INTERNATIONAL TELECOMMUNICATION UNION

ITU-T G.808.1

(12/2003)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

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

Digital networks – General aspects

Generic protection switching – Linear trail and subnetwork protection

ITU-T Recommendation G.808.1

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
TESTING EQUIPMENTS	G.500–G.599
TRANSMISSION MEDIA CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
General	G.700–G.709
Coding of analogue signals by pulse code modulation	G.710–G.719
Coding of analogue signals by methods other than PCM	G.720–G.729
Principal characteristics of primary multiplex equipment	G.730–G.739
Principal characteristics of second order multiplex equipment	G.740–G.749
Principal characteristics of higher order multiplex equipment	G.750–G.759
Principal characteristics of transcoder and digital multiplication equipment	G.760–G.769
Operations, administration and maintenance features of transmission equipment	G.770–G.779
Principal characteristics of multiplexing equipment for the synchronous digital hierarchy	G.780–G.789
Other terminal equipment	G.790–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
QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DIGITAL TERMINAL EQUIPMENTS	G.7000–G.7999
DIGITAL NETWORKS	G.8000–G.8999

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

ITU-T Recommendation G.808.1

Generic protection switching – Linear trail and subnetwork protection

Summary

This Recommendation defines the generic functional models, characteristics and processes associated with various linear protection schemes for connection-oriented layer networks; e.g., Optical Transport Networks (OTN), Synchronous Digital Hierarchy (SDH) networks and Asynchronous Transfer Mode (ATM) networks.

It also defines the objectives and applications for these schemes. Protection schemes described in this Recommendation are trail protection and subnetwork connection protection with various monitoring alternatives for individual signals or groups of signals. Furthermore, survivability offered by the Link Capacity Adjustment Scheme (LCAS) is described.

Generic functional models, characteristics and processes for ring protection and interconnected subnetwork (e.g., ring) protection schemes are defined in other Recommendations.

Source

ITU-T Recommendation G.808.1 was approved on 14 December 2003 by ITU-T Study Group 15 (2001-2004) under the ITU-T Recommendation A.8 procedure.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

CONTENTS

ITU-T Recommendation G.808.1

Generic protection switching – Linear trail and subnetwork protection

1 Scope

This Recommendation provides an overview of generic aspects of linear protection switching. It covers OTN-, SDH- and ATM-based protection schemes. Overviews of ring protection and dual node subnetwork (e.g., ring) interconnection schemes will be provided in other Recommendations.

2 References

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

– ITU-T Recommendation G.783 (2004), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*.

– ITU-T Recommendation G.798 (2002), *Characteristics of optical transport network hierarchy equipment functional blocks*.

– ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

– ITU-T Recommendation G.841 (1998), *Types and characteristics of SDH network protection architectures*.

– ITU-T Recommendation G.842 (1997), *Interworking of SDH network protection architectures*.

– ITU-T Recommendation G.873.1 (2003), *Optical Transport Network (OTN): Linear protection*.

– ITU-T Recommendation I.630 (1999), *ATM protection switching*.

– ITU-T Recommendation I.732 (2000), *Functional characteristics of ATM equipment*.

– ITU-T Recommendation M.495 (1988), *Transmission restoration and transmission route diversity: Terminology and general principles*.

3 Terms and definitions

3.1 This Recommendation uses the following terms:

A Endpoint 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 Endpoint designation used when describing a protected domain; Z is the end at which switch request signalling is initiated.

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

a) Adapted Information (AI)

b) Characteristic Information (CI)

c) Link connection

d) Network

e) Serial compound link connection

f) Subnetwork

g) Trail

3.3 This Recommendation defines the following terms:

3.3.1 Action

3.3.1.1 switch: For the selector, the action of selecting normal traffic from the (currently) standby transport entity rather than the (currently) active transport entity. For the bridge (case of permanent connection to working), the action of connecting or disconnecting the normal traffic to the protection transport entity. (For the case of non-permanent connection to working) the action of connecting the normal traffic signal to the (currently) standby transport entity.

3.3.2 APS protocol

3.3.2.1 1-phase: A means to align the two ends of the protected domain via the exchange of a single message (Z → 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.

3.3.2.2 2-phase: A means to align the two ends of the protected domain via the exchange of two messages (Z → A, A → 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.

3.3.2.3 3-phase: A means to align the two ends of the protected domain via the exchange of three messages (Z → A, A → Z, Z → 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.

3.3.3 Protection class

3.3.3.1 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.

3.3.3.2 subnetwork connection protection: Transport entity protection for the case 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:

3.3.3.2.1 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.

3.3.3.2.2 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.

3.3.3.2.3 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.

3.3.3.2.4 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.

3.3.3.3 network connection protection: Special case of subnetwork connection protection.

3.3.3.4 individual: Protection is performed for a single transport entity.

3.3.3.5 group: Protection is performed for a set of transport entities.

3.3.4 Protection subclass

3.3.4.1 end-to-end overhead/OAM (e): Overhead/OAM associated with the layer network's trail. Examples: OTN ODUk PM overhead, ATM VPC e-t-e OAM.

3.3.4.2 sublayer overhead/OAM (s): Overhead/OAM associated with a sublayer's trail (tandem connection, segment). Examples: SDH VC-n TC overhead, ATM VCC segment OAM.

3.3.5 Component

3.3.5.1 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. It begins from the selector/bridge of one endpoint to the selector/bridge of the other endpoint.

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

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

3.3.5.2.2 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.

3.3.5.2.3 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.

NOTE 1 – In SDH, the broadcast bridge is preferred as cross-connect fabrics use connection tables which are typically organized by output. In a bridge where there are two outputs and 1 input, the table would be populated with "OUTx1:INy", "OUTx2:INy". Using a broadcast bridge does not require the modification of the working matrix connection, only the addition of a protection matrix connection.

NOTE 2 – In ATM, the selector bridge is preferred as connection tables are typically organized by input. A broadcast bridge would require e.g., "INx:OUTy1" "INx:OUTy2", which is more complicated than a selector bridge, which only has "INx:OUTy1" changing to "INx:OUTy2". This also applies to other packet switching technologies.

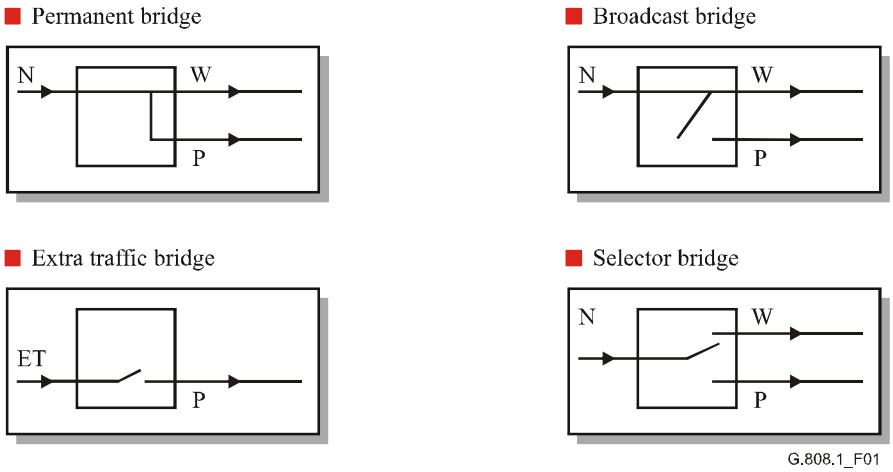


Figure 1/G.808.1 – Protection bridges

3.3.5.3 **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 AIS signal will be output.

3.3.5.3.1 **selective selector**: A selector, which connects the normal traffic signal output with either the working or protection transport entity inputs.

3.3.5.3.2 **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 1 – This alternative works only in combination with a selector bridge. To prevent that AIS/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 kind of a distributed selective selector.

NOTE 2 – In ATM, connections can be assigned but cells do not necessarily flow over them. A selector bridge only sends cells over working or protection and, therefore, there will only be one copy arriving at the selector. Hence, the connection table can have two permanent matrix connections "INx1:OUTy" and "INx2:OUTy". This also applies to other packet switching technologies.

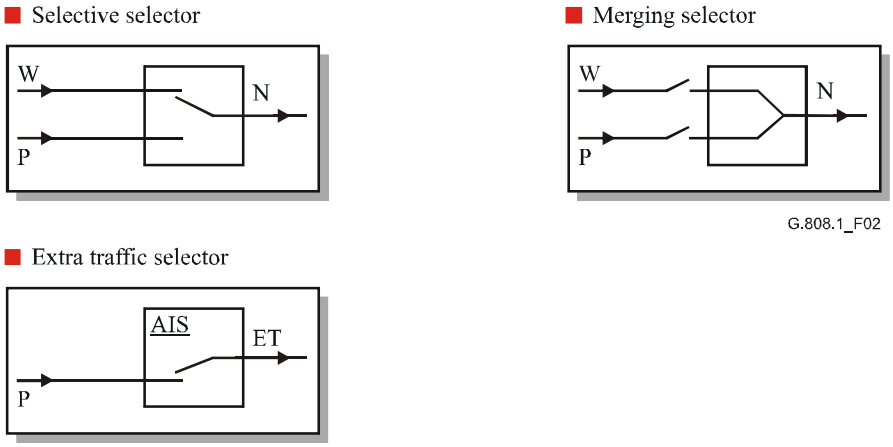


Figure 2/G.808.1 – Protection selectors

3.3.5.4 head end: The head end of the linear 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 both ends of the protection group.

3.3.5.5 tail end: The tail end of the linear 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 both ends of the protection group.

3.3.5.6 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.

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

3.3.5.8 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.

3.3.6 Fault condition

3.3.6.1 Signal Degrade (SD): A signal indicating the associated data has degraded in the sense that a degraded defect (e.g., dDEG) condition is active.

3.3.6.2 Signal Fail (SF): A signal indicating the associated data has failed in the sense that a signal interrupting near-end defect condition (not being the degraded defect) is active.

3.3.6.3 Signal Degrade Group (SDG): A signal indicating the associated group data has degraded.

3.3.6.4 Signal Fail Group (SFG): A signal indicating the associated group has failed.

3.3.6.5 Server Signal Degrade (SSD): A signal degrade indication output at the connection point of an adaptation function.

3.3.6.6 Server Signal Fail (SSF): A signal fail indication output at the connection point of an adaptation function.

3.3.6.7 Trail Signal Degrade (TSD): A signal degrade indication output at the access point of a termination function.

3.3.6.8 Trail Signal Fail (TSF): A signal fail indication output at the access point of a termination function.

3.3.7 Architecture

3.3.7.1 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 protection transport entity. 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 architecture does not allow an unprotected extra traffic signal to be provided.

3.3.7.2 1:n (protection) architecture (n ≥ 1): A 1:n protection architecture has n normal traffic signals, n working transport entities and 1 protection transport entity. It may have 1 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 (case of broadcast bridge), or is connected to either its working or the protection transport entity (case of selector bridge). At the sink end, the normal traffic signal is selected from either its working or 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.

3.3.7.3 m:n (protection) architecture: A 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 (case of broadcast bridge), or is connected to either its working or one of the protection transport entities (case of 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.

3.3.7.4 $(1:1)^n$ 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 (e.g., ATM, MPLS).

3.3.8 External commands

3.3.8.1 lockout of protection transport entity #i (LO #i): A temporarily 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).

3.3.8.2 lockout of normal traffic signal #i: A temporarily 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.

3.3.8.3 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 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.

3.3.8.4 freeze: A temporarily configuration 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.

3.3.8.5 Forced Switch for normal traffic signal #i (FS #i): A switch action initiated by an operator command. It switches normal traffic signal #i to the protection transport entity, unless an equal or higher priority switch command is in effect.

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

3.3.8.6 Forced Switch for null signal (FS #0): A switch action initiated by an operator command. For 1:n architectures, it switches the null signal to the protection transport entity, unless an equal or higher priority switch command is in effect. A normal traffic signal present on the protection transport entity is transferred to and selected from its working transport entity. For 1+1 architectures, it selects the normal traffic signal from the working transport entity.

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

3.3.8.7 Forced Switch for extra traffic signal (FS #ExtraTrafficSignalNumber): A switch action initiated by an operator command. It switches the extra traffic signal to the protection transport entity, unless an equal or higher priority switch command is in effect. A normal traffic signal present on the protection transport entity is transferred to and selected from its working transport entity.

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

3.3.8.8 Manual Switch for normal traffic signal #i (MS #i): A switch action initiated by an operator command. It switches normal traffic signal #i to the protection transport entity, unless a fault condition exists on other transport entities (including the protection transport entity) or an equal or higher priority switch command is in effect.

3.3.8.9 Manual Switch for null signal (MS #0): A switch action initiated by an operator command. For 1:n architectures, it switches 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. A normal traffic signal present on the protection transport entity is transferred to and selected from its working transport entity. For 1+1 architectures, it selects the normal traffic signal from the working transport entity.

3.3.8.10 Manual Switch for extra traffic signal (MS #ExtraTrafficSignalNumber): A switch action initiated by an operator command. It switches extra traffic 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. A normal traffic signal present on the protection transport entity is transferred to and selected from its working transport entity.

3.3.8.11 Exercise signal #i (EX): 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 released by an exercise request. The exercise functionality is optional.

3.3.8.12 Clear (CLR): Clears the active near-end lockout of protection, forced switch, manual switch, WTR state, or exercise command.

3.3.9 States

3.3.9.1 Do Not Revert normal traffic signal #i (DNR #i): In non-revertive operation, this is used to maintain a normal traffic signal to be selected from the protection transport entity.

3.3.9.2 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.

3.3.9.3 Wait-to-Restore normal traffic signal #i (WtR): 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 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.

3.3.10 Operation

3.3.10.1 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.

3.3.10.2 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.

3.3.11 Signal

3.3.11.1 traffic signal: Characteristic or adapted information.

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

3.3.11.3 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 protection transport entity is 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.

3.3.11.4 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.

Examples of null signals are: unequipped VC-n (SDH), ODUk-OCI (OTN), no signal (ATM, MPLS), a test signal, one of the normal traffic signals, an AIS/FDI signal.

3.3.12 Switching

3.3.12.1 bidirectional (protection) switching: A protection switching mode in which, for a unidirectional fault, the normal traffic signal in both directions (of the "trail", "subnetwork connection", etc.), including the affected direction and the unaffected direction, is switched to protection.

3.3.12.2 unidirectional (protection) switching: A protection switching mode in which, for a uni-directional fault (i.e., a fault affecting only one direction of transmission), only the normal traffic signal transported in the affected direction (of the "trail", "subnetwork connection", etc.) is switched to protection.

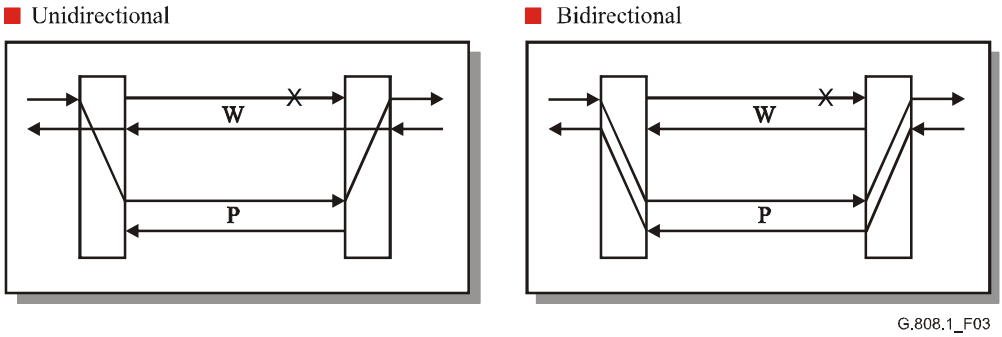


Figure 3/G.808.1 – Switching types

3.3.13 Time

3.3.13.1 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.

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

3.3.13.3 wait-to-restore time: A period of time that must elapse before a transport entity (from a SF or SD recovered) can be used again to transport the normal traffic signal and/or to select the normal traffic signal from.

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

3.3.14 Transport entity

3.3.14.1 transport entity: an architectural component which transfers information between its inputs and outputs within a layer network. Examples are: trail, network connection, subnetwork connection, link connection.

3.3.14.2 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).

3.3.14.3 protection transport entity: The transport entity allocated to transport the normal traffic signal during a switch event. 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).

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

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

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

3.3.14.7 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.

3.3.15 protection: This makes use of pre-assigned capacity between nodes. The simplest architecture has one dedicated protection entity for each working entity (1+1). The most complex architecture has m protection entities shared amongst n working entities (m:n).

3.3.16 restoration: This makes use of any capacity available between nodes. In general, the algorithms used for restoration will involve rerouting. When restoration is used, some percentage of the transport network capacity will be reserved for rerouting of normal traffic. Further description of restoration is not within the scope of this Recommendation.

3.3.17 escalation: A network survivability action caused by the impossibility of the survivability function in lower layers.

3.3.18 hitless protection switch: Protection switch which does not cause characteristic or adapted information loss, duplication, disorder, or bit errors upon protection switching action.

3.3.19 impairment: Fault or performance degradation which may lead to SF or SD trigger.

3.3.20 network survivability: The set of capabilities that allow a network to restore affected traffic in the event of an impairment. The degree of survivability is determined by the network's capability to survive single impairments, multiple impairments, and equipment impairments.

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

3.3.22 subnetwork interworking: A network topology where two subnetworks (e.g., rings) are interconnected at two points and operate such that failure at either of these two points will not cause loss of any traffic, except possibly that dropped or inserted at the point of failure.

3.3.23 survivable network: A network that is capable of restoring traffic in the event of an impairment. The degree of survivability is determined by the network's ability to survive single link impairments, multiple link impairments, and equipment impairments.

3.3.24 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.

4 Abbreviations

This Recommendation uses the following abbreviations:

ABR Available Bit Rate

AI Adapted Information

AIS Alarm Indication Signal

AP Access Point

APS Automatic Protection Switching

ATM Asynchronous Transfer Mode

AU Administrative Unit

B Bandwidth

BER Bit Error Rate

BR Bridge

CC	Continuity Check
CI	Characteristic Information
CP	Connection Point
DEG	DEGraded
ET	Extra Traffic (signal)
F4	Flow #4 (ATM)
FDI	Forward Defect Indication
HO	Hold Off
LCAS	Link Capacity Adjustment Scheme
MPLS	Multi-Protocol Label Switching
MS	Multiplex Section
N	Normal (signal)
NE	Network Element
NIM	Non-Intrusive Monitoring
NR	No Request
NUT	Non-preemptible Unprotected Traffic
OAM	Operations, Administration and Maintenance
OCh	Optical Channel
OH	Overhead
OTN	Optical Transport Network
P	Protection
PDH	Plesiochronous Digital Hierarchy
POH	Path OverHead
PP	Pointer Processing
PU	Port Unit
RDI	Remote Defect Indication
REI	Remote Error Indication
RI	Remote Information
RS	Regenerator Section
SD	Signal Degrade
SDG	Signal Degrade Group
SDH	Synchronous Digital Hierarchy
SEL	Selector
SES	Severely Errored Second
SF	Signal Fail
SFG	Signal Fail Group
Sm	lower order VC-m layer (n = 11, 12, 2)

Sn	higher order VC-n layer (n = 3, 4, 4-Xc) or lower order VC-3 layer
SNC	Subnetwork Connection
SNC/I	Inherently monitored SubNetwork Connection protection
SNC/N	Non-intrusively monitored SubNetwork Connection protection
SNC/Ne	SNC/N, monitoring of end-to-end OH
SNC/Ns	SNC/N, monitoring of sub-layer OH
SNC/S	SNCP with Sublayer monitoring
SNC/Ss	SNC/S, monitoring of sublayer OH
SNC/T	SNCP with Test trail monitoring
SNC/Te	SNC/T, monitoring of end-to-end OH
SNC/Ts	SNC/T, monitoring of sublayer OH
SNCP	SubNetwork Connection Protection
Sn-Xv	VC-n-Xv layer
SOH	Section OverHead
SSD	Server Signal Degrade
SSF	Server Signal Fail
STM-N	Synchronous Transport Module, level N
TCP	Termination Connection Point
TSD	Trail Signal Degrade
TSF	Trail Signal Fail
TSI	TimeSlot Interchange
TT	Trail Termination
TU	Tributary Unit
UBR	Unspecified Bit Rate
UPSR	Unidirectional Path Switch Ring
VC	Virtual Channel (ATM)
VCG	Virtual Concatenation Group
VC-n	Virtual Container-n
VC-n-Xv	Virtual concatenation of X virtual containers (of level n)
VP	Virtual Path (ATM)
VPI	Virtual Path Identifier
W	Working
WTR	Wait-to-Restore
X,Y,Z	Layer (for non-specified layers) or group size designations

5 Conventions

None.

6 Individual and group protection concept

The individual protection concept applies to the situations where it is useful to protect only a part of the traffic signals which need high reliability. The rest of the traffic signals in the network layer remains unprotected. This helps to reduce the necessary bandwidth for protection.

The group protection concept applies to the situations where:

i) it is useful to protect a large number (but not all) of the traffic signals transported via the same server layer trails, with protection times in the same order as individual protection (of a small set of traffic signals). Fast protection switching is obtained through the treatment of a logical bundle of transport entities as a single entity after the commencement of protection actions;

ii) the protection of a group of traffic signals that realize a single traffic signal by means of e.g., virtual concatenation, inverse multiplexing.

The complexity of the protection process is reduced by treating the group of signals as a single entity, within a single protection process. The status of the working and protection groups is represented by SF-Group and SD-Group indications.

The complexity can be further reduced by the introduction of an additional test signal (transported over the same server layer trails), of which the SF and SD indications are used to represent the status of the group. The *disadvantage* of this latter complexity reduction technique is the inability to monitor the individual signals in each group for their connectivity, continuity and performance. One of these faults within one of the signals in the group will not be detected, and thus not protected.

7 Architecture types

The protection architecture can be a 1+1, a 1:n, a m:n, or a $(1:1)^n$ architecture type.

Possible advantages of the 1+1 architecture include:

1) low complexity;

2) for the case of unidirectional switching, the possibility to support dual node interconnection of protected subnetworks.

Possible disadvantages of the 1+1 architecture include:

3) 100% extra capacity.

Possible advantages of the 1:n, m:n, $(1:1)^n$ architecture include:

1) possibility to provide protection access; the protection transport entity/bandwidth can transport an extra traffic signal during periods when the protection transport entity/bandwidth is not required to transport a normal traffic signal;

2) extra capacity restricted to 100/n % or m × 100/n %;

3) for the case of m:n, protection is possible for up to m faults.

Possible disadvantages of the 1:n, m:n, $(1:1)^n$ architecture include:

4) complexity;

5) for the case of SNC protection class, the need for additional sublayer termination functions at ingress and egress points of the protected domain on each working and protection transport entity;

6) does not support dual node interconnection of protected subnetworks;

7) $n \geq 2$: each of the n working transport entities must be routed via different facilities and equipment to prevent the existence of common points of failure that cannot be protected by the single protection transport entity in a 1:n and $(1:1)^n$ architecture.

NOTE 1 – Typically, n+1 alternative paths between two nodes in the network will not be available. As such, 1:n and $(1:1)^n$, with $n \geq 2$, architectures will *not provide adequate protection* for the n normal traffic signals transported normally via the n working transport entities. n = 1 seems the only reasonable choice.

NOTE 2 – In ATM, protection access is not explicitly required to allow usage of the normally unused protection bandwidth; ABR and UBR traffic could use this protection bandwidth by means of an over-subscription of the bandwidth of the server signal containing the protection transport entity. The ABR/UBR higher layer control mechanism is assumed to reduce the traffic when the protection is actually used. The ingress/egress nodes of the protection domain do not have to align with ingress/egress nodes of ABR/UBR traffic. This adds flexibility to the network, and reduces complexity.

7.1 1+1 protection architecture

In the 1+1 architecture type, a protection transport entity is dedicated as a backup facility to the working transport entity with the normal traffic signal bridged onto the protection transport entity at the source endpoint of the protected domain. The normal traffic on working and protection transport entities is transmitted simultaneously to the sink endpoint of the protected domain where a selection between the working and protection transport entity is made, based on some predetermined criteria, such as signal fail and signal degrade indications.

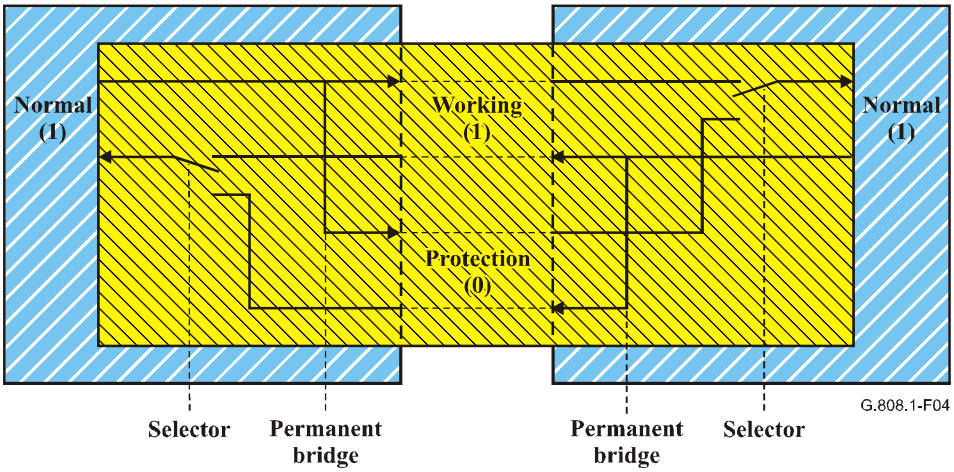


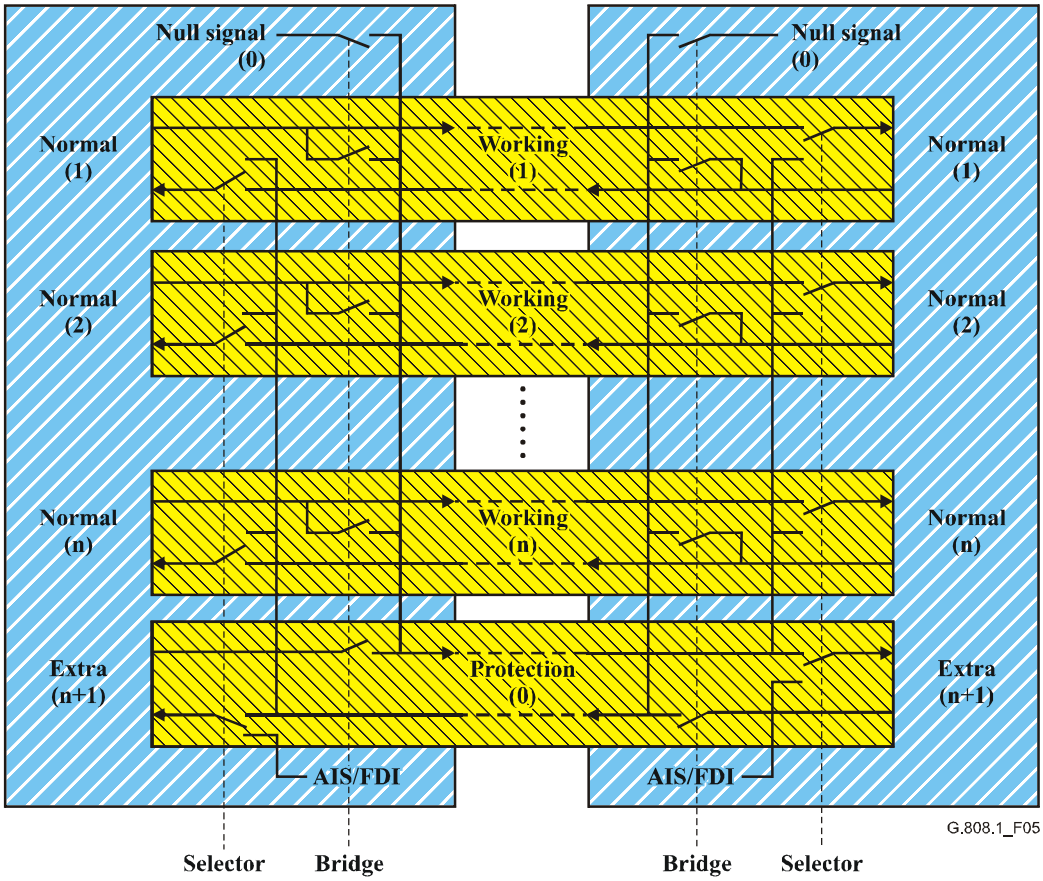
Figure 4/G.808.1 – 1+1 protection architecture

7.2 1:n protection architecture

In the 1:n architecture type, a dedicated protection transport entity is a shared backup facility for n working transport entities. The bandwidth of the protection transport entity should be allocated in such a way that it may be possible to protect any of the n working transport entities in case the protection transport entity is available.

When a working transport entity is determined to be impaired, its normal traffic signal must be transferred from the working to the protection transport entity at both the source and sink endpoints of the protected domain. It is noted that, when more than one working transport entities is impaired, only one normal traffic signal can be protected.

The bridge can be realized in two ways: selector bridge or broadcast bridge. With selector bridge connectivity (Figure 6) the normal traffic signal is connected either to the working transport entity, or the protection transport entity. With broadcast bridge connectivity (Figure 5) the normal traffic signal is permanently connected to the working transport entity, and occasionally to the protection transport entity also. Interworking between the two options is guaranteed.



[Broadcast bridge option: normally permanently connected to working and occasionally to protection]

Figure 5/G.808.1 – 1:n protection architecture

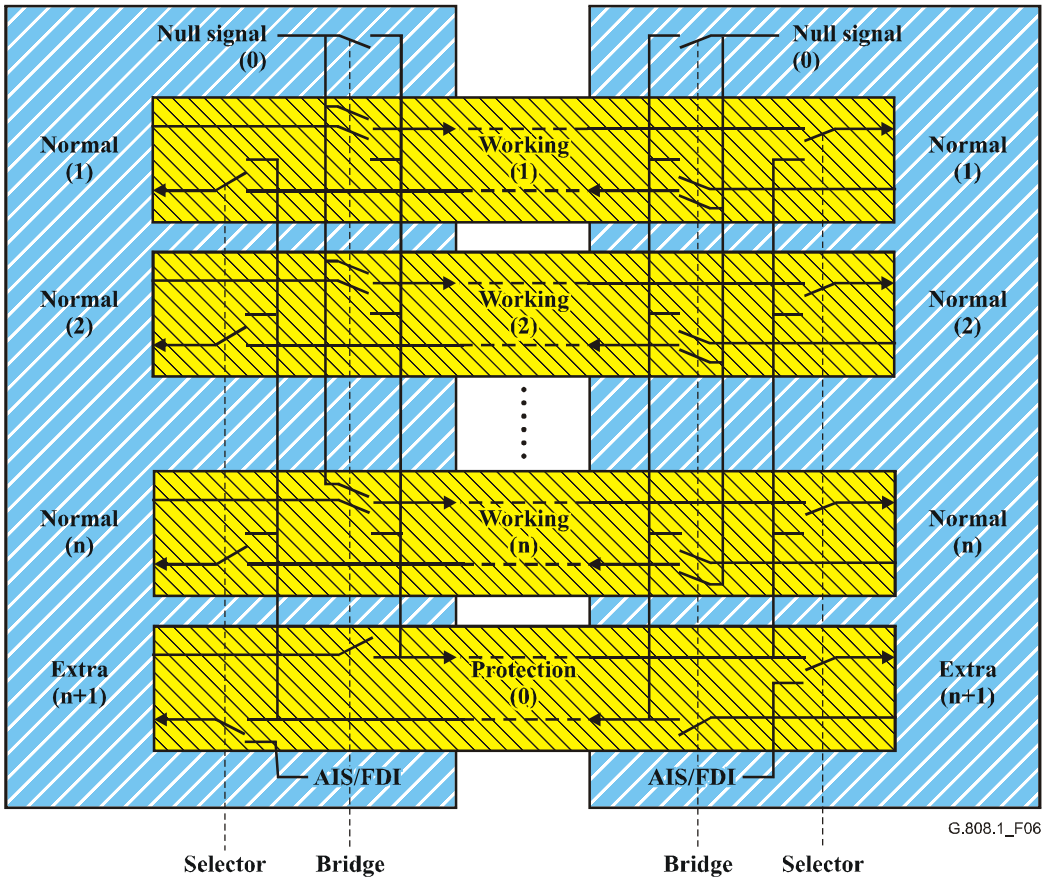
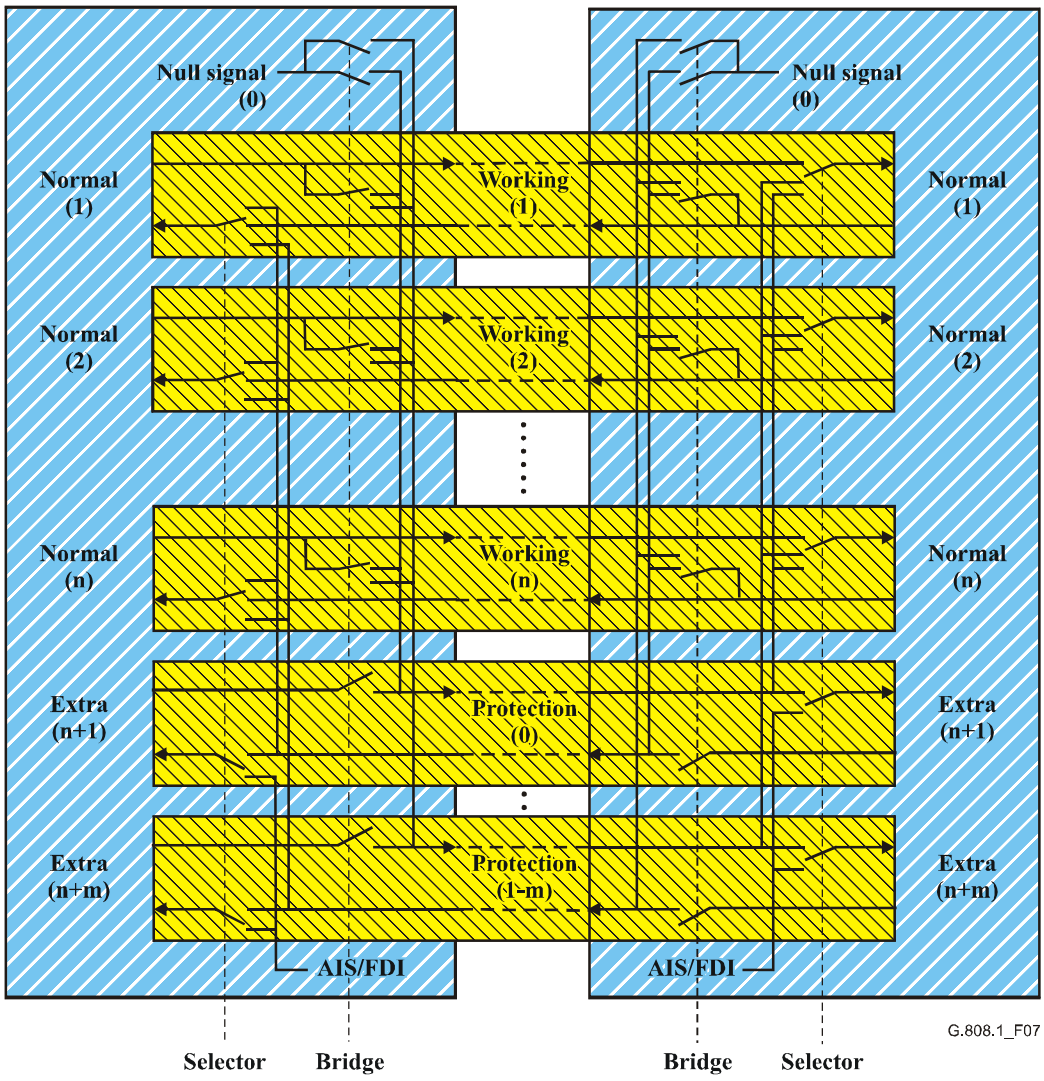


Figure 6/G.808.1 – 1:n protection architecture

7.3 m:n protection architecture

In the m:n architecture type, m dedicated protection transport entities are sharing backup facilities for n working transport entities, where m ≤ n typically. The bandwidth of each protection transport entity should be allocated in such a way that it may be possible to protect any of the n working transport entities in case at least one of the m protection transport entities is available. When a working transport entity is determined to be impaired, its normal traffic signal first must be assigned to an available protection transport entity followed by transition from the working to the assigned protection transport entity at both the source and sink endpoints of the protected domain. It is noted that when more than m working transport entities are impaired, only m working transport entities can be protected.

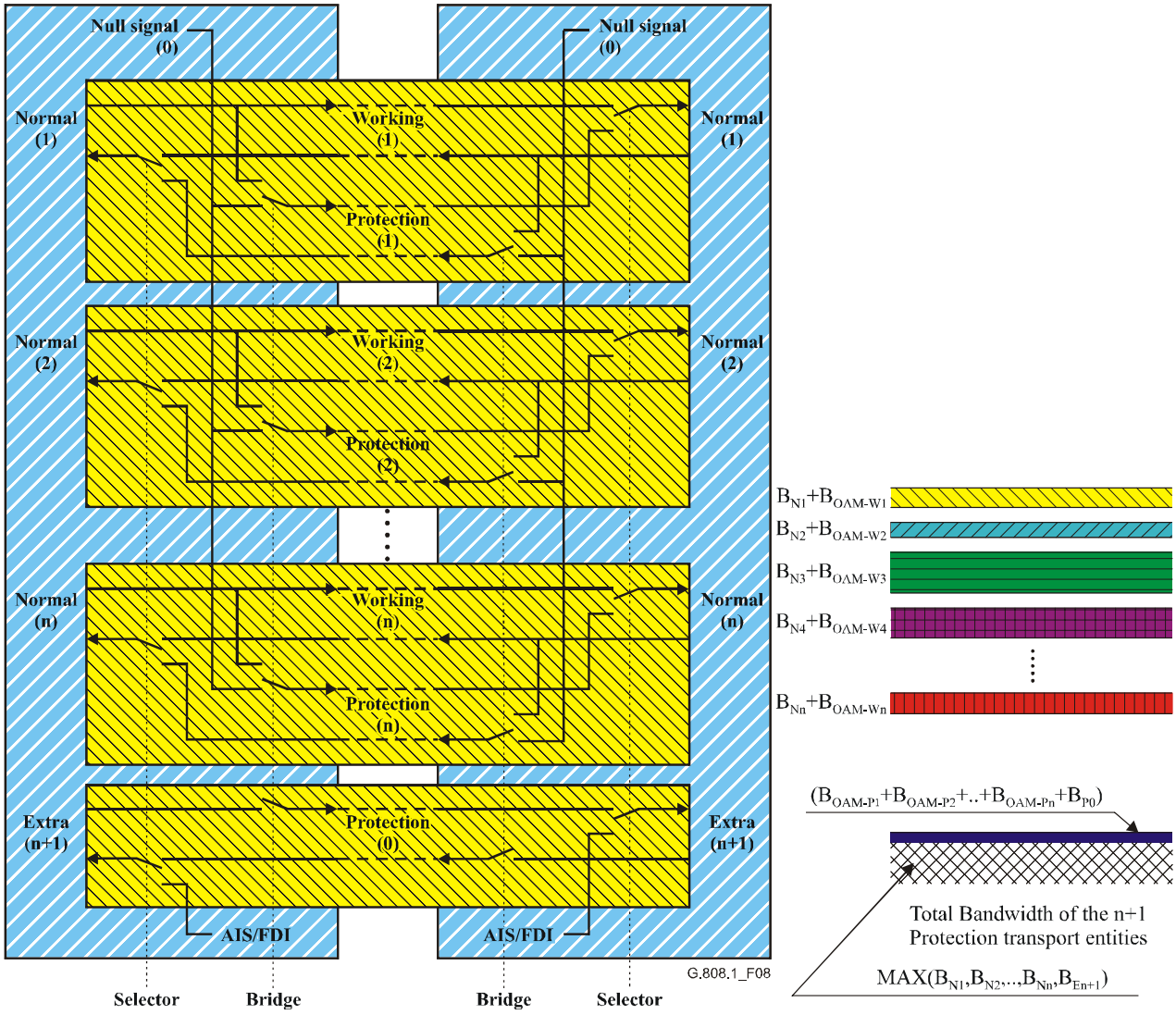


[Broadcast bridge option: normally permanently connected to working and occasionally to protection]

Figure 7/G.808.1 – m:n protection architecture

7.4 $(1:1)^n$ protection architecture

In the $(1:1)^n$ protection architecture, n dedicated protection transport entities sharing the same bandwidth are backup facilities for n working transport entities. The protection bandwidth should be allocated in such a way that it may be possible to protect any of the n working transport entities in case the protection transport bandwidth, and the specific protection transport entity associated with the working transport entity to be switched, is available. When a working transport entity is determined to be impaired, its normal traffic signal must first be assigned to the associated available protection transport entity followed by transition from the working to the assigned protection transport entity at both the source and sink endpoints of the protected domain. It is noted that when more than one working transport entity is impaired, only one working transport entity can be protected.



Broadcast bridge option: normaly permanently connected to working and occasionally to protection.

Figure 8/G.808.1 – Band width sharing $(1:1)^n$ protection architecture

All "n" working transport entities are routed via different facilities and equipment (to prevent a common point of failure that cannot be protected). All "n+1" protection transport entities are routed via the same facilities and equipment, diverse from the working facilities and equipment. Refer to Appendix IV for an example.

The bandwidth occupied by each working transport entity is $B_{Wi} = B_{Ni}+B_{OAM-Wi}$; i.e., the bandwidth for the normal traffic signal #i, plus the bandwidth for the tandem connection/segment OAM used to monitor the working transport entity #i. The bandwidth occupied by the protection transport entities is $Bp = MAX(B_{N1},B_{N2},..,B_{Nn},B_{En+1}) + (B_{OAM-P1}+B_{OAM-P2}+..+B_{OAM-Pn}+B_{OAM-P0})$. From a bandwidth perspective, this $(1:1)^n$ protection architecture behaves as a 1:n architecture.

Misconnection of a normal traffic signal #i at the ingress of the protected domain to the output for a normal traffic signal #j ($j \neq i$) at the egress of the protected domain cannot occur. A 3-phase APS protocol is, as such, not required.

Note that this architecture is intended for packet/cell-based traffic, not for constant bit rate-type traffic.

8 Switching types

The protection switching types can be a unidirectional switching type or a bidirectional switching type.

In **unidirectional** switching, the switching is complete when the traffic signal (service) is selected from standby at the end detecting the fault. For the case of the 1+1 architecture, the selector at the sink end is operated only (without communication with the source end). For the case of the 1:n, m:n, $(1:1)^n$ architectures, the selector at the sink end, as well as the bridge at the source end, are operated.

In **bidirectional** switching, the traffic signal (service) is switched from the active to the standby transport entity at both ends of the protection span. For the case of the 1+1 architecture, the selectors at the sink and source ends are operated. For the case of the 1:n, m:n, $(1:1)^n$ architectures, the selectors at the sink and source ends, as well as the bridges at the source and sink ends, are operated.

NOTE 1 – All switching types except 1+1 unidirectional switching, require a communications channel between the two ends of the protected domain; this is called the Automatic Protection Switching (APS) channel. The APS channel is terminated in the connection functions at each end of the protected domain.

Under bidirectional switching protocols, switching (operating selector and bridge) at only one end is not allowed. The two ends communicate to initiate transfer of the normal traffic signal. If the priority of the request of the source end is lower than that of the sink end, or does not exist, the sink end initiates transfer of the normal traffic signal and the source end follows this transfer.

In the unidirectional switching type, possible advantages include:

1) Unidirectional protection switching is a simple scheme to implement and does not require a protocol in a 1+1 architecture.

   NOTE 2 – Unidirectional switching in a 1:n architecture (typically applied in radio/satellite links) requires a protocol to operate between the two endpoints of the protected domain.

2) For a 1+1 architecture, unidirectional protection switching can be faster than bidirectional protection switching because it does not require a protocol.

3) Under multiple failure conditions, there is a greater chance of restoring traffic by protection switching if unidirectional protection switching is used, than if bidirectional protection switching is used.

4) Unidirectional switching allows simple realization of a reliable network by means of cascaded protected subnetworks. Two subnetworks are connected in a dual node interconnect/dual subnetwork interworking architecture.

In the bidirectional switching type, possible advantages include:

1) With bidirectional protection switching, the same equipment is used for both directions of transmission after a failure. This means that there will be fewer disruptions in the service for repair and reversion to the original working path. In unidirectional switching, the following switches occur:

   i) Protection switch;

   ii) Forced switch for the direction unaffected by the failure;

   iii) Revertive switch.

   In bidirectional switching, only two switches will occur:

   i) Protection switch;

   ii) Revertive switch.

   Each switch will result in one or two severely errored seconds. Fewer SESs will result from bidirectional switching.

2) With bidirectional protection switching, if there is a fault in one transport entity of the network, transmission of both transport entities between the affected nodes is switched to the alternative direction around the network. No traffic is then transmitted over the faulty section of the network and so it can be repaired without further protection switching.

3) Bidirectional protection switching is easier to manage because both directions of transmission use the same equipment along the full length of the transport entity.

4) Bidirectional protection switching maintains equal delays for both directions of transmission. This may be important where there is a significant imbalance in the length of the transport entities e.g., transoceanic links where one transport entity is via a satellite link and the other via a cable link.

5) Bidirectional protection switching also has the ability to carry extra traffic on the protection transport entity.

9 Operation types

The protection operation types can be a non-revertive operation type or a revertive operation type.

In **revertive** operation, the traffic signal (service) always returns to (or remains on) the working transport entity if the switch requests are terminated. That is, when the working transport entity has recovered from the defect, or the external request is cleared.

In **non-revertive** operation, the traffic signal (service) does not return to the working transport entity if the switch requests are terminated.

Some protection schemes are inherently revertive. For other schemes either revertive or non-revertive operation is possible. An advantage of non-revertive operation is that, in general, it will have less impact on traffic performance. However, there are situations where revertive operation may be preferred. Examples of cases where revertive operation may be appropriate are:

1) Where parts of the protection transport entity may be taken to provide capacity to meet a more urgent need. For example, where protection transport entity can be taken out of service to release capacity for use in restoring other traffic.

2) Where the protection transport entity may be subject to frequent rearrangement. For example, where a network has limited capacity and protection routes are frequently rearranged to maximize network efficiency when changes occur in the network.

3) Where the protection transport entity is of significantly lower performance than the working transport entity. For example, where the protection transport entity has a worse error performance or longer delay than the working transport entity.

4) When an operator needs to know which transport entities are carrying normal traffic in order to simplify the management of the network.

10 Protocol types

Except for the case of 1+1 unidirectional switching, all protection types require that both ends, A and Z, of the protected domain coordinate their actions of bridging and selecting. Different protocols are required according to the type of protection and selector and bridge types. Nodes A and Z communicate, therefore, with each other via the Automatic Protection Switching (APS) channel.

There are two basic requirements for a protection protocol:

1) The prevention of misconnections.

2) The minimization of the number of communication cycles between A and Z ends of the protected domain, in order to minimize the protection switching time. The communication may be once (Z → A), twice (Z → A and A → Z), or three times (Z → A, A → Z and Z → A). This is referred to as 1-phase, 2-phase, and 3-phase protocols.

The conditions under which the different protocol types can be used are shown in Table 1.

Table 1/G.808.1 – Protocol types related to protection architectures and selector/bridge types

Protocol type	Types of protection using protocol	Bridge type	Selector type
No protocol	1+1 unidirectional only	Permanent	Selective
1-phase	$(1:1)^n$ unidirectional only	Selector	Selective or merging
2-phase	1+1 architectures only	Permanent	Selective
3-phase	All architecture types	Any	Selective
		Selector	Merging (cell/packet based technologies)

In the 3-phase protocol type, possible advantages include:

1) operates in all architecture types;

2) prevents a misconnection occuring under all circumstances;

3) operates a selector or bridge only after confirmation of priority with other end of protected domain.

In the 3-phase protocol type, possible disadvantages include:

4) triple message exchange necessary between two ends of protected domain, increasing the switching time.

In the 2-phase protocol type, possible advantages include:

1) reduced switching time compared to 3-phase protocol.

In the 2-phase protocol type, possible disadvantages include:

2) operates in 1+1 architectures only.

In the 1-phase protocol type, possible advantages include:

1) short switching time, due to single message interchange needed between two ends of protected domain.

In the 1-phase protocol type, possible disadvantages include:

2) operates in $(1:1)^n$ architectures only;

3) requires "n" extra transport entities (compared to 1:n architecture) to be setup in the protection bandwidth, to prevent misconnections occurring;

4) operates a bridge/selector before priority is confirmed by the other end of a protected domain. As such, a switch action may have to be reverted and replaced by other bridge/selector action initiated by the other end;

5) more complex protocol as there are "n" parallel 1:1 protection types.

11 Protection classes and subclasses

11.1 Trail protection

Trail protection is a protection class used to protect a trail across an entire operator's network or multiple operators' networks. It is a dedicated end-to-end protection architecture, which can be used in different network structures: meshed networks, rings, etc. As trail protection is a dedicated protection mechanism, there is no fundamental limitation on the number of NEs within the trails.

Trail protection operates in all combinations of protection architectures, switching and operation.

Trail protection generically protects against faults in the server layer, and connectivity faults and performance degradations in the client layer.

For the case of trail protection, the Adapted Information (AI) (i.e., the payload of the network layer's Characteristic Information (CI) is protected. See Figure 9.

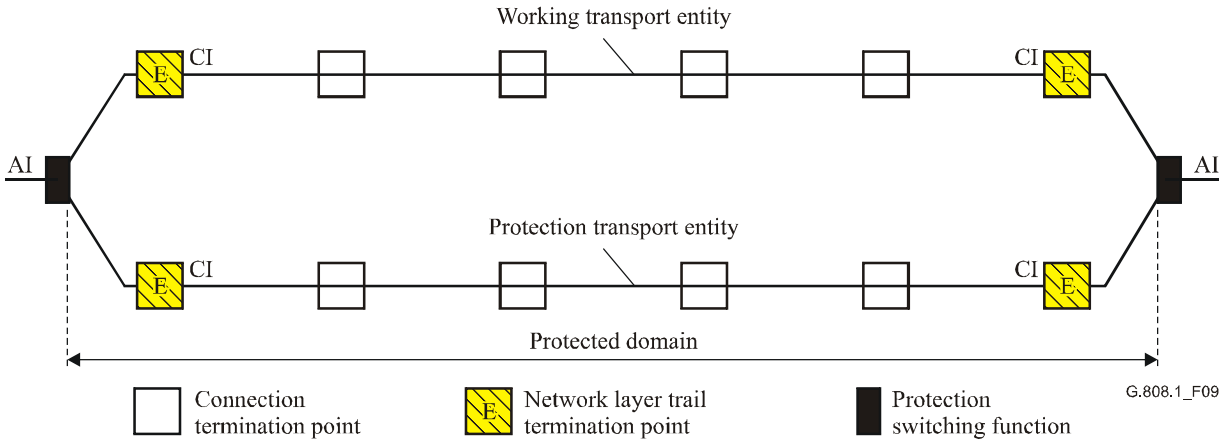


Figure 9/G.808.1 – Generic concept of trail protection

NOTE 1 – As 1:1, 1:n, m:n trail protections are linear protection mechanisms, the normal and extra traffic trail termination functions are located in the same NE. In a network application, this implies that the normal and extra traffic patterns must coincide.

Trail protection does not support network architectures which make use of cascaded protected subnetworks in the same layer. Consequently, traffic can be restored under single-fault conditions only. To restore traffic under multiple-fault conditions, SNC protection has to be used, or trail protection has to be supplemented with protection at server layers.

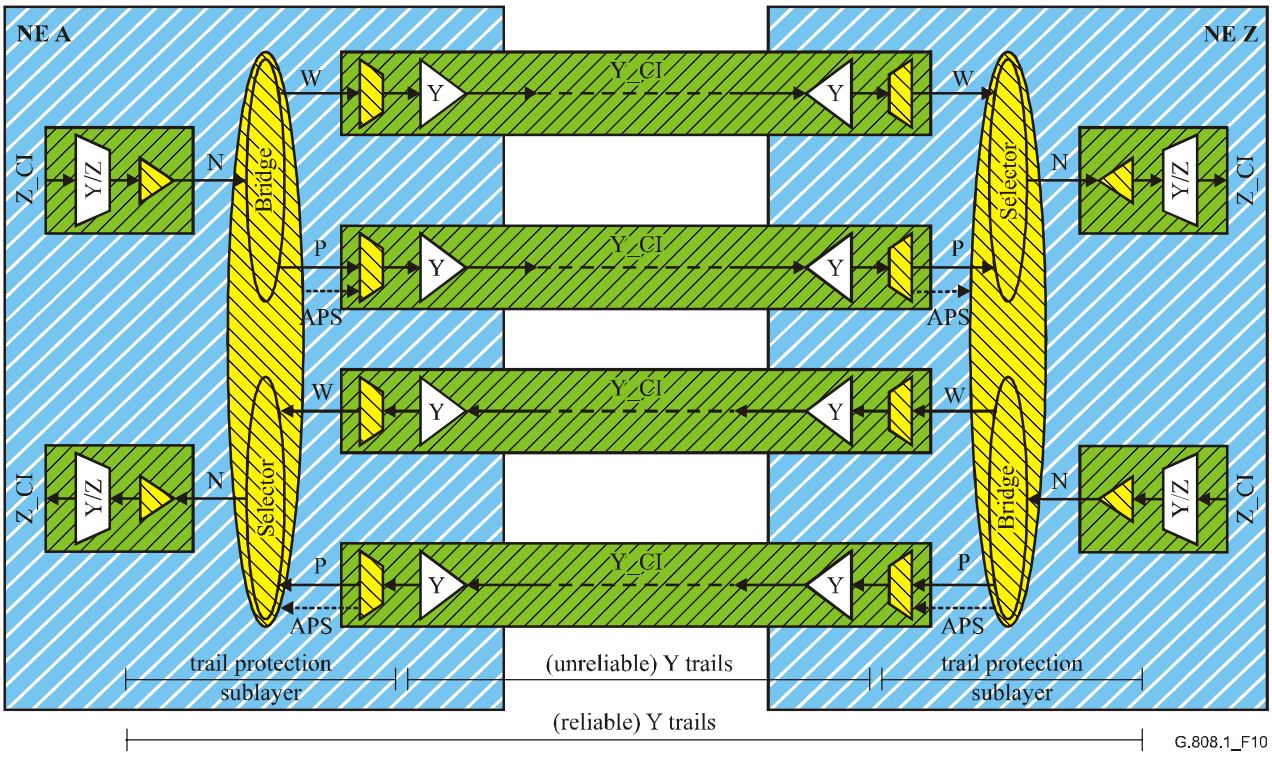
NOTE 2 – For the case of an 1:1, m:n, or $(1:1)^n$ architecture in ATM, the protection trail(s) should contain a signal that allows accurate monitoring of its status. In normal conditions, in which the normal traffic signal is transported via the working trail, there is no signal to be transported via protection. If Continuity Check (CC) would be inactive, such protection trail will not transport any information under normal fault-free conditions. When a fault occurs, AIS cells are inserted. When the fault is present for a short period only (e.g., due to a "physical layer protection action"), the AIS defect detector at the protection trail endpoint will detect the AIS defect condition for 2 to 3 seconds according to the I.610-defined AIS state definition. With CC activated, the AIS defect condition will clear on the receipt of a CC cell, i.e., within a period of 1 second after the traffic interruption was cleared.

NOTE 3 – If trail protection is used at path level, this may result in taking up an additional port in a fabric compared to SNC protection. This is the case when the protection selector is located in the egress port of the equipment.

11.1.1 Individual trail protection

Figure 10 illustrates the case of 1+1 trail protection and 1:1 trail protection without extra traffic between ingress and egress of the protected domain between NEs A and Z. Two independent trails (in layer network Y) exist which act as working and protection transport entities for the (protected) normal (payload) traffic signal. The TT functions generate/insert and monitor/extract the end-to-end overhead/OAM information to determine the status of the working and protection transport entities. APS information is transported over the protection trail, except for the case of 1+1 unidirectional switching.

The cases of 1:n, m:n and $(1:1)^n$ architectures with/without extra traffic are extensions of the 1+1/1:1 architecture, in accordance with the architecture type descriptions in clause 7.



NOTE – APS signal not applicable for 1+1 unidirectional switched case

Figure 10/G.808.1 – 1+1/1:1 trail protection functional model

11.1.2 Group trail protection

Figure 11 illustrates the case of 1+1/1:1 group trail protection between NEs A and Z. In this example, two times three parallel independent trails (in layer network Y) exist which act as working and protection transport entity groups for the three (protected) normal (payload) traffic signals. The three parallel normal traffic signals in the group are protected jointly by the trail protection sublayer connection function. The TT functions generate/insert and monitor/extract the end-to-end overhead/OAM information to determine the status of the working and protection transport entities. APS information is transported over one of the protection trails, except for the case of 1+1 unidirectional switching.

The cases of 1:n, m:n and $(1:1)^n$ architectures with/without extra traffic are extensions of the 1+1/1:1 architecture, in accordance with the architecture type descriptions in clause 7.

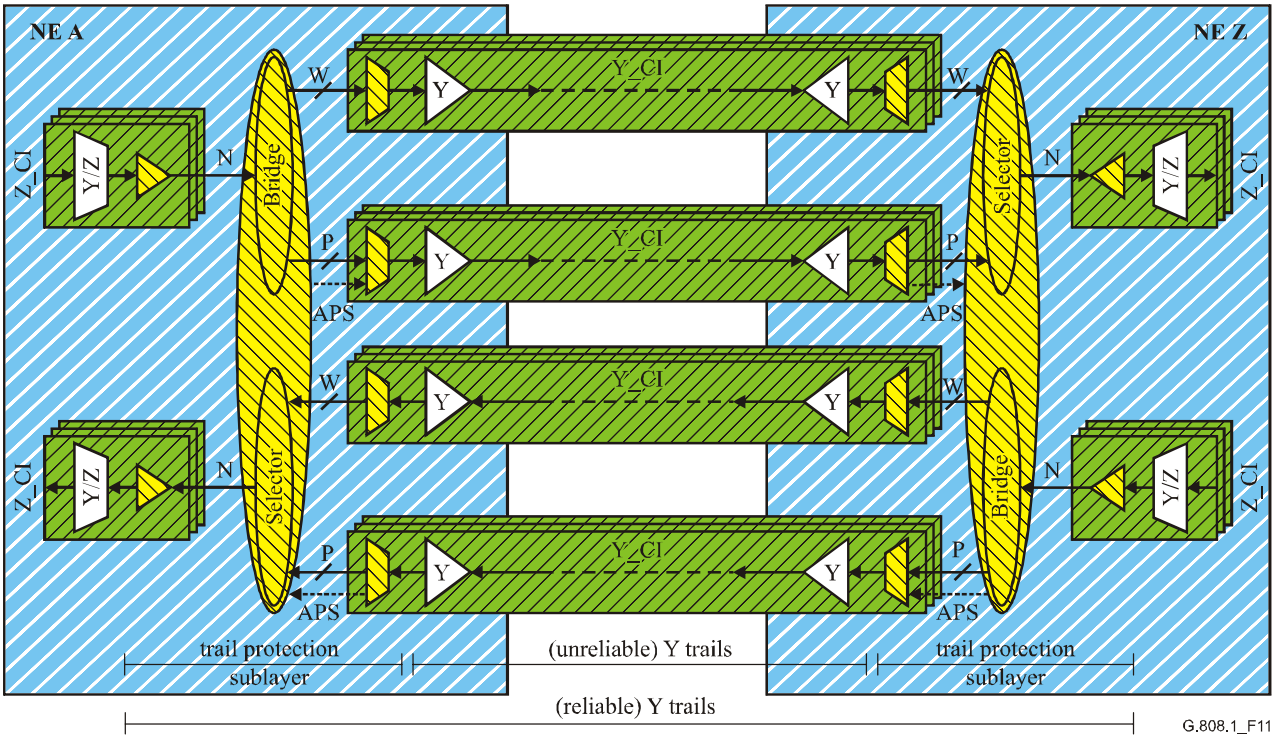


Figure 11/G.808.1 – 1+1/1:1 Group trail protection functional model

Figure 12 presents additional detail of this protection connection function's processes. Specific for group protection is the SFG/SDG logic process. This process "merges" the three individual trail signal fail (TSF) signals into a single SF Group (SFG) and the individual trail signal degrade (TSD) signals into a single SDG.

The SFG/SDG logic may operate in different modes:

- W-SFG = W1-TSF or W2-TSF or W3-TSF
  P-SFG = P1-TSF or P2-TSF or P3-TSF;
- W-SFG = W1-TSF
  P-SFG = P1-TSF;
- W-SFG = X% of the Wi-TSF signals are active
  P-SFG = X% of the Pi-TSF signals are active;
- idem for SDG.

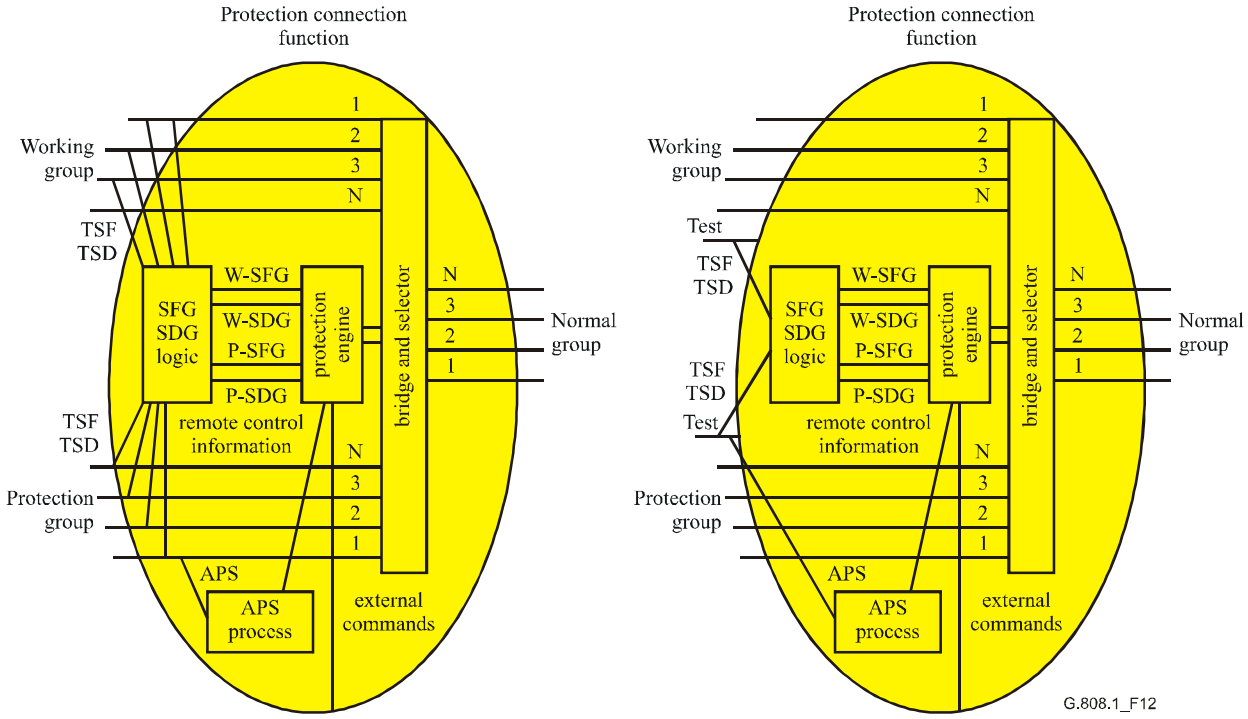


Figure 12/G.808.1 – SFG/SDG logic within group protection process

As a result of the large number of tributary slots in some transmission technologies (e.g., ATM), extra tributary slots in the working and protection server layer signals can be allocated to transport test signals via test transport entities (Figures 13 and 14). These test signals (one per working, one per protection) can be used instead of the SFG, SDG information as described above. The APS signal is transported via the test protection transport entity.

The SFG/SDG logic operates now as follows:

- W-SFG = Wt-TSF
  P-SFG = Pt-TSF;
- W-SDG = Wt-TSD
  P-SDG = Pt-TSD.

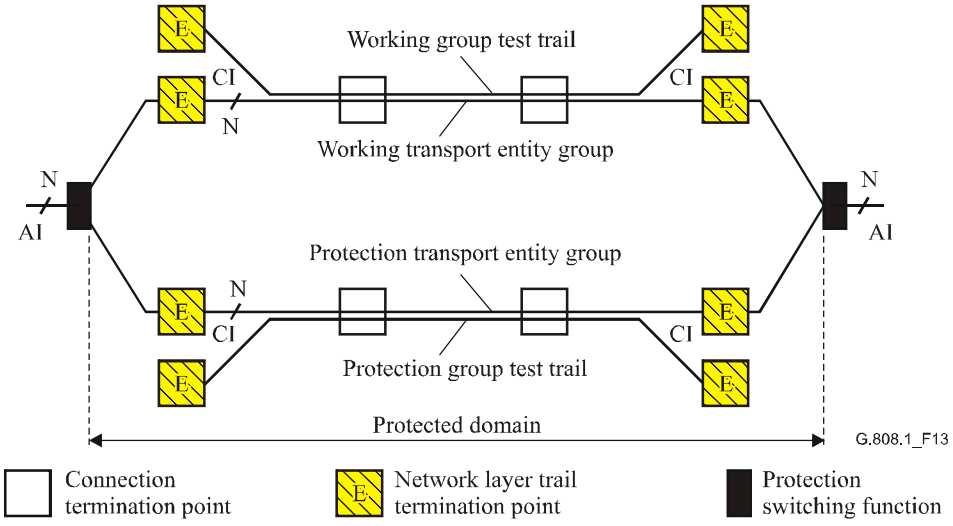


Figure 13/G.808.1 – Generic concept of group trail/T protection

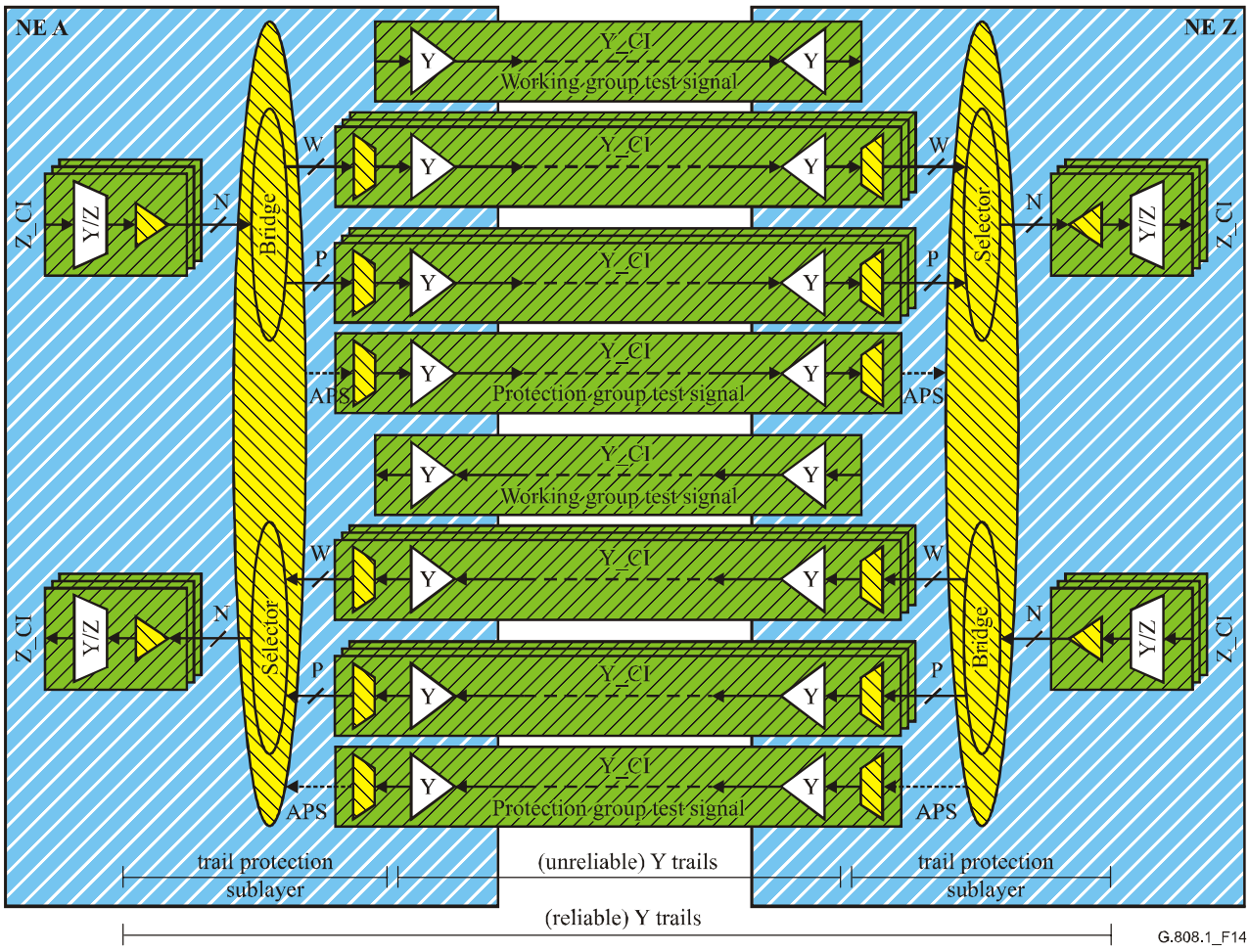


Figure 14/G.808.1 – 1+1/1:1 Group trail/T protection functional model

11.2 SNC protection

Subnetwork connection protection is the protection class used to protect a portion of a trail (e.g., that portion where two separate routes are available) within an operator's network or multiple operators' networks.

The subnetwork connection that is protected can be between two Connection Points (CPs) (Figure 15), between a CP and a Termination Connection Point (TCP) (Figure 16), or the full end-to-end network connection between two TCPs (Figure 17).

As subnetwork connection protection is a dedicated protection mechanism, it can be used on any physical structure (i.e., meshed, rings, or mixed), and there is no fundamental limitation on the number of NEs within the subnetwork connection. It may be applied at any layer in a layered network.

SNC protection operates in all combinations of protection architectures, switching and operation.

SNCP can be further split into subclasses that represent the defect conditions that contribute to SF/SD:

1) Inherent: the server layer's trail termination and adaptation functions are used to determine the SF/SD condition. It supports detection of server layer defect conditions only.

2) Non-intrusive: non-intrusive monitoring functions are deployed to determine the SF/SD condition.

a) End-to-end: detection of server layer defect conditions, continuity/connectivity defect conditions in the layer network, and error degradation conditions in the layer network. The end-to-end overhead/OAM is used.

b) Sublayer: detection of server layer defect conditions, continuity/connectivity defect conditions in the layer network, and error degradation conditions in the layer network. The sublayer overhead/OAM is used.

3) Sublayer: Tandem connection/segment sublayer functions are deployed to determine the SF/SD condition. It supports detection of server layer defect conditions, continuity/connectivity defect conditions in the layer network, and error degradation conditions in the layer network. The sublayer overhead/OAM is used.

In general, SNC protection requires the creation of sublayer trails (tandem connections, segments) on the working and protection transport entities to distinguish a fault or degradation occurring "in front of" from "within" the protected domain. When the sublayer trail includes a single server layer trail, that server layer trail can be used instead (providing inherent monitoring). If a sublayer trail cannot be created, or a single server layer trail is not available between the ingress and egress points of the protected domain, SNC protection can be realized by means of dual feeding the normal traffic signal to both working and protection transport entities, non-intrusive monitoring both copies of the signal at the egress point and comparing the SF/SD status obtained from both monitors. If the fault or degradation occurred in front of the protected domain, both working and protection monitors will discover the impairment and a switch action will not be performed. Otherwise, only one of the two monitors will detect a SF/SD condition and, with a switch action, the traffic flow can be restored.

NOTE 1 – For SDH, due to the treatment of AU/TU pointers during server layer TSF conditions, 1+1 SNC/I can be deployed instead of 1+1 SNC/N if server layer defects are to be protected only.

For the case of SNC protection, the Characteristic Information (CI) (i.e., payload and its layer overhead) is protected. See Figures 15 to 18.

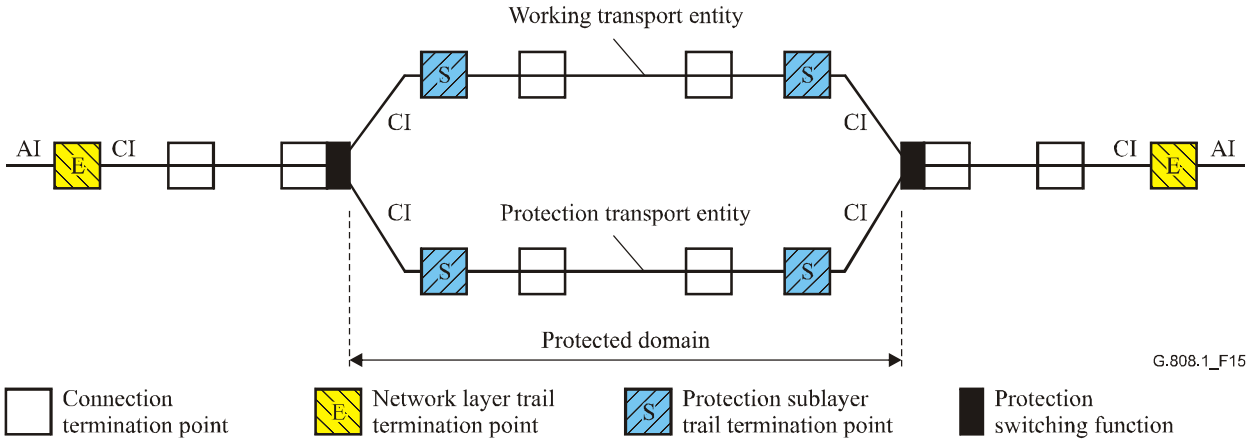


Figure 15/G.808.1 – SNC/S protection example 1

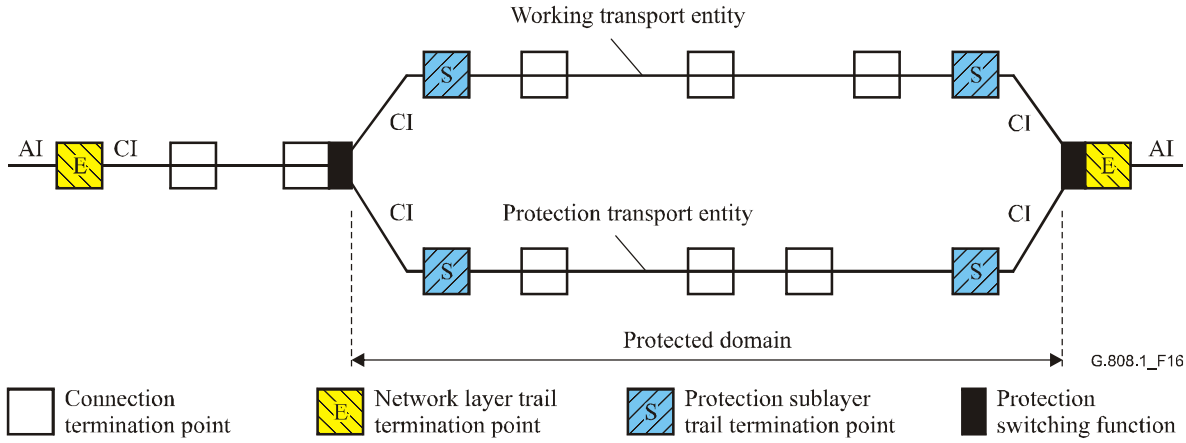


Figure 16/G.808.1 – SNC/S protection example 2

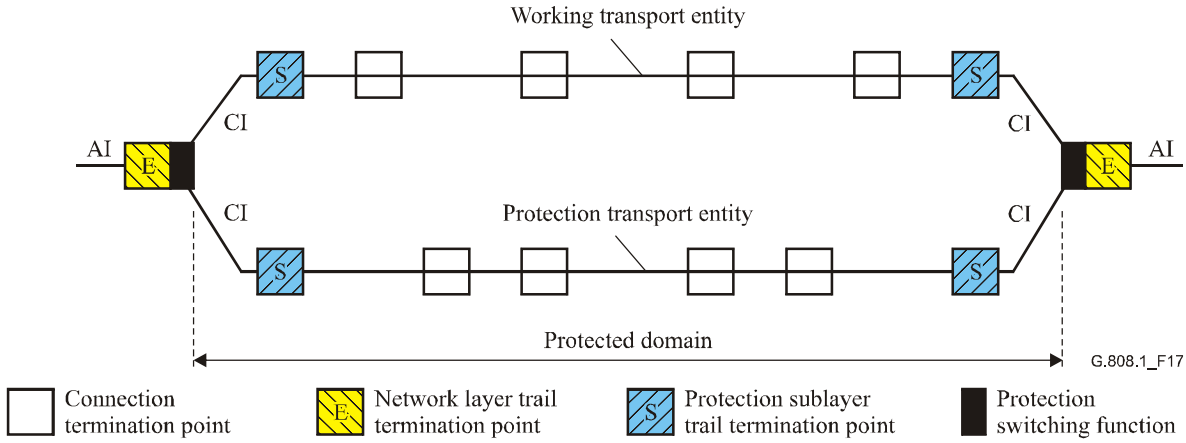


Figure 17/G.808.1 – SNC/S protection example 3

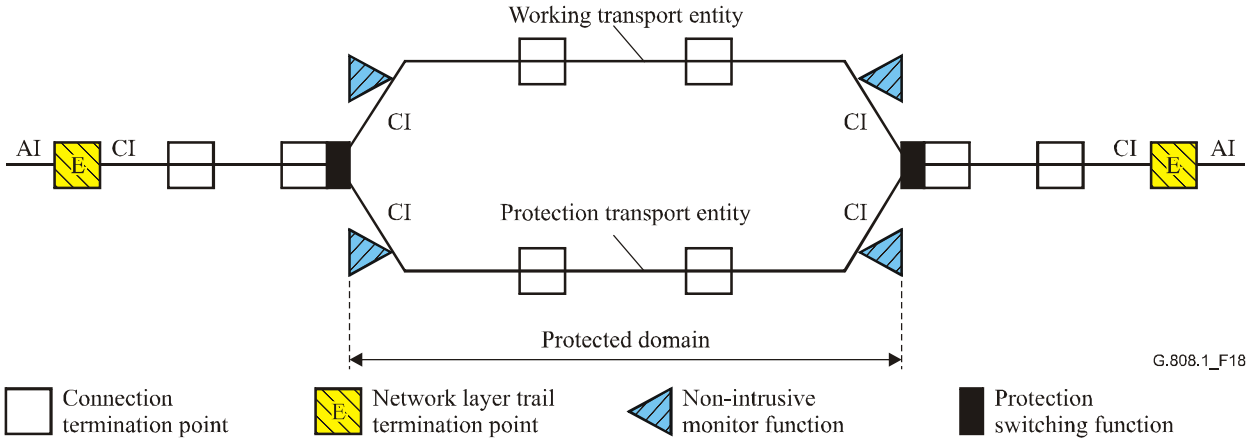


Figure 18/G.808.1 – 1+1 SNC/N protection

SNC protection supports network architectures, which make use of cascaded protected subnetworks. Such network architectures are able to restore traffic for the case of multiple faults (one fault per protected subnetwork); refer to Figure 19.

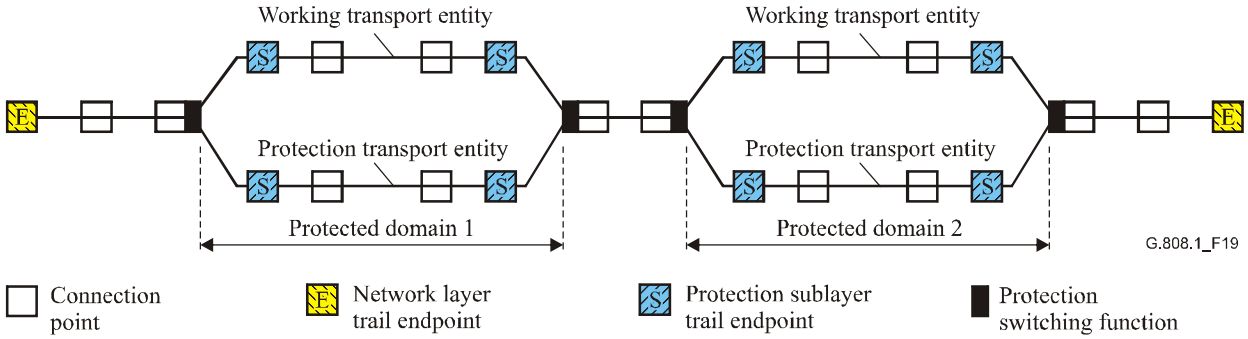


Figure 19/G.808.1 – Cascaded SNC/S protection

The fault tolerance (and reliability) of the cascaded SNC protected subnetworks is increased when the interconnection between the subnetworks is duplicated (Figure 20), removing the single point of failure. This requires the use of 1+1, unidirectional switched SNC/N or SNC/I protection types. Using 1:n, m:n, $(1:1)^n$ and/or bidirectional switching is not possible.

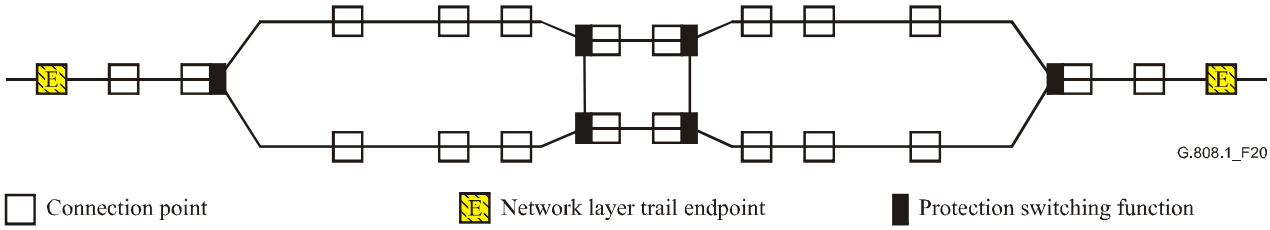


Figure 20/G.808.1 – Cascaded 1+1 SNC protection with fault tolerant subnetwork interconnects

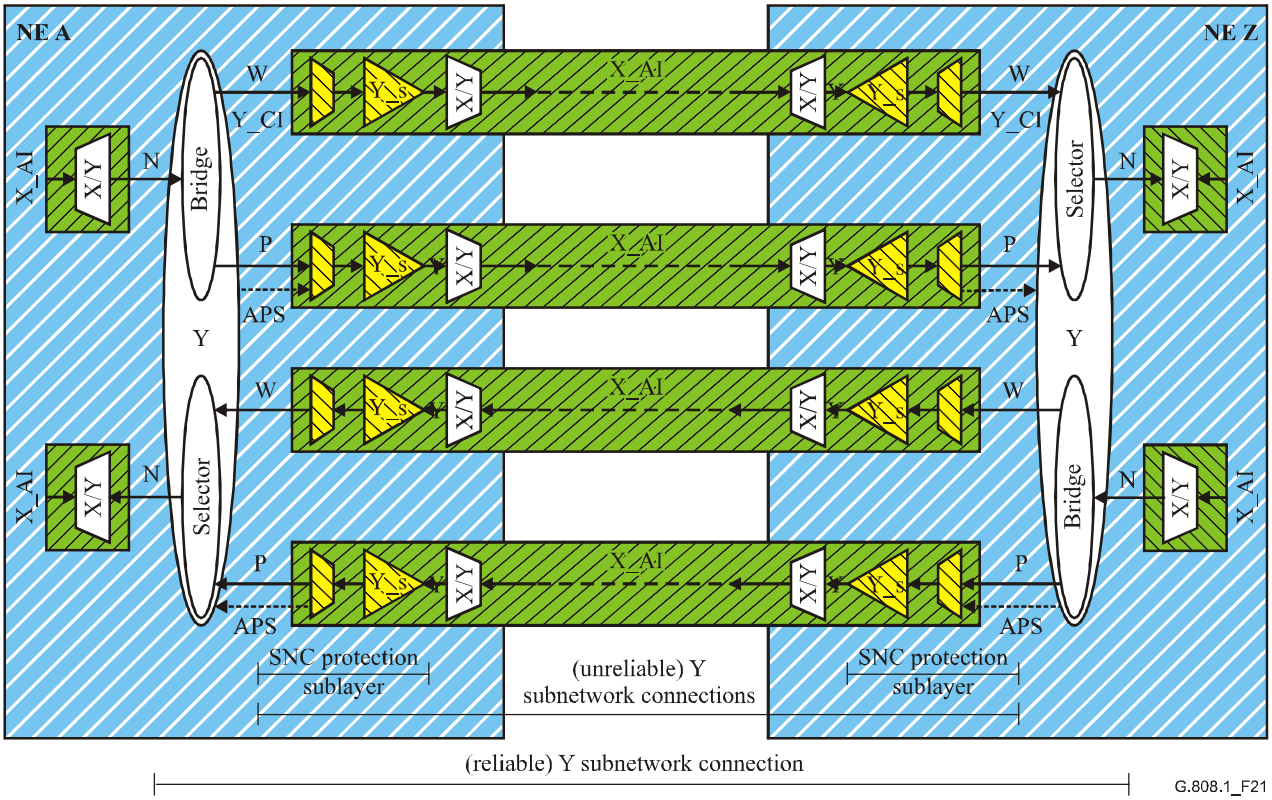
NOTE 2 – For the case of an 1:1, m:n, or $(1:1)^n$ architecture in ATM, the protection subnetwork connection(s) should contain a signal that allows accurate monitoring of its status. In normal conditions, in which the normal traffic signal is transported via the working SNC, there is no signal to be transported via protection. If the CC is inactive, such protection SNC will not transport any information under normal fault-free conditions. When a fault occurs, AIS cells are inserted. When the fault is present for a short period only (e.g., due to a "physical layer protection action"), the AIS defect detector at the protection segment endpoint will detect the AIS defect condition for 2 to 3 seconds according to the I.610-defined AIS state definition. With the CC activated, the AIS defect condition will clear on the receipt of a CC cell, i.e., within a period of 1 second after the traffic interruption was cleared.

11.2.1 Individual SNC protection

11.2.1.1 1+1, 1:n, m:n, $(1:1)^n$ SNC/S

Figure 21 illustrates the case of 1+1 SNC/S protection and 1:1 SNC/S protection without extra traffic between ingress and egress of the protected domain between NEs A and Z. Two independent sublayer trails exist, which act as working and protection transport entities for the (protected) normal traffic signal. The sublayer TT functions generate/insert and monitor/extract the sublayer overhead/OAM information to determine the status of the working and protection transport entities. APS information is transported over the protection SNC, except for the case of 1+1 unidirectional switching.

The cases of 1:n, m:n and $(1:1)^n$ architectures with/without extra traffic are extensions of the 1+1/1:1 architecture, in accordance with the architecture type descriptions in clause 7.



NOTE – APS signal not applicable for 1+1 unidirectional switched case

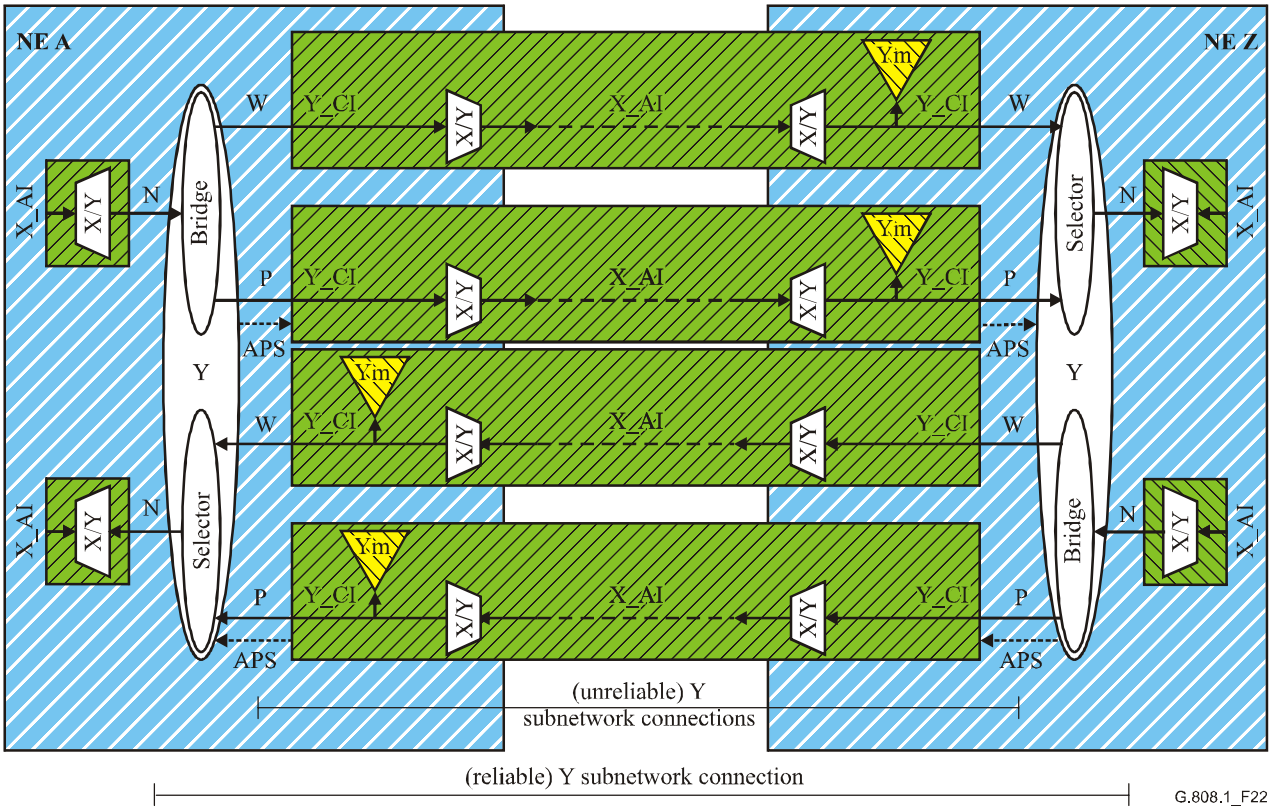
Figure 21/G.808.1 – 1+1/1:1 SNC/S protection functional model

NOTE – The sublayer trail termination functions (e.g., tandem connection/segment termination functions) are used for administrative purposes (to monitor the quality of service of the transport through the administrative network domain) and for protection purposes. For protection purposes, the location of the sublayer trail terminations is as indicated in the SNC/S figures. For administrative purposes, the optimum location is at the other side of the connection function.

11.2.1.2 1+1 SNC/N

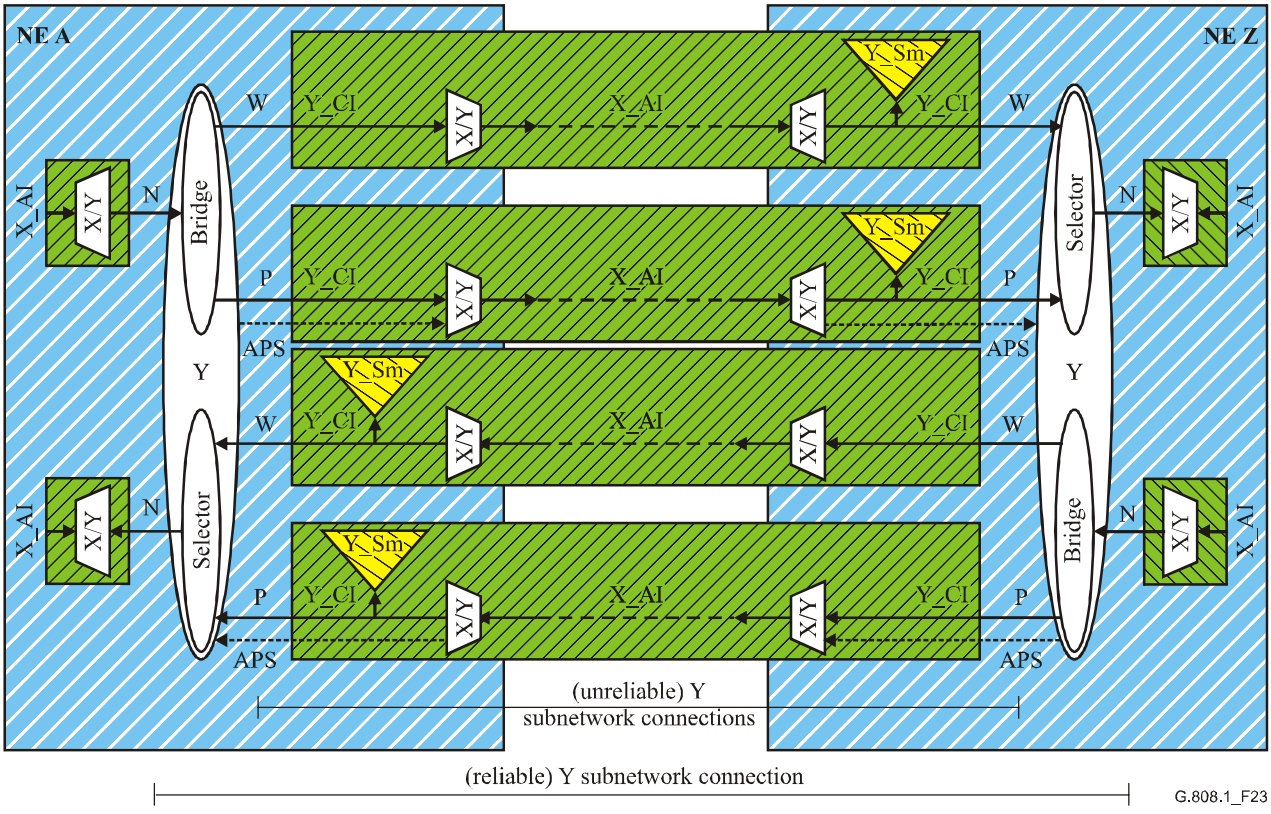
For the case of 1+1 SNC protection, a *reduced complexity* scheme is defined: SNC/N.

Figures 22 and 23 illustrate the case of 1+1 SNC/N protection between ingress and egress of the protected domain between NEs A and Z. Two independent subnetwork connections exist, which act as working and protection transport entities for the (protected) normal traffic signal. The Non-Intrusive Monitoring (NIM) functions (Ym_TT_Sk, Y_Sm_TT_Sk) monitor the end-to-end (SNC/Ne) or sublayer (SNC/Ns) overhead/OAM information to determine the status of the working and protection transport entities. APS information is transported over the protection SNC, except for the case of 1+1 unidirectional switching.



NOTE – APS signal not applicable for 1+1 unidirectional switched case

Figure 22/G.808.1 – 1+1 SNC/Ne protection functional model



NOTE – APS signal not applicable for 1+1 unidirectional switched case

Figure 23/G.808.1 – 1+1 SNC/Ns protection functional model

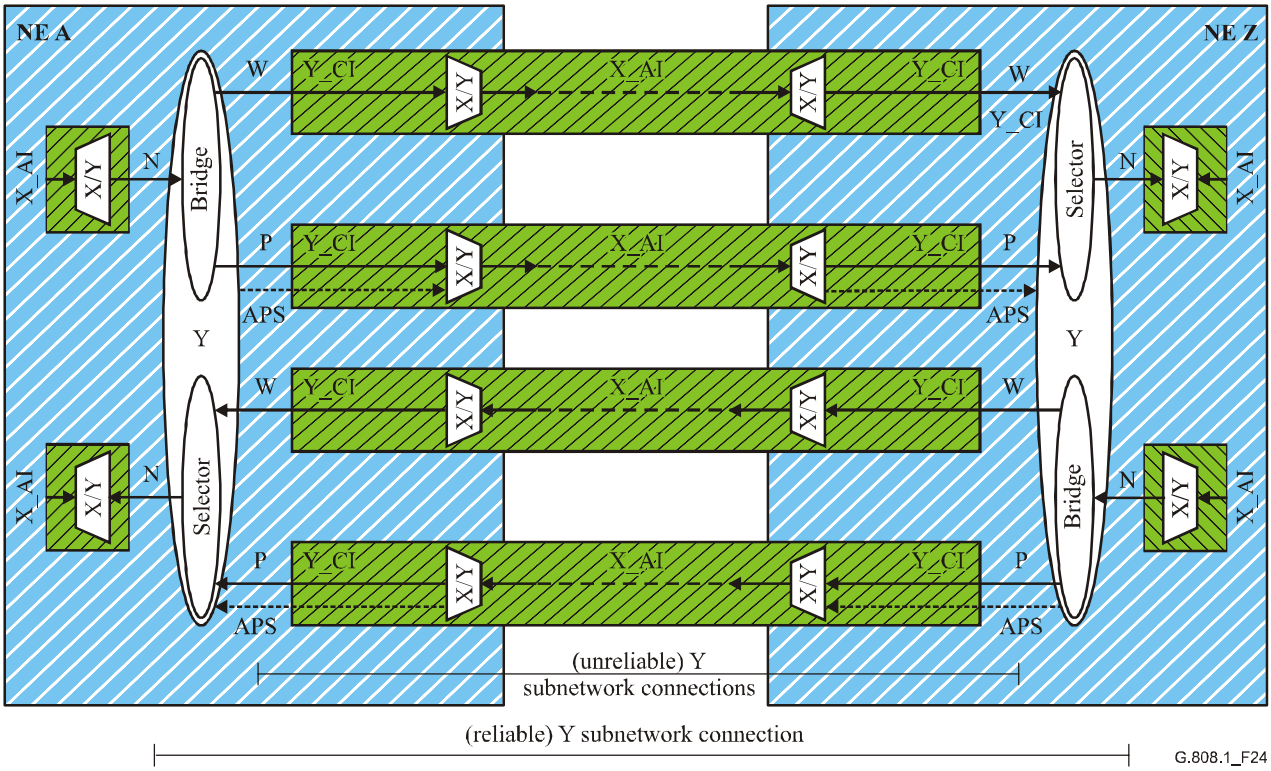
11.2.1.3 1+1/1:n SNC/I

For the case of 1+1/1:n SNC protection, another *reduced complexity* scheme is: SNC/I.

Figure 24 illustrates the case of 1+1/1:1 SNC/I protection between ingress and egress of the protected domain between NEs A and Z. Two independent subnetwork connections exist, which act as working and protection transport entities for the (protected) normal traffic signal. The X/Y adaptation functions monitor the server layer's adapted information for signal fail, to determine the status of the working and protection transport entities. APS information is transported over the protection SNC, except for the case of 1+1 unidirectional switching.

In general SNC/I protection is a protection scheme for a single link connection (spanning one server layer trail only) as the adaptation functions derive their SSF and SSD conditions from the server layer trail's TSF/TSD. The TSF status is forwarded as a client layer AIS/FDI maintenance signal and is not visible as such at downstream adaptation functions. The TSD information is not forwarded.

An exception exists for SDH VC-n SNC/I protection; SNC/I is able to protect a serial compound link connection as the AIS maintenance signal is detected in every adaptation function downstream of the insertion point.



NOTE – APS signal not applicable for 1+1 unidirectional switched case

Figure 24/G.808.1 – 1+1/1:1 SNC/I protection functional model

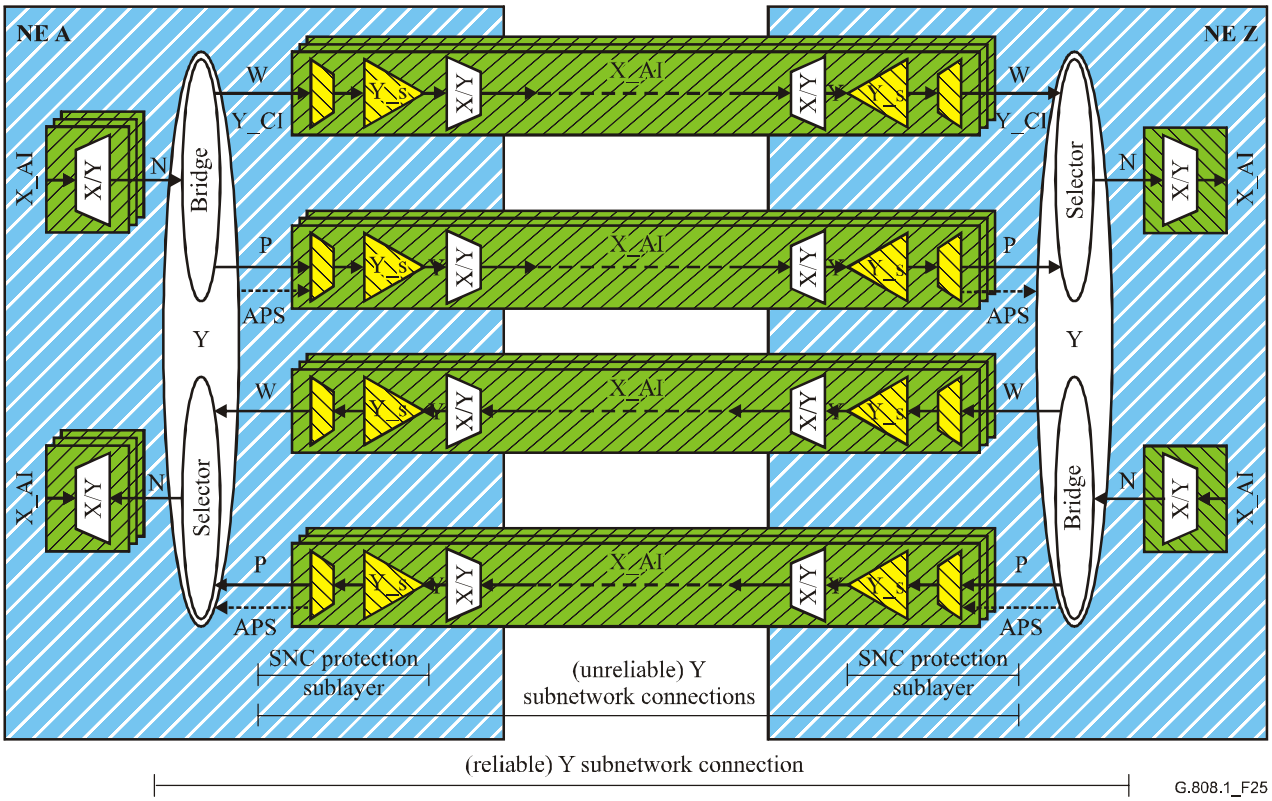
11.2.2 Group SNC protection

11.2.2.1 SNC/S

Figure 25 illustrates the case of 1+1/1:1 group SNC/S protection between NEs A and Z. In this example, two times three parallel independent sublayer trail monitored subnetwork connections exist, which act as working and protection transport entity groups for the three (protected) normal traffic signals. The three parallel normal traffic signals in the group are protected jointly by the layer's connection function. The sublayer TT functions generate/insert and monitor/extract the

sublayer overhead/OAM information to determine the status of the working and protection transport entities. APS information is transported over one of the protection SNCs, except for the case of 1+1 unidirectional switching.

The cases of 1:n, m:n and $(1:1)^n$ architectures with/without extra traffic are extensions of the 1+1/1:1 architecture, in accordance with the architecture type descriptions in clause 7.



NOTE – APS signal not applicable for 1+1 unidirectional switched case

Figure 25/G.808.1 – 1+1/1:1 Group SNC/S protection functional model

Figure 12 presents additional detail of this protection connection function's processes. Specific for group protection is the SFG/SDG logic process. This process "merges" the three individual trail signal fail (TSF) signals into a single SF Group (SFG) and the individual trail signal degrade (TSD) signals into a single SDG.

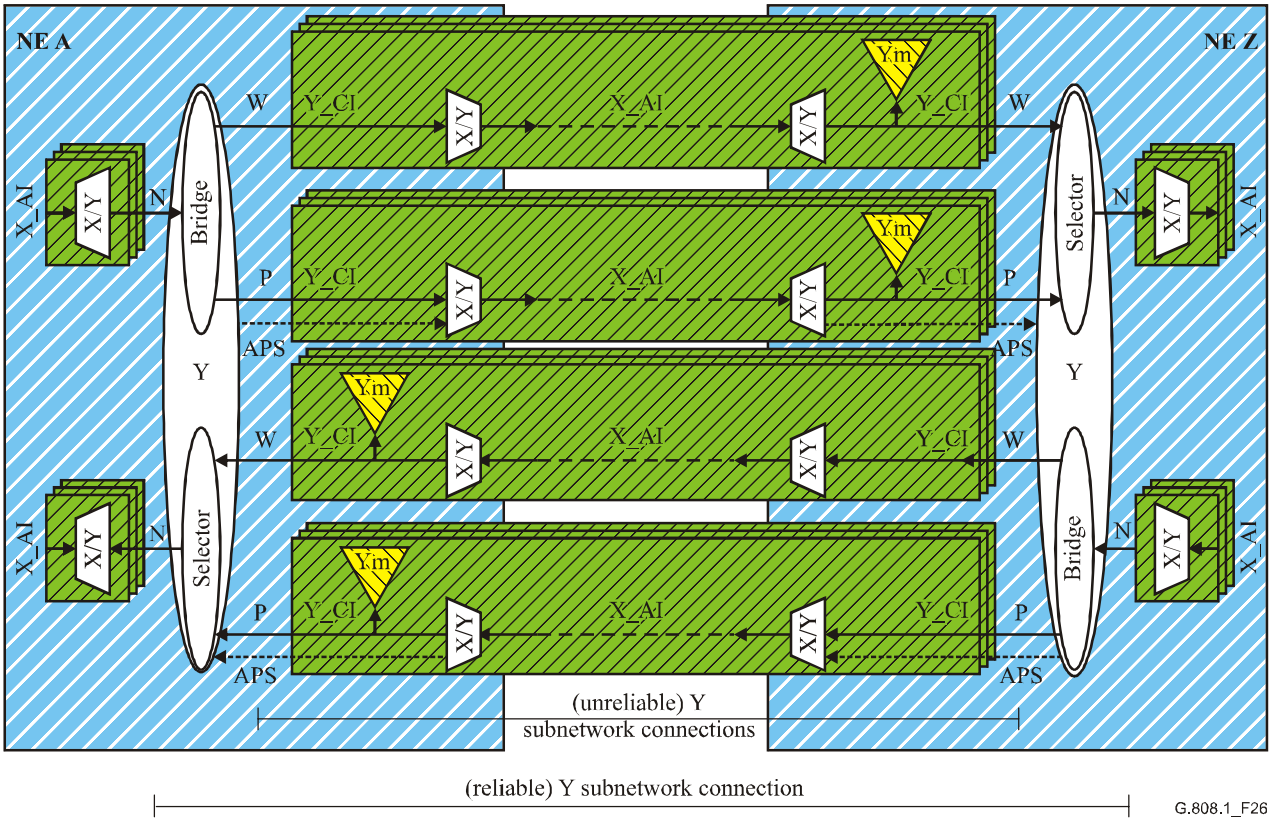
The SNC/S SFG/SDG logic may operate in different modes:

- W-SFG = W1-TSF or W2-TSF or W3-TSF; P-SFG = P1-TSF or P2-TSF or P3-TSF;
- W-SFG = W1-TSF; P-SFG = P1-TSF;
- W-SFG = X% of the Wi-TSF signals are active; P-SFG = X% of the Pi-TSF signals are active;
- idem for SDG.

11.2.2.2 1+1 SNC/N

Figure 26 illustrates the case of 1+1 group SNC/N protection between NEs A and Z. In this example, two times three parallel independent subnetwork connections exist, which act as working and protection transport entity groups for the three (protected) normal traffic signals. The three parallel normal traffic signals in the group are protected jointly by the layer's connection function. The NIM functions monitor the end-to-end (SNC/Ne) or sublayer (SNC/Ns) overhead/OAM information to determine the status of the working and protection transport entities. APS

information is transported over one of the protection SNCs, except for the case of 1+1 unidirectional switching.



NOTE – APS signal not applicable for 1+1 unidirectional switched case

Figure 26/G.808.1 – 1+1 Group SNC/Ne protection functional model

Figure 12 presents additional detail of this protection connection function's processes. Specific for group 1+1 SNC/N protection is the SFG/SDG logic process. This process "merges" the three individual trail signal fail (TSF) signals into a single SF Group (SFG) and the individual trail signal degrade (TSD) signals into a single SDG.

The SNC/N SFG/SDG logic may operate in different modes:

- W-SFG = (W1-TSF and not P1-TSF) or (W2-TSF and not P2-TSF) or (W3-TSF and not P3-TSF);

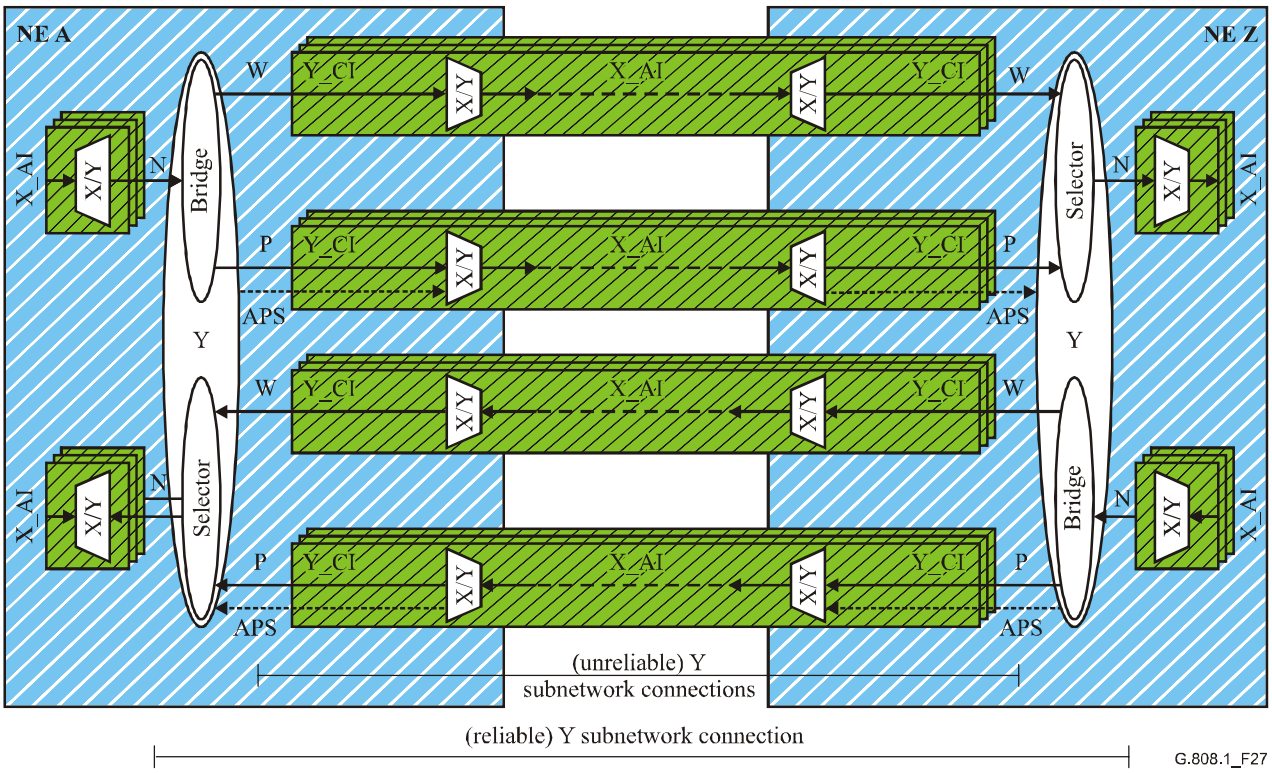
  P-SFG = (P1-TSF and not W1-TSF) or (P2-TSF and not W2-TSF) or (P3-TSF and not W3-TSF);
- W-SFG = (W1-TSF and not P1-TSF); P-SFG = (P1-TSF and not W1-TSF);
- W-SFG = X% of the (Wi-TSF and not Pi-TSF) signals are active; P-SFG = X% of the (Pi-TSF and not Wi-TSF) signals are active;
- idem for SDG.

For virtual concatenated SDH VC-n signals (VC-n-Xv), the group SF and SD conditions should be declared as soon as one of the X signals in the group is failed or degraded.

- W-SFG = W1-TSF or W2-TSF or W3-TSF; P-SFG = P1-TSF or P2-TSF or P3-TSF;
- idem for SDG.

11.2.2.3 1+1 SNC/I

Figure 27 illustrates the case of 1+1 group SNC/I protection between NEs A and Z. In this example, two times three parallel independent subnetwork connections exist, which act as working and protection transport entity groups for the three (protected) normal traffic signals. The three parallel normal traffic signals in the group are protected jointly by the layer's connection function. The X/Y adaptation functions monitor the server layer's adapted information for signal fail, to determine the status of the working and protection transport entities. APS information is transported over one of the protection SNCs, except for the case of 1+1 unidirectional switching.



NOTE – APS signal not applicable for 1+1 unidirectional switched case

Figure 27/G.808.1 – 1+1 Group SNC/I protection functional model

Figure 12 presents additional detail of this protection connection function's processes. Specific for group 1+1 SNC/I protection is the SFG logic process. This process "merges" the three individual server signal fail (SSF) signals into a single SF Group (SFG).

The SNC/I SFG logic may operate in different modes:

- W-SFG = (W1-SSF and not P1-SSF) or (W2-SSF and not P2-SSF) or (W3-SSF and not P3-SSF);

  P-SFG = (P1-SSF and not W1-SSF) or (P2-SSF and not W2-SSF) or (P3-SSF and not W3-SSF);
- W-SFG = (W1-SSF and not P1-SSF); P-SFG = (P1-SSF and not W1-SSF);
- W-SFG = X% of the (Wi-SSF and not Pi-SSF) signals are active; P-SFG = X% of the (Pi-SSF and not Wi-SSF) signals are active.

For virtual concatenated SDH VC-n signals (VC-n-Xv), the group SF and SD conditions should be declared as soon as one of the X signals in the group is failed or degraded.

- W-SFG = W1-SSF or W2-SSF or W3-SSF; P-SFG = P1-SSF or P2-SSF or P3-SSF;
- idem for SDG.

11.2.2.4 SNC/T

As a result of the large number of tributary slots in some transmission technologies (e.g., ATM) extra tributary slots in the working and protection server layer signals can be allocated to transport test signals via test transport entities (Figures 28 and 30). These test signals (one per working, one per protection) can be used instead of the SFG, SDG information as described above. The APS signal is transported via the test protection transport entity.

The SFG/SDG logic operates now as follows:

- W-SFG = Wt-TSF;
  P-SFG = Pt-TSF;
- W-SDG = Wt-TSD;
  P-SDG = Pt-TSD.

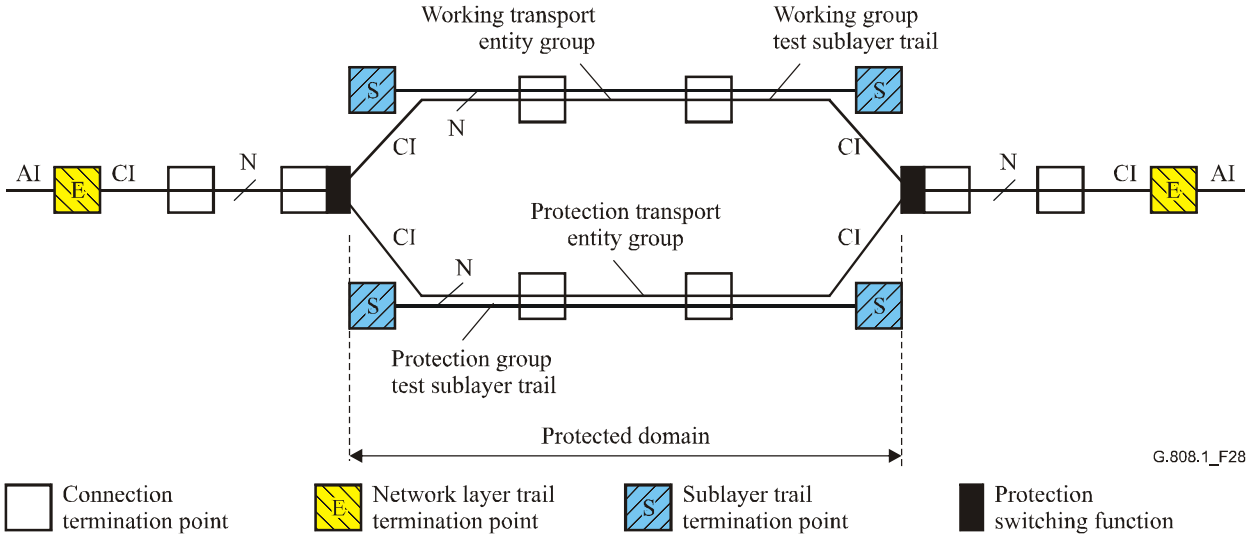


Figure 28/G.808.1 – 1:1 or 1+1 SNC/Ts group protection using sublayer trail terminations

Group SNC/T protection can also use the end-to-end overhead/OAM to create an end-to-end layer network trail as a test trail (Figure 29). Equipment designs typically locate those layer termination functions at port units at the "other side" of the connection function; i.e., not readily available for group protection test trail purposes.

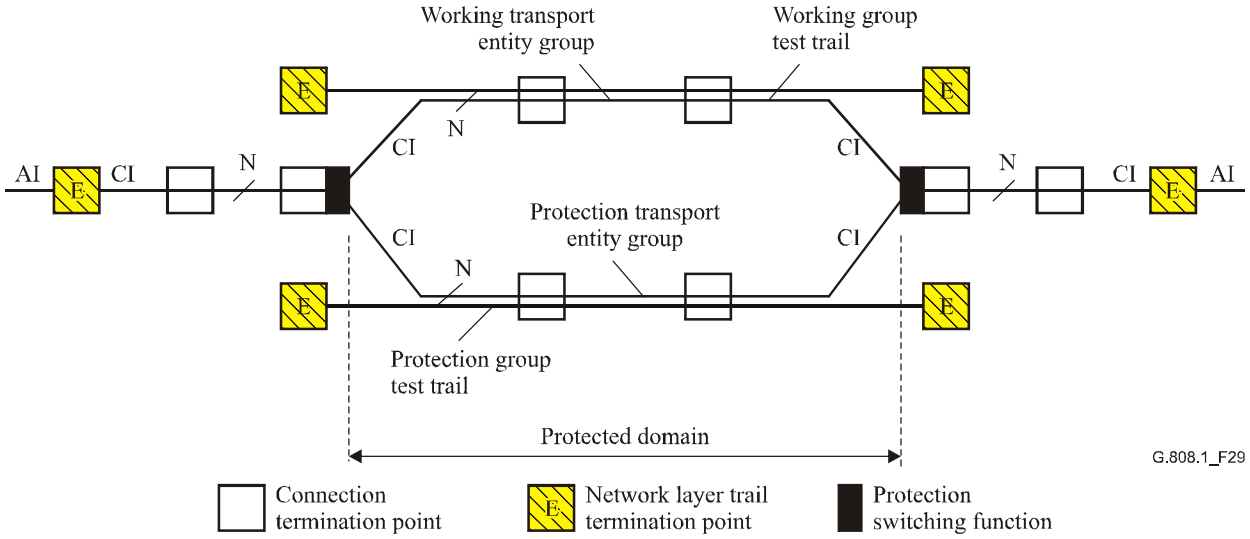
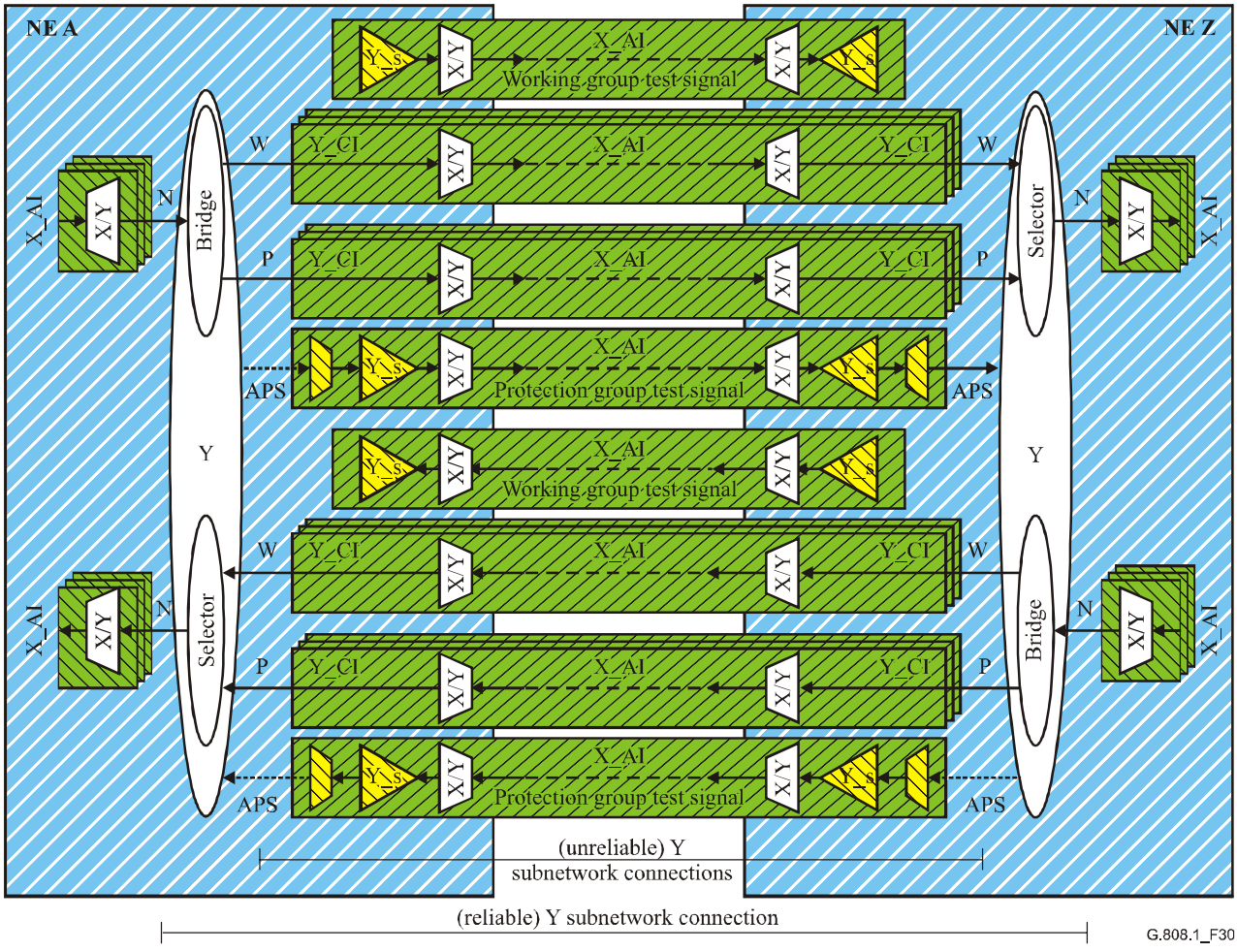


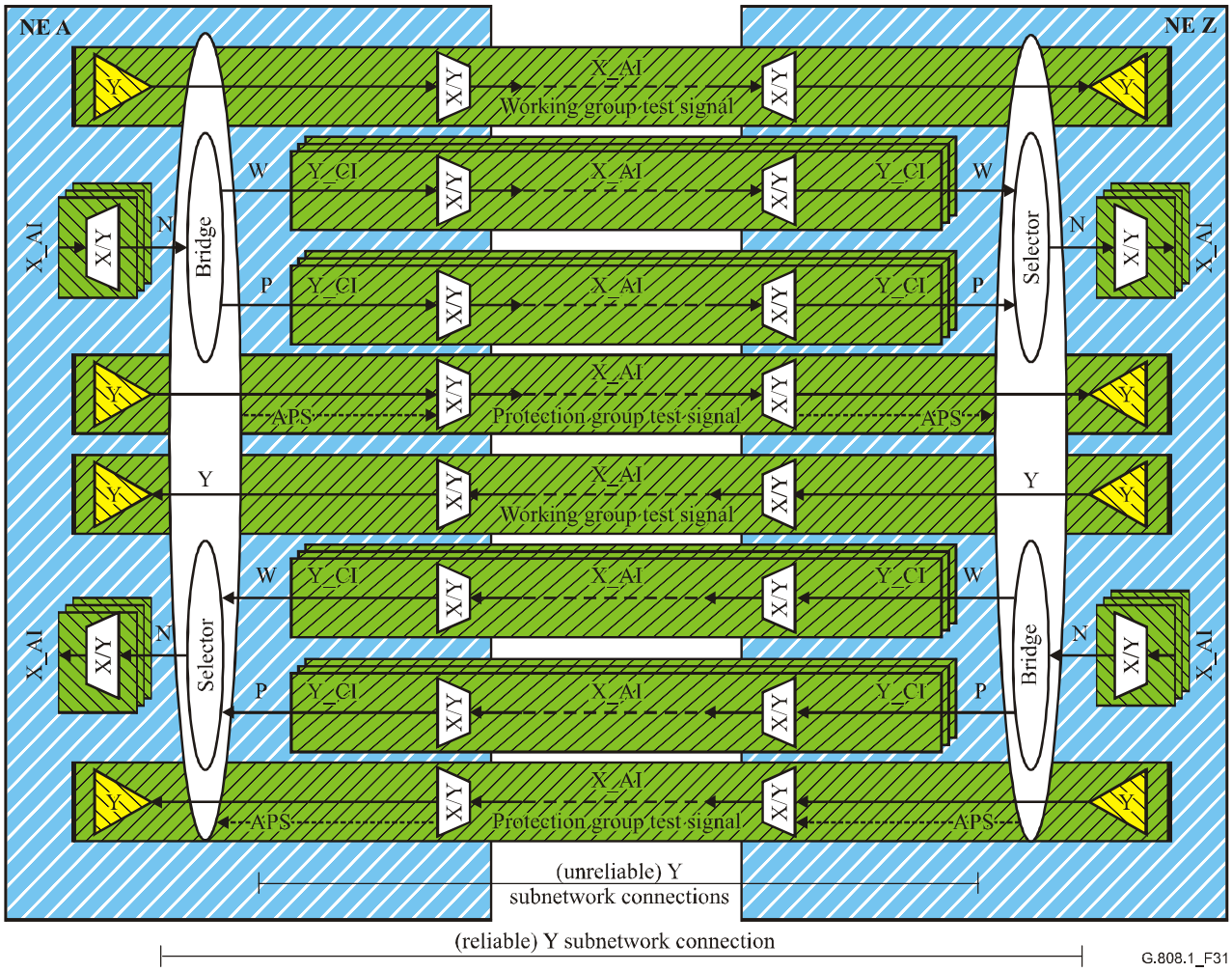
Figure 29/G.808.1 – 1:1 or 1+1 SNC/Te group protection using layer network trail terminations



NOTE – APS signal not applicable for 1+1 unidirectional switched case

Figure 30/G.808.1 – 1+1/1:1 Group SNC/Ts protection functional model using sublayer trail terminations

NOTE – For the case of ATM, the test (sublayer) trail should contain a test signal that has Continuity Check (CC) activated. If the CC is inactive, such a test (sublayer) trail would not transport any information under normal fault-free conditions. When a fault occurs, AIS cells are inserted. When the fault is present for a short period only (e.g., due to a "physical layer protection action"), the AIS defect detector at the test (sublayer) trail endpoint will detect the AIS defect condition for 2 to 3 s according to the I.610-defined AIS state definition. With the CC activated, the AIS defect condition will clear on the receipt of a CC cell, i.e., within a period of 1 second after the traffic interruption was cleared.



NOTE – APS signal not applicable for 1+1 unidirectional switched case

Figure 31/G.808.1 – 1+1/1:1 Group SNC/Te protection functional model using layer network trail terminations

12 Survivability offered by LCAS

Link Capacity Adjustment Scheme (LCAS) provides accommodation to network faults. It is used to offer survivability to a VC-n-Xv trail (across an entire operator's network or multiple operators networks). It is a dedicated end-to-end survivability architecture, which can be used in different network structures: meshed networks, rings, etc. As LCAS survivability is a dedicated survivability mechanism, there is no fundamental limitation on the number of NEs within the trails.

LCAS operates in all combinations of protection architectures, switching and operation.

LCAS generically protects against faults in the server layer, and connectivity faults and performance degradations in the client layer.

For the case of LCAS, the Adapted Information (AI) i.e., the total payload of the network layer's individual Characteristic Information (CI) is protected. See Figure 32.

The accommodation consists of removing the fractional payload transported by any member in the Virtual Concatenation Group (VCG) that experiences a transport entity fault condition. The result is a reduced AI payload size.

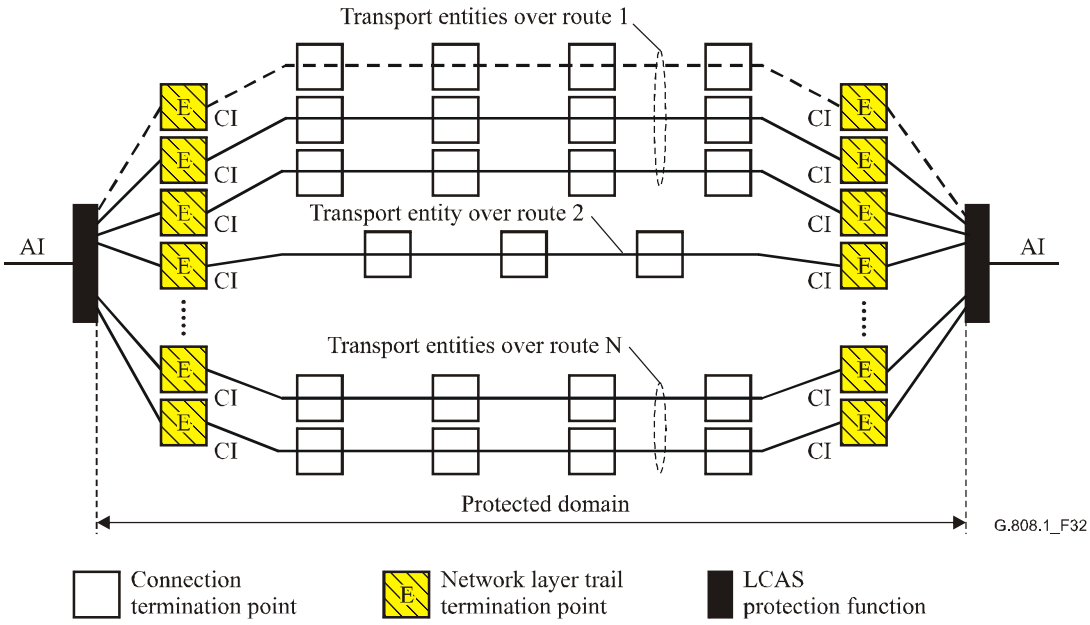


Figure 32/G.808.1 – Generic concept of LCAS-offered survivability

The AI is transported using a Virtual Concatenated Group (VCG) with X members (VC_n_Xv, ODUk_Xv), distributed over N routes, where:

- N = number of routes ($1 \leq N \leq X$) each containing one or more network connections within the VCG;
- X = number of members in the VCG required to transport the client's bandwidth AI + extra/protection capacity Z ($X \geq 1, Z \geq 0$);
- X_{ACT} = actual transported payload ($0 \leq X_{ACT} \leq X$); due to failure of one or more of the trails, the bandwidth of one or more members in the VCG will not be used to transport the AI.

LCAS is independent of protection at the server layers.

12.1 LCAS functional model

Figure 33 illustrates the case of LCAS for transport between NEs A and Z. Multiple independent trails (in layer network Y) are used as transport entities for the normal (payload) traffic signal Z_CI. The X/Y_TT functions generate/insert and monitor/extract the end-to-end overhead information to determine the status of the individual transport entities. The virtual concatenation Y-Xv/Y-X-L_A functions generate/insert and monitor/extract the end-to-end virtual concatenation and LCAS overhead information to determine and align the status of the members in the VCG.

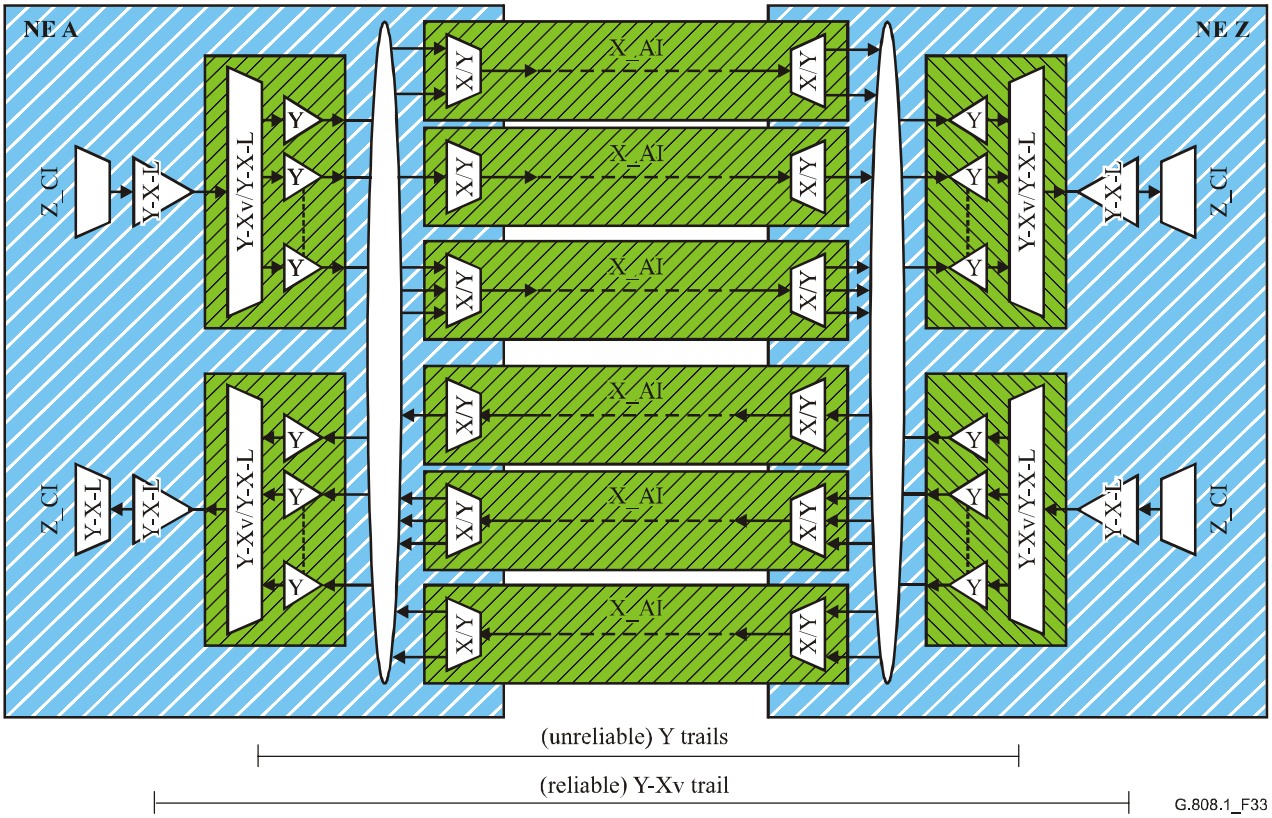


Figure 33/G.808.1 – LCAS functional model

The virtual concatenation Y-Xv/Y-X-L_A functions distribute/collect the transported payload using the X_{ACT} available layer network Y trails out of the X provisioned layer network Y trails.

Example: To transport a 10 Mbit/s signal, a VC-12-5v is required. Five VC-12 trails are set up in this VCG, two are routed via route 1 and three VC-12 are routed via route 2 (Figure 34). In this case, the survivable bandwidth is 2 × VC-12 or 40%, and the non-survivable bandwidth is 3 × VC-12 or 60%. Should one extra VC-12 had been provisioned (Z=1) and routed via route 1, the survivable bandwidth is 3 × VC-12 or 60% and the unprotected bandwidth 2 × VC-12 or 40%.

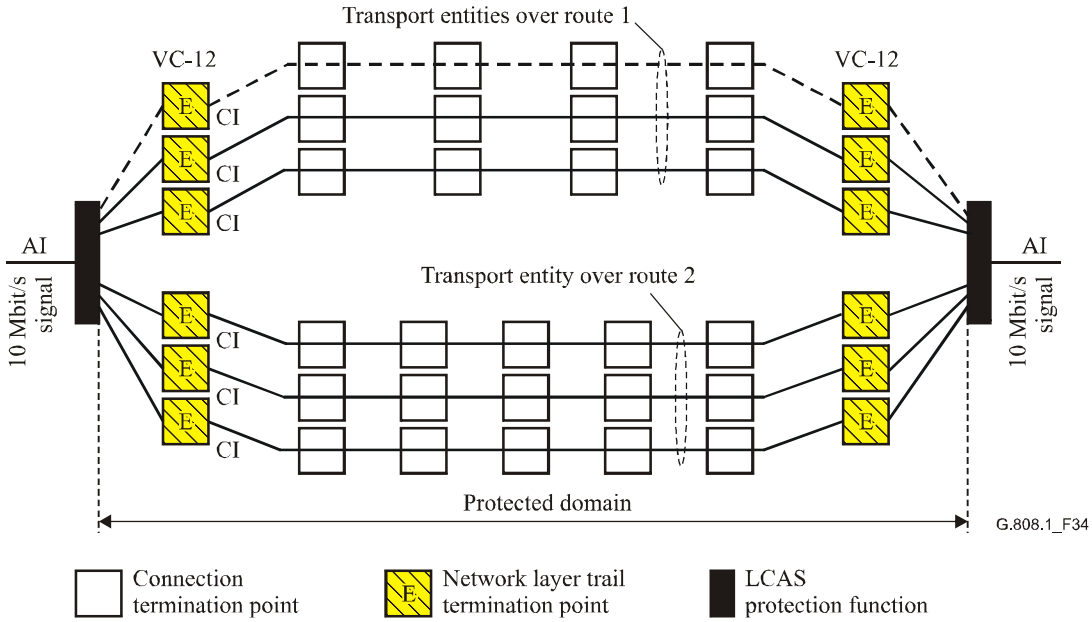


Figure 34/G.808.1 – Example LCAS survivability for 10 Mbit/s signal over VC-12-(X+Z)v (X=5, Z=0,1)

13 Protection switching performance

The protection switching temporal model derived from ITU-T Rec. M.495 is illustrated in Figure 35. Model parameters are defined as follows.

13.1 detection time, T_1: Time interval between the occurrence of a network impairment and the detection of a signal fail (SF) or signal degrade (SD) triggered by that network impairment.

13.2 hold-off time, T_2: Time interval after the detection of a SF or SD and its confirmation as a condition requiring the protection switching procedure.

NOTE – ITU-T Rec. M.495 identifies time T_2 as the "waiting time".

13.3 protection switching operations time, T_3: Time interval between the confirmation of a SF or SD and completion of the processing and transmission of the control signals required to effect protection switching.

13.4 protection switching transfer time, T_4: 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.

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

NOTE – This may include the verification of switching operations, resynchronization of digital transmission, etc.

13.6 confirmation time, T_c: The time from the occurrence of the network impairment to the instant when the triggered SF or SD is confirmed as requiring protection switching operations: $T_c = T_1 + T_2$.

13.7 transfer time, T_t: The time interval after the confirmation that a SF or SD requires protection switching operations to the completion of the protection switching operations: $T_t = T_3 + T_4$.

13.8 protected traffic restoration time, T_r: The time from the occurrence of the network impairment to the restoration of protected traffic:

$$T_r = T_1 + T_2 + T_3 + T_4 + T_5 = T_c + T_t + T_5.$$

NOTE – An apparent network impairment might be detected by an equipment and not confirmed after confirmation operations. In this case, only times T_1 and T_2 are relevant.

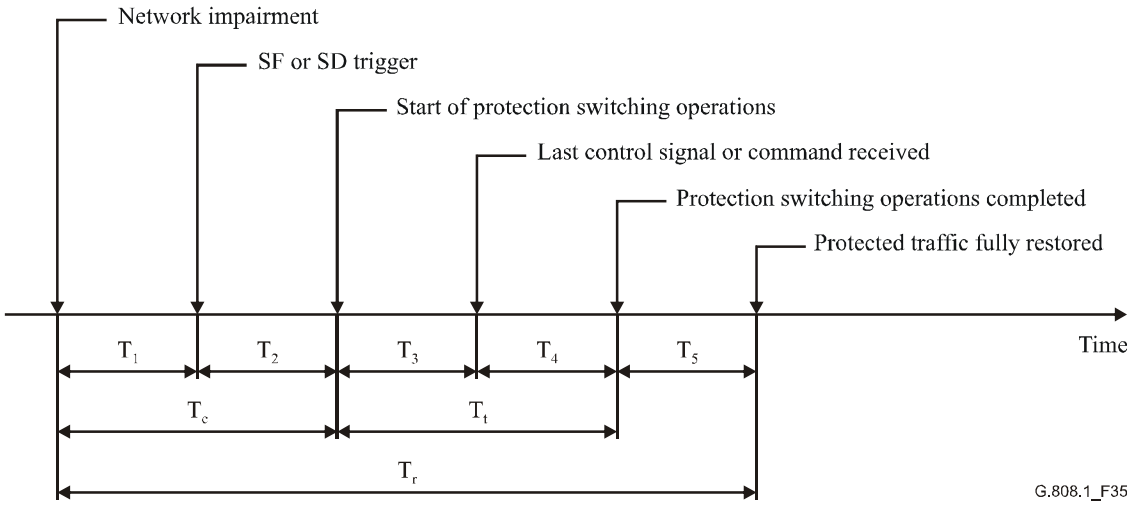


Figure 35/G.808.1 – Protection switching temporal model

14 Hold-off timer

Hold-off timers are intended to operate when a signal is protected by means of nested protection. They allow an inner protection group to restore the traffic before the outer protection group tries to do so, in order to limit the number of switch actions.

Hold-off timers are also applied in 1+1 SNC/N and SNC/I protection types to prevent too early switching due to the differential delay difference between the short and long route.

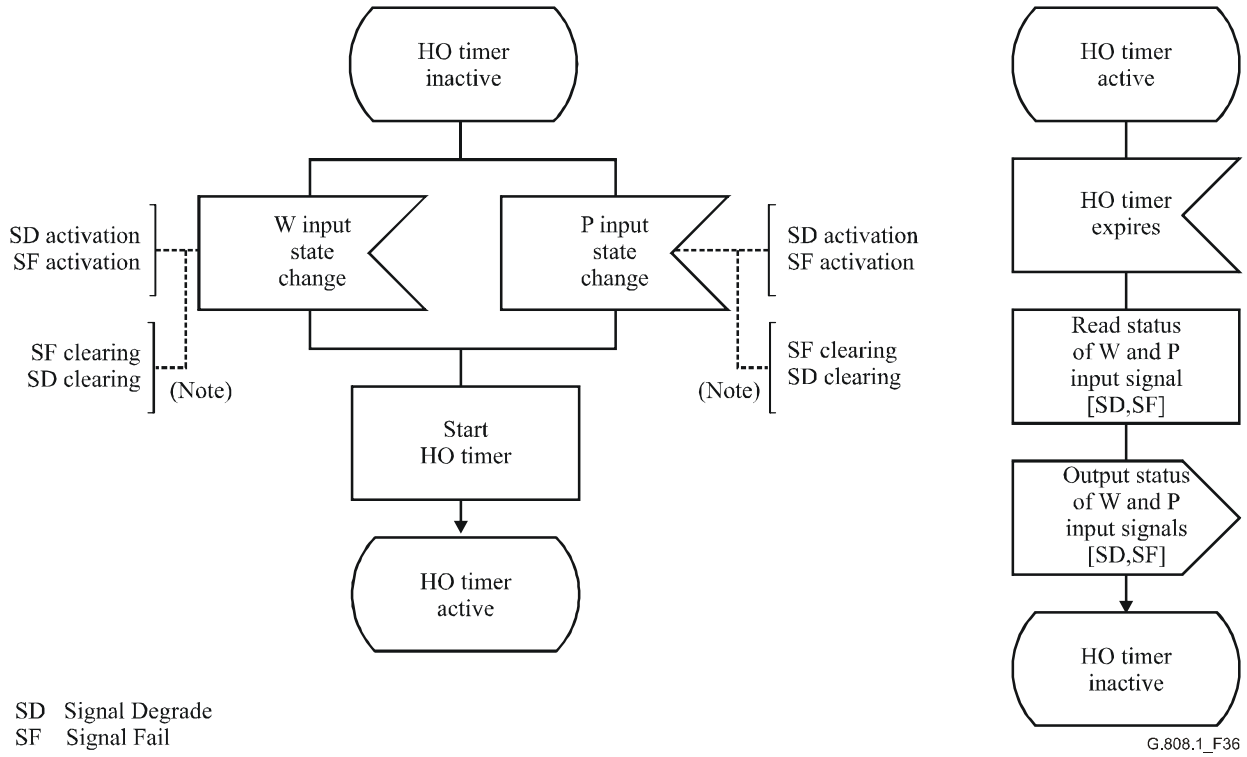
Each protection selector may have one hold-off timer.

A hold-off timer is started when one or more of the SF or SD conditions in the protection group become active, and runs for a non-resettable period which is provisionable from 0 to 10 s in steps of X ms. X is 100 ms (SDH, OTN) and 500 ms (ATM).

During this period, the modified SF/SD statuses are not passed to the protection switching process.

When the timer expires, the SF/SD status of all signals is read and passed through to the protection switching process. The protection switching process will react on the new SF/SD status at this point.

NOTE – An SF/SD condition does not have to be present for the entire duration of the hold-off period, only the state at the expiry of the hold-off timer is relevant. Further, the SF/SD condition that triggers the hold-off timer does not need to be of the same one as the one at the expiry of the hold-off period.



SD Signal Degrade
SF Signal Fail

NOTE – The use of SF/SD clearing events as triggers for the start of the hold-off timer is not mandatory, but is recommended in order to prevent unnecessary protection switches that can otherwise occur under certain circumstances.

Figure 36/G.808.1 – Hold-off timer operation

15 Wait-to-restore timer

In revertive mode of operation, to prevent frequent operation of the protection switch due to an intermittent defect (e.g., BER fluctuating around the SD threshold), a failed working transport entity must become fault-free (e.g., BER less than a restoration threshold). After the failed working transport entity meets this criterion, a fixed period of time shall elapse before a normal traffic signal uses it again. This period, called wait-to-restore (WTR) period, is of the order of 5-12 minutes and should be capable of being set. A SF or SD condition will override the WTR.

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

16 Automatic Protection Switching (APS) signal

An APS signal is used to synchronize the actions at the A and Z ends of the protected domain. Communicated are:

– Request/state type;

– Requested signal;

– Bridged signal;
– Protection configuration.

The request/state type information identifies the highest priority fault condition, external command or protection process state.

The requested and bridged signal information when transported in an n-bit field identify:

0 null signal;

1.. $2^n - 2$ normal traffic signal 1 to $2^n - 2$;

$2^n - 1$ extra traffic signal.

The protection configuration information identifies:

– use of an APS channel;
– protection architecture (1+1, 1:n);
– switching type (uni-, bidirectional);
– operation type (non-revertive, revertive).

The APS signal is transported via the APS channel. In principle, it is possible to allocate an APS channel on every transport entity. Allocation of this channel on a working transport entity, however, would not provide sufficient survivability; i.e., when the working transport entity would fail, communication between the two endpoints will fail as well, and protection is not possible. Therefore the APS channel is allocated to one or more protection transport entities.

17 Non-preemptible Unprotected Traffic (NUT)

Non-preemptible unprotected traffic is one of three traffic classes in (1:1) and $(1:1)^n$ protection schemes, the others being protected traffic and extra traffic (3.18.3). NUT has no protection associated with it, but cannot be dropped from the network to allow protection of other traffic.

Extra traffic or protection channel access allows the use of the protection entities for additional traffic during normal operation in (1:1) or $(1:1)^n$ architectures. When a protection switch occurs, this traffic is dropped. Extra traffic provides a cheaper service than either protected traffic or non-preemptible unprotected traffic. It is unrelated to the protected traffic, coming from a different customer and may be used, for example, to provide additional capacity in response to a major event.

18 Extra traffic (protection) transport entity overhead/OAM

For the case of $(1:1)^n$ SNC/S protection with extra traffic, the extra traffic (protection) transport entity does not require the addition of a sublayer trail termination. The extra traffic (protection) transport entity has a dedicated tributary slot within the aggregate signal, separate from the tributary slots of the protection transport entities used to carry a normal traffic signal.

The status of the extra traffic (protection) transport entity does not impact the protection switching operation and, as such, it is not required to monitor this transport entity.

19 External commands

The autonomous behaviour of the protection switch process on the fault conditions of its transport entities can be modified by means of external (switch) commands. That is, an external (switch) command issues an appropriate external request on to the protection process.

NOTE – Only one external (switch) command can be issued per protection group. External commands which are pre-empted or denied by other higher priority conditions, states or requests, are discarded.

External commands are defined to allow the following types of actions (refer to section 3.3.8 above, for exact definitions of the external commands):

1) Configuration modifications and maintenance to be performed on the protection group or its transport entities:
   - **Lockout of protection** temporarily disables access to the protection transport entity for all signals;
   - **Forced Switch for signal #i** temporarily forces signal #i to be routed over the protection transport entity;
   - **Manual Switch for signal #i** temporarily routes signal #i over the protection transport entity, unless a fault condition (SF, SD) requires another signal to be routed over this transport entity.
2) Lockout signals from the protection process:
   - **Lockout of signal #i** temporarily disables access to the protection transport entity for the specific signal;
   - **Clear Lockout of signal #i**.
3) Freeze the protection process:
   - **Freeze** temporarily 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 and fault condition changes and received APS messages are ignored.
   - **Clear Freeze**: When the freeze command is cleared, the state of the protection group is recomputed based on the fault conditions and received APS message.
4) Testing the protection process and APS channel between the two endpoints:
   - **Exercise** emulates a switch request without performing the actual switch action, unless the protection transport entity is being used.
5) Clearing previous external (switch) command:
   - **Clear** clears all switch commands.

20 Protection switching process states

The following protection switching process states exist:

Do Not Revert normal traffic signal #i (DNR #i) – In non-revertive operation, this is used to maintain a normal traffic signal to be selected from the protection transport entity.

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.

Wait-to-Restore normal traffic signal #i (WtR) – 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 state will be changed to NR. This is used to prevent frequent operation of the selector in the case of intermittent failures.

21 Priority

Fault conditions, external commands and protection states are defined to have a relative priority with respect to each other. Priority is applied to these conditions/command/states locally at each endpoint and between the two endpoints.

Refer to the specific protection switching Recommendations for these priorities.

22 SF and SD trigger conditions

An SF condition is either a TSF or a SSF, which depends on the protection type.

Figure 37 illustrate the defect combination rules. SSF is given by adaptation function specific defects and AI_TSF. TSF is given by any defect of the layer network trail and CI_SSF.

An SF trigger condition is either directly detected by the trail termination function of the protected layer network, or it is passed through one or more layers according to the combination rules of specific defects, CI_SSF and AI_TSF.

TSD is the only SD trigger condition. It is issued on the detection of dDEG. TSD is always local to a trail termination function, i.e., it does not pass layer boundaries.

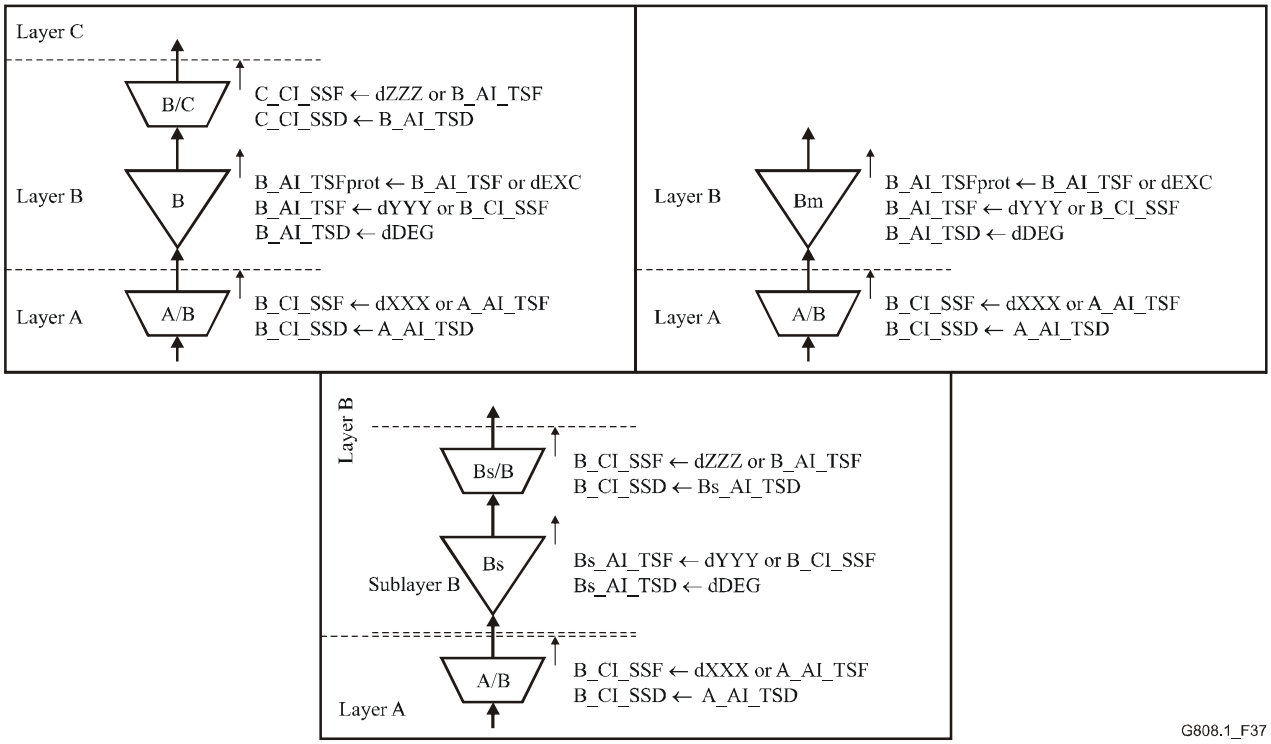


Figure 37/G.808.1 – Combination rules of defects

22.1 Overview of SF conditions

Table 2 presents an overview of defects that contribute to SF conditions in several transmission technologies. Refer to equipment Recommendations (e.g., ITU-T Recs G.783, G.798, I.732) for specific SF specifications.

Table 2/G.808.1 – Overview of defects contributing to SF condition

	ATM	OTN	SDH
Continuity defects	LOC	LOS, LOS-P, LCK, LTC	LOS, LTC
Connectivity defects	None	TIM, OCI	TIM, UNEQ
Adaptation defects	LCD	MSIM, LOM, PLM, LOFLOM	LOF, LOM, LOP, PLM
Upstream server layer defects (Note 1)	AIS	FDI, FDI-P	AIS
Excessive errored Trail			EXC (Note 2)
Virtual concatenation defects (Note 3)		LOM, LOA	LOM, LOA
NOTE 1 – Any detected defect causes the generation of an AIS/FDI client layer signal that is transported downstream. Depending on the specific layer, AIS/FDI may be detected at an adaptation or a trail termination sink function. NOTE 2 – EXC does not contribute to TSF and, therefore, it is only a local trigger condition for the protected layer network (via TSFprot) and not for any client layer. NOTE 3 – The virtual concatenation defects are applicable for LCAS only.			

22.2 Overview of SD conditions

Table 3 presents an overview of defects that contribute to SD conditions in several transmission technologies. Refer to equipment Recommendations (e.g., ITU-T Recs G.783, G.798) for specific SD specifications.

Table 3/G.808.1 – Overview of defects contributing to SD condition

	ATM	OTN	SDH
Digital degradations	None	DEG	DEG
Optical degradations	Not applicable	ffs (Note)	None
NOTE – Thresholds for optical degradations are ffs. Whether defects of the OTM overhead signal (OOS) contribute to the SD or not is ffs, since the OOS is not yet specified.			

23 Working and protection allocation

1+1 linear protection switching can be used as a protection application on a physical ring. As the ring is often part of a larger network, and only a portion of the trail traverses the ring, this application is normally used for subnetwork connection transport entities.

Bidirectional traffic can be engineered in two ways:

- The working transport entities for both directions may follow **different** physical paths, and the whole ring may be used. This is called Unidirectional Path Switch Ring (UPSR) and is shown in Figure 38. It is defined in SONET. In general, it can be used for SNC/I, SNC/N architectures. It should not be used for SNC/S architectures and trail protection architectures.

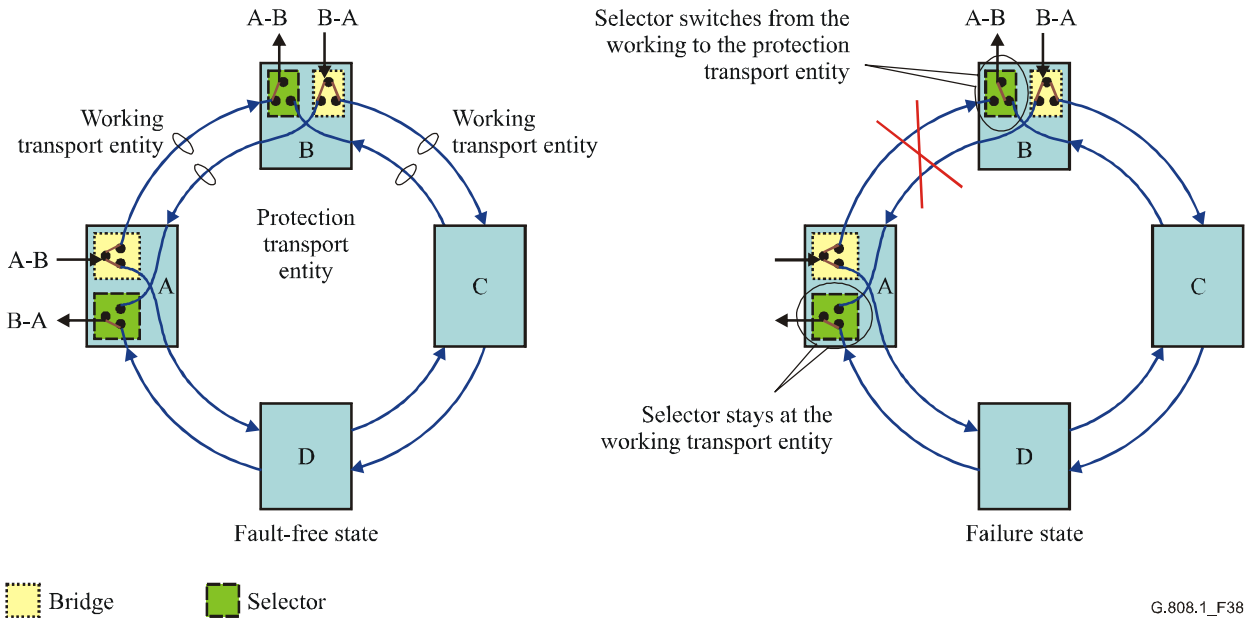


Figure 38/G.808.1 – Unidirectional Path Switch Ring (UPSR)

- The working transport entities for both directions follow the **same** physical path, normally the shortest. The protection transport entities will use the other portion of the ring. This is shown in Figure 39 and is called SubNetwork Connection Protection (SNCP). In a fault-free situation, this application minimizes the transfer delay and is the same for both directions. It is defined in SDH, OTN and ATM, and can be used in all protection architectures. Unidirectional Path Switched Rings may be operated in this way as well.

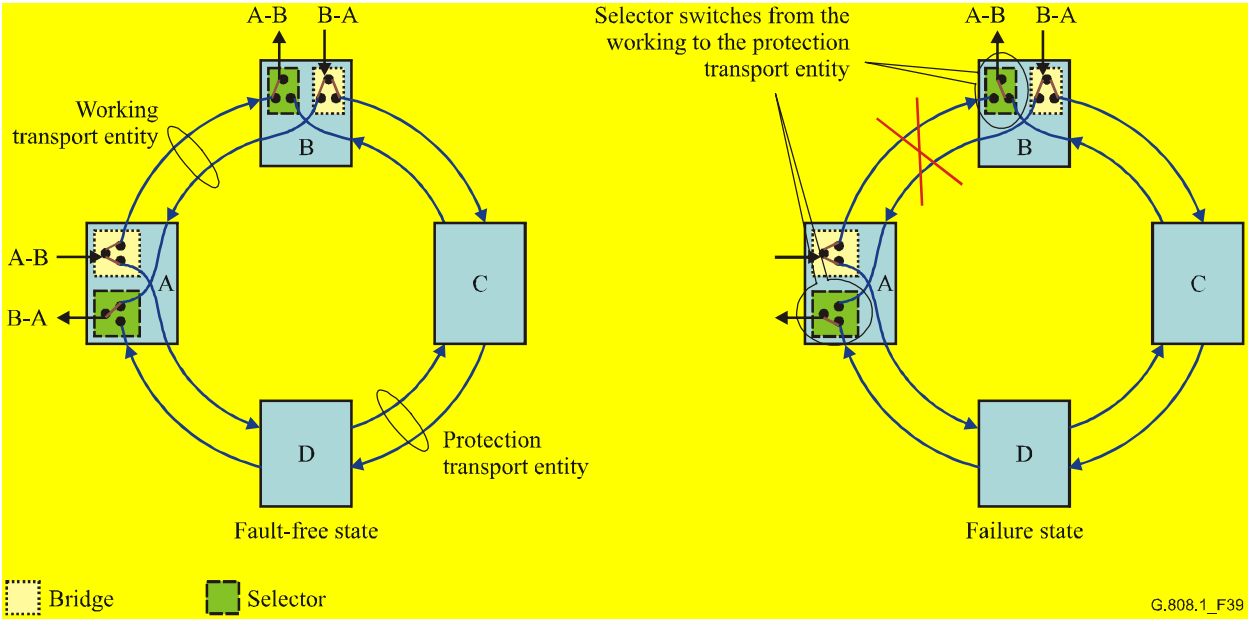


Figure 39/G.808.1 – SubNetwork Connection Protection (SNCP) ring

24 APS protocol

Generic definitions of APS protocol types are covered in 3.3.2. This clause addresses behavioural characteristics of the protocols and their applicability to the different protection architectures defined by this Recommendation. Exact details of the protocol coding schemes, and the

identification of the overhead channels used for protocol transport, are defined by technology-specific protection switching Recommendations (e.g., ITU-T Recs G.841, G.873.1 and I.630).

3-phase

– for all architecture types;

– prevents a misconnection to occur under all circumstances;

– operates a selector or bridge only after confirmation of priority.

2-phase

– for 1+1 and $(1:1)^n$ architectures;

– shorter protection switch time.

1-phase

– for $(1:1)^n$ architecture;

– shortest protection switch time;

– operates bridge/selector before priority is confirmed;

– more complex protocol.

24.1 1-phase

A means to align the two ends of the protected domain via the exchange of a single message (Z → A).

Applicable for $(1:1)^n$ and 1+1 architectures.

The bridge/selector at Z are operated before it is known if Z's condition has priority over the condition at A.

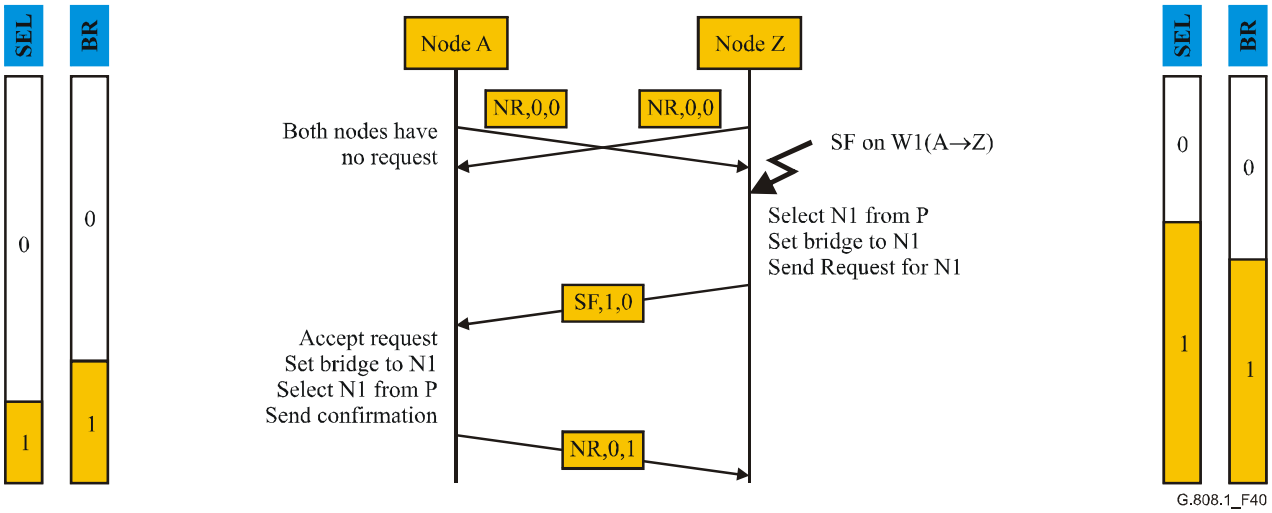


Figure 40/G.808.1 – 1-phase protocol example

24.2 2-phase

A means to align the two ends of the protected domain via the exchange of two messages (Z → A, A → Z).

Applicable for 1+1 architectures with its permanent bridges.

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 selector. On receipt of confirmation, Z operates its selector.

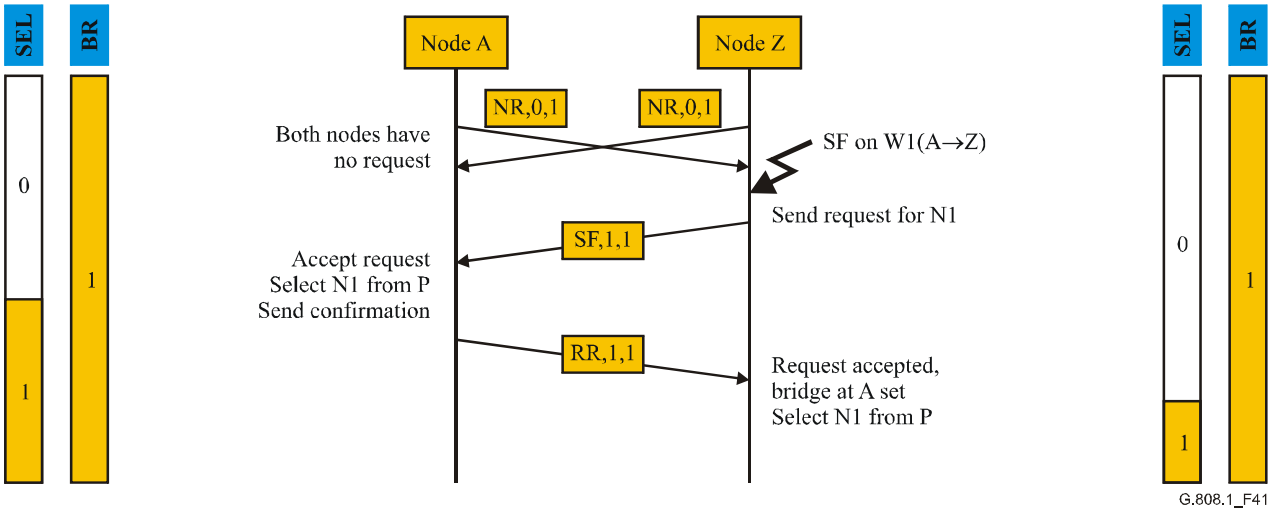


Figure 41/G.808.1 – 2-phase protocol example

24.3 3-phase

A means to align the two ends of the protected domain via the exchange of three messages (Z → A, A → Z, Z → A).

Applicable for 1:n and m:n architectures and for 1+1 architectures with its permanent bridges.

For case of 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.

In the case of 1+1 architecture with its permanent bridges, selectors are operated only as described for case 1:n.

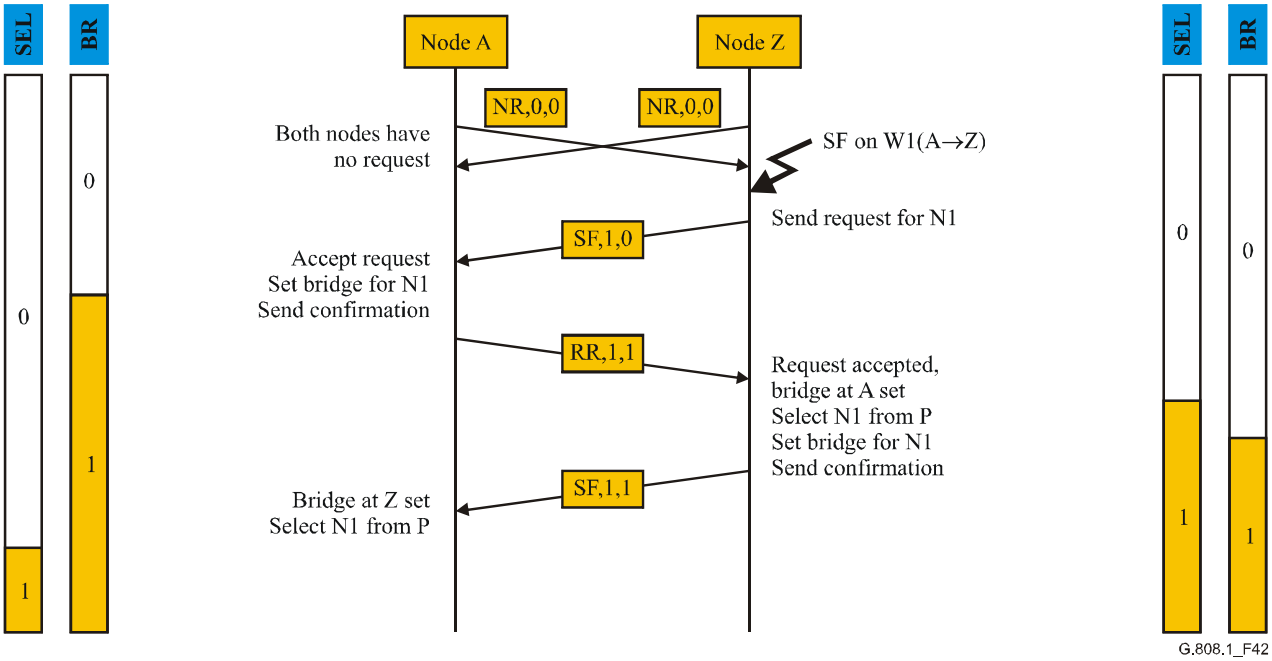


Figure 42/G.808.1 – 3-phase protocol example

Appendix I

Implementation of hold-off timer

An implementation of a hold-off timer may use a counter, which is decremented every X milliseconds. This quantization introduces an accuracy limitation in realizing the hold-off time. Figure I.1 presents two examples: decrement actions every 10 ms [25 ms]. For a hold-off time of 100 ms, the hold-off counter can be loaded with a value of 10 [4] at the moment of SF/SD occurrence, decrement at the end of every 10 ms [25 ms] decrement period, and expiring when reaching value 0. The hold-off time realized in this implementation is 95 ± 5 ms [82.5 ± 12.5 ms].

NOTE – For the case of a decrement period of 100 ms, the 100 ms hold-off time is actually 50 ± 50 ms; i.e., between 0 and 100 ms.

Instead of loading with a value of 10 [4], the counter can be loaded with 11 [5] realizing hold-off times of 105 ± 5 ms [112.5 ± 12.5 ms].

The accuracy of this type of hold-off timer is 0.5 times the decrement period.

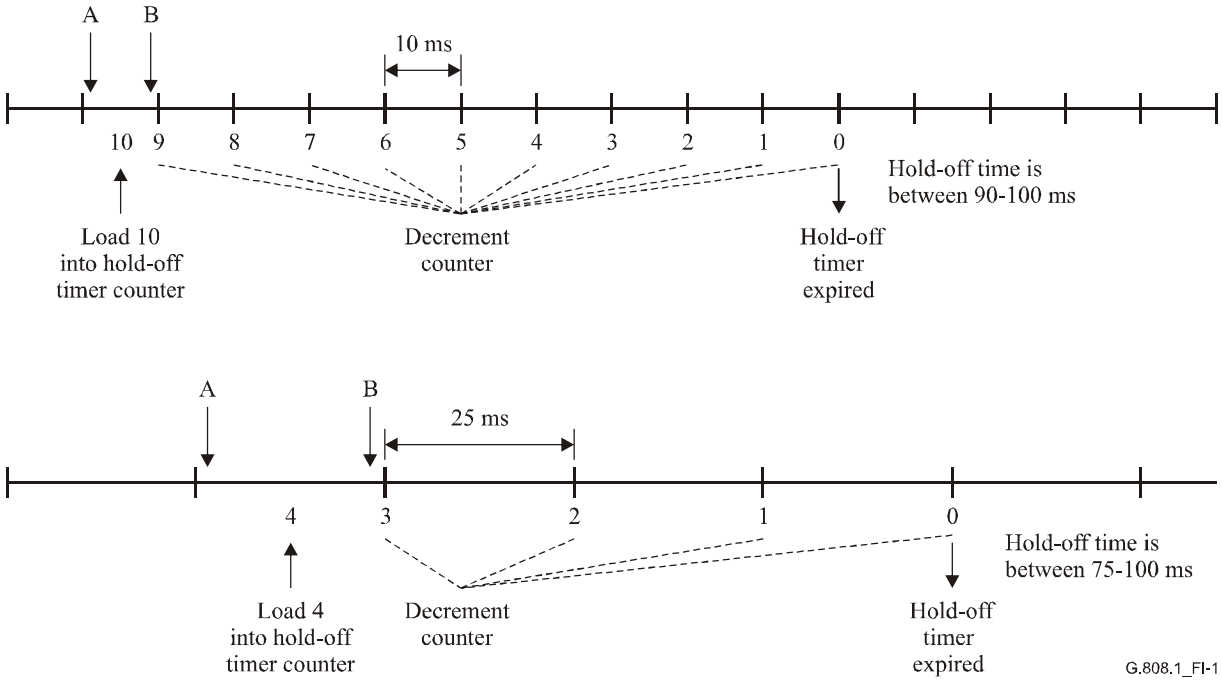


Figure I.1/G.808.1 – Hold-off timer accuracy

With a 10 ms decrement period, the effect of transfer delay differences between working and protection transport entities in 1+1 SNC/I and SNC/N protection can be compensated when a hold-off time of "0" is selected. When the hold-off timer is actually used (instead of disabled), and the counter is loaded with a value of "2", differential delays of 10 ms can be compensated. Refer to ITU-T Rec. G.873.1.

Appendix II

Automatic conditions (SF, SD) in group SNC protection

In 1+1 SNC/N [and SNC/I] protection, SF and SD conditions for the group are the SFG and SDG SF and SD conditions that are the inputs for the SNC protection process. The logic that computes the SFG and SDG conditions operates as follows:

- Working SFG = (W-SF1 and not P-SF1) or (W-SF2 and not P-SF2) or ....
- Protection SFG = (P-SF1 and not W-SF1) or (P-SF2 and nor W-SF2) or ....
- Working SDG = (W-SD1 and not P-SD1) or (W-SD2 and not P-SD2) or ....
- Protection SDG = (P-SD1 and not W-SD1) or (P-SD2 and nor W-SD2) or ....

This definition of SFG and SDG allows differentiating between a fault occurring "in front of" or "within" the protected domain. A fault in front of the protected domain in a single signal will neither activate W-SFG [SDG] nor P-SFG [SDG], while in both the W-bundle and the P-bundle SF-i will be activated; the terms "(W-SF-i and not P-SF-i)" and "(P-SF-i and not W-SF-i)" will, however, be "false".

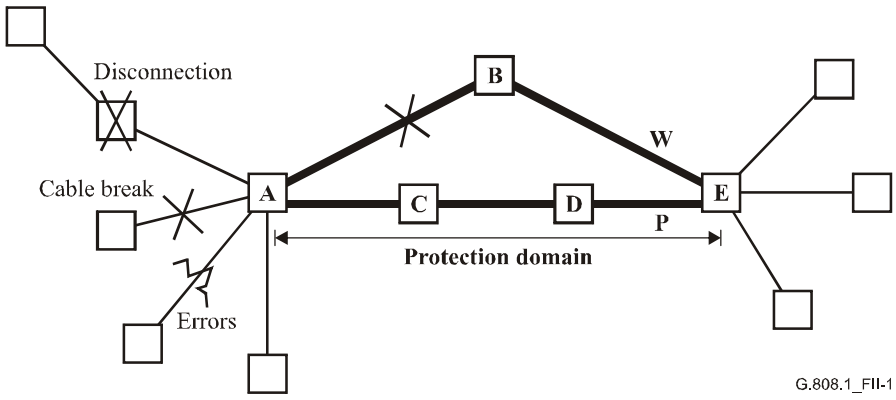


Figure II.1/G.808.1 – Example of fault within the protected domain

A fault between Network Elements (NE) A and B (Figure II.1) will cause W-SFG [or W-SDG] to be activated. If it is a server signal fault, all signals within the bundle will experience a SF condition. If it is a connectivity fault, a single signal may experience a SF condition. Both situations will cause W-SFG to be activated.

If, at the same time, e.g., a disconnection or cable break before NE A is present (impacting one of the signals in the group), W-SF-i and P-SF-i will be active. When the fault in the protection domain is a server fault, W-SFG will still be active, and P-SFG is inactive. In the other case (connectivity fault in the protection domain), the group will be switched if the failed signals in front of and within the protection domain are different.

NOTE – The special case where all signals have already failed before the protection domain, results in inactive W-SFG and P-SFG. But this special case does not corrupt the operation of the protection process; there is nothing left to protect.

The errors/faults within the protected domain that cause AIS and DEG defects will do this on all members of the group at the same moment (assuming it is required that all signals within the group *are transported in the same server signal)*. As such, the "ORing" of the individual SF and SD conditions can be used as a trigger.

With respect to a signal loss (e.g., loss of continuity, unequipped), or a connectivity (e.g., trace identifier mismatch) defect, this group behaviour might not be present. The signals are (in principle) individually cross-connected in each network element. As such, the ORing of the individual signals will initiate a protection switch for the group when only one (or a subset) of the signals has a signal loss defect condition. This is the *consequence of the complexity reduction*.

Appendix III

Implementation observations

In a technology, commonly available and in use today SDH or other technology (e.g., ATM, OTN) NEs consist of "port units" (PU) and "switch units". The switch units perform the cross-connection/switching, the port units perform all necessary SDH [PDH] overhead (and ATM OAM) processing.

For SDH VC-12 cross-connecting Network Elements (NE), a port unit will perform SOH, AU4 pointer, VC-4 POH and TU12 pointer processing (Figure III.1). The resulting SDH VC-12 signals are then handed off to the switch unit to be routed to their respective output port units.

It is possible to use the same port unit when the SDH VC-4 signal should not be terminated, but instead passed through as a VC-4 signal.

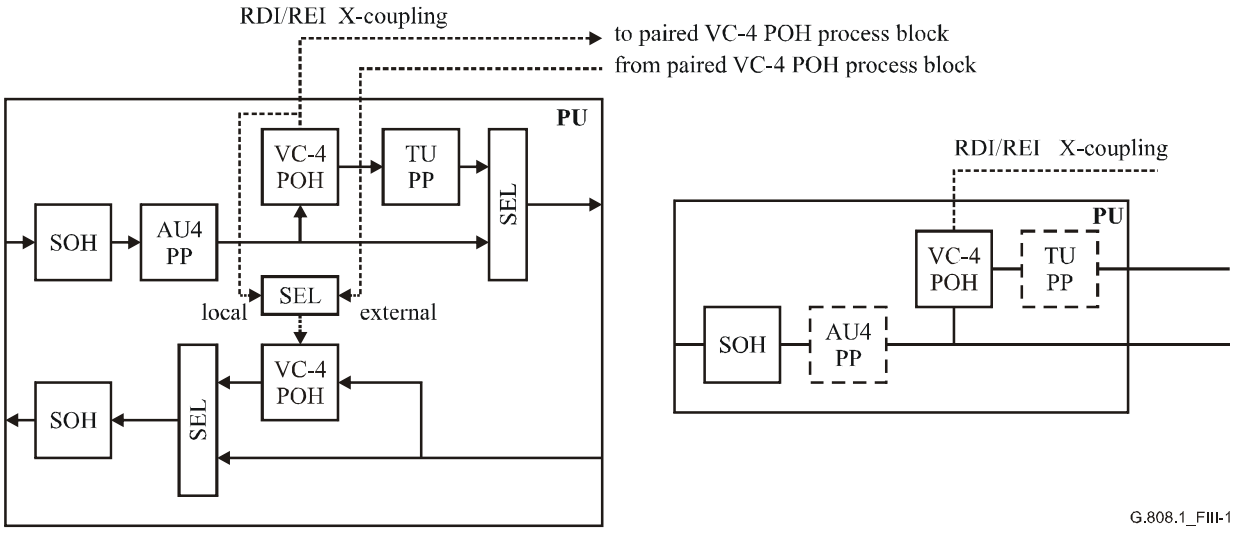


Figure III.1/G.808.1 – Port unit detailed view (left) and compressed view (right) (basic functionality only)

III.1 Analysis

Consider as an example the case of 1+1 MS protection (Figure III.2); two port units are used for this purpose, both with hardware performing SOH, AU PP, VC-4 POH and TU PP processing, while a protection switch is implemented at the switch unit by switching the total group of LOVC signals.

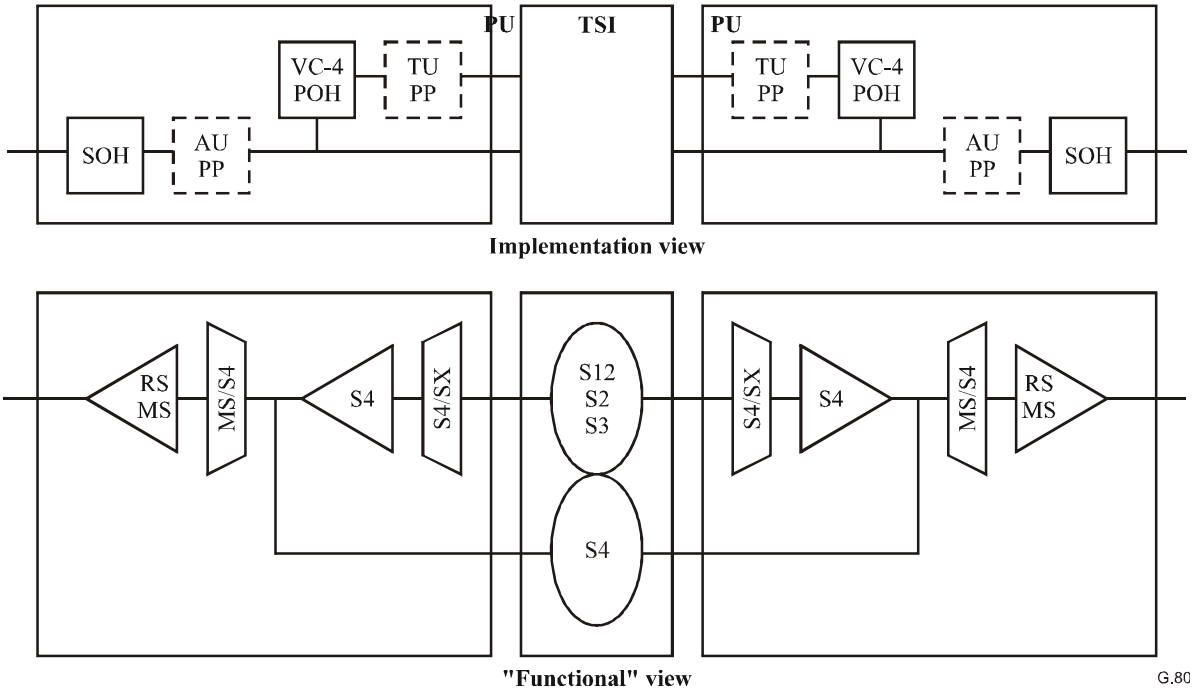
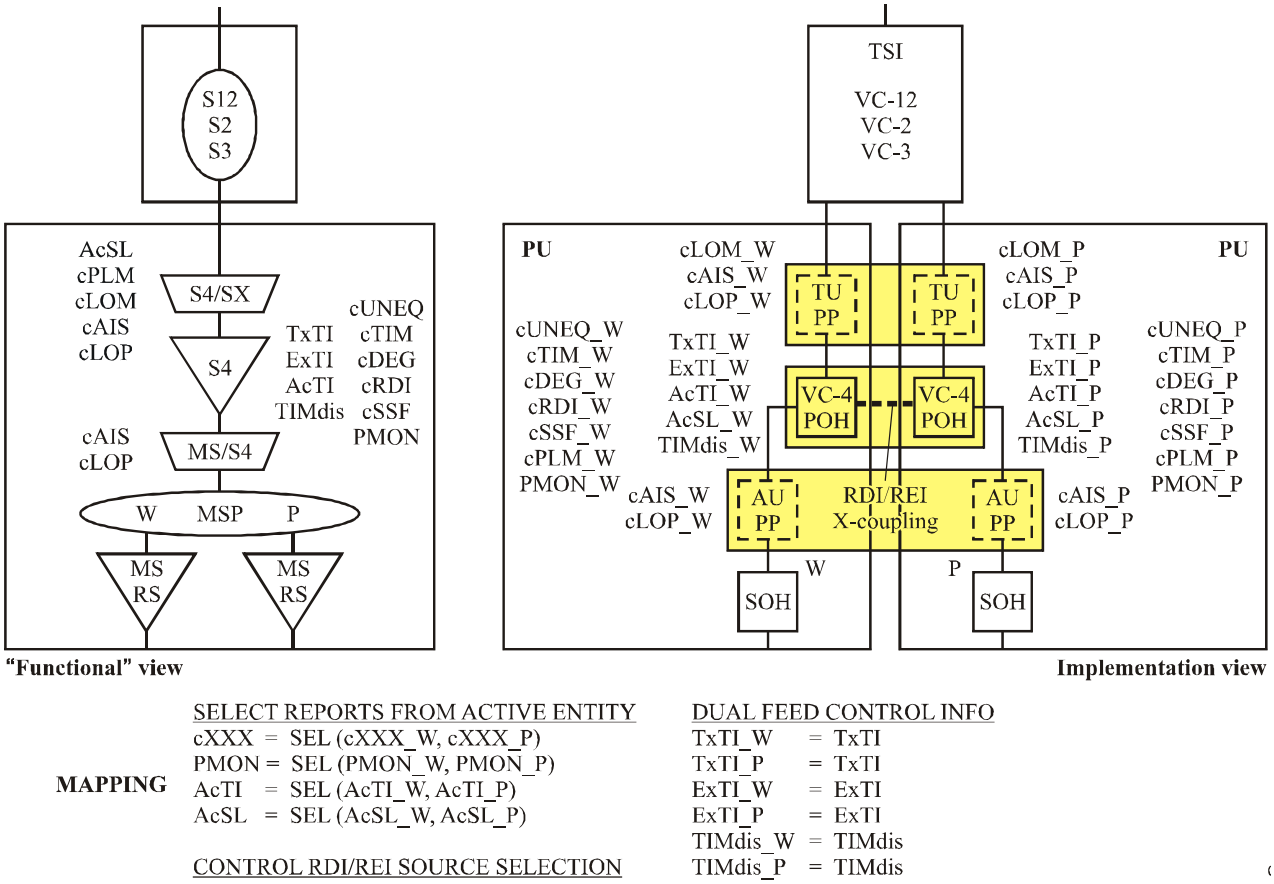


Figure III.2/G.808.1 – Mapping of implementation into functional view: Basic operation

According to the functional model, too much functionality is present (Figure III.3); i.e., SOH processing is expected to be present twice, while AU PP, VC-4 POH and TU PP processing should be present only once.



MAPPING

SELECT REPORTS FROM ACTIVE ENTITY
cXXX = SEL (cXXX_W, cXXX_P)
PMON = SEL (PMON_W, PMON_P)
AcTI = SEL (AcTI_W, AcTI_P)
AcSL = SEL (AcSL_W, AcSL_P)

CONTROL RDI/REI SOURCE SELECTION

DUAL FEED CONTROL INFO
TxTI_W = TxTI
TxTI_P = TxTI
ExTI_W = ExTI
ExTI_P = ExTI
TIMdis_W = TIMdis
TIMdis_P = TIMdis

Figure III.3/G.808.1 – Mapping of implementation into functional view: MS protection

With the software an NE can present the expected functionality; it hides the standby AU PP, VC-4 POH and TU PP processes for the manager.

For the transmission interfaces, a masking is also required; the two STM-N interfaces are expected to output the same AU4(s), the same VC-4(s), and the same TU(s).

The most straightforward implementation will output "different" AU(s) and TU(s). The difference is the actual pointer value; these do not have to be the same in the working and protection STM-N signals.

The fact that the AU/TU pointer values might be different does not have any impact on network operation. That is, this "non-compliance" in the strict sense is without consequences: i.e., no compensation is required for this.

Such is not the case, however, for the VC-4 POH processing. Here it is necessary to make sure that the RDI and REI signals that are output via both STM-N interfaces are identical. That is, the VC-4 POH monitor process at the active STM-N port unit must forward its RI_RDI/RI_REI signals to the VC-4 POH generation processes on both (working and protection) port units.

Similarly, this is required when VC-4 SNC protection is selected instead of MS protection (Figure III.4).

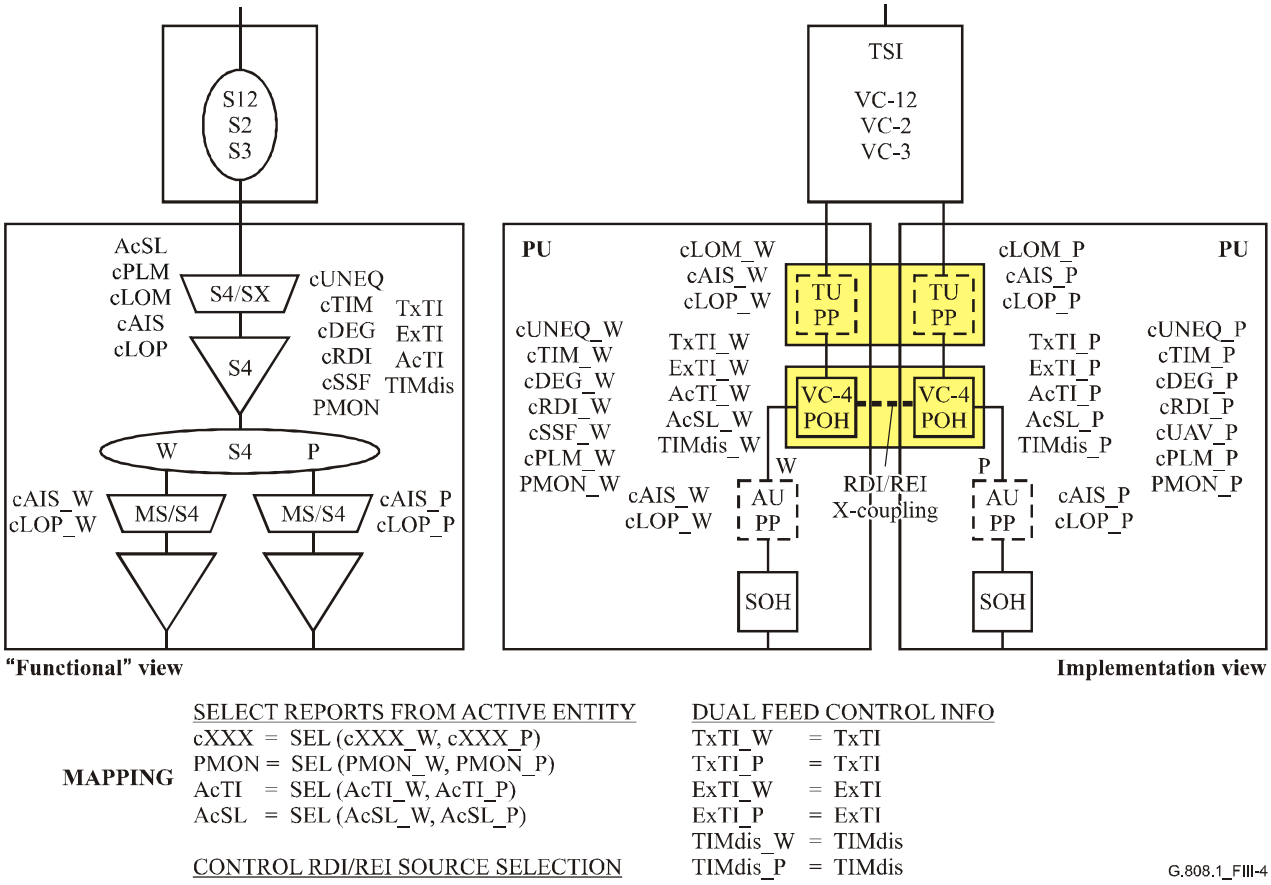


Figure III.4/G.808.1 – Mapping of implementation into functional view: VC-4 SNC/I protection

In the case where the RDI/REI X-coupling is not implemented, it will not be possible to add G.826 performance monitoring to networks in which the above protection implementations are operational. ITU-T Rec. G.826 requires bidirectional (services based) performance monitoring to be supported. This requires that the far-end information be used. This far-end information must represent the error/defects detected in the signal path that is actually transporting the client information.

Unidirectional switching causes each end of the protection span to independently select between working and protection trail/SNC. If, in the direction A → Z, the working VC-4 SNC is selected and, in the direction Z → A, the protection VC-4 SNC, the far-end information extracted at each end is inserted by the VC-4 POH generator on the standby port unit; i.e., the one that is not selected at this end. If it (now) uses its local RI_RDI/RI_REI signals (instead of its companion RI_RDI/RI_REI signals), the far-end would receive far-end information that is not related to the actually selected VC-4.

The bidirectional performance monitoring registers would (in this case) represent the wrong information; i.e., it cannot be used.

Of course, the same problem exists for the unidirectional (maintenance based) far-end registers.

For the case of a 64 kbit/s routing NE with STM-N interfaces, the same problem will be present at the VC-12 level.

NOTE – Figures III.3 and III.4 only represent the issue from the RDI/REI viewpoint. These figures do not show the tandem connection/segment termination or non-intrusive monitor functions that are required to control the protection switch.

Appendix IV

An example of $(1:1)^n$ protection

This appendix gives an example of $(1:1)^n$ protection switching (for n = 3) in an ATM network. In this case, there are three working entities which are diversely routed. They are protected by a single protection entity which, during normal operation, transports extra traffic. The protection entity must have sufficient bandwidth to transport the largest of the three normal traffic signals or the extra traffic signal. Each of the working entities is an ATM virtual path, whose size and Virtual Path Identifier (VPI) are shown in Figure IV.1.

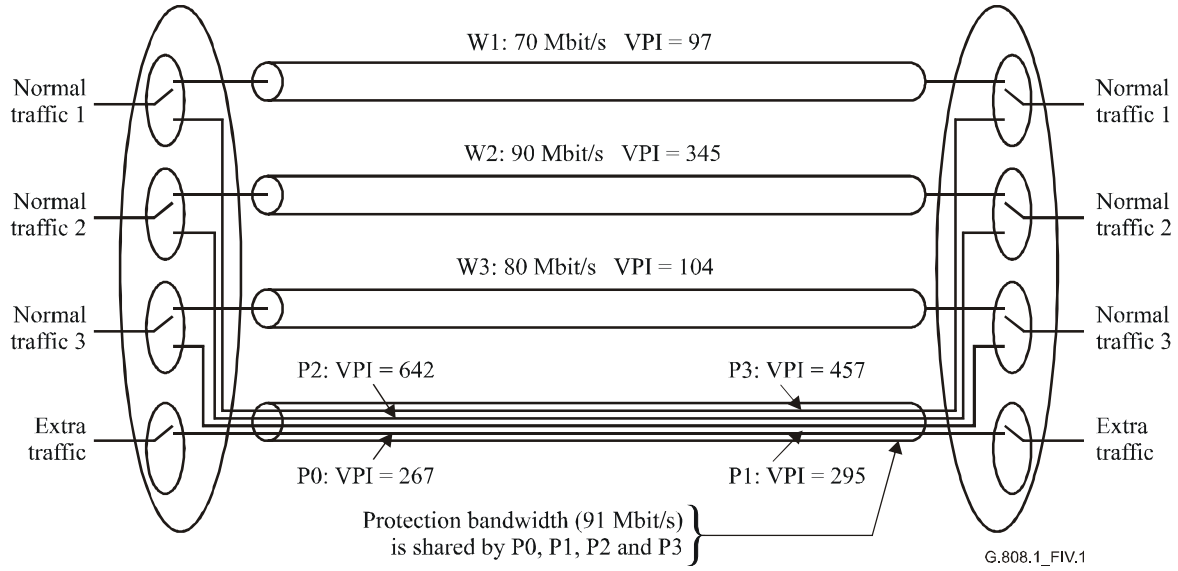


Figure IV.1/G.808.1 – An example of $(1:1)^n$ protection

In this example, 90 Mbit/s plus the OAM cells for P0 (includes VP-APS OAM), P1, P2 and P3 are required to provide protection switching. For unidirectional switching, a 1-phase protocol can be used because when a fault condition is detected: all that is needed is that a signal be sent from the Z end to the A end to initiate switching at the bridge. No misconnection can occur as the signal, which is on the protection entity, is uniquely identified by its VPI.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
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	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
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, 2004