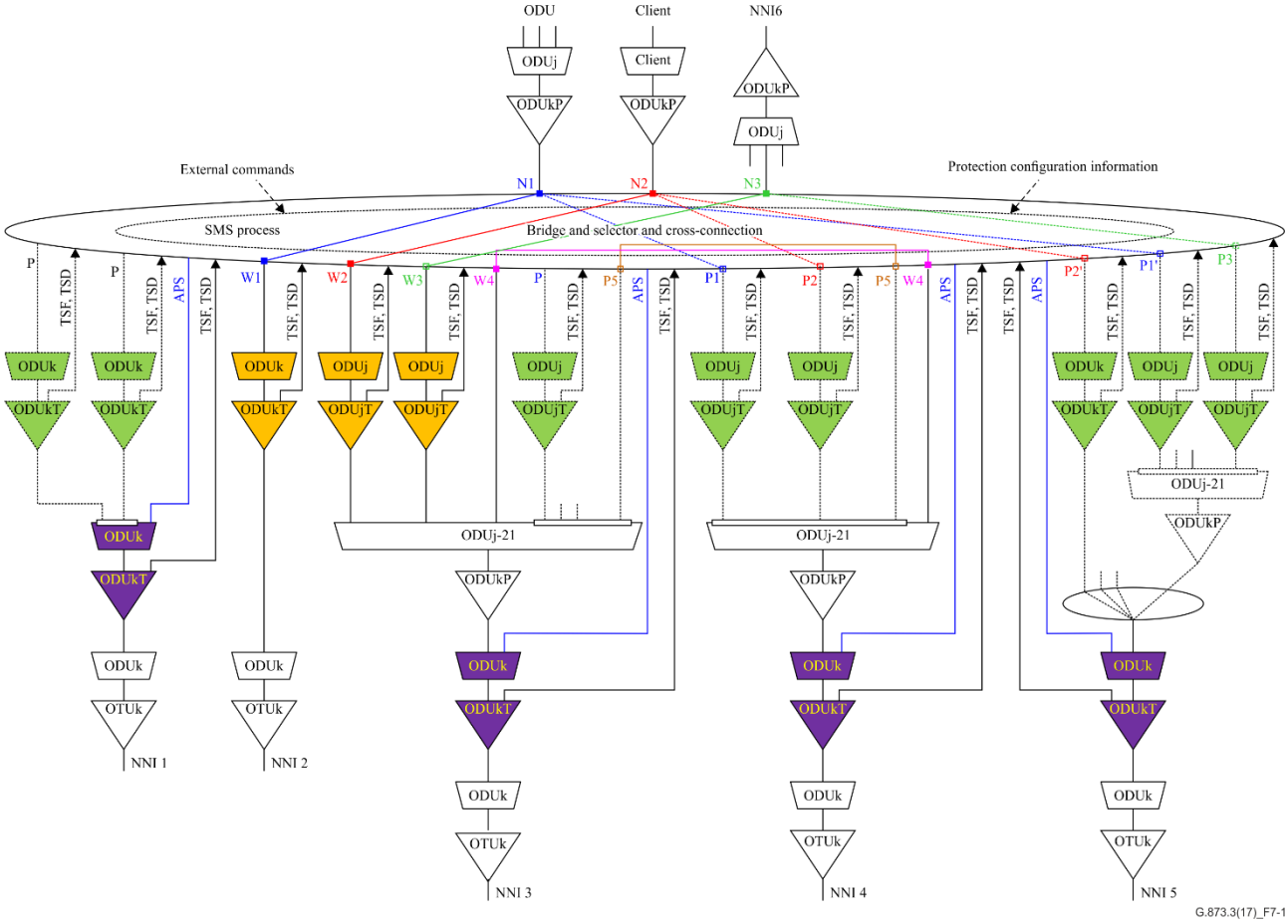

Figure 7-1 – Functional model for ODU SMP

The operation of ODU SMP is based on detection of defects along the working transport entity at the edges of the ODU SMP domain. Monitoring of the working transport entity is accomplished via a tandem connection that covers the entire working transport entity, as shown by the orange TCM terminations in Figures 7-1, 7-2 and 7-3. ODU SMP protection switching is triggered when this tandem connection detects signal degrade (SD) or signal fail (SF). The process of activating a protection transport entity causes the pre-reserved cross-connections in each node to be established in the ODU_C function. When the end-to-end sequence of cross-connections is completely established, the data path will be established through the protection transport entity.

Monitoring of protection resources that are not in use is required; this is accomplished via high order ODU TCM monitoring between adjacent nodes as shown by the purple TCM terminations in Figures 7-1, 7-2 and 7-3. It is assumed that the bit error ratio (BER) of the high order ODU sufficiently approximates the BER of each tributary slot within the high order ODU.

It is also necessary to monitor a protection transport entity after it has been activated. A tandem connection that covers the entire protection transport entity is used for this purpose as shown by green TCM terminations in Figures 7-1 and 7-3. Note that this may require multiple tandem connections within the same layer network in an end node, as shown with NNI1 in Figure 7-1.

Figure 7-2 shows an example network and identifies the monitoring points that are required for ODU SMP in the case that there are no failures. The orange monitors are for the working transport entities. The purple ones are for each link that can be part of a protection transport entity.

Figure 7-3 shows the same network in the case where W1 has failed. An additional tandem connection to monitor the entire P1 transport entity has been added, as shown with the green triangles and the protection transport entity P1 is now active, as shown by the solid line. The protection transport entities P2 and P3 are still monitored, as based on priority they could preempt P1 from using the resources that are shared.

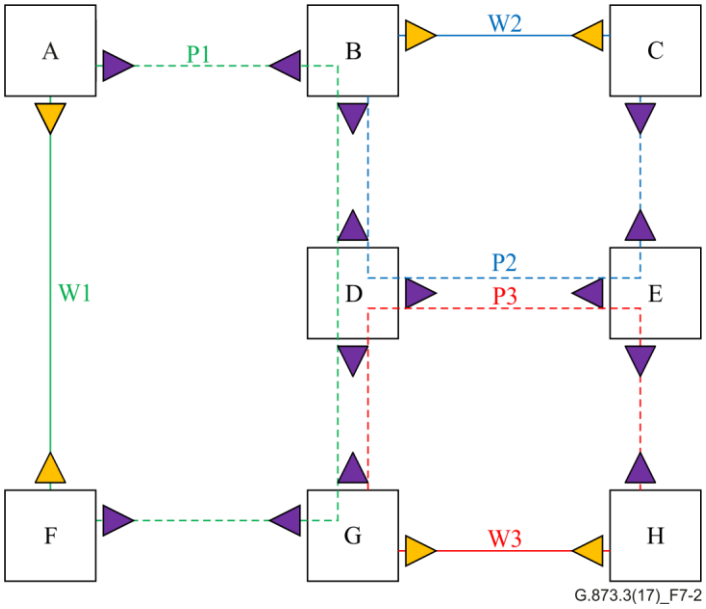

Figure 7-2 – Monitoring with no faults

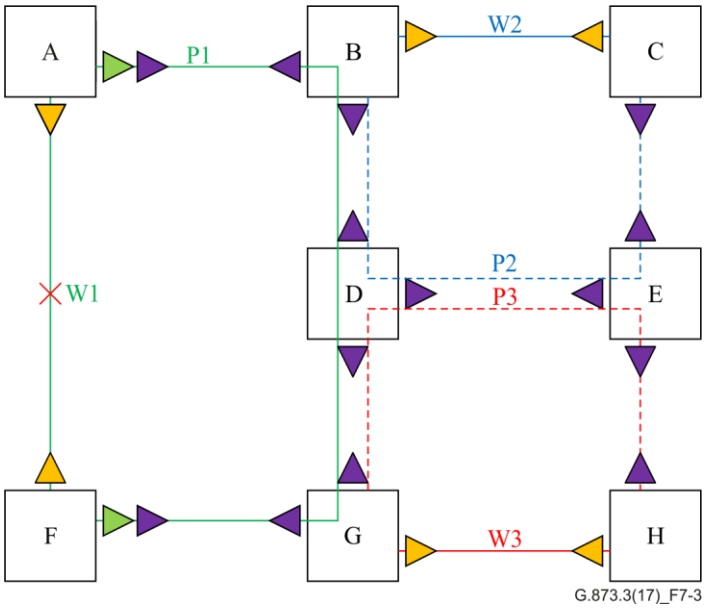

Figure 7-3 – Monitoring with a protection transport entity active

8 Commands

8.1 APS channel

An ODU SMP domain may protect connections in the HO ODUk layer or LO ODUj layer. APS/PCC bytes for the appropriate TCM level in the ODUk layer are used to carry the ODU SMP APS protocol information.

The protocol provides APS information for each tributary slot of the OPUk, which requires a further multi-frame. Details of the additional multi-frame within the APS/PCC bytes are not in the scope of this Recommendation.

The APS protocol information is processed hop-by-hop. When a protection transport entity is activated, APS signalling occurs simultaneously in all tributary slots it occupies.

8.2 Request type

The ODU SMP request types are derived from the OTN linear protection protocol in [ITU-T G.873.1] and are shown in order of priority from highest to lowest in Table 8-1.

Table 8-1 – Request type for ODU SMP

Request type
Forced Switch (FS)
Signal Fail (SF)
Signal Degrade (SD)
Manual Switch (MS)
Wait-to-Restore (WTR)
Exercise (EXER)
Reverse Request (RR)
No Request (NR)

8.3 Lockout of protection

In the context of ODU SMP, lockout of protection is a local command and as such is not signalled in the APS protocol. A lockout request is applied to a protection transport entity at a node and causes the node to behave as if the locked out protection transport entity is pre-empted by a higher priority service. An entire link (i.e., one hop between nodes) can be locked out by locking out all the protection transport entities that use the link. It is recommended that a lockout be applied to both end nodes of a link or protection transport entity.

9 ODU SMP APS protocol configuration and behaviour

This clause defines the information elements that are required by the ODU SMP mechanism. The encoding of these elements into the APS channel is not specified in this Recommendation.

A node is considered to be either an end node or an intermediate node in the context of a given protection transport entity.

9.1 Local node configuration

For each protection transport entity, resources must be configured in advance in every node the protection transport entity traverses. Because end nodes and intermediate nodes have different behaviour, they require different information to be configured.

The information that needs to be configured in an end node and intermediate node for each protection connection is shown in Tables 9-1 and 9-2, respectively.

Table 9-1 – Protection information table for end nodes

W_ID	P_ID	ODU type	Pre-emption priority	Adjacency on Segment1	Protection resource(s) on Segment 1

Table 9-2 – Protection information table for intermediate nodes

P_ID	ODU type	Pre-emption priority	Adjacency on Segment1	Protection resource(s) on Segment 1	Adjacency on Segment2	Protection resource(s) on Segment 2

W_ID: The identity of the working transport entity for which a corresponding protection transport entity is configured. The W_ID uniquely identifies the working transport entity within the context of an ODU SMP domain.

P_ID: The identity of the protection transport entity. The P_ID uniquely identifies the protection transport entity within the context of a node.

ODU type: The type of ODU and in the case of ODUflex, the bit rate.

Pre-emption priority: The pre-emption priority of the protection transport entity, as defined in clause 12 of [ITU-T G.808.3].

Adjacency: The identity of the adjacent node (at the ODU layer) in the protection transport entity.

Protection resource(s): The resources used by the connection in the given segment. This includes all the information needed to create the link connection, e.g., the tributary slots, tributary port number and TCM endpoints that will be used by the protection transport entity (when necessary).

9.2 Node behaviour for switching

9.2.1 End node behaviour

An end node is responsible for switching between the working transport entity and protection transport entity. In the context of a protection switching process, an end node is either a tail-end node that detects the need to switch and initiates the protocol, or a head-end node that receives a switching request via the APS protocol.

The switching procedure for the tail-end nodes is triggered by an SD or SF on the working transport entity. The tail-end node will send a protection switching request APS message (for example SF) to its adjacent (downstream) intermediate node to request setting up the corresponding protection transport entity. After this, the tail-end node will wait for the confirmation message (RR) from its adjacent (downstream) intermediate node. The adjacent (downstream) intermediate node will confirm the availability of the protection resource after receiving the switching request message (SF) and send a confirmation message (RR) to the tail-end node. When the confirmation message is received, the protection resource is available and the cross-connection on the tail-end node is established. At this time the signal is bridged to and selected from the protecting transport entity.

The switching procedure for the head-end node is initiated by reception of a switching request APS message from the adjacent (upstream) intermediate node. Receipt of this signal implies the protection transport entity between head-end and tail-end nodes is activated with the exception of the connection in the head-end node itself. If the required resources in the head-end node are

available, the pre-configured cross-connection on the head-end node will be set up by bridging to and selecting from the protecting path and a confirmation message (RR) will be sent back to its adjacent (upstream) intermediate node.

9.2.2 Intermediate node behaviour

Intermediate nodes are responsible for activating/deactivating the cross-connections that form the protection transport entity, which may be shared by different working transport entities. Unlike end nodes, an intermediate node will interact with both the upstream adjacent node and the downstream adjacent node.

In each intermediate node, the interaction with an upstream adjacent node is started by receiving a protection switching request message from an adjacent (upstream) node. Upon receiving the switching request message, the intermediate node needs to identify which protection transport entity should be activated and check the availability of corresponding preconfigured protection resource(s). If the resource is not available (due to failure or being used by higher priority connections), the switching will not be successful; the intermediate node may send a message to notify the end node, or keep trying until the resource is available or the switching request is cancelled. If the resource is idle, the intermediate node will send a confirmation message (RR) to the adjacent node (upstream) to notify the availability of the protection resource and then forward the switching request message to the adjacent (downstream) node, which triggers the interaction with the downstream adjacent node. Then the intermediate node will wait for the confirmation message (RR) from the adjacent (downstream) node, which triggers the intermediate node to set up the cross-connection for the protection transport entity being activated. If the resource is in use by a lower priority protection entity, the lower priority service will be removed and then the intermediate node will follow the procedure as described for the case when the resource is idle.

10 Operational considerations

The proper operation of SMP depends on each node having a consistent configuration for how the protection resources are to be used. As the traffic demands on the network shift, it will be necessary to re-compute the assignment of working transport entities to protecting resources to optimize resource utilization and ensure availability requirements are being met. After the information has been computed, all the nodes must be updated. During the time that the configuration updates are being installed in the nodes, there is a risk of misconnected traffic unless suitable precautions are taken within the control or management plane; these mechanisms are outside the scope of this Recommendation. Appendix II discusses potential ways to address this situation.

Appendix I

ODU SMP configuration examples

(This appendix does not form an integral part of this Recommendation.)

An example for ODU SMP is shown in Figure I.1:

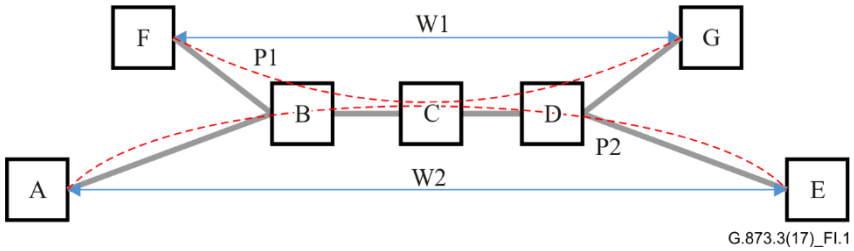

Figure I.1 – ODU SMP example

In this example, there are two ODU0 transport entities: W1 from node F to node G and W2 from node A to node E. The protection path for W1 is named as P1 (F-B-C-D-G). The protection transport entity for W2 is named as P2 (A-B-C-D-E). The section of B-C-D is shared by P1 and P2. There are four end nodes (A, E, F and G) and three intermediate nodes (B, C and D) in this example. P2 has higher priority than P1, setting the pre-emption priority for P2 and P1 to 2 and 1, respectively.

The local configurations of all nodes are shown in Tables I.1 through I.7:

Table I.1 – Protection information table for node A

W_ID	P_ID	ODU type	Pre-emption priority	Adjacency on Segment1	Protection resource on Segment 1
W2	P2	ODU0	2	Node B	List of tributary slots to be used and TCMs to be instantiated

Table I.2 – Protection information table for node B

P_ID	ODU type	Pre-emption priority	Adjacency on Segment1	Protection resource on Segment 1	Adjacency on Segment2	Protection resource on Segment 2
P1	ODU0	1	Node F	List of tributary slots to be used	Node C	List of tributary slots to be used
P2	ODU0	2	Node A	List of tributary slots to be used	Node C	List of tributary slots to be used

Table I.3 – Protection information table for node C

P_ID	ODU type	Pre-emption priority	Adjacency on Segment1	Protection resource on Segment 1	Adjacency on Segment2	Protection resource on Segment 2
P1	ODU0	1	Node B	List of tributary slots to be used	Node D	List of tributary slots to be used
P2	ODU0	2	Node B	List of tributary slots to be used and TCMs to be instantiated	Node D	List of tributary slots to be used

Table I.4 – Protection information table for node D

P_ID	ODU type	Pre-emption priority	Adjacency on Segment1	Protection resource on Segment 1	Adjacency on Segment2	Protection resource on Segment 2
P1	ODU0	1	Node C	List of tributary slots to be used	Node G	List of tributary slots to be used
P2	ODU0	2	Node C	List of tributary slots to be used	Node E	List of tributary slots to be used

Table I.5 – Protection information table for node E

W_ID	P_ID	ODU type	Pre-emption priority	Adjacency on Segment1	Protection resource on Segment 1
W2	P2	ODU0	2	Node D	List of tributary slots to be used and TCMs to be instantiated

Table I.6 – Protection information table for node F

W_ID	P_ID	ODU type	Pre-emption priority	Adjacency on Segment1	Protection resource on Segment 1
W1	P1	ODU0	1	Node B	List of tributary slots to be used and TCMs to be instantiated

Table I-7 – Protection information table for node G

W_ID	P_ID	ODU type	Pre-emption priority	Adjacency on Segment1	Protection resource on Segment 1
W1	P1	ODU0	1	Node D	List of tributary slots to be used and TCMs to be instantiated

Appendix II

ODU SMP operational considerations

(This appendix does not form an integral part of this Recommendation.)

Clause 10 identifies some operational considerations when deploying ODU SMP related to the need to update the configuration of the protection resources in all nodes and the need to ensure misconnections do not happen during this interval.

One potential mechanism would be to prevent protection switching events by using the lockout of protection command for all services. However, in a large network, this approach may not be practical.

A second option would be to choose an encoding that allows for a large amount of protection transport entities to share a protecting resource. This would allow a mechanism similar to the idea of creating 'alternate protection transport entities' within the network or 'alternate connection maps' within single switch fabrics.

The control and/or management plane could establish the new protection transport entities (with new identifiers and protection resource configuration in all nodes in the network). The control and/or management plane would then modify the endpoints of the services to lockout the old protection transport entities (in this way, the traffic will be switched away from the old active protection transport entities and the new protection transport entities will be used, if needed) before deleting them.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018