International Telecommunication Union

ITU-T G.808.2

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(08/2019)

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

Digital networks – General aspects

Generic protection switching – Ring protection

Recommendation ITU-T G.808.2

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
General aspects	**G.800–G.809**
Design objectives for digital networks	G.810–G.819
Synchronization, quality and availability targets	G.820–G.829
Network capabilities and functions	G.830–G.839
SDH network characteristics	G.840–G.849
Management of transport network	G.850–G.859
SDH radio and satellite systems integration	G.860–G.869
Optical transport networks	G.870–G.879
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

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

Recommendation ITU-T G.808.2

Generic protection switching – Ring protection

Summary

Recommendation ITU-T G.808.2 defines the generic functional models, characteristics and processes associated with various ring protection schemes for connection oriented networks; e.g., optical transport networks (OTNs), synchronous digital hierarchy (SDH) networks, and multi-protocol label switching – transport profile (MPLS-TP) networks. It also defines the objectives and applications for these schemes. The protection scheme described in this Recommendation is shared ring protection (SRP).

Generic functional models, characteristics and processes for linear protection and interconnected subnetwork protection schemes are defined in other Recommendations.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.808.2	2013-11-22	15	11.1002/1000/7504
2.0	ITU-T G.808.2	2019-08-29	15	11.1002/1000/13998

Keywords

MPLS-TP, OTN, ring protection, SDH.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T G.808.2

Generic protection switching – Ring protection

1 Scope

This Recommendation describes the generic aspects of ring protection switching. It covers synchronous digital hierarchy (SDH), optical transport network (OTN), and multi-protocol label switching – transport profile (MPLS-TP) based protection schemes. Ethernet ring protection scheme is not covered in this version of the Recommendation.

Overviews of ring protection and dual node subnetwork (e.g., dual ring) interconnect 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 G.783] Recommendation ITU-T G.783 (2006), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*.

[ITU-T G.798] Recommendation ITU-T G.798 (2017), *Characteristics of optical transport network hierarchy equipment functional blocks*.

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

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

[ITU-T G.8121] Recommendation ITU-T G.8121/Y.1381 (2018), *Characteristics of MPLS-TP equipment functional blocks.*

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

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 long path [ITU-T G.841]

3.1.2 non-revertive (protection) operation [ITU-T G.808]

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

3.1.4 ring switching [ITU-T G.841]

3.1.5 short path [ITU-T G.841]

3.1.6 span switching [ITU-T G.841]

3.1.7 switching time [ITU-T G.808]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 extra traffic: This is the traffic that will be discarded as soon as protection of the normal traffic is required. It will have the lowest availability of the three types of traffic because every protection switch in the ring affects it.

3.2.2 non–pre-emptible unprotected traffic: This is the traffic that will not be affected by the protection switch. It will have availability between that of the normal traffic and the extra traffic as it will be affected only by a defect in a section it passes.

3.2.3 normal traffic: This is the traffic that will be protected and will have the highest availability.

3.2.4 ring map: This is a map (table) present in each node on a ring that contains information regarding the order in which the nodes appear on the ring including their node IDs.

NOTE – Also present in each node is a ring circuit map, containing the cross-connection (added, dropped, and passed-through client traffic) maps of all nodes in the ring with the squelch table per node as a subset.

3.2.5 span: A bidirectional adjacency between two nodes that participate in a shared ring protection (SRP) mechanism, in the layer in which the SRP mechanism operates.

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

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

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AIS	Alarm Indication Signal
APS	Automatic Protection Switching
BER	Bit Error Rate
DEG	Degraded
DLRing	Dedicated section Link Ring
ET	Extra Traffic (signal)
EXER-R	Exercise – Ring
EXER-S	Exercise – Span
FS-R	Forced Switch to protection – Ring
FS-S	Forced Switch to protection – Span
HO	Hold-Off
ID	Identifier
LOW-R	Lockout of Working channels – Ring switch
LOW-S	Lockout of Working channels – Span switch
LP-S	Lockout of Protection – Span
LSP	Label Switched Path

MPLS Multi-Protocol Label Switching

MPLS-TP MPLS – Transport Profile

MS-N Multiplex Section – N

MS-R Manual Switch to protection – Ring

MS-S Manual Switch to protection – Span

NR No Request

NUT Non-pre-emptible Unprotected Traffic (signal)

OTN Optical Transport Network

RR-R Reverse Request – Ring

RR-S Reverse Request – Span

SD Signal Degrade

SDH Synchronous Digital Hierarchy

SD-P Signal Degrade – Protection

SD-R Signal Degrade – Ring

SD-S Signal Degrade – Span

SF Signal Fail

SF-P Signal Fail – Protection

SF-R Signal Fail – Ring

SF-S Signal Fail – Span

SLRing Shared section Link Ring protection

SPRing Shared Protection Ring

SRP Shared Ring Protection

SSF Server Signal Fail

TSD Trail Signal Degrade

TSF Trail Signal Fail

TT Trail Termination

VC-n Virtual Container – n

WTR Wait-To-Restore

5 Conventions

None.

6 Individual and group protection concept

6.1 Individual protection

In individual protection, the protection mechanism relies on defects detected in the server layer that affect all individual protected entities in the physical section at the same time. In general, individual protection is used in synchronous digital hierarchy (SDH) and optical transport network (OTN) technologies in physical rings.

6.2 Group protection

In group protection, the protection mechanism relies on defects detected by one of the members of the group or by the whole group in a logical section.

7 Architecture and traffic types

In general, shared ring protection mechanisms operate on a ring of two or more nodes. In the case of MPLS-TP, the minimum number of nodes of a ring required for proper ring protection operation is three. Nodes on a ring are adjacent to each other in the layer network in which the shared ring protection mechanism operates, with bidirectional spans between each pair of nodes. The layer network in which a shared ring protection mechanism operates is connection-oriented; it may be circuit switched or packet switched.

Each bidirectional span on the ring provides, in each direction, a working transport entity, a protection transport entity and, optionally, an entity to transport non-pre-emptible unprotected traffic (NUT), as shown in Figure 7-1.

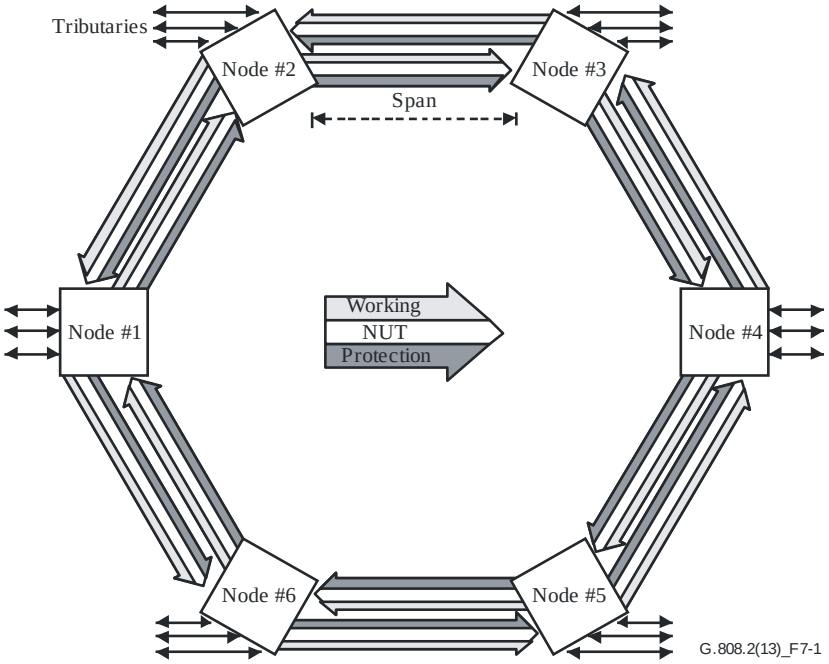

Figure 7-1 – Ring topology

7.1 Protection classes

7.1.1 Shared section link ring protection (SLRing)

Shared section link ring protection requires only two links for each span of the ring and forms two rings. Each link in the ring carries both working transport entities and protection transport entities. On each ring, up to half the entities are defined as working transport entities and up to half are defined as protection transport entities, that is to say working transport entities go around the ring clockwise and anti-clockwise, same for protection transport entities. The normal traffic carried on working transport entities is protected by the protection transport entities travelling in the other ring in the opposite direction (see Figure 7-2). This enables the bidirectional transport of normal traffic.

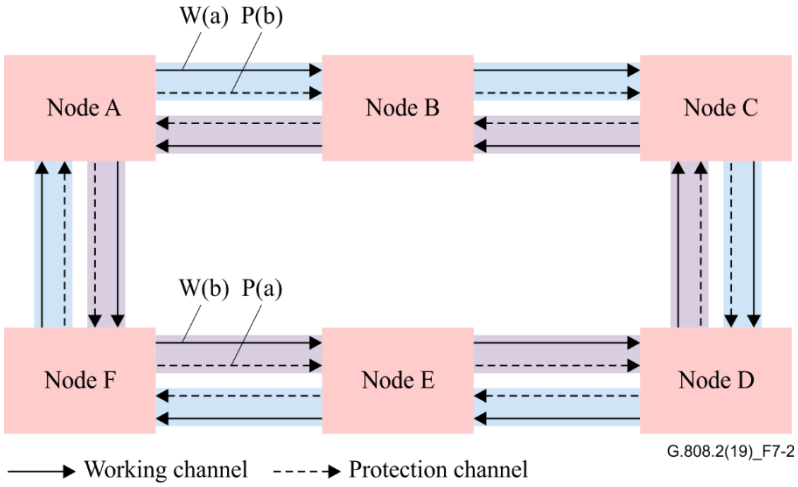

Figure 7-2 – Working transport entity and protection transport entity in shared section link ring protection

The normal traffic carried on working transport entity W(a) is protected by protection transport entity P(a), and the normal traffic carried on working transport entity W(b) is protected by protection transport entity P(b).

If a shared section link is carried directly over a fibre, the term 2-Fibre SPRing may be used instead of SLRing.

7.1.2 Dedicated section link ring protection (DLRing)

Dedicated section link ring protection requires four links for each span of the ring and forms four rings. Working and protection transport entities are carried over different rings: two rings transmitting in opposite directions carry the working transport entities; while two rings, also transmitting in opposite directions, carry the protection transport entities (see Figure 7-3).

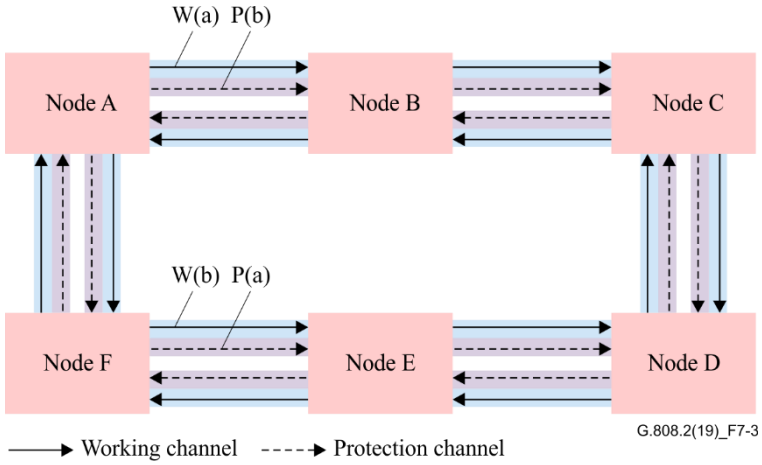

Figure 7-3 – Working transport entity and protection transport entity in dedicated section link ring protection

The normal traffic carried on working transport entity W(a) is protected either by protection transport entity P(b) in case of span-switch or by protection transport entity P(a) in case of ring-switch. Similarly, the normal traffic carried on working transport entity W(b) is protected either by protection transport entity P(a) in case of span-switch or by protection transport entity P(b) in case of ring-switch.

If a dedicated section link is carried directly over fibres the term 4-Fibre SPRing may be used instead of DLRing.

7.2 Traffic types

7.2.1 Normal (protected) traffic

Normal traffic uses resources within the working transport entity, and can be protected by resources within the protection transport entity during protection switching conditions. All shared protection rings support normal traffic.

In circuit switched networks, a shared ring protection mechanism is typically described as existing in a server layer network, while the actual protection switching is implemented as group protection in a client layer network. For example, SDH MS-SPRing is described as a sublayer of the MS layer, but the virtual container – n (VC-n) within the multiplex section – N (MS-N) are wrapped or steered as a result of failures.

In packet switched networks, a shared ring protection mechanism typically uses unique identifiers for each working or protection transport entity and for each egress node at which these transport entities terminate, allowing one or more logical rings to share the same server layer.

7.2.2 Non-pre-emptible unprotected traffic (NUT)

Non-pre-emptible unprotected traffic (NUT) has no protection associated with it, but cannot be dropped from the network to allow protection of other traffic signals. It may be present on the server layer supporting working transport entity and/or the server layer supporting the protection transport entity.

In a circuit switched network, NUT must be specifically identified within the protection mechanism. For example, SDH MS-SPRing is described as a sub-layer of the MS layer. The use of NUT means that some VC-n within the MS-N signal are not protected, which is only possible if the actual switching of traffic is occurring in the VC-n layer. In this case, if NUT is configured for a particular VC-n timeslot in the working transport entity, the corresponding VC-n in the protection transport entity is also designated for NUT (since it is not otherwise needed for protection).

In the case of a ring based on packet switching, the shared ring protection mechanism is not aware of the NUT because the working and protection transport entities use specific identifiers. For example, MPLS-TP uses tunnel labels to identify shared protection rings. NUT LSPs do not have the tunnel label, and would thus be excluded from the actions of the MPLS-TP shared ring protection scheme.

7.2.3 Extra traffic (ET)

Extra traffic (ET) allows the use of the protection transport entities for additional traffic signals during normal operation in ring architectures. When a protection switch occurs, this traffic can be dropped. Extra traffic provides a less reliable service than either protected traffic or non-pre-emptible unprotected traffic. It is unrelated to the normal traffic signal.

In circuit switched networks, extra traffic must be specifically identified as such, so that it can be pre-empted in the event of a failure that requires use of the resources in the protection transport entity to protect normal traffic.

In packet switched networks, the existence of a connection does not guarantee that traffic for that connection will be forwarded; forwarding decisions are taken on a per-packet basis based on priority of the traffic available to be switched. As such, extra traffic needs to be lower in priority than all normal traffic and NUT that is using the protection transport entity, but it does not have to be explicitly disconnected when a failure occurs on the working transport entity. Extra traffic will continue to be forwarded as bandwidth allows even when a failure has occurred in the working

transport entity. For example, MPLS-TP uses tunnel labels to identify shared protection rings. LSPs that are ET will not have the tunnel label, and will have lower priority than the tunnel or any NUT.

7.3 Architecture types

7.3.1 Wrapping protection

The normal traffic signal is wrapped from the working transport entity to the protection transport entity in the nodes adjacent to the failed section or node.

During a ring protection switch, normal traffic signal transmitted toward the failed section/node is switched (wrapped) at the node just before the failure to the protection transport entity in the opposite direction (away from the failure). This bridged traffic signal travels around the ring on the protection transport entities to the node just after the failure where the normal traffic signal from the protection transport entity is switched (wrapped) back onto the working transport entity. In the other direction, the normal traffic signal is bridged and switched in the same manner.

Figure 7-4 illustrates a ring protection switch in response to a section failure.

Since the protection transport entity of each section (except the failed section) is used for recovery, the protection capacity is effectively shared by all sections.

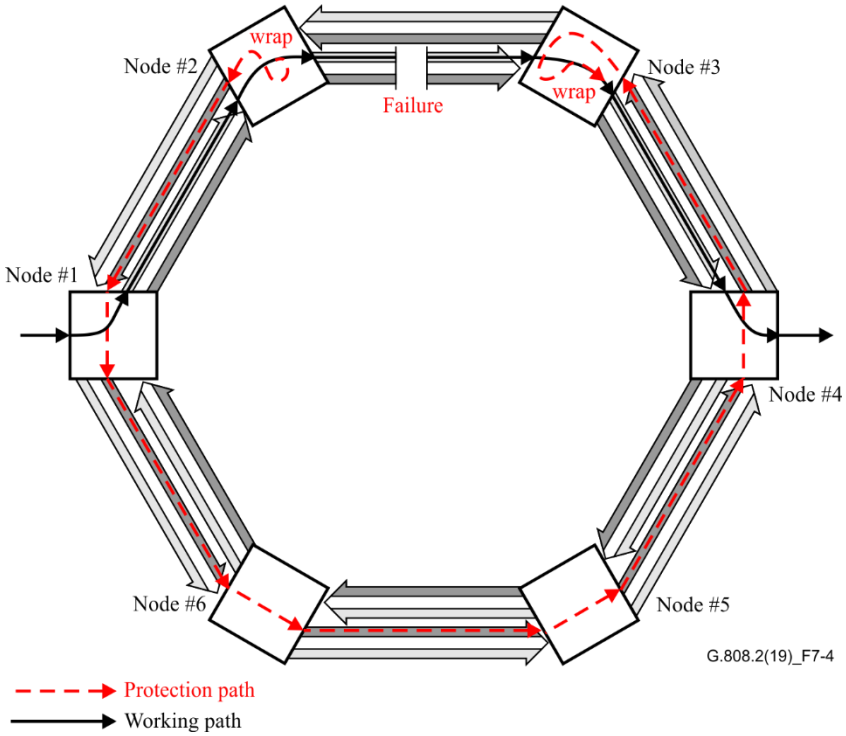

Figure 7-4 – Wrapping

7.3.2 Steering protection

The normal traffic signal is switched to the protection transport entity at its ingress and egress nodes.

During a ring protection switch, normal traffic signal transmitted toward the failed section/node is switched (steered) at the node where it enters the ring to the protection transport entity in the opposite direction (away from the failure). This bridged traffic signal travels around the ring on the protection transport entities to the node where the normal traffic signal exits the ring and where the normal traffic signal from the protection transport entity is switched (steered) back to the output. In the other direction, the normal traffic signal is bridged and switched in the same manner.

Figure 7-5 illustrates a ring protection switch in response to a section failure.

Since the protection transport entity of each section (except the failed section) is used for recovery, the protection capacity is effectively shared by all spans.

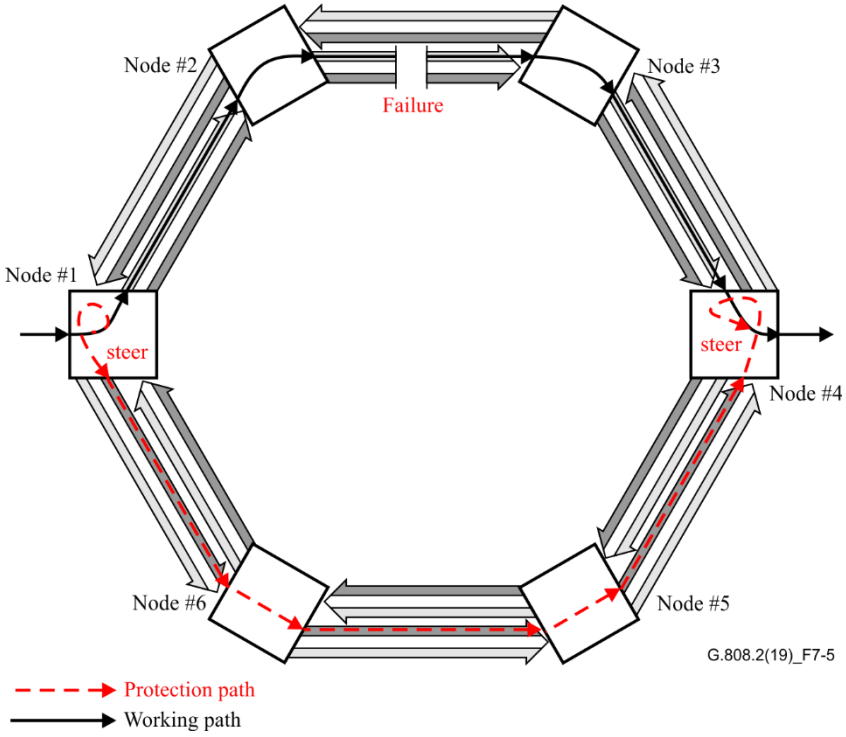

Figure 7-5 – Steering

7.3.3 Short wrapping protection

The normal traffic signal is wrapped from the working transport entity to the protection transport entity only at the upstream node of the failed section or node and exits the ring at the egress node.

During a ring protection switch, normal traffic signal transmitted toward the failed section/node is switched (wrapped) at the node just before the failure to the protection transport entity in the opposite direction (away from the failure). This bridged traffic signal travels around the ring on the protection transport entities to the node where the normal traffic signal from the protection transport entity is switched (steered) to the output. In the other direction, the normal traffic signal is bridged and switched in the same manner.

Figure 7-6 illustrates a ring protection switch in response to a section failure.

Short wrapping is an optimization to wrapping protection in terms of latency and bandwidth consumption during protection switching. However, the protected bidirectional normal traffics are not co-routed due to the discrepancy of the switching nodes used in each direction.

Since the protection transport entity of each section (except the failed section) is used for recovery, the protection capacity is effectively shared by all spans.

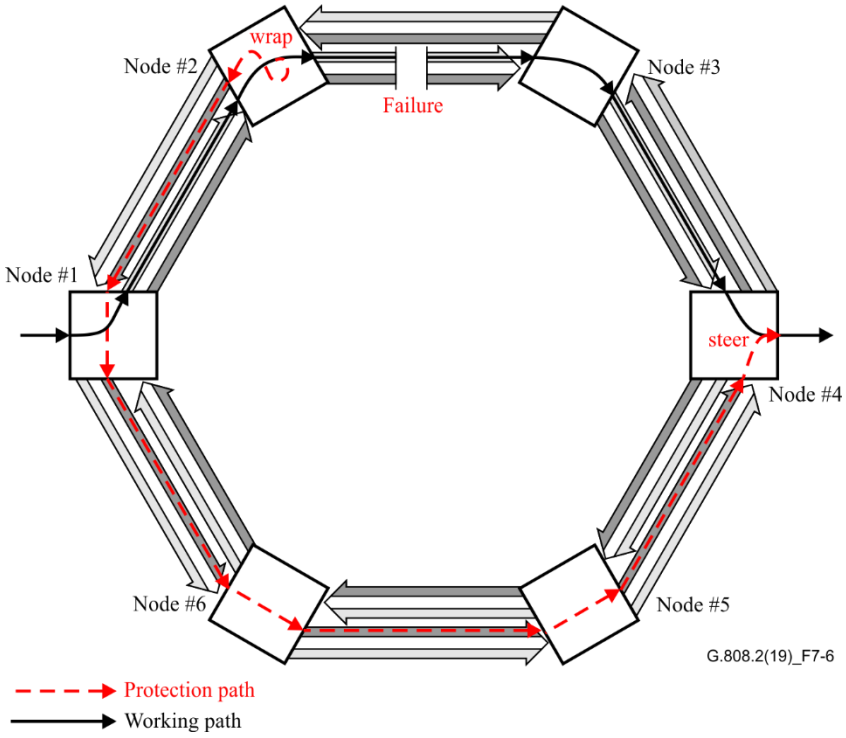

Figure 7-6 – Short wrapping

8 Switching types

- Shared ring protection switching is bidirectional.

9 Operation types

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

- In a revertive (protection) operation, the normal traffic signal always returns to (or remains on) the working transport entity if the switch requests are terminated, that is to say, when the working transport entity has recovered from the defect or the external request is cleared.
- In non-revertive (protection) operation, the normal traffic signal does not return to the working transport entity if the switch requests are terminated.

NOTE – Non-revertive switching is not recommended because the protection entities are shared.

10 Switching protocol and ring topology information

Shared ring protection requires that all nodes in the ring coordinate their actions of bridging and selecting. Therefore, ring nodes maintain a ring map that describes the topology of the ring and communicate with each other via a protocol carried over the automatic protection switching (APS) channel.

The ring map provides an ordered list of the node IDs of all the nodes in the ring, so every node is aware of how the nodes are connected in the ring. This information is used in conjunction with the APS protocol to make switching decisions. The ring map may be provisioned by management or exchanged among the nodes via other control protocols.

There are two basic requirements for a protection protocol:

1) The prevention of misconnections.
2) The minimization of the number of communication cycles among the ring nodes in order to minimize the protection switching time.

The details of the ring map and the APS protocol are technology-specific.

11 Functional models for ring protection

11.1 Functional models for SLRing

Figure 11-1 shows the bidirectional functional model of the connection function of the client layer that is protected by the shared section link ring protection in each node of a protected ring when no protection switch is activated.

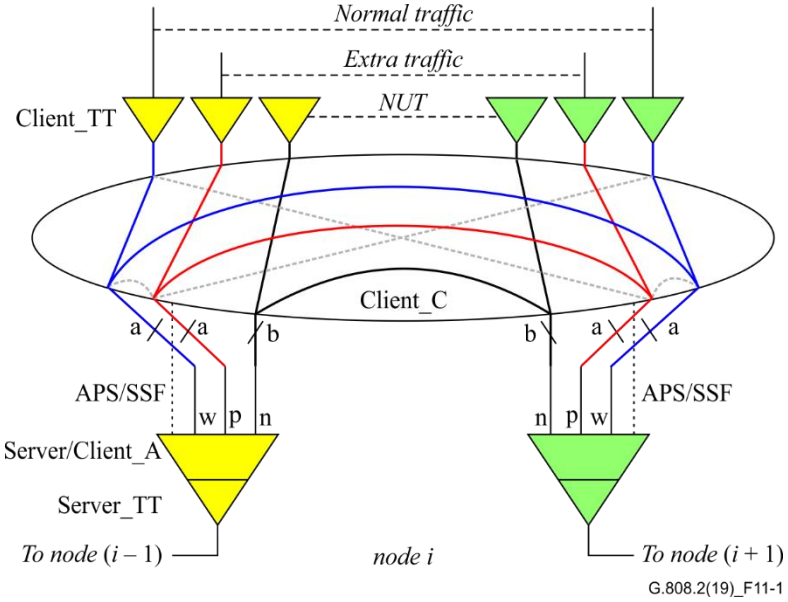

Figure 11-1 – Shared section link ring protection functional model

The following types of traffic will be transported over the section between adjacent nodes:

- normal traffic. It is transported in the working transport entity ('w' in Figure 11-1).
- extra traffic. It is transported in the protection transport entity ('p' in Figure 11-1).
- non–pre-emptible unprotected traffic (NUT). It is transported in the NUT transport entity ('n' in Figure 11-1).

The maximum payload capacity of the working transport entity is equal to the capacity of the protection transport entity, as indicated by 'a' in Figure 11-1. The payload capacity of the NUT transport entity is different from the working and protection transport entity as indicated by 'b' in Figure 11-1. The values 'a' and 'b' are provisioned to have the same value in all nodes of the ring. Note that the 'a' and 'b' entities will carry traffic originating locally or traffic passed through from node (i-1) to node (i+1) and vice versa.

In general, the following limits apply: $0 < a \leq N/2$, $0 \leq b < N$ and $(2a + b) \leq N$ where N is the total bandwidth capacity of the server section.

11.1.1 Functional models for wrapping protection on a SLRing

Figure 11-2 shows the functional model in a node adjacent to the failed section or node when wrapping protection is activated on a SLRing.

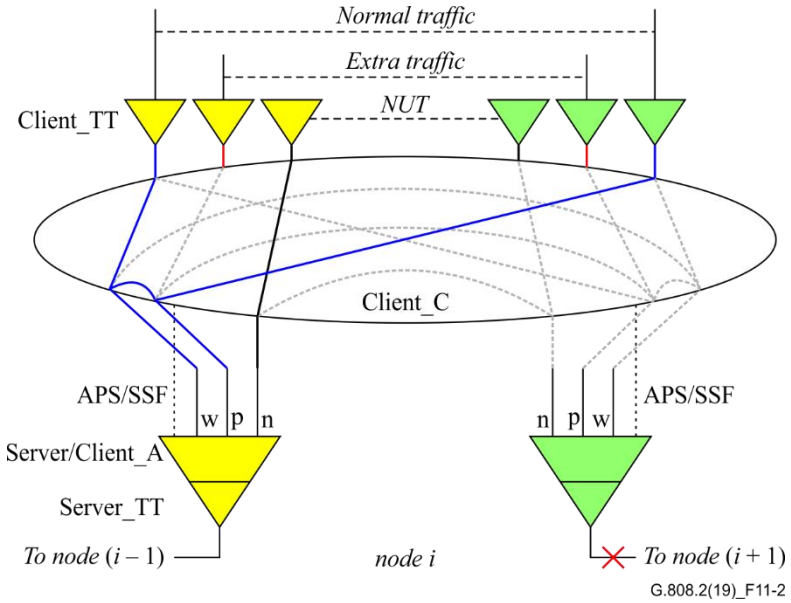

Figure 11-2 – Functional model of a node adjacent to a failure in wrapping protection on a SLRing

Figure 11-3 shows the functional model of an intermediate (non-adjacent) node when wrapping protection is activated on a SLRing.

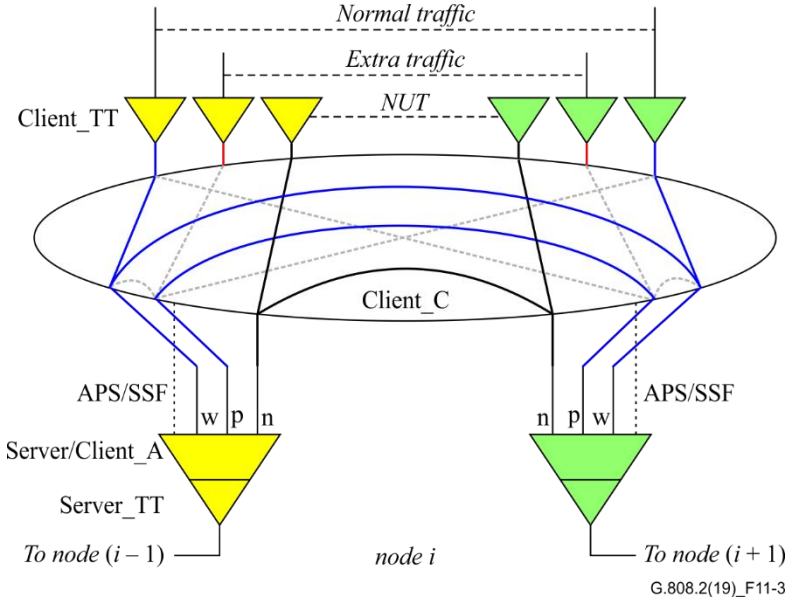

Figure 11-3 – Functional model of an intermediate node in wrapping protection on a SLRing

11.1.2 Functional models for steering protection on a SLRing

Figure 11-4 shows the functional model in a node adjacent to the failed section or node when steering protection is activated on a SLRing.

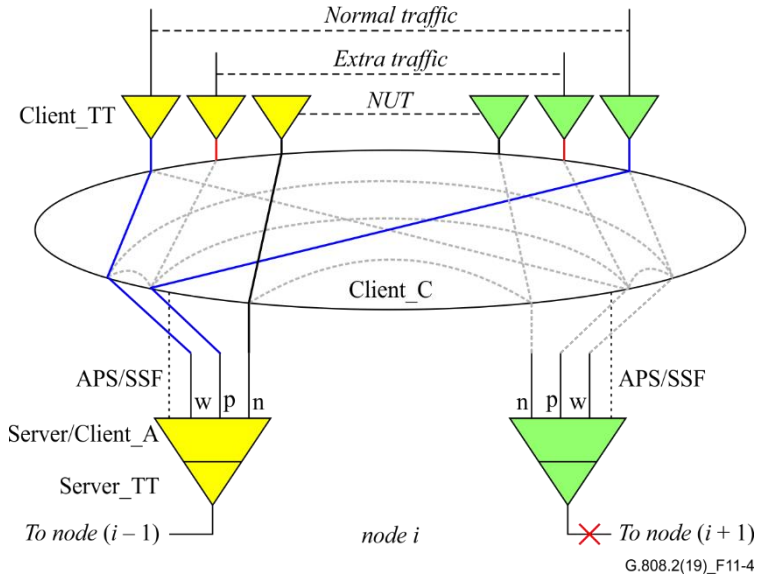

Figure 11-4 – Functional model of an ingress or egress node of normal traffic signal in steering protection on a SLRing

Figure 11-5 shows the functional model of an intermediate (non-adjacent) node when steering protection is activated on a SLRing. The normal traffic signal is switched to the protection transport entity if the normal traffic signal is affected by the failed section or node as indicated by blue dashed lines in Figure 11-5. Otherwise, the normal traffic signal keeps to be transported by the working transport entity as indicated by blue solid lines in Figure 11-5. The protection transport entity may be used for extra traffic if the protection transport entity is not occupied by the normal traffic signal even when the steering protection is activated as indicated by red dashed lines in Figure 11-5.

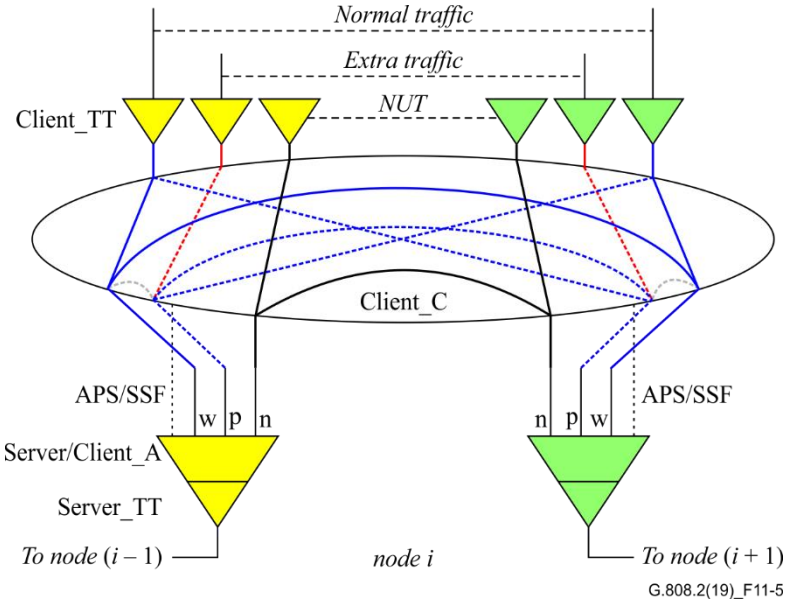

Figure 11-5 – Functional model of an intermediate node in steering protection on a SLRing

11.1.3 Functional models for short wrapping protection on a SLRing

Figure 11-6 shows the functional model in a node adjacent to the failed section or node when short wrapping protection is activated on a SLRing. The difference from the functional model of the

wrapping protection shown in Figure 11-2 is that wrapping is performed only in the direction from the working transport entity to the protection transport entity.

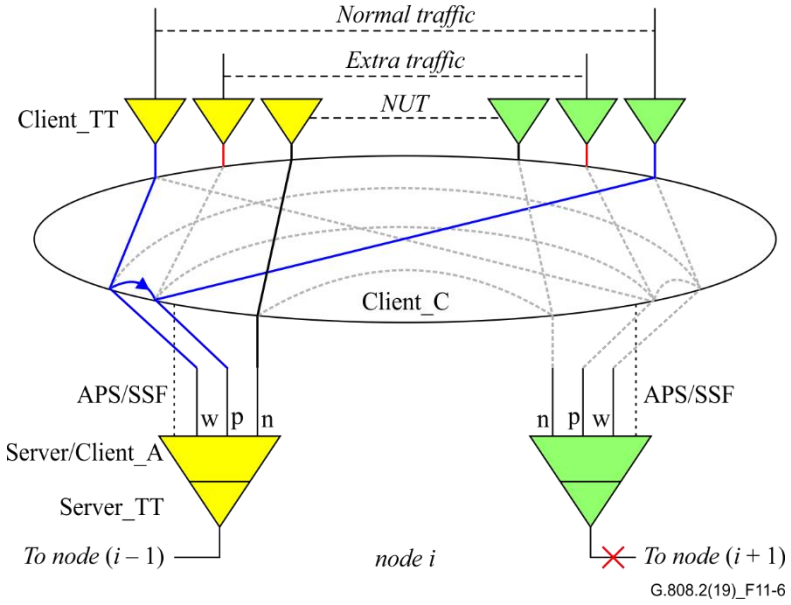

Figure 11-6 – Functional model of a node adjacent to a failure in short wrapping protection on a SLRing

Figure 11-7 shows the functional model of an intermediate (non-adjacent) node when short wrapping protection is activated on a SLRing. The normal traffic signal entering the ring is transmitted to the working transport entity, while the normal traffic signal to be exiting the ring is received from the protection transport entity.

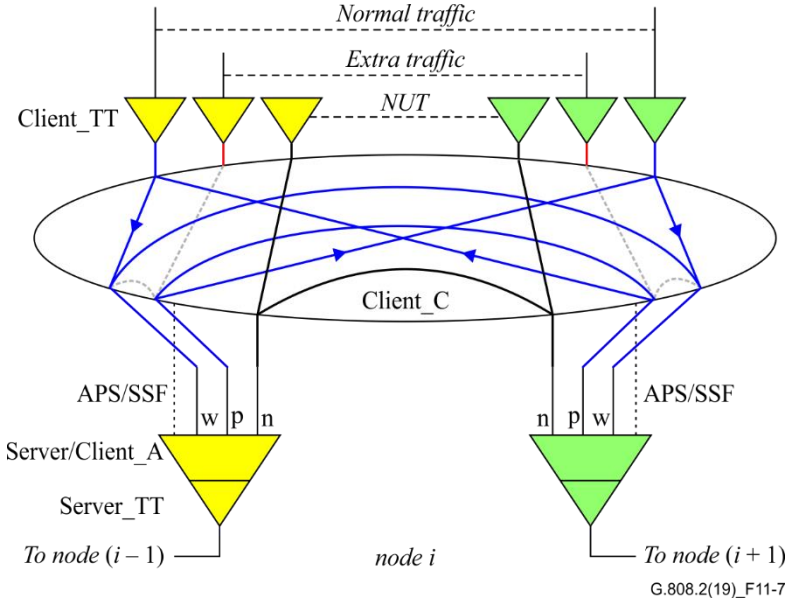

Figure 11-7 – Functional model of an intermediate node in short wrapping protection on a SLRing

11.2 Functional models for DLRing

Figure 11-8 shows the bidirectional functional model of the connection function of the client layer that is protected by the dedicated section link ring protection in each node of a protected ring when no protection switch is activated. The difference from the functional model of the SLRing shown in

Figure 11-1 is that the working transport entity and the protection transport entity are carried over two different server sections.

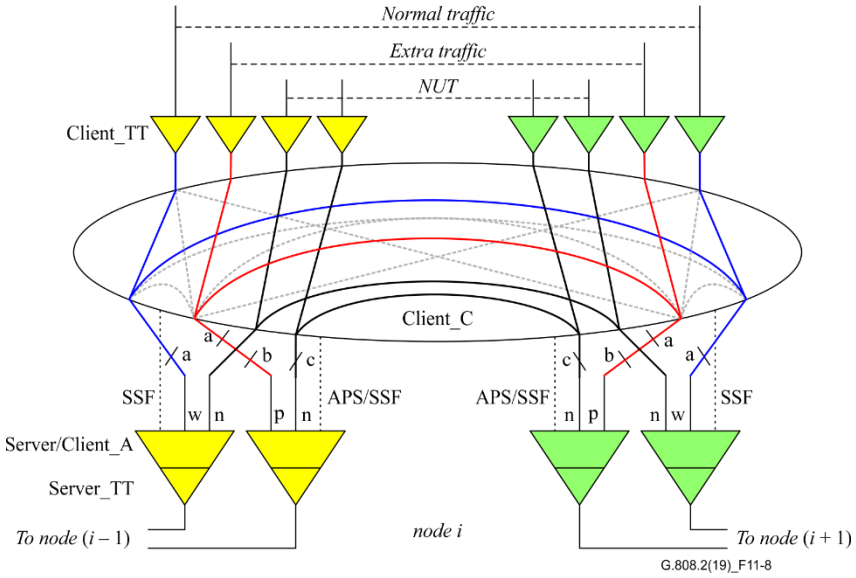

Figure 11-8 – Dedicated section link ring protection functional model

The maximum payload capacity of the working transport entity is equal to the capacity of the protection transport entity, as indicated by 'a' in Figure 11-8. The payload capacity of the NUT transport entity is different from the working and protection transport entity as indicated by 'b' or 'c' in Figure 11-8. The values 'a', 'b', and 'c' are provisioned to have the same respective values in all nodes of the ring. Note that the 'a', 'b', and 'c' entities will carry traffic originating locally or traffic passed through from node (i-1) to node (i+1) and vice versa.

In general, the following limits apply: $0 < a \leq \min(N1, N2)$, $0 \leq b < N1$, $0 \leq c < N2$, $(a + b) \leq N1$, and $(a + c) \leq N2$ where N1 is the total bandwidth capacity of the server section carrying working transport entities and N2 is the total bandwidth capacity of the server section carrying protection transport entities.

11.2.1 Functional models for span switch protection on a DLRing

Figure 11-9 shows the functional model in a node adjacent to the failed section or node when span switch protection is activated on a DLRing.

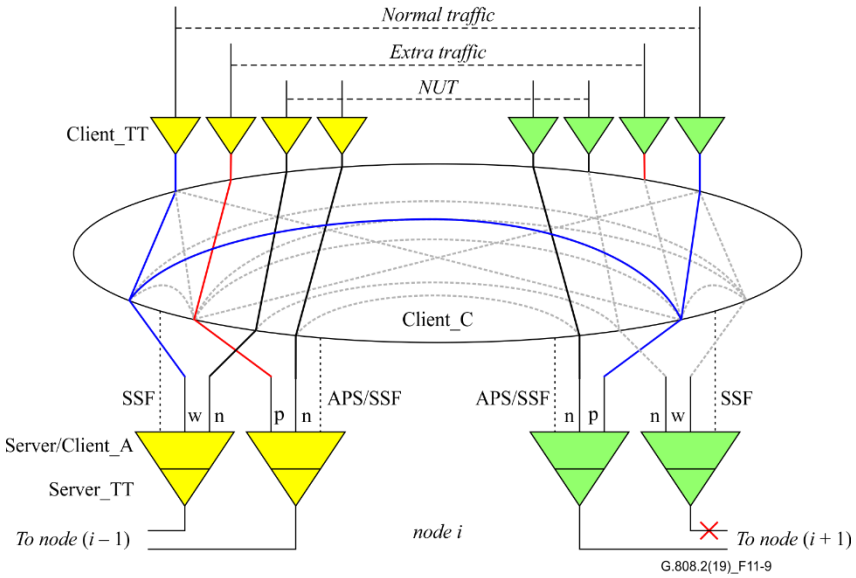

Figure 11-9 – Functional model of a node adjacent to a failure in span switch protection on a DLRing

NOTE – Functional models for wrapping, steering and short-wrapping protection on a DLRing are identical with those on a SLRing except that the DLRing has two sever sections in each span while the SLRing has only one (see Figure 11-1 and Figure 11-8).

12 Multi-ring scenario

In actual networks, multi-ring scenarios are widely applied, including tangent rings and intersecting rings (see Figure 12-1). The multi-ring mechanism should inherit and be compatible with the single ring mechanism, to simplify the equipment implementation.

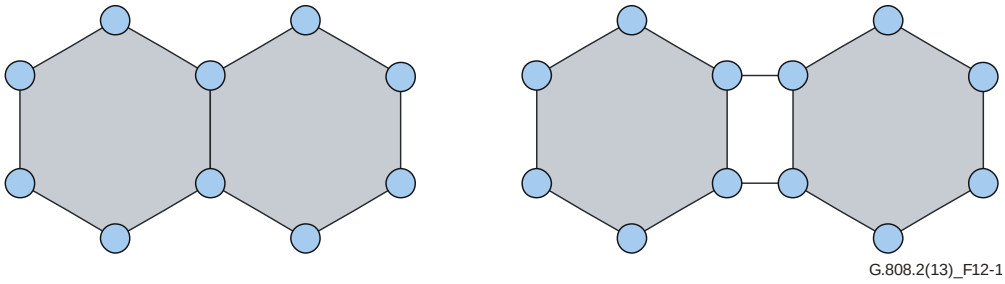

Figure 12-1 – Multiple rings scenario

13 Protection switching performance

The protection switching temporal model derived from [ITU-T M.495] and model parameters are defined in [ITU-T G.808].

14 Hold-off timer

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

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 seconds in steps of X ms. X is 100 ms (SDH, OTN, and MPLS-TP).

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 are 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 1 – 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.

NOTE 2 – Clearing of SF or SD does not result in a start of the hold-off timer. Instead the wait-to-restore (WTR) timer may be started.

15 Wait-to-restore timer

To prevent frequent operation of the protection switch due to an intermittent defect (e.g., BER fluctuating around the SD threshold), a failed server layer section which carries the working transport entities must become fault-free (e.g., BER less than a restoration threshold). After such a failed server layer section meets this criterion, a fixed period of time shall elapse before normal traffic signals use it again. This period, called wait-to-restore (WTR) period, is of the order of 0…12 minutes and should be capable of being set. An SF or SD condition will override the WTR.

In revertive mode of operation, when the protection is no longer requested, that is to say, the failed server layer section which carries the working transport entities is no longer in SD or SF condition (and assuming no other relevant requests exist), 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 server layer section on their protection transport entities. This state shall normally time out unless 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;
- Source Node ID;
- Destination Node ID;
- Additional Information.

The Request/State Type information identifies the highest priority fault condition, external command or protection process state at the source node.

The Source Node ID identifies the node transmitting the request.

The Destination node ID identifies the other node that is adjacent to the fault that was detected by the source node.

The Additional Information provides other information necessary for the protocol, and may include elements that identify:

- type of request (short/long path);
- signal status (idle, bridged, bridged and switched, …).

APS information is communicated between nodes on the ring by a technology-specific mechanism.

17 Blank clause

This clause is intentionally left blank.

18 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 to say an external (switch) command issues an appropriate external request on to the protection process.

NOTE – Only one external (switch) command can be issued per side of the protection group. Not accepted or overruled external commands are released/forgotten.

External commands are defined to allow:

1. Configuration modifications and maintenance to be performed on the protection group or its transport entities:
    - **Clear**: This command clears the externally initiated command and WTR at the node to which the command was addressed. The node-to-node signalling following removal of the externally initiated commands is performed using the no request (NR) code.

      The following two commands are useful if one span has excessive switching to protection. Another use for these commands includes blocking protection access for some spans that have only traffic that does not need protection. The commands are not time critical (that is to say they do not need to be completed in tens of milliseconds). Thus, they can be transmitted over the management system to each affected node.
    - **Lockout of Working channels – Ring switch (LOW-R)**: This command prevents the normal traffic from working channels over the addressed span from accessing the protection channels for a ring switch by disabling the node's capability to request a ring protection switch of any kind. If any normal traffic is already on protection, the ring bridge is dropped regardless of the condition of the working channels. If no other bridge requests are active on the ring, the NR code is transmitted. This command has no impact on the use of protection channels for any other span. For example, the node can go into any of the pass-through modes.
    - **Lockout of Working channels – Span switch (LOW-S)**: This command prevents the normal traffic from the working channels over the addressed span from accessing the protection channels for a span switch. If any normal traffic is already on protection, the span switch is dropped regardless of the condition of the working channels. If no other bridge requests are active on the ring, the NR code is transmitted. This command has no impact on the use of protection channels for any other span.
    - **Lockout of Protection – Span (LP-S)**: This command prevents the usage of the span for any protection activity and prevents using ring switches anywhere in the ring. If any ring switches exist in the ring, this command causes the switches to drop. If there is a span switch for this span, it is dropped. Thus, all ring switching is prevented (and pre-empted), and span switching is prevented only on the locked-out span.
    - **Forced Switch to protection – Ring (FS-R)**: This command performs the ring switch of normal traffic signal from working entities to the protection entities for the span between the node at which the command is initiated and the adjacent node to which the command is destined. This switch occurs regardless of the state of the protection entities, unless the protection entities are satisfying a higher priority bridge request.
    - **Forced Switch to protection – Span (FS-S)**: This command switches the normal traffic signal from the working entities to the protection entities of that span. This switch occurs regardless of the state of the protection entities, unless the protection

entities are satisfying a higher priority bridge request, or a signal failure exists on the protection entities of the span.

- **Manual Switch to protection – Ring (MS-R)**: This command performs the ring switch of the normal traffic signal from the working entities to the protection entities for the span between the node at which the command is initiated and the adjacent node to which the command is destined. This occurs if the protection entities are not in an SD condition and are not satisfying an equal or higher priority bridge request (including failure of the protection entities).
- **Manual Switch to protection – Span (MS-S)**: This command switches the normal traffic signal from the working entities to the protection entities for the same span over which the command is initiated. This occurs if the protection entities are not in an SD condition and are not satisfying an equal or higher priority bridge request (including failure of the protection entities).

2. Testing the protection process and APS channel between the two endpoints:

- **Exercise – Ring (EXER-R)**: This command exercises ring protection switching of the requested channel without completing the actual bridge and switch. The command is issued and the responses are checked, but no normal traffic signal is affected.
- **Exercise – Span (EXER-S)**: This command exercises span protection of the requested channel without completing the actual bridge and switch. The command is issued and the responses are checked, but no normal traffic signal is affected.

19 Automatic commands

The following automatically initiated commands shall be supported:

- **Signal Fail – Span (SF-S)**: An SF is defined as the presence of the trail signal fail (TSF) condition detected on a span. For Dedicated section Link rings, if the failure affects only the working entities, traffic can be restored by switching to the protection entities on the same span. The SF-S bridge request is used to initiate span switching for an SF on the working entities of a dedicated section link ring.
- **Signal Fail – Ring (SF-R)**: For shared section link rings, all SFs (as defined previously for span switching) are protected using the ring switch. For dedicated section link rings, the ring switch is used only if traffic cannot be restored using span switching. If failures exist on both the working and protection entities within a span, it is necessary to initiate a ring bridge request. Hence, this command is used to request ring switching for signal failures. For a dedicated section link ring (DLRing), a SF-R results from the combination of LOW-S and a detected or received working entity failure on the same span or the following combination of detected or received conditions on the working and protection entities:
  - working entity failed AND protection entity failed on the same span;
  - working entity failed AND protection entity degraded on the same span;
  - working entity degraded AND protection entity failed on the same span.
- **Signal Fail – Protection (SF-P)**: This command is used to indicate to an adjacent node that the protection entities are in a Signal Fail state (as defined previously for span switching). A signal failure of the protection entities is equivalent to a lockout of protection for the span that is affected by the failure. SF-P is used only for dedicated section link rings.
- **Signal Degrade – Span (SD-S)**: Signal degrade is defined as the presence of the trail signal degrade (TSD) condition detected on a span. In dedicated section link rings, the working entities on the degraded span can be protected using the protection entities on the same span. This bridge request is used to switch the normal traffic signal to the protection entities in the same span where the failure is located.

- **Signal Degrade – Ring (SD-R)**: For shared section link rings, any degraded span is protected using the ring switch (degradation is defined above under Signal Degrade – Span). For dedicated section link rings, a SD-R results from the combination of LOW-S and a detected or received working entity degrade on the same span or the combination of detected or received signal degrade conditions on the working and protection entities on the same span.
- **Signal Degrade – Protection (SD-P)**: This command is used when a node detects a degradation on its protection entities, and there are no higher priority bridge requests existing on the working entities (degradation is defined above under Signal degrade – Span). This bridge request is used only for dedicated section link rings.
- **Reverse Request – Span (RR-S)**: This command is transmitted to the tail-end node as an acknowledgment for receiving the short-path span bridge request. It is transmitted on the short path only.
- **Reverse Request – Ring (RR-R)**: This command is transmitted to the tail-end node on the short path as an acknowledgment for receiving the short-path ring bridge request.
- **Wait-To-Restore (WTR)**: This command is issued when working entities meet the restoral threshold after an SD or SF condition. It is used to maintain the state during the WTR period unless it is pre-empted by a higher priority bridge request.
- **No Request (NR)**: This command is issued when there is no need to use the protection entities. The protection transport entity carries either no (null) signal or extra traffic signal.

20 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 node of the ring.

- Lockout of Protection (Span) LP-S
- Signal Fail (Protection) SF-P

  NOTE – In SDH MS-SPRing, LP-S and SF-P share the same priority code. See [ITU-T G.841] for further details.
- Forced Switch (Span) FS-S
- Forced Switch (Ring) FS-R
- Signal Fail (Span) SF-S
- Signal Fail (Ring) SF-R
- Signal Degrade (Protection) SD-P
- Signal Degrade (Span) SD-S
- Signal Degrade (Ring) SD-R
- Manual Switch (Span) MS-S
- Manual Switch (Ring) MS-R
- Wait-To-Restore WTR
- Exerciser (Span) EXER-S
- Exerciser (Ring) EXER-R
- Reverse Request (Span) RR-S
- Reverse Request (Ring) RR-R
- No Request NR

21 SF and SD trigger conditions

An SF condition is a TSF in the server section trail termination function.

TSD in the server section trail termination function is the only SD trigger condition. It is issued on the detection of dDEG. TSD is always local to a Trail Termination function (TT), that is to say, it does not pass layer boundaries. The SF and SD conditions are described in the individual equipment specifications.

- For SDH in [ITU-T G.783]
- For OTN in [ITU-T G.798]
- For MPLS-TP in [ITU-T G.8121]

NOTE – MPLS-TP shared ring protection mechanism defined in [b-ITU-T G.8132] protects normal traffics against SF only.

22 Mechanisms to prevent misconnections

Because ring protection mechanisms share the protection resources across multiple working resources, it is necessary to consider mechanisms to avoid misconnection of traffic during protection switching events. This is particularly important in the case where the protection resources support extra traffic, or in the case of multiple failures that can lead to ring segmentation.

22.1 Circuit-switched technologies

In a ring protection mechanism based on circuit-switched technology, the protection transport entities are essentially shared among each span of the ring (that is to say a protection transport entity on one span can support a ring switch for the working transport entity on every other span). Extra traffic may reside in the protection transport entity on a span when the protection transport entity is not currently being used to restore normal traffic transported on the working transport entities of other spans. Thus, each protection transport entity is subject to use by multiple services (services from the working transport entities on different spans, as well as service from extra traffic). A number of scenarios can lead to multiple services contending for access to the same protection transport entity, and thus the potential for misconnection. With no extra traffic on the ring, under certain multiple failure conditions, such as those that cause node(s) isolation, services (from the working transport entity on different spans) may contend for access to the same protection transport entity. With extra traffic on the ring, even under single point failures, normal traffic on the working transport entity may contend for access to the same protection transport entity that carries the extra traffic.

22.1.1 Wrapping protection

A potential misconnection is determined by identifying the nodes that will act as the switching nodes for a bridge request, and by examining the traffic that will be affected by the switch. The switching nodes can be determined from the node addresses in the APS protocol. The switching nodes determine the traffic affected by the protection switch from the information contained in their ring maps and from the identifications of the switching nodes.

Squelching by inserting the appropriate alarm indication signal (AIS) signal in those entities where misconnected traffic could occur shall avoid potential misconnections. Specifically, the traffic that is sourced or dropped at the node(s) isolated from the ring by the failure shall be squelched. The squelching is performed at the switching nodes and is applied to the normal or extra traffic into or out of the protection transport entity, that is to say normal traffic into or out of a working transport entity is never squelched.

22.1.2 Steering protection

The avoidance of misconnections for the steering application is for further study.

22.2 Packet switched technologies

Packet switched shared ring protection mechanisms do not require special mechanisms to prevent misconnected traffic because the destination of each traffic unit is explicitly identified within that traffic unit. In the case of MPLS-TP shared ring protection, the protection resource has a specific label that is added to the normal traffic when it transits a protection tunnel. When a failure occurs, extra traffic does not have to be explicitly blocked; rather, the normal priority mechanisms used in packet networks will ensure that the protected normal traffic and NUT traffic receives higher priority than the extra traffic. The extra traffic will continue to be forwarded to the extent that there is bandwidth available for it to use.

Bibliography

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

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

[b-ITU-T G.873.2] Recommendation ITU-T G.873.2 (2012), *ODUk shared ring protection*.

[b-ITU-T G.8132] Recommendation ITU-T G.8132/Y.1383 (2017), *MPLS-TP shared ring protection*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019