

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.808

Amendment 1
(03/2018)

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

Digital networks – General aspects

Terms and definitions for network protection and
restoration

Amendment 1

Recommendation ITU-T G.808 (2016) – Amendment 1

ITU-T



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.808

Terms and definitions for network protection and restoration

Amendment 1

Summary

Recommendation ITU-T G.808 provides terms, definitions and abbreviations used in Recommendations that describe network protection and restoration. It contains a list of the definitions and abbreviations introduced in Recommendations associated with network protection and restoration. This Recommendation can be considered to be a companion to Recommendations ITU-T G.870/Y.1352, ITU-T G.8001/Y.1354, ITU-T G.8081/Y.1353 and ITU-T G.8101/Y.1355. The goal of this Recommendation is to be a single normative source for terms in this subject area.

Amendment 1 clarifies the terms used to describe the time intervals related to protection switching (clause 3.2.9).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.808	2016-11-13	15	11.1002/1000/13083
1.1	ITU-T G.808 (2016) Amd. 1	2018-03-16	15	11.1002/1000/13525

* 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 2018

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	10
5 Conventions	10
Annex A – Terms specific to ring protection.....	11
Bibliography.....	12

Recommendation ITU-T G.808

Terms and definitions for network protection and restoration

Amendment 1

Editorial note: This is a complete-text publication. Modifications introduced by this amendment are shown in revision marks relative to Recommendation ITU-T G.808 (2016).

1 Scope

This Recommendation contains a complete listing of the terms, definitions and abbreviations introduced in the Recommendations associated with network protection and restoration in a generic manner. Terms specific to particular types of protection or restoration, or to protection and restoration of specific technologies, are not included.

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 (2012), *Characteristics of transport equipment – Description methodology and generic functionality*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 adaptation function (A)** [ITU-T G.806]
- 3.1.2 adapted information (AI)** [ITU-T G.805]
- 3.1.3 characteristic information** [ITU-T G.805]
- 3.1.4 connection** [ITU-T G.805]
- 3.1.5 connection function (C)** [ITU-T G.806]
- 3.1.6 defect** [ITU-T G.806]
- 3.1.7 failure** [ITU-T G.806]
- 3.1.8 fault** [ITU-T G.806]
- 3.1.9 function** [ITU-T G.806]

- 3.1.10 **layer** [ITU-T G.780]
- 3.1.11 **link connection** [ITU-T G.805]
- 3.1.12 **network connection** [ITU-T G.805]
- 3.1.13 **process** [ITU-T G.806]
- 3.1.14 **reference point** [ITU-T G.780]
- 3.1.15 **section** [ITU-T G.806]
- 3.1.16 **signal degrade (SD)** [ITU-T G.806]
- 3.1.17 **signal fail (SF)** [ITU-T G.806]
- 3.1.18 **subnetwork connection** [ITU-T G.805]
- 3.1.19 **trail** [ITU-T G.805]
- 3.1.20 **transport entity** [ITU-T G.805]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 General protection terms

3.2.1.1 hitless protection switch: A protection switch that does not cause characteristic or adapted information loss, duplication, disorder, or bit errors upon protection switching action.

3.2.1.2 impairment: Fault or performance degradation, which may lead to triggering of SF or SD.

3.2.1.3 network survivability: The set of capabilities that allow a network to restore affected traffic in the event of an impairment.

3.2.1.4 protection: The use of pre-assigned capacity between nodes.

3.2.1.5 protection control: The information and set of processes for providing control of protection switching for a trail or subnetwork connection.

3.2.1.6 protected domain: The protected domain defines one or more transport entities (trails, subnetwork connections), for which a survivability mechanism is provided in the event of impairment affecting that or those transport entities.

3.2.1.7 protection group: The collection of head-end and tail-end functions, 1 to n normal traffic signals, optionally an extra traffic signal, 1 to n working transport entities, and a single protection transport entity that are used to provide extra reliability for the transport of normal traffic signals.

3.2.1.8 protection ratio: The quotient of the actually protected bandwidth divided by the traffic bandwidth, which is intended to be protected.

3.2.1.9 restoration: The use of any capacity available between nodes for protection. In general, the algorithms used for restoration will involve re-routing. When restoration is used, a percentage of the transport network capacity will be reserved for the re-routing of normal traffic.

3.2.1.10 signal degrade group (SDG): A signal indicating the associated group data has degraded.

3.2.1.11 signal fail group (SFG): A signal indicating the associated group has failed.

3.2.1.12 switch:

- 1) (*For the selector*) The action of selecting normal traffic from the (current) standby transport entity rather than the (current) active transport entity.
- 2) (*For the bridge – in the case of permanent connection to working*) The action of connecting or disconnecting the normal traffic to the protection transport entity.

- 3) (*For the case of non-permanent connection to working*) The action of connecting the normal traffic signal to the (current) standby transport entity.

3.2.1.13 switch event: A switch event exists if either a fault condition on a working transport entity or an external command exists, and the protection algorithm has concluded that this fault condition or external command is the highest priority event.

3.2.2 Transport entities related to protection

3.2.2.1 active transport entity: The transport entity from which the protection selector selects the normal traffic signal.

3.2.2.2 protection transport entity: The transport entity allocated to transport the normal traffic signal during a switch event. The protection transport entity may be used to carry extra traffic in the absence of a switch event. When there is a switch event, normal traffic on the affected working transport entity is bridged onto the protection transport entity, pre-empting the extra traffic (if present).

3.2.2.3 standby transport entity: The transport entity from which the protection selector does not select the normal traffic signal.

3.2.2.4 transport entity protection: A method that allows transporting a traffic signal via more than one pre-assigned transport entity. The transport of a normal traffic signal via a working transport entity is replaced by the transport of this normal traffic signal via a protection transport entity if the working transport entity fails (SF condition), or if its performance falls below a required level (SD condition).

3.2.2.5 working transport entity: The transport entity over which the normal traffic signal is transported.

3.2.3 Signal types

3.2.3.1 extra traffic signal: Traffic signal that is carried over the protection transport entity and/or bandwidth when that transport entity/bandwidth is not being used for the protection of a normal traffic signal; i.e., when the protection transport entity is on standby. Whenever the protection transport entity/bandwidth is required to protect or restore the normal traffic on the working transport entity, the extra traffic is pre-empted. Extra traffic is not protected.

3.2.3.2 normal traffic signal: Traffic signal that is protected by two alternative transport entities, called working and protection transport entities.

3.2.3.3 null signal: The null signal can be any kind of signal that conforms to the signal structure (characteristic or adapted information) of the reference point in the specific layer. By default, it is the signal inserted by a connection function on an output, which is not connected to one of its inputs. The null signal is ignored (not selected) at the sink end of the protection. The null signal is indicated in the APS protocol if the protection transport entity is not used to carry the normal or extra traffic signal.

3.2.4 Protection architecture terms

3.2.4.1 1+1 (protection) architecture: A 1+1 protection architecture has one normal traffic signal, one working transport entity, one protection transport entity and a permanent bridge.

At the source end, the normal traffic signal is permanently bridged to both the working and the protection transport entities. At the sink end, the normal traffic signal is selected from the better of the two transport entities.

Due to the permanent bridging, the 1+1 (protection) architecture does not allow an unprotected extra traffic signal to be provided.

3.2.4.2 1:n (protection) architecture ($n \geq 1$): A 1:n protection architecture has n normal traffic signals, n working transport entities and one protection transport entity. It may have one extra traffic signal.

At the source end, a normal traffic signal is either permanently connected to its working transport entity and may be connected to the protection transport entity (in the case of a broadcast bridge), or is connected to either its working or the protection transport entity (in the case of a selector bridge). At the sink end, the normal traffic signal is selected from either the working or the protection transport entity.

An unprotected extra traffic signal can be transported via the protection transport entity, whenever the protection transport entity is not used to carry a normal traffic signal.

3.2.4.3 (1:1)ⁿ protection architecture: n parallel 1:1 protection architectures, which have their n protection transport entities share (and compete for) the protection bandwidth. It has n normal traffic signals, n working transport entities and n protection transport entities. It may have an extra traffic signal, in which case an additional protection transport entity will be present.

NOTE – This architecture is applicable in cell/packet layer networks.

3.2.4.4 m:n (protection) architecture: An m:n protection architecture has n normal traffic signals, n working transport entities and m protection transport entities. It may have up to m extra traffic signals.

At the source end, a normal traffic signal is either permanently connected to its working transport entity and may be connected to one of the protection transport entities (in the case of a broadcast bridge), or is connected to either its working or one of the protection transport entities (in the case of a selector bridge). At the sink end, the normal traffic signal is selected from either its working or one of the protection transport entities.

Up to m unprotected extra traffic signals can be transported via the m protection transport entities whenever the protection transport entities are not used to carry a normal traffic signal.

3.2.5 Types of nodes in protection groups

3.2.5.1 head-end: The head-end of a protection group is the end where the bridge process is located. In the case where traffic is protected in both directions of transmission, the head-end process is present at every end of the protection group.

3.2.5.2 intermediate node: A node on either the working transport entity physical route or the protection transport entity physical route in-between the source and sink nodes of the corresponding protected domain.

3.2.5.3 sink node: The node at the egress of a protected domain, where a normal traffic signal may be selected from either the working transport entity or the protection transport entity.

3.2.5.4 source node: The node at the ingress to a protected domain, where a normal traffic signal may be bridged to the protection transport entity.

3.2.5.5 tail-end: The tail-end of a protection group is the end where the selector process is located. In the case where traffic is protected in both directions of transmission, the tail-end process is present at every end of the protection group.

3.2.6 Characteristics of protection groups

3.2.6.1 group: Two or more transport entities, which are treated as a single entity for protection switching. Typically, those transport entities are routed over the same links within the protected domain.

3.2.6.2 non-revertive (protection) operation: A protection switching operation, where the transport and selection of the normal traffic signal does not return to the working transport entity if the switch requests are terminated.

3.2.6.3 protection class: group: Protection is performed for a set of transport entities.

3.2.6.4 protection class: individual: Protection is performed for a single transport entity.

3.2.6.5 protection class: network connection protection: Special case of subnetwork connection protection.

3.2.6.6 protection class: trail protection: Transport entity protection for the case where the transport entity is a trail. The trail is protected by adding bridges and selectors at both ends of the trail, and an additional trail between these bridges and selectors.

The determination of a fault condition on a trail within the protected domain is performed by means of trail monitoring.

3.2.6.7 revertive (protection) operation: A protection switching operation, where the transport and selection of the normal traffic signal (service) always returns to (or remains on) the working transport entity if the switch requests are terminated; i.e., when the working transport entity has recovered from the defect or the external request is cleared.

3.2.6.8 subnetwork connection protection: Transport entity protection for the case where the transport entity is a subnetwork connection. The serial compound link connection within the subnetwork connection is protected by adding bridges and selectors in the connection functions at the edges of the protected domain and an additional serial compound link connection between these connection functions.

The determination of a fault condition on a serial compound link connection within the protected domain can be performed as follows:

- sublayer monitored (/S): Each serial compound link connection is extended with tandem connection monitoring or segment termination/adaptation functions to derive the fault condition status independent of the traffic signal present.
- non-intrusive monitored (/N): Each serial compound link connection is extended with a non-intrusive monitoring termination sink function to derive the fault condition status from the traffic signal that is present.
- inherent monitored (/I): The fault condition status of each link connection is derived from the status of the underlying server layer trail.
NOTE – This inherent monitoring is also applicable for SDH VC-n serial compound link connections.
- test monitored (/T): Each serial compound link connection's fault condition status is derived from an additional monitored serial compound link connection transported via the same serial compound link.

3.2.7 Terms for bridges and selectors

3.2.7.1 bridge: The function that connects the normal and extra traffic signals to the working and protection transport entities.

3.2.7.2 broadcast bridge: For 1:n, m:n, (1:1)ⁿ architectures, the bridge permanently connects the normal traffic signal to the working transport entity. In the event of protection switching, the normal traffic signal is additionally connected to the protection transport entity. The extra traffic signal is either not connected or connected to the protection transport entity.

3.2.7.3 permanent bridge: For a 1+1 architecture, the bridge connects the normal traffic signal to both the working and protection entities.

3.2.7.4 selector: The function that extracts the normal traffic signal either from the working or the protection transport entity. The extra traffic signal is either extracted from the protection transport entity, or is not extracted; in the latter case, an alarm indication signal (AIS) signal will be output.

3.2.7.5 selector bridge: For 1:n, m:n, (1:1)ⁿ architectures, the bridge connects the normal traffic signal to either the working or the protection transport entity. The extra traffic signal is either not connected or connected to the protection transport entity. See Figure 1.

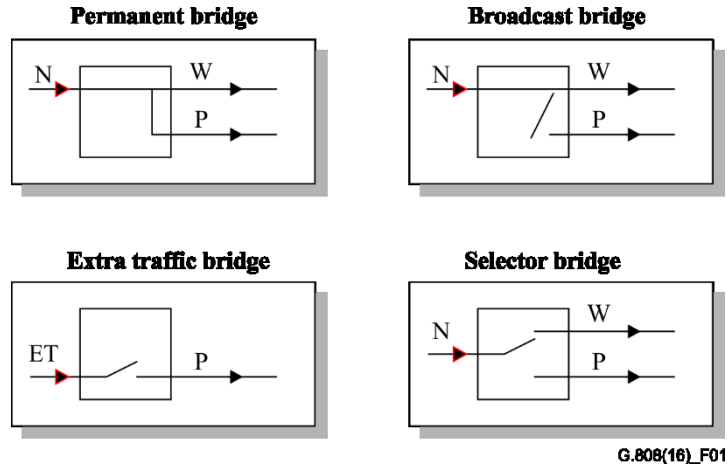


Figure 1 – Protection bridges

3.2.7.6 merging selector: For 1:1 and (1:1)ⁿ architectures, a selector which connects permanently the normal traffic signal output with both the working and protection transport entity inputs.

NOTE – This alternative works only in combination with a selector bridge. To prevent that AIS/forward defect indication (FDI) or misconnected/mismerged traffic on the standby transport entity is merged with the normal traffic signal selected from the active transport entity, the merging selector includes switches in both working and protection inputs. The active transport entity will have its switch closed, while the standby transport entity will have its switch opened. Consequently, a merging selector is like a distributed selective selector.

3.2.7.7 selective selector: A selector, which connects the normal traffic signal output with either the working or protection transport entity inputs, but not both simultaneously. See Figure 2.

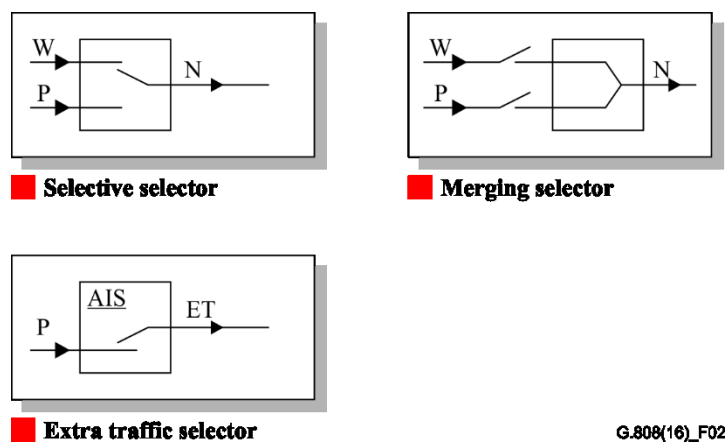


Figure 2 – Protection selectors

3.2.8 APS protocol-related terms

3.2.8.1 APS channel: Automatic protection switch (APS) channel is used to carry information between the two ends of a linear protection group to coordinate the head-end bridge with the tail-end selector for 1:n protection, and to coordinate the selectors in both directions in the case of bidirectional protection.

3.2.8.2 APS protocol: 1-phase: A means to align the two ends of the protected domain via the exchange of a single message ($Z \rightarrow A$).

For (1:1)ⁿ architectures, the bridge/selector at Z are operated before it is known if Z's condition has priority over the condition at A. When A confirms the priority of the condition at Z, it operates the bridge and selector. For unidirectional switching, the priority is determined by Z only and the selector at Z and bridge at A are operated. For 1+1 architectures, the bridges are permanent and only the selectors are to be operated.

3.2.8.3 APS protocol: 2-phase: A means to align the two ends of the protected domain via the exchange of two messages ($Z \rightarrow A, A \rightarrow Z$).

For (1:1)ⁿ architectures, Z signals the switch condition to A and operates the bridge. When A confirms the priority of the condition at Z, it operates the bridge and selector. On receipt of confirmation, Z operates its selector. For unidirectional switching, the priority is determined by Z only and the selector at Z and bridge at A are operated. For 1+1 architectures, the bridges are permanent and only the selectors are to be operated.

3.2.8.4 APS protocol: 3-phase: A means to align the two ends of the protected domain via the exchange of three messages ($Z \rightarrow A, A \rightarrow Z, Z \rightarrow A$).

For 1:n, m:n architectures, Z does not perform any switch action until A confirms the priority of the condition at Z. When A confirms the priority, it operates the bridge. On receipt of confirmation, Z operates its selector and bridge and indicates the bridge action to A. A finally operates the selector. For 1+1 architectures, the bridges are permanent and only the selectors are to be operated.

3.2.8.5 automatic switch: A switch action initiated automatically as a result of an SD or SF being detected. SF is higher priority than SD. It switches normal traffic signal #i to the protection transport entity, unless an equal or higher priority switch commands is in effect. Normal traffic signal that is present on the protection transport entity with a lower priority request is transferred to and selected from its working transport entity.

3.2.8.6 clear: Clears the active near-end lockout of protection, forced switch, manual switch, WTR state, or exercise command.

3.2.8.7 clear lockout of normal traffic signal #i: Clears the lockout of normal traffic signal #i command.

NOTE – In bidirectional 1:n switching, remote bridge requests for normal traffic signal #i will still be honoured to prevent APS protocol failures. As a result, a normal traffic signal must be locked out at both ends to prevent it from being selected from the protection entity as a result of a command or fault condition at either end. Multiples of these commands may coexist for different normal traffic signals.

3.2.8.8 do not revert normal traffic signal #i: In non-revertive operation, this is used to maintain a normal traffic signal to be selected from the protection transport entity.

3.2.8.9 exercise signal: Issues an exercise request for that signal (null signal, normal traffic signal, extra traffic signal) and checks responses on APS messages, unless the protection transport entity is in use. The switch is not actually completed, i.e., the selector is not operated by an exercise request.

3.2.8.10 forced switch: A switch action initiated by an operator command. It switches the extra traffic signal, normal traffic signal #i, or the null signal to the protection transport entity, unless an equal or higher priority switch command is in effect. In the case of forced switching extra traffic or null signal to the protection transport entity, a normal traffic signal that is present on the protection transport entity is transferred to and selected from its working transport entity.

For the case where an APS protocol is in use, an SF on the protection transport entity (over which the APS signal is routed) has priority over the forced switch.

3.2.8.11 freeze: A temporarily configured action initiated by an operator command. It prevents any switch action to be taken and as such freezes the current state. Until the freeze is cleared, additional near-end external commands are rejected. Fault condition changes and received APS messages are ignored. When the freeze command is cleared (**clear freeze**), the state of the protection group is recomputed based on the fault conditions and received APS message.

3.2.8.12 lockout of normal traffic signal #i: A temporary configuration action initiated by an operator command. It ensures that the normal traffic signal #i is temporarily not allowed to be routed via its protection transport entity. Commands for normal traffic signal #i will be rejected. SF or SD will be ignored for normal traffic signal #i.

3.2.8.13 lockout of protection transport entity #i: A temporary configuration action initiated by an operator command. It ensures that the protection transport entity #i is temporarily not available to transport a traffic signal (either normal or extra traffic).

3.2.8.14 manual switch: A switch action initiated by an operator command. It switches the extra traffic signal, normal traffic signal #i, or the null signal to the protection transport entity, unless a fault condition exists on other transport entities or an equal or higher priority switch command is in effect. In the case of a manual switch of extra traffic or null signal, a normal traffic signal present on the protection transport entity is transferred to and selected from its working transport entity.

3.2.8.15 no request (NR): All normal traffic signals are selected from their corresponding working transport entities. The protection transport entity carries either the null signal, extra traffic, or a bridge of the single normal traffic signal in a 1+1 protection group.

3.2.8.16 protection communication channel: A control channel for exchanging configuration information between head-end and tail-end about a protection group.

3.2.8.17 wait-to-restore normal traffic signal #i: In revertive operation, after the clearing of an SF or SD on working transport entity #i, maintains normal traffic signal #i as selected from the protection transport entity until a wait-to-restore timer expires. If the timer expires prior to any other event or command, the normal traffic signal will be transferred to the working transport entity and the protection group state will be changed to NR. This is used to prevent frequent operation of the selector in the case of intermittent failures. The wait-to-restore state will only be entered if there is no SF or SD condition for the protection transport entity.

3.2.9 Time intervals related to protection switching

~~**3.2.9.1 detection time:** The time between the occurrence of the fault or degradation and its detection as a defect condition and consequential activation of SF or SD condition.~~

~~**3.2.9.2 hold-off time:** The time between the declaration of an SF or SD condition and the initialization of the protection switching algorithm.~~

~~**3.2.9.3 switching time:** Time between the initialization of the protection switching algorithm and the moment the traffic is selected from the standby transport entity.~~

~~NOTE—This definition for "switching time" is different in context to the definition found in [b-ITU-T G.671].~~

~~**3.2.9.4 wait-to-restore time:** A period of time that must elapse before a transport entity that has recovered from an SF or SD condition can be used again to transport the normal traffic signal and/or to select the normal traffic signal from.~~

3.2.9.1 detection time, T_1 : The time interval between the occurrence of the network impairment (e.g., a fault or a degradation) and its detection as an SF or SD defect condition.

3.2.9.2 hold-off time, T_2 : The time interval between the detection of an SF or SD condition and the confirmation of an SF or SD condition as the starting condition of the protection switching operations.

3.2.9.3 confirmation time, T_c : The time interval between the occurrence of the network impairment and the confirmation of an SF or SD condition as the starting condition of the protection switching operations: $T_c = T_1 + T_2$. See Figure 3.

3.2.9.4 protection switching operations time, T_3 : The time interval between the start of the protection switching operations (e.g., the confirmation of an SF or an SD condition) and the completion of the processing and transmission of the control signals required to effect protection switching.

3.2.9.5 protection switching transfer time, T_4 : The time interval between completion of the processing and transmission of the control signals required to effect protection switching and the completion of protection switching operations.

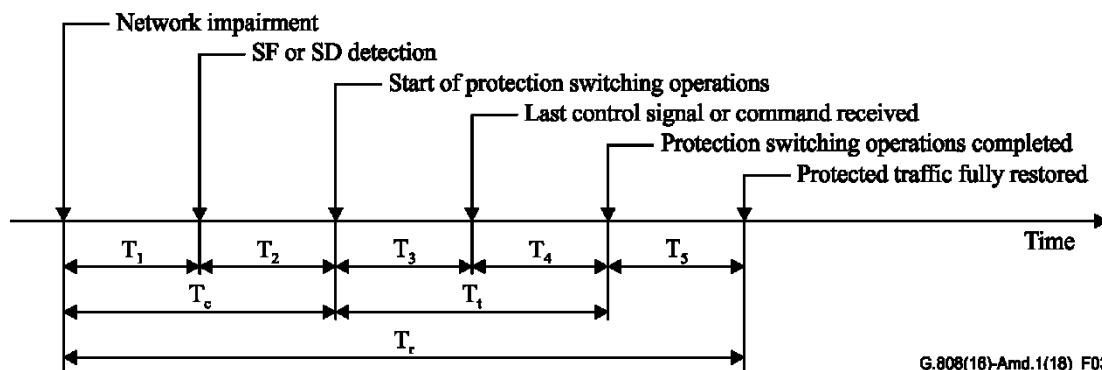
3.2.9.6 transfer time, T_t : The time interval between the start of the protection switching operations (e.g., the confirmation of an SF or an SD condition) and the completion of the protection switching operations: $T_t = T_3 + T_4$. See Figure 3.

3.2.9.7 switching time: The time interval between the start of the protection switching algorithm and the moment the traffic is selected from the standby transport entity. The switching time is also called transfer time as defined in 3.2.9.6.

NOTE – This definition for "switching time" is different in context to the definition found in [b-ITU-T G.671].

3.2.9.8 recovery time, T_5 : The time interval between the completion of protection switching operations and the full restoration of protected traffic.

3.2.9.9 protected traffic signal restoration time, T_r : The time interval between the occurrence of the network impairment and the full restoration of protected traffic: $T_r = T_1 + T_2 + T_3 + T_4 + T_5 = T_c + T_t + T_5$. See Figure 3.



G.808(16)-Amd.1(18)_F03

Figure 3 – Protection switching temporal model

3.2.9.10 wait-to-restore time: The time interval that must elapse before a transport entity that has recovered from an SF or SD condition can be used again to transport the normal traffic signal and/or to select the normal traffic signal from.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AIS	Alarm Indication Signal
APS	Automatic Protection Switch
FDI	Forward Defect Indication (indicator)
NR	No Request
ODU	Optical Data Unit
SD	Signal Degrade
SDG	Signal Degrade Group
SDH	Synchronous Digital Hierarchy
SF	Signal Fail
SFG	Signal Fail Group
VC-n	Virtual Container, level n
WTR	Wait To Restore

5 Conventions

A: End-point designation used when describing a protected domain; A is the source end of protected signals for which switch request signalling is initiated from the other, Z, end.

Z: End-point designation used when describing a protected domain; Z is the end at which switch request signalling is initiated.

Annex A

Terms specific to ring protection

(This annex forms an integral part of this Recommendation)

Terms specific to ring protection are listed below. These terms will be removed after being moved to a ring protection Recommendation, e.g., [b-ITU-T G.808.2] or [b-ITU-T G.873.2].

APS-byte pass-through: The action of transmitting the same APS-bytes that are being received. Protection channels are not passed through. APS-byte pass-through is bidirectional.

crossing APS-bytes: When a node sees ring bridge requests of equal priority on both 'sides' (This includes a switching node receiving a ring bridge request from the other end).

full pass-through: The action of transmitting the same APS-bytes, and protection channels that are being received. Full pass-through may be either unidirectional or bidirectional as specified in the text. When a node enters unidirectional full pass-through, it shall continue sourcing the previously sourced APS-bytes in the opposite direction, with the exception that status information APS byte 1, bits 6-8 shall reflect the appropriate status code.

SRP-1: Shared ring protection supporting 1 optical data unit (ODU) per Lambda: This shared protection architecture is based on ODUk connectivity not further sub-structured in respect to the protection switching. The ODUk may be member of a wavelength group for link group protection.

SRP-p: Shared ring protection supporting p ODU per Lambda: This shared protection architecture is based on ODUj entities multiplexed into a HO ODUk. The ODUj may be member of a group for link group protection.

steering: A protection method in which a source node redirects a traffic to the ring section into the direction retaining connectivity to a destination node.

wrapping: The transmission of the traffic into the opposing direction in the ring, in order to route around a fault in a given ring segment.

Bibliography

- [b-ITU-T G.671] Recommendation ITU-T G.671 (2012), *Transmission characteristics of optical components and subsystems*.
- [b-ITU-T G.808.2] Recommendation ITU-T G.808.2 (2013), *Generic protection switching – Ring protection*.
- [b-ITU-T G.873.2] Recommendation ITU-T G.873.2 (2015), *ODUk shared ring protection*.

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