International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.808.3

(10/2012)

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

Digital networks – General aspects

Generic protection switching – Shared mesh protection

Recommendation ITU-T G.808.3

ITU-T

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
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.808.3

Generic protection switching – Shared mesh protection

Summary

Recommendation ITU-T G.808.3 provides an overview of generic aspects of a shared mesh protection (SMP) mechanism for connection-oriented layer networks that does not depend upon the presence of a control plane. SMP provides a method for sharing resources in the mesh network for protection against one or more failures in the network.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.808.3	2012-10-29	15

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 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 2013

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

Recommendation ITU-T G.808.3

Generic protection switching – Shared mesh protection

1 Scope

This Recommendation provides an overview of generic aspects of a shared mesh protection (SMP) mechanism for connection-oriented layer networks that does not depend upon the presence of a control plane. This mechanism is targeted for mesh network architectures, which offer further efficiencies in protection resource utilization. The primary characteristics of this path-based protection approach involve usage of pre-computation and pre-allocation of resources to maximize speed of recovery. The technology-specific shared mesh protection mechanisms will be defined in technology-specific Recommendation(s).

This version of the Recommendation provides an architecture framework for SMP.

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.780] Recommendation ITU-T G.780/Y.1351 (2010), *Terms and definitions for synchronous digital hierarchy (SDH) networks*.

[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 (2006), *Characteristics of transport equipment – Description methodology and generic functionality*.

[ITU-T G.808.1] Recommendation ITU-T G.808.1 (2010), *Generic protection switching – Linear trail and subnetwork protection*.

[ITU-T G.870] Recommendation ITU-T G.870/Y.1352 (2010), *Terms and definitions for optical transport network*.

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Terms related to actions

3.1.1.1 switch [ITU-T G.870]

3.1.2 Terms related to components

3.1.2.1 bridge [ITU-T G.870]

3.1.2.2 selector [ITU-T G.870]

3.1.2.3 intermediate node [ITU-T G.870]

3.1.3 Terms related to fault conditions

3.1.3.1 signal degrade (SD) [ITU-T G.805]

3.1.3.2 signal fail (SF) [ITU-T G.805]

3.1.4 Terms related to architecture

3.1.4.1 m:n (protection) architecture [ITU-T G.870]

3.1.5 Terms related to operation

3.1.5.1 revertive (protection) operation [ITU-T G.870]

3.1.6 Terms related to signals

3.1.6.1 traffic signal [ITU-T G.870]

3.1.6.2 normal traffic signal [ITU-T G.870]

3.1.6.3 extra traffic signal [ITU-T G.870]

3.1.7 Terms related to switching

3.1.7.1 bidirectional (protection) switching [ITU-T G.780]

3.1.7.2 unidirectional (protection) switching [ITU-T G.780]

3.1.8 Terms related to transport entities

3.1.8.1 link [ITU-T G.805]

3.1.8.2 transport entity [ITU-T G.870]

3.1.8.3 protection transport entity [ITU-T G.870]

3.1.8.4 working transport entity [ITU-T G.870]

3.1.9 protection [ITU-T G.870]

3.1.10 restoration [ITU-T G.870]

3.1.11 switch event [ITU-T G.870]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 protection segment: A link between two SMP nodes on a protection transport entity.

3.2.2 shared mesh protection: A shared mesh protection (SMP) architecture involves multiple normal traffic signals, where each signal has one corresponding working transport entity and one or more protection transport entities, in a meshed network. In an SMP, the protection resources are shared among two or more protection transport entities. Only one of these protection transport entities can use the shared protection resources at any point of time.

3.2.3 shared protection segment: A link between two SMP nodes, where the bandwidth resource on the link is shared by multiple protection transport entities.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APS	Automatic Protection Switching
NUT	Non-pre-emptible Unprotected Traffic
OTN	Optical Transport Network
P	Protection

SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SF	Signal Fail
SMP	Shared Mesh Protection
W	Working

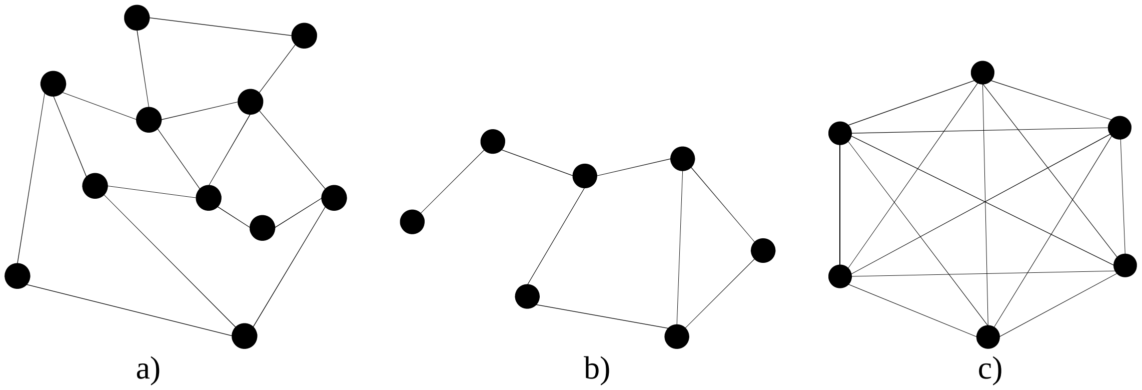
5 Conventions

None.

6 Overview

6.1 Mesh topologies

A meshed transport network is one in which each node in the network is interconnected by at least two links whose remote ends are on different nodes from each other (see example a) of Figure 1). It should be noted that while the overall transport network may contain nodes that do not satisfy the above criteria (see left two nodes in example b) of Figure 1), such nodes would not be considered part of the portion of the transport network defined as being a mesh. A fully meshed topology is one in which each node is directly connected to every other node in a network (see example c) of Figure 1).



1-a: Example of a mesh network
1-b: Example of a network, only a portion of which is meshed
1-c: Example of a fully meshed network

Figure 1 – Examples of mesh network

Most mesh transport networks are only partially meshed (as in example a) of Figure 1), with some nodes fully meshed and others connecting to one or more nodes, but not to all of them (i.e., their maximum number being less than the total number of nodes – 1). While fully meshed network topologies offer the highest degree of survivability in the event of failures, they have the highest degree of transport resource redundancy. Most mesh transport networks are only partially meshed and generally require traversing intermediate nodes to go from each node to every other node.

6.2 Capacity efficiency considerations

Increased sharing of protection resources in mesh network architectures inherently allows for reduction of network costs by eliminating dedicated protection resources. Such architectures may also be designed according to the level of "guaranteed protection" and capacity efficiency desired by the operator, according to the grades of services offered. Capacity efficiency in mesh network architectures can be measured in various ways, including [b-BLTJ.1999]:

i) The fraction of demands that can be protected given the network capacities, point-to-point demands, and working path for each demand;

ii) The needed network capacities for providing 100% protection given point-to-point demands and working path for each demand; or

iii) The total network capacities for working and protection paths given point-to-point demands and provided 100% protection.

The first approach involves finding protection paths for as many demands as possible under link capacity constraints in an existing network. This is distinguished from the latter two approaches, which assume that capacity planning is underway to assure 100% protection for all demands.

It should be noted that at some point the desired degree of network resource optimization (resulting in insufficient link capacity) becomes inversely proportional to the degree of "guaranteed protection" that can be offered. In real capacity-constrained situations, it is necessary to be capable of prioritizing the demands and ensuring that those demands with high availability requirements are always assigned protection paths.

Within this Recommendation, the focus is upon achieving maximal possible protection considering a given network's capabilities, including mechanisms for prioritizing demands to enable those demands with high availability requirements to be assigned protection paths.

7 SMP architecture types

7.1 SMP architecture overview

SMP may be employed in fully meshed and partially meshed transport networks, which include, but are not limited to, long-haul and metro networks. Depending on the degree of inter-connection between network nodes, SMP protection can significantly improve network resource utilization, as compared with alternative 1:1 protection mechanisms.

An SMP architecture involves multiple normal traffic signals, where each signal is associated with a working transport entity and one or more protection transport entities. SMP architecture is based upon m:1 protection (where m may be greater than or equal to one).

In the m:1 SMP architecture, each working transport entity is protected by m protection transport entities. In this architecture, the working transport entity can be protected when one of the m protection transport entities is available.

Each protection transport entity is constructed of one or multiple protection segments. The bandwidth of each protection segment can be shared by multiple protection transport entities. To prevent a network failure from interrupting the protected normal traffic signal, it is recommended that all working transport entities that share protection resources should be disjoint.

The shared bandwidth for the protection segment should be capable of supporting the largest of the corresponding protection transport entities.

NOTE – The protection resources and the information of protection transport entities are pre-configured through a control or management plane, and the detailed description of the pre-configuration process is out of the scope of this Recommendation. The (shared) mesh restoration mechanism based on a control plane is also out of the scope of this Recommendation.

Figure 2 shows an example of a simple m:1 SMP architecture. There are two working transport entities, which are W1 (A-B) and W2 (E-F). The protection transport entities in this example have been configured as follows:

- For W1, there are two protection transport entities P1 (A-C-D-B) and P1' (A-G-H-B);
- For W2, there is a protection transport entity P2 (E-C-D-F).

If a failure of W2 is detected, the corresponding protection transport entity P2 will be activated to transmit the traffic. As a result of the bandwidth for protection segment PS3 being fully occupied by P2, the protection transport entity P1 has no protection capability to provide protection for the working transport entity W1, but the other protection transport entity P1' can be used to protect the working transport entity W1.

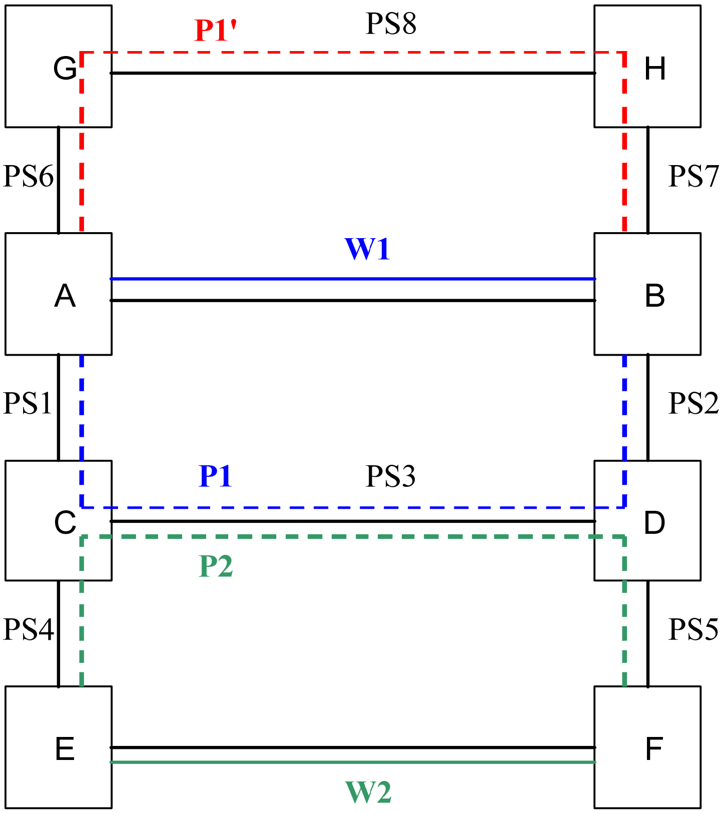


Figure 2 – Example of an m:1 SMP architecture

Figure 3 shows a simple m:1 SMP architecture example where m=1.

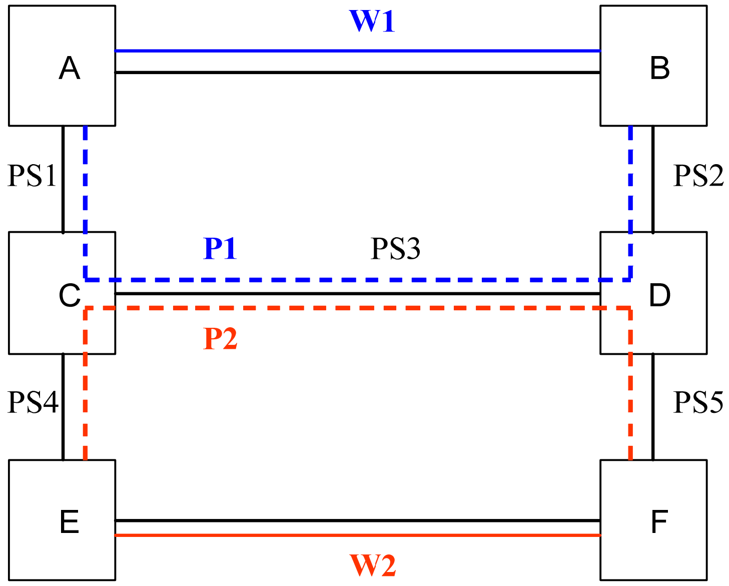
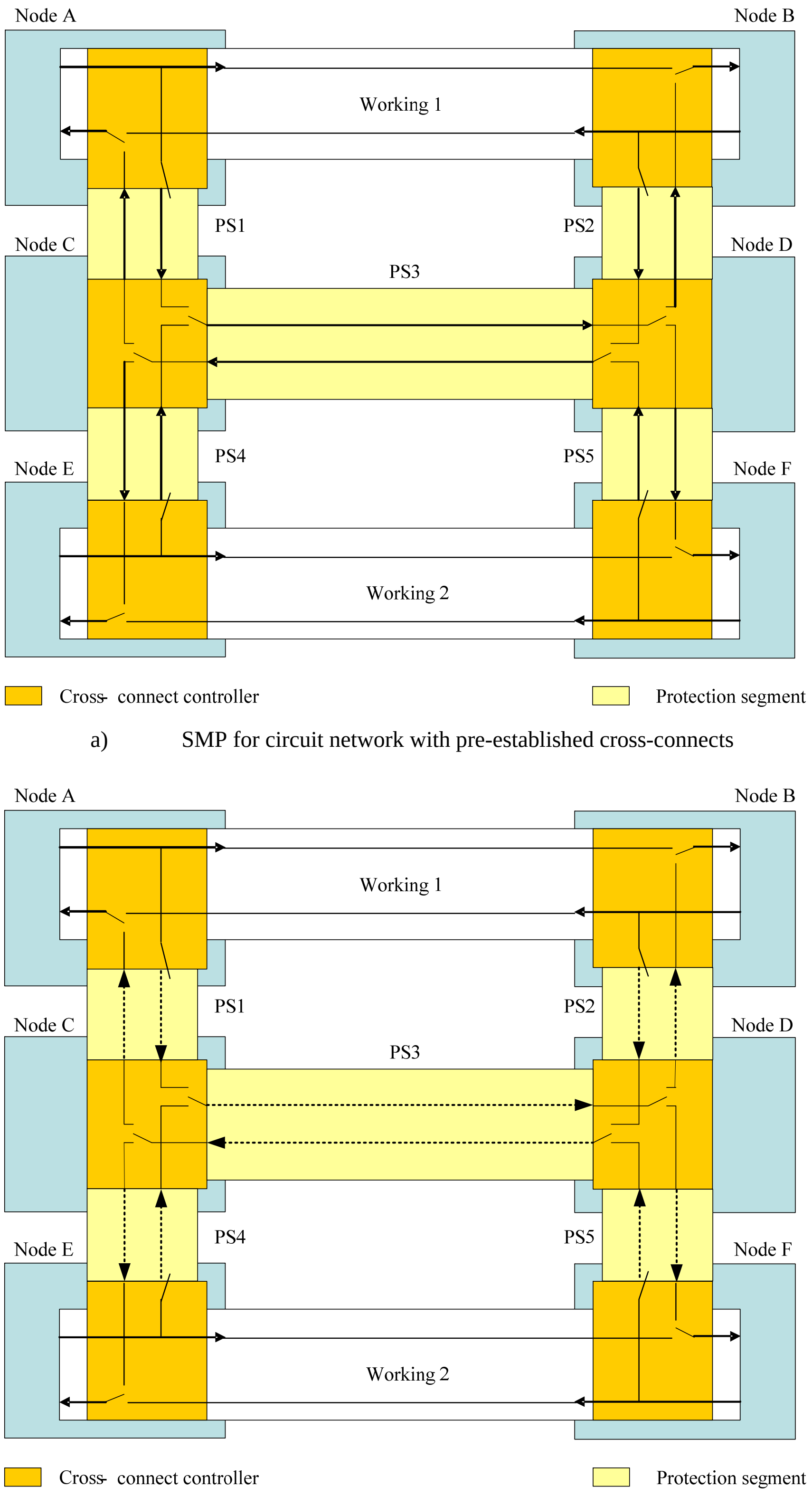


Figure 3 – Example of a 1:1 SMP architecture

7.1.1 SMP for circuit networks

In circuit switch networks (e.g., SDH/OTN, the cross-connects in the intermediate nodes of the protection transport entity cannot be pre-established when the protection segment is shared by multiple protection transport entities. In this case, the intermediate nodes need to establish the cross-connects for the protection transport entity when the protected working transport entity is detected in failure.

The end points of each working transport entity should have the monitoring functions to monitor the status of the working transport entity. The detected signal fail/signal degrade (SF/SD) status will trigger the protection switch procedure. Meanwhile, the nodes along the protection transport entity should also have the monitoring functions to monitor the status of the resources of each protection segment. The worst status among the statuses of the protection segments along a protection transport entity will be notified to the end points. If the status of the protection transport entity is worse than the status of the working transport entity, the end points should prevent the normal traffic signal from being switched to the protection transport entity.



a) SMP for circuit network with pre-established cross-connects

b) SMP for circuit network without pre-established cross-connects

Figure 4 – Examples of SMP for a circuit network

Figure 4 shows the SMP for a circuit network. The cross-connects in the intermediate nodes of the protection transport entities are not pre-established. The link connections may not be allocated before failure is detected, as showed in diagram b) of Figure 4.

The end points (e.g., Node A/B, Node E/F) will monitor the status of Working 1 (W1) and Working 2 (W2). The nodes along the two protection transport entities (i.e., P1 and P2) will monitor the status of each.

When the working transport entity W1 is detected to be impaired or failed and if the status of the protection transport entity is available, upon receiving the APS signal, node C needs to establish the cross-connect between PS1 and PS3 and node D needs to establish the cross-connect between PS3 and PS2 to activate the protection transport entity P1. For the case showed in diagram b) of Figure 4, the link connections of PS1, PS3 and PS2 should be established.

NOTE – Figure 4 illustrates, for simplicity, a 1:1 SMP architecture for circuit networks. This example can be extended to illustrate the m:1 SMP architecture, where there are multiple protection transport entities for one working transport entity.

7.1.2 SMP for packet networks

In packet switch networks, it is possible to pre-establish different protection transport entities sharing the same bandwidth of the shared protection segment. In normal conditions, in which normal traffic signals are transported via working transport entities, only APS and OAM packets are transported via protection transport entities. The bandwidth of a shared protection segment should be allocated in such a way that it may be possible to protect any of the working transport entities whose protection transport entities are sharing the protection segment.

The end points of each working transport entity should have monitoring functions to monitor the status of the working transport entity. The detected SF/SD status will trigger the protection switch procedure. Because the protection transport entity is pre-established, the status of the protection transport entity can also be monitored at the end points.

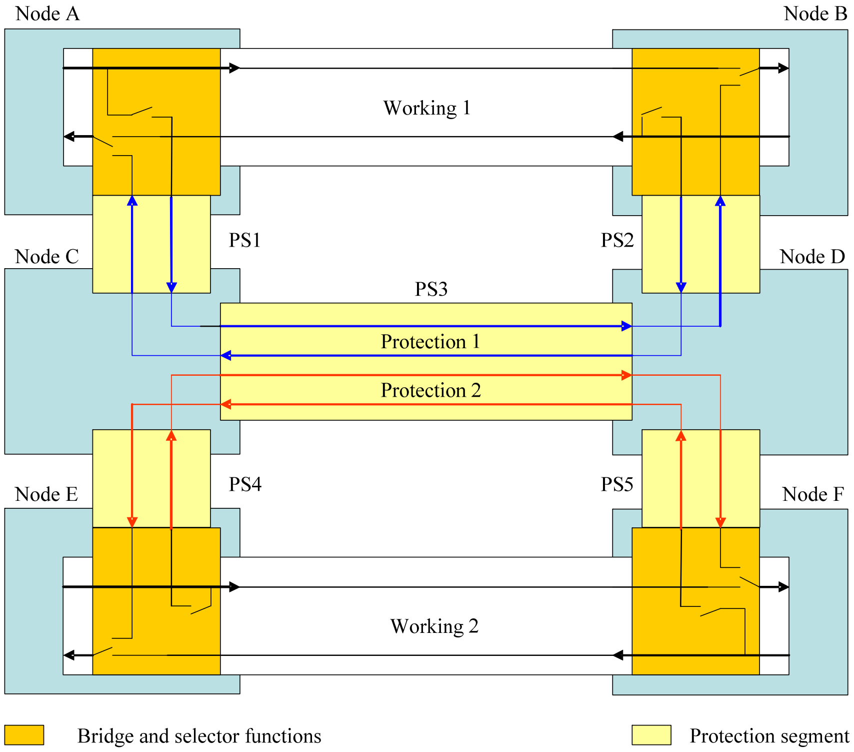


Figure 5 – Example of SMP for a packet network

Figure 5 shows the 1:1 SMP architecture for packet networks. PS3 is shared by the two protection transport entities which are pre-established through A-C-D-B and E-C-D-F, respectively. The two pairs of end points, node A and B pair and node E and F pair will monitor the status of Working 1 and Protection 1, and Working 2 and Protection 2, respectively. When one of the working transport entities is detected to be impaired or failed and if its corresponding protection transport entity is determined to be available, its normal traffic signal must be switched from the working to the protection transport entity. In the intermediate nodes (C and D), there is no need to create cross-connects because they have been already created in advance.

NOTE – Figure 5 illustrates, for simplicity, a 1:1 SMP architecture for packet networks. This example can be extended to illustrate the m:1 SMP architecture, where there are multiple protection transport entities for one working transport entity.

8 Switching types

The SMP mechanism supports the bidirectional switching type, as defined in [ITU-T G.808.1].

For bidirectional SMP, the selectors and bridges at both ends of the protection transport entity are operated. In addition, the bidirectional cross-connects at the intermediate nodes (if they are not pre-established) are activated.

9 Operation types

The SMP mechanism supports only revertive operation, as defined in [ITU-T G.808.1].

10 Non-pre-emptible unprotected traffic (NUT) and extra traffic

SMP scheme supports non-pre-emptible unprotected traffic (NUT).

NUT here is generic, which means that this traffic class does not use any protection resources and is not protected in the event of a failure along its path, but cannot be dropped from the network to allow protection of other traffic.

Extra traffic is for further study.

11 Automatic switch

For further study.

12 Pre-emption principle

For SMP, pre-emption principles are applied for the case when multiple protection transport entities are competing for the same shared resource.

To resolve the competition, two types of information should be taken into account:

- Pre-emption priority: Every protection transport entity is assigned a pre-emption priority that is configured in advance.
- Request type priority: The relative priority of events (fault conditions and external commands) that trigger the protection. The assignment of these priorities is for further study.

Both priorities must be taken into consideration by all the nodes along the protection transport entity.

1) When a resource competition occurs between multiple protection transport entities having different pre-emption priorities, the protection transport entity with the higher pre-emption priority occupies the resources.
2) When a resource competition occurs between multiple protection transport entities having the same pre-emption priority, the protection transport entity having the higher priority request type occupies the resources.

3) In the case where the resource competition occurs between multiple protection transport entities having the same pre-emption and request-type priorities, their transport entity IDs can be used for resolving the contention.

13 Path status monitoring

The status of the working transport entity can be monitored using similar methods as those defined for existing linear protection schemes in [ITU-T G.808.1]. Specific monitoring methods are technology dependent.

Depending on the underlying network transport technology, the protection transport entity may not be established in advance. In this case, there is no direct monitoring of the end-to-end status of the protection transport entity at the protection end points. Therefore, each protection segment needs to notify the end points of the protection transport entity of its status.

If it is possible to pre-establish the protection transport entity, then its status can be monitored using similar methods as those defined for existing linear protection schemes in [ITU-T G.808.1]. Specific monitoring methods are technology dependent.

Each protection segment needs to notify the end points of the protection transport entity of its resource availability. This notification is intended to reduce the likelihood of unnecessary protection switching requests which will otherwise fail once the request reaches the unavailable protection resource.

14 Automatic protection switching (APS) protocol

For further study.

Annex A

Objectives

(This annex forms an integral part of this Recommendation.)

A.1 Shall allow backwards compatibility with core structures/formats of technology-specific Recommendations.

A.2 Shall not impact usage of existing technology-specific linear and ring APS protection mechanisms and communications channels (i.e., co-existence with existing APS specifications).

A.3 Shall allow for any intra-/inter-operator applications for cascaded or nested protection deployments.

A.4 Shall allow for co-existence of ASON-based protection/restoration and SMP protection at inter-domain boundaries.

A.5 Shall be capable of supporting protection of one or more point-to-point bidirectional normal traffic signals from the ingress to the egress of the SMP domain.

A.6 Shall not require that multiple working transport entities sharing the same protection resource(s) have the same end points.

A.7 Shall monitor the status of the working transport entities for SMP protection switching triggers (e.g., SF, SD).

A.8 Shall monitor availability of the shared protection resources along the protection transport entities.

A.9 Shall include support for communicating information on the availability of the shared protection resources along the protection transport entities to the end points of the working transport entities that utilize the resources.

A.10 Shall include support for communicating information among network nodes to perform protection switching. The message encoding and communicating channel between the nodes depends on the specific technology.

A.11 Shall be capable of recovering a normal traffic signal from network failure(s) in a deterministic manner. For example, the protection switching shall complete within a finite (bounded) time, as described within the technology-specific Recommendations.

A.12 Shall include support for a mechanism to detect protocol failures.

A.13 Shall include support for a mechanism to detect possible inconsistencies in configuration between the ingress and egress nodes of an SMP domain.

A.14 Shall be capable of supporting nesting of multiple levels of protection (whether SMP or other schemes such as SNC protection). To achieve this, shall include support for mechanism(s) that allow for coordination of protection activities (e.g., hold-off timer).

A.15 Shall provide a mechanism to avoid protection switching flapping (e.g., wait-to-restore timer).

A.16 Shall include support for multiple links between nodes, allowing for link and node diversity, and should be scalable with respect to the number of links and nodes within the SMP protection domain.

A.17 Shall provide a contention resolution mechanism for permitting only one working transport entity to occupy protection resources in the case that these protection resources are shared by more than one working transport entity having the same priority (due to network topology and resource limitations).

A.18 Shall be capable of supporting the ability to set an upper limit on the maximum number of working transport entities that can share protection resources (which is governed by the specific technology).

A.19 Shall include support for the ability to set an upper bound on the fraction of link resources that can be allocated to protecting transport entities.

A.20 Shall allow for configuration (which may be via the management or control plane) of the protection transport entity identifiers, required bandwidth, and additionally for circuit SMP, the assignment of TSs to ensure the proper operation of the protection switching process.

A.21 Shall support assignment of priority to support the request of a higher-priority transport entity to pre-empt the shared protection resource taken by a lower-priority transport entity.

A.22 Shall only support revertive operation type.

A.23 Shall only support bidirectional switching type.

A.24 Shall be capable of supporting external commands from network operators.

A.25 Shall be capable of supporting protection for more than one failure, including failures that are concurrent and/or failures involving shared resources.

A.26 Shall be capable of protection switching activation initiated by either end or both ends (which may be simultaneous) of the SMP domain.

Appendix I

SMP scenarios

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

This appendix provides some typical scenarios for SMP.

Note that not all the scenarios will be illustrated in this appendix.

I.1 A simple SMP scenario

A simple scenario is illustrated in Figure I.1.The working connection W1 along the path A-B is protected by the protection connection P1 along the path A-P-Q-B, and the other working connection W2 along the path C-D is protected by the other protection connection P2 along the path C-P-Q-D. The protection connection P1 and P2 can share some common resource (i.e., the protection link P-Q can be shared by P1 and P2), because W1 and W2 are disjointed from each other.

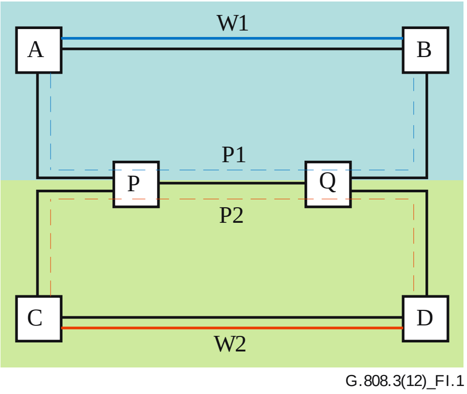


Figure I.1 – Simple SMP scenario

I.2 SMP in mesh network

The more general mesh network in Figure I.2 is used to describe various SMP scenarios.

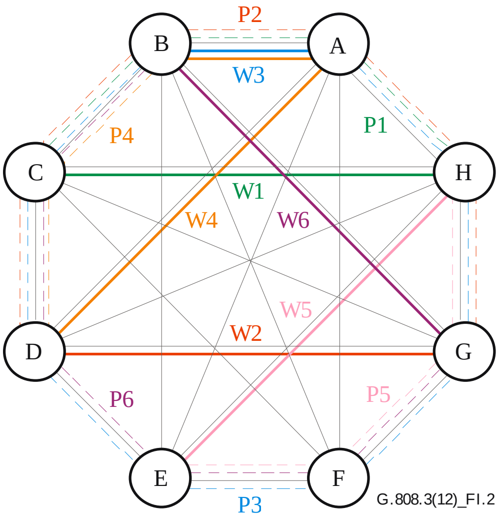


Figure I.2 – Example of SMP

The mesh network in Figure I.2 shows six working paths (W1, W2, W3, W4, W5 and W6) and their protection paths (P1, P2, P3, P4, P5 and P6), as summarized in Table I.1.

Table I.1 – Summary

Colour	Working path	Protection path
Green (W1, P1)	C-H	H-A-B-C
Red (W2, P2)	D-G	G-H-A- B-C-D
Blue (W3, P3)	A-B	B-C-D-E-F-G-H-A
Orange (W4, P4)	B- A-D	B-C-D
Pink (W5, P5)	H-E	H-G-F-E
Purple (W6, P6)	B-G	B-C-D-E-F-G

W3, W4 and W6 have a same end node B.W2 and W4 have a same end node D. W2 and W6 have a same end node G. W1 and W5 have a same end node H. Node A is an intermediate node of W4, but also an end node of W3.

NOTE – Each scenario is separated from each other.

Scenario 1

A simple scenario of SMP is that two protection paths share common resources.

Colour	Working path	Protection path
Green (W1, P1)	C-H	H-A-B-C
Red (W2, P2)	D-G	G-H-A- B-C-D

In Figure I.2, the working path W1 along the link C-H is protected by the protection path P1 along the segment H-A-B-C, and the working path W2 along the link D-G is protected by the other protection path P2 along the segment G-H-A- B-C-D. P1 and P2 can share some common resource (i.e., the protection segment H-A-B-C).

Scenario 2

A port or link can have some resources that are used for working paths and other resources that are used for protection paths.

Colour	Working path	Protection path
Green (W1, P1)	C-H	H-A-B-C
Red (W2, P2)	D-G	G-H-A- B-C-D
Blue (W3, P3)	A-B	B-C-D-E-F-G-H-A
Orange (W4, P4)	B- A-D	B-C-D

As shown in Figure I.3, the link A-B contains both working traffic for W3/W4 and also a protection resource that is used by P1/P2.

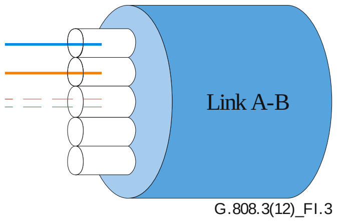


Figure I.3 – Detail of Link A-B

Scenario 3

There are multiple protection resources on a link. In this case, the working paths that have links in common can still use the same protection link for protection purpose as long as different resource is assigned for their corresponding protection paths.

Colour	Working path	Protection path
Blue (W3, P3)	A-B	B-C-D-E-F-G-H-A
Orange (W4, P4)	B- A-D	B-C-D

For example, as shown in Figure I.4, the segment B-C-D supports two protection paths on a single link but with different resources. Therefore, although W3 and W4 both have link A-B, they are still allowed to use segment B-C-D as part of their protection paths (P3 and P4).

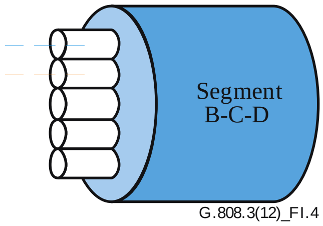


Figure I.4 – Detail of Segment B-C-D

Scenario 4

A particular resource used for protection can be an end point for some protection paths and an intermediate point for other protection paths.

Colour	Working path	Protection path
Orange (W4, P4)	B- A-D	B-C-D
Pink (W5, P5)	H-E	H-G-F-E
Purple (W6, P6)	B-G	B-C-D-E-F-G

For example, in Figure I.2, Node G, and in particular the port associated with the link G-F, illustrates how the protection resource can be an intermediate point for a path (i.e., P5) and an end point for another path (i.e., P6). Similarly Node D, and in particular the port associated with the link D-C, is an intermediate point for P6 and an end point for P4.

Scenario 5

A working path may be a member of multiple disjoint shared risk groups (SRGs).

Colour	Working path	Protection path
Blue (W3, P3)	A-B	B-C-D-E-F-G-H-A
Orange (W4, P4)	B- A-D	B-C-D
Pink (W5, P5)	H-E	H-G-F-E
Purple (W6, P6)	B-G	B-C-D-E-F-G

As shown in Figure I.5, W6 (in purple) is a member of three shared risk groups: W6 and W4 represent a SRG because of protection segment B-C-D; W6 and W3 represent the second SRG because of protection segment D-E-F-G; W6 and W5 represent the third SRG because of protection segment E-F-G.

In this case, W3 and W5 also represent an SRG because of segments E-F-G, but W4 and W5 do not represent a SRG since they do not share protection resource (i.e., there are two protection resources available in segment B-C-D). Thus, W4 can share risk with both W3 and W5.

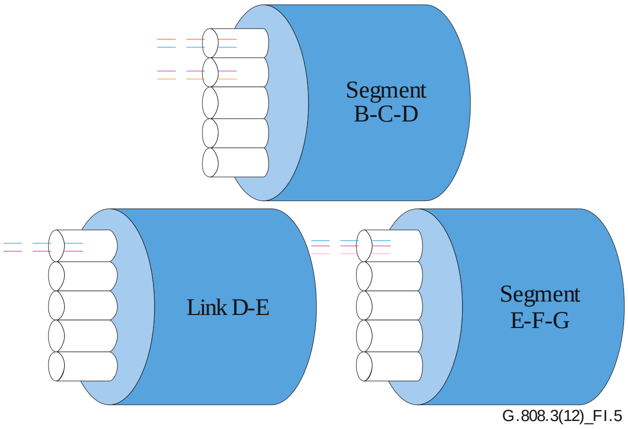


Figure I.5 – Detail of the Segment B-C-D and Segment D-E-F-G

Scenario 6

A protection resource associated with one node may support multiple protection paths. While each of the protection paths is a point-to-point connection, if the paths happen to share some resources, there are some elements of point-to-multipoint and multipoint-to-point circuits that must be taken into account when setting up monitoring of the protection path.

Colour	Working path	Protection path
Orange (W4, P4)	B- A-D	B-C-D
Purple (W6, P6)	B-G	B-C-D-E-F-G

As shown in Figure I.6, the port associated with Node B that terminates segment B-C-D illustrates a scenario where two protection paths (i.e., P4 and P6) share segment B-C-D, but P4 and P6 have different end nodes (i.e., P4 ends in Node D, P6 ends in Node G). At any point in time, at the port in Node B, there will either be no path, or P4, or P6. Because of this, care must be taken in the configuration of trail trace identifier (TTI) values and trace identifier mismatch defect (dTIM) detection criteria in the case where there is to be a tandem connection that monitors the entire protection path.

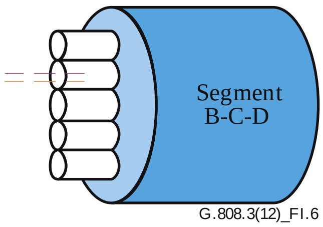


Figure I.6 – Detail of Segment B-C-D

These scenarios need to be taken into account when designing the APS protocol and monitoring architectures.

Appendix II

Overview of shared mesh restoration (SMR) and shared mesh protection (SMP) operation

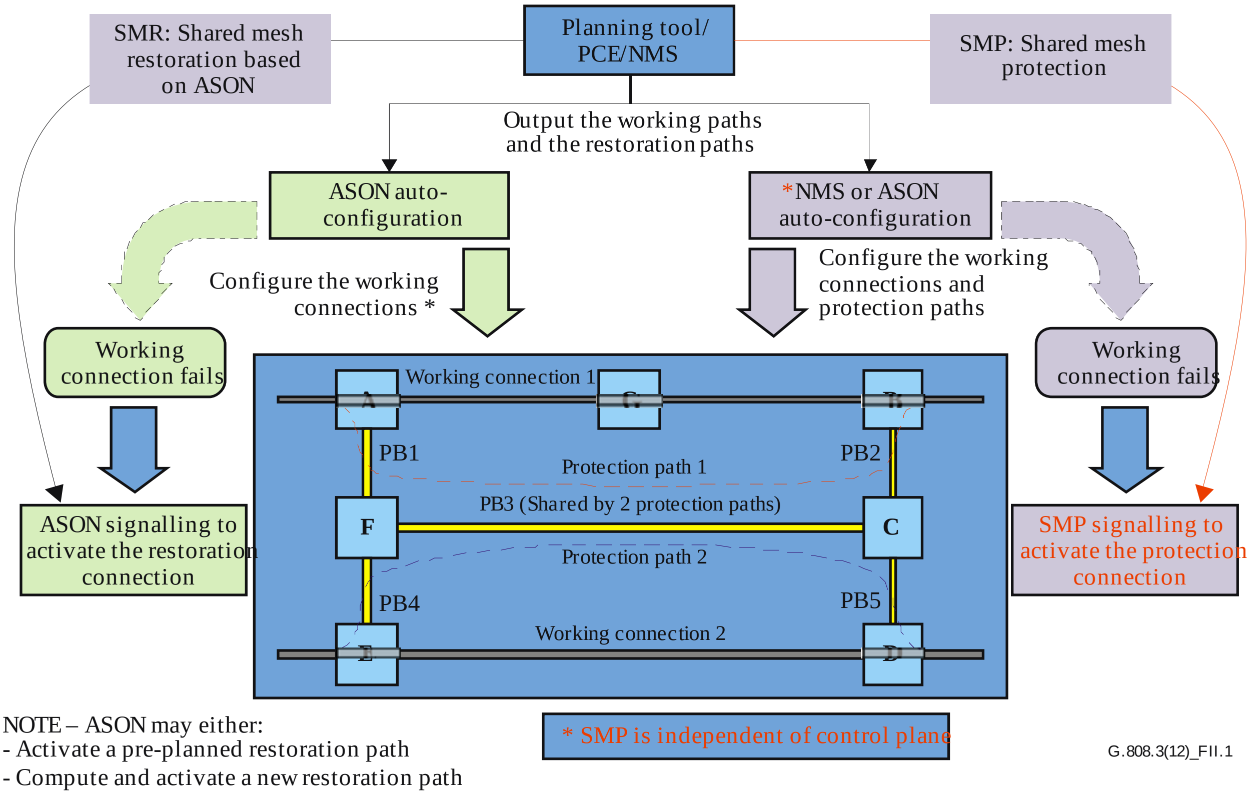
(This appendix does not form an integral part of this Recommendation.)

[ITU-T G.805] describes transport network availability enhancement techniques, where "protection" denotes replacement of a failed resource with a pre-assigned standby and "restoration" denotes replacement of a failed resource by re-routing using spare capacity.

[b-ITU-T G.8080] describes protection as a mechanism for enhancing availability of a connection through the use of additional, assigned capacity. Automatically switched optical network (ASON) restoration of a call (connection service) is described as the replacement of a failed connection by re-routing the call using spare capacity.

Different mechanisms have been defined for restoration in ASON networks. Note that the restoration mechanism that has the greatest similarity to SMP is often called shared mesh restoration with pre-calculated and pre-signalled restoration paths. This means that upon the successful creation of a new connection along its nominal/active path, a backup path is calculated (which should be fully disjoint with respect to the nominal/active path). A signalling session is subsequently established along this backup path and the availability of free resources checked during the establishment of the signalling session. Once, this process is complete, the backup path is activated when the nominal/active path is affected by a failure.

Figure II.1, illustrates the distinction between ASON shared mesh restoration and SMP.


SMR: Shared mesh restoration based on ASON
Planning tool/ PCE/NMS
SMP: Shared mesh protection
Output the working paths and the restoration paths
ASON auto-configuration
*NMS or ASON auto-configuration
Configure the working connections *
Configure the working connections and protection paths
Working connection fails
Working connection fails
ASON signalling to activate the restoration connection
SMP signalling to activate the protection connection
Working connection 1
A
G
B
PB1
PB2
Protection path 1
PB3 (Shared by 2 protection paths)
F
C
Protection path 2
PB4
PB5
Working connection 2
E
D
* SMP is independent of control plane

NOTE – ASON may either:
- Activate a pre-planned restoration path
- Compute and activate a new restoration path

G.808.3(12)_FII.1

Figure II.1 – SMR and SMP

Bibliography

[b-ITU-T G.8080] Recommendation ITU-T G.8080/Y.1304 (2012), *Architecture for the automatically switched optical network*.

[b-BLTJ.1999] Doshi, B. T. et al. (1999), *Optical network design and restoration*, Bell Labs. Technical Journal, pp. 58-84, Jan.-Mar. 1999.

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	Terminals and subjective and objective assessment methods
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

Printed in Switzerland
Geneva, 2013