International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.873.2

(04/2012)

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

Digital networks – Optical transport networks

ODUk shared ring protection

Recommendation ITU-T G.873.2

International Telecommunication Union

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

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

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

Recommendation ITU-T G.873.2

ODUk shared ring protection

Summary

Recommendation ITU-T G.873.2 provides the first set of necessary equipment-level specifications to implement shared ring protection architectures in optical transport networks (OTNs). In this version of the Recommendation shared ring protection on base of wrapping method is specified.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.873.2	2012-04-22	15
1.1	ITU-T G.873.2 (2012) Amd.1	2012-10-29	15

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T G.873.2

ODUk shared ring protection

1 Scope

This Recommendation describes the automatic protection switching (APS) protocol to support optical data unit k (ODUk) shared ring protection (SRP) in the optical transport network (OTN).

Shared ring protection provides two types of switching: SRP-1 with 1 ODU per lambda, and SRP-p with p ODUs per lambda. SRP protects ODUs within a physical ring with ODU cross-connects.

The interconnects are in general of type optical transport module-n (OTM-n), as specified in [ITU-T G.709]. The network objectives are given in Annex A.

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.709] Recommendation ITU-T G.709/Y.1331 (2012), *Interfaces for the optical transport network*.

[ITU-T G.798] Recommendation ITU-T G.798 (2010), *Characteristics of optical transport network hierarchy equipment functional blocks*.

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

[ITU-T G.806] Recommendation ITU-T G.806 (2006), *Characteristics of transport equipment – Description methodology and generic functionality*.

[ITU-T G.808.1] Recommendation ITU-T G.808.1 (2006), *Generic protection switching – Linear trail and subnetwork protection.*

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

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

[ITU-T G.872] Recommendation ITU-T G.872 (2001), *Architecture of optical transport networks*.

[ITU-T G.873.1] Recommendation ITU-T G.873.1 (2006), *Optical Transport Network (OTN): Linear protection*.

[ITU-T G.874] Recommendation ITU-T G.874 (2001), *Management aspects of the optical transport network element*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 APS-byte pass-through: See [ITU-T G.870].

3.1.2 APS channel: See [ITU-T G.870].

3.1.3 crossing APS-bytes: See [ITU-T G.870].

3.1.4 entity: See [ITU-T G.870].

3.1.5 extra traffic signal: See [ITU-T G.870].

3.1.6 full pass-through: See [ITU-T G.870].

3.1.7 head end: See [ITU-T G.870].

3.1.8 normal traffic signal: See [ITU-T G.870].

3.1.9 null signal: See [ITU-T G.870].

3.1.10 protection communication channel: See [ITU-T G.870].

3.1.11 protection group: See [ITU-T G.870].

3.1.12 signal: See [ITU-T G.870].

3.1.13 SRP-1: See [ITU-T G.870].

3.1.14 SRP-p: See [ITU-T G.870].

3.1.15 steering: See [ITU-T G.870].

3.1.16 tail end: See [ITU-T G.870].

3.1.17 pass-through: See [ITU-T G.841].

3.1.18 ring switch: See [ITU-T G.841].

3.1.19 span switch: See [ITU-T G.841].

3.1.20 wrapping: See [ITU-T Rec. G.870].

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AIS Alarm Indication Signal

APS Automatic Protection Switching

DNR Do Not Revert

EXER Exercise

FS Forced Switch

GCC General Communication Channel

HO Highest Order

LO Lowest Order

MS	Manual Switch
NE	Network Element
NIM	Non-Intrusive Monitor
NR	No Request
NUT	Non-pre-emptible Unprotected Traffic
ODUk	Optical Channel Data Unit k
OPU	Optical Payload Unit
OTN	Optical Transport Network
OTUk	Optical Channel Transport Unit k
PCC	Protection Communication Channel
RR	Reverse Request
SD	Signal Degrade
SF	Signal Fail
SNC	Sub-Network Connection
SNC/N	Sub-Network Connection with Non-intrusive monitoring
SNCP	Sub-Network Connection Protection
SRP-n	Shared ring protection of n ODU per Lambda (n=1, p)
TCM	Tandem Connection Monitoring
WTR	Wait-to-Restore

5 Conventions

As used in this Recommendation, highest order (HO) and lowest order (LO) are referring to the shared ring sub-network viewpoint.

6 Applications of OTN shared ring protection

6.1 Attributes of shared ring protection

- Shared ring protection of p optical data unit lambda (SRP-p) protection switching is on a per-highest order (HO) optical data unit (ODU) basis between all nodes in the ring. A bundle of lowest order (LO) ODU signals is switched when LO ODUk is carried by an HO ODUk around the ring. Automatic protection switching (APS) is used for each HO ODUk.
- SRP-1 protection switching is on a per-LO ODUk sun-network connection (SNC) or tandem connection basis between the ingress/egress points on the ring for that ODUk when the LO ODU is carried by an OTUk around the ring.
- For SRP-p, the payload type considered is PT21. While, in principle, PT20 could also be supported, the use of mixed payload structures creates interworking issues and is not recommended.
- There are no two-/four-fibre architectural differences for LO ODU SRP. Whether working/protection are on the same or different, diversely routed fibres across a span affects the ultimate reliability, but not the architecture or switching.
- There are two-/four-lambda architectural differences for SRP-p (also quoted as HO ODU). In the two-lambda architecture, the HO OPU payload must be split into working, protection

and a non-pre-emptible parts. In the four-lambda architecture, all working traffic is carried in one HO ODU and all protection traffic is carried in another HO ODU.

In ITU-T G.709 OTN, per-wavelength failure modes provide value for span switches even when working and protection ODUks are on the same fibre.

- Each connection between adjacent nodes in a given ring consists of a working and a protection entity. These entities may either be provided over the same fibre, or over two diversely routed fibres between the adjacent nodes.
- When many ODUks in one fibre belong to one group, group protection can reduce the number of APS instances in one fibre. Group protection can be triggered on the basis of signal fail group/signal degrade group (SFG/SDG) specifications as described in clauses 11.1.2 and 11.3.1 of [ITU-T G.808.1].

6.2 Protection classifications

This clause describes, in general terms, the types of ODU SRP architectures described within this Recommendation.

ODU SRP is an ODU ring-based sub-network connection group with inherent monitoring (SNCG/I) protection.

Figure 6-1 illustrates the model of a two-fibre/two-lambda ODUj SRP node with an N OPUk tributary slot capacity (ODU SRP-p). OTUk section monitoring and ODUk path monitoring endpoints terminate the OTUk and ODUk signals. ODUj signals within the ODUk are either protected by means of SRP, or are pre-emptible or non-pre-emptible unprotected.

Figure 6-2 illustrates the model of a four-lambda ODUj SRP with a 2N OPUk tributary slot capacity. The four-lambdas may be transported over either four-fibres or two-fibres. When transported over two-fibres, working and protection are part of the same shared risk group and provide a double capacity version of the two-fibre/two-lambda ODU SRP case. OTUk section monitoring and ODUk path monitoring endpoints are terminating the OTUk and ODUk signals. ODUj signals within the ODUk are either protected by means of SRP, or are pre-emptible or non-pre-emptible unprotected.

Figure 6-3 illustrates the model of a four-lambda ODUk SRP for a single ODUk capacity (ODU SRP-1). OTUk section monitoring and ODUk tandem connection monitoring (TCM) endpoints are terminating the OTUk and an ODUk TCM level; the ODUk is either protected by means of SRP, or pre-emptible unprotected.

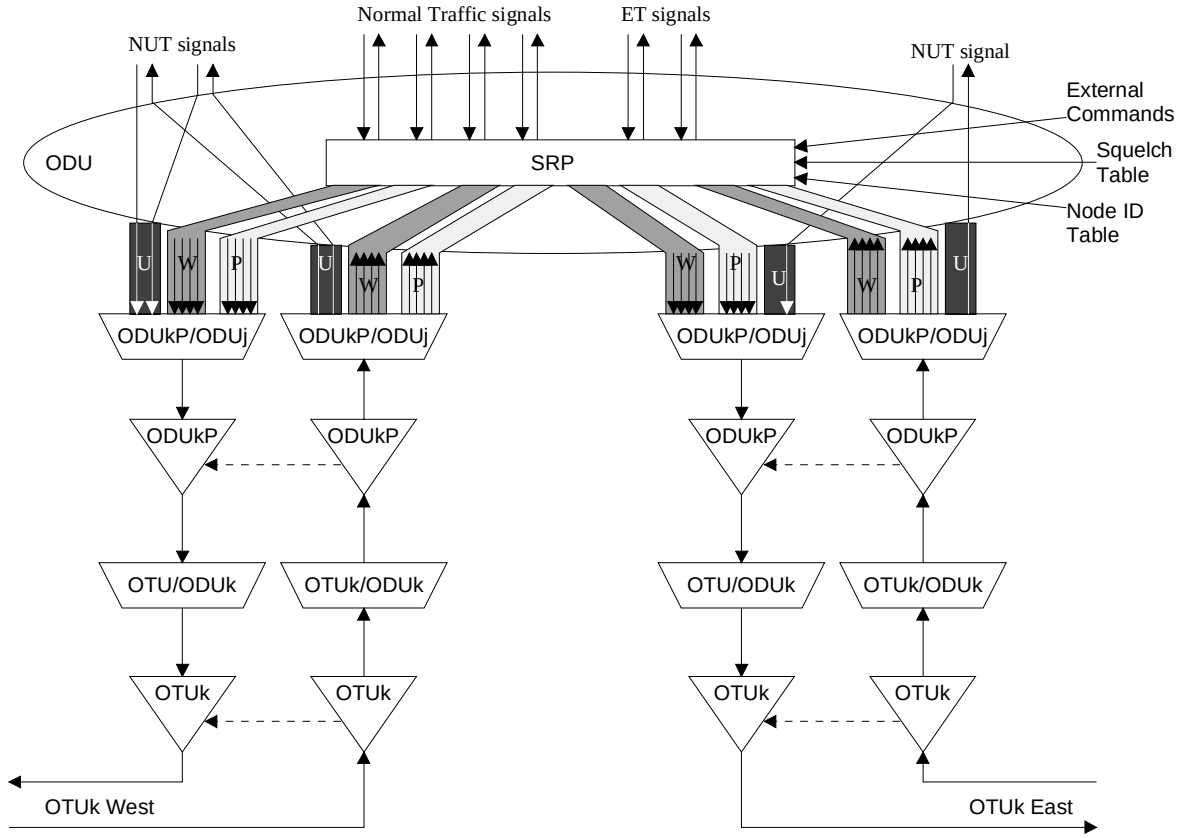


Figure 6-1 – Functional model for a two-fibre/two-lambda protection ring with N OPUk tributary slot capacity with extra traffic and non-pre-emptible unprotected traffic

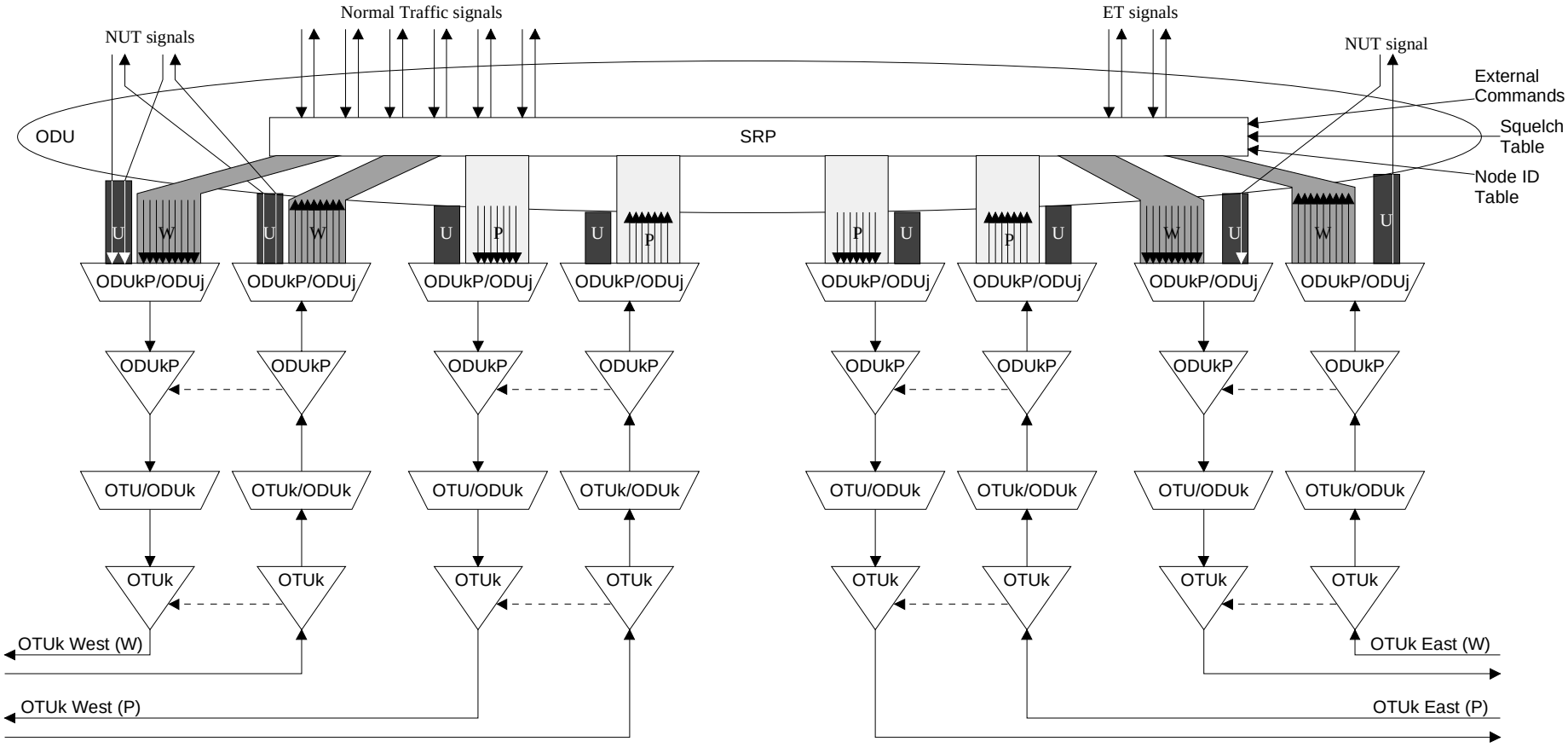


Figure 6-2 – Functional model for a four-lambda ODU SRP ring with 2N OPUk tributary slot capacity with extra traffic and non-pre-emptible unprotected traffic

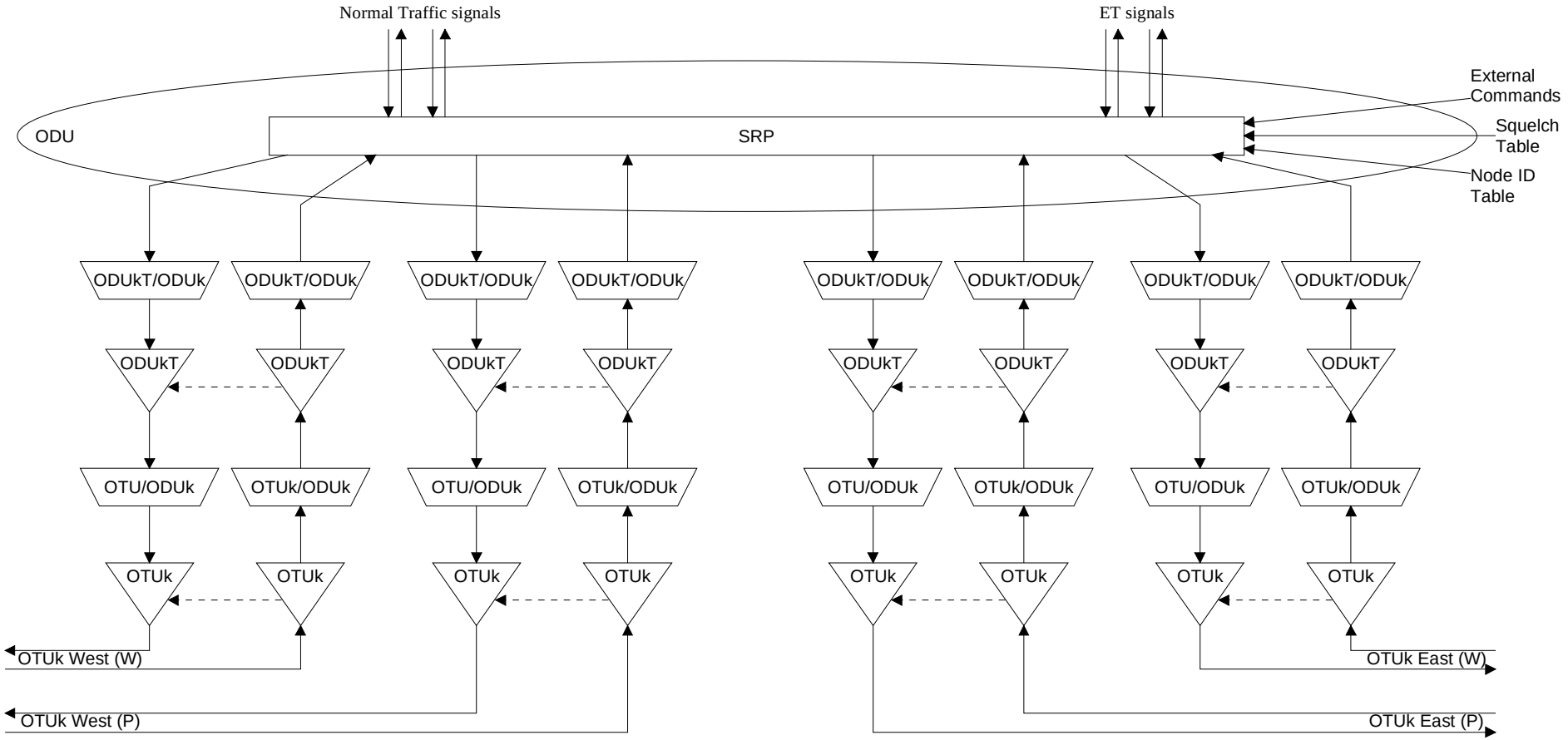


Figure 6-3 – Functional model for a four-lambda ODU SRP ring with single ODUk capacity with extra traffic

6.3 Applications considerations

This clause describes in general terms some of the possible advantages to be gained by the various protection architectures.

6.3.1 ODU SRP (wrapping application)

ODU SRP can be categorized into the following types: two-fibre/two-lambda, two-fibre/four-lambda and four-fibre/four-lambda. The ring APS protocol accommodates all types.

For ODU SRP, the working tributary slots carry the normal traffic signals to be protected while the protection tributary slots are reserved for protection of this service. Protection tributary slots may be used to carry extra traffic (ET) (i.e., pre-emptible unprotected traffic (PUT)) when not being used for protection of normal traffic. Normal traffic signals are transported bidirectionally over spans, where an incoming normal traffic signal travels in one direction of the working tributary slots while its associated outgoing normal traffic signal travels in the opposite direction but over the same spans.

The pair of normal traffic signals (i.e., incoming and outgoing) only use capacity along the spans between the nodes where the pair is added and dropped. Thus, as illustrated in Figure 6-4, the pattern that these pairs of normal traffic signals place on the ring impacts the maximum load that can be placed on ODU SRP. The sum of the normal traffic signals that traverse a span cannot exceed the maximum tributary slot capacity of that particular span.

Depending upon the normal traffic signal pattern, the maximum load that can be placed on a (bidirectional) ODU SRP can exceed the maximum load that can be placed on the equivalent type of unidirectional ring (i.e., SNC protection) with the same optical rate and the same number of fibres/lambdas. This gives the bidirectional ring a capacity advantage over unidirectional rings, except when the normal traffic signals are all destined for only one node on the ring, in which case they are equivalent.

One advantage of ODU SRP is that this service can be routed on the ring in either one of two different directions, the long way around the ring or the short way around the ring. Although the short way is usually preferred, occasionally routing the service the long way permits some load balancing capabilities.

When the protection tributary slots are not being used to restore the normal traffic signals, they can be used to carry extra traffic signals. In the event of a protection switch, the normal traffic on the working tributary slots will access the protection tributary slots causing any extra traffic to be removed from the protection tributary slots.

During a ring switch, normal traffic transmitted toward the failed span is switched at one switching node to the protection tributary slots transmitted in the opposite direction (i.e., away from the failure). This bridged traffic travels the long way around the ring on the protection tributary slots to the other switching node where the normal traffic from the protection tributary slots are switched back onto the working tributary slots. In the other direction, the normal traffic is bridged and switched in the same manner. Figure 6-5 illustrates a ring switch in response to a cable cut.

During a ring switch, the failed span is effectively "replaced" with the protection tributary slots between the switching nodes, travelling the long way around the ring. Since the protection tributary slots along each span (except the failed span) are used for recovery, the protection capacity is effectively shared by all spans.

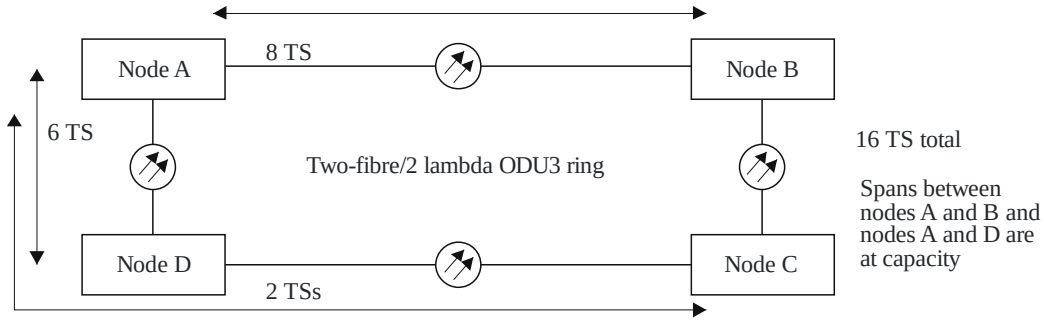
ODU SRP protocols allow the available bandwidth to be partitioned into the following three types of tributary slots: working tributary slots, used to carry normal traffic, protection tributary slots, used to carry extra traffic, and Non-pre-emptible unprotected traffic (NUT) tributary slots, used to carry non-pre-emptible unprotected traffic. Normal traffic is protected against failure events via the ODU SRP APS protocol, while extra traffic is pre-emptible unprotected traffic carried on the protection tributary slots. Any failure event that may require the protection tributary slots for protection purposes shall pre-empt the extra traffic.

NUT is unprotected traffic that is carried on tributary slots which are not governed by the ODU SRP APS protection switching mechanism (i.e., working tributary slots and their corresponding protection tributary slots). Traffic carried on these tributary slots is unprotected and non-pre-emptible. Thus, NUT carried on non-pre-emptible unprotected tributary slots afford a higher level of survivability as compared to extra traffic, but lower level of survivability as compared to normal traffic.

Examples of how NUT tributary slots can be used are given in Figures 6-6 and 6-7:

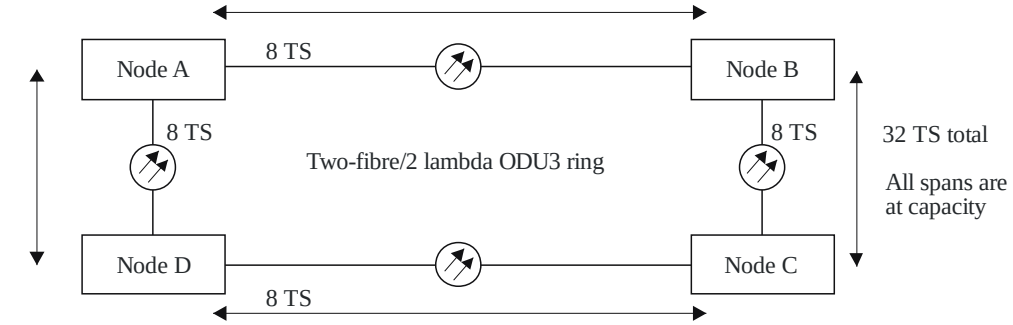
– Figure 6-6 shows a logical ring in which sub-network connection protection (SNCP) is used as a protection mechanism partially embedded in an ODU SRP using NUT. This arrangement avoids unnecessary layering of protection mechanisms and is more bandwidth efficient than the same application without NUT.

– Figure 6-7 shows a similar application, but in this case with the NUT tributary slots supporting ODU connectivity among packet transport layer network (PTN) switches. Under the assumption that the PTN traffic is protected by other means or does not need to be protected, this application of NUT has the same advantages as the previous example.

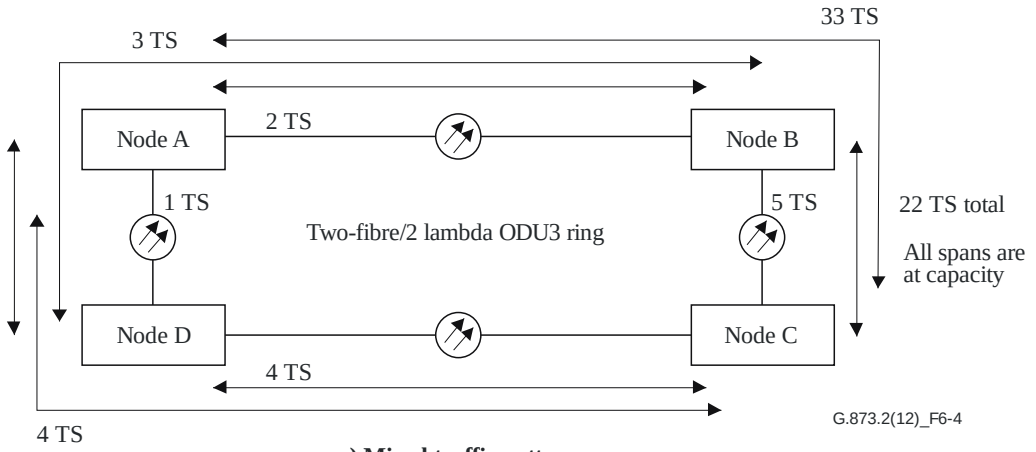


NOTE – Since all the traffic is destined for Node A, and the span between Node A and Node B is full , traffic from Node C routes through Node D, leaving the span between Node B and Node C vacant.

a) All traffic destined for one node, Node A

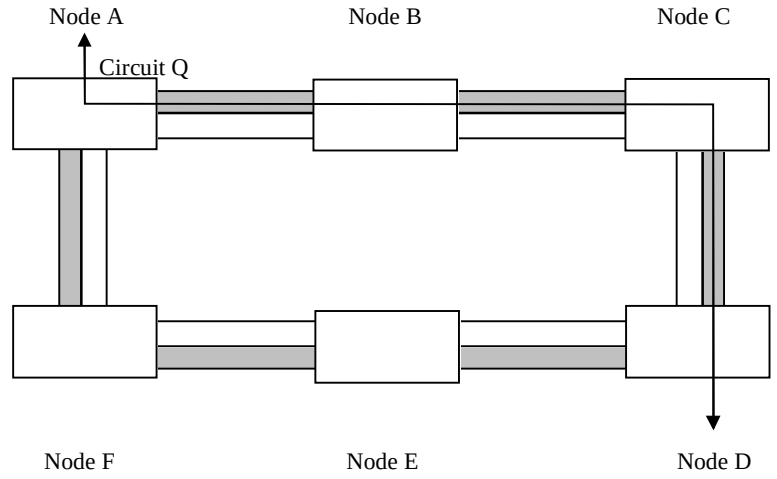


b) All traffic destined for adjacent nodes only

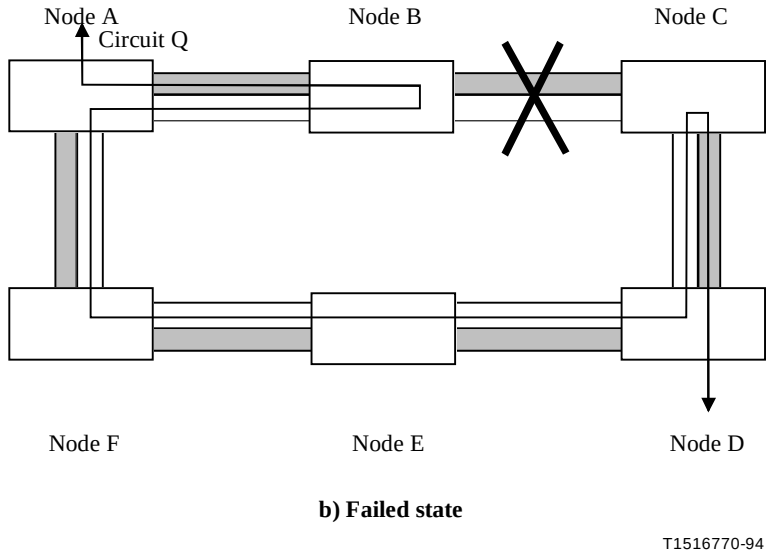


c) Mixed traffic pattern

Figure 6-4 – Effects of demand pattern on capacity of bidirectional ODU SRPs



a) Normal state



b) Failed state

T1516770-94

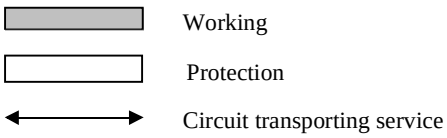


Figure 6-5 – Example of circuit routing in failure state for a ring switch

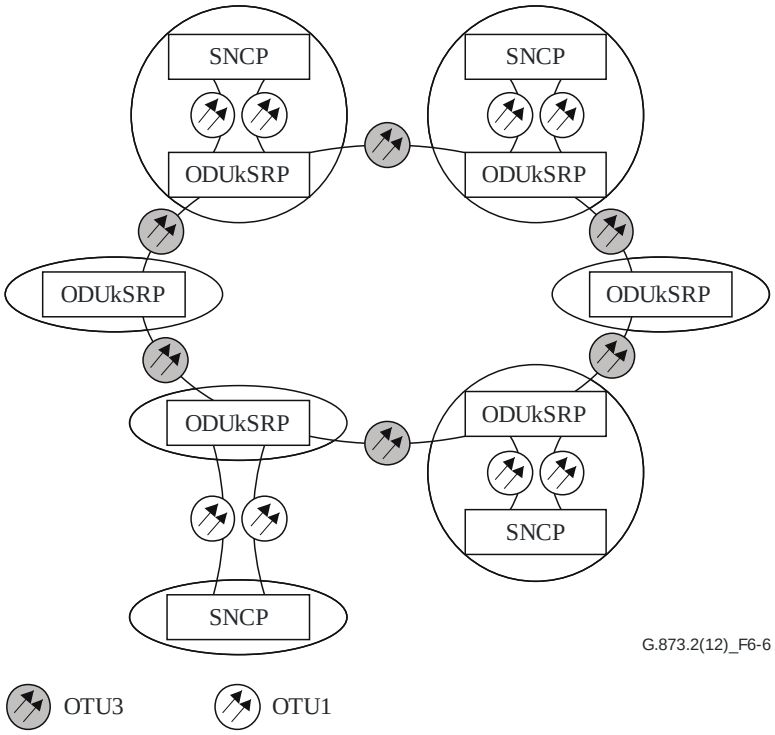


Figure 6-6 – Logical ring in which SNCP is used as a protection mechanism partially embedded in an ODU shared ring protection

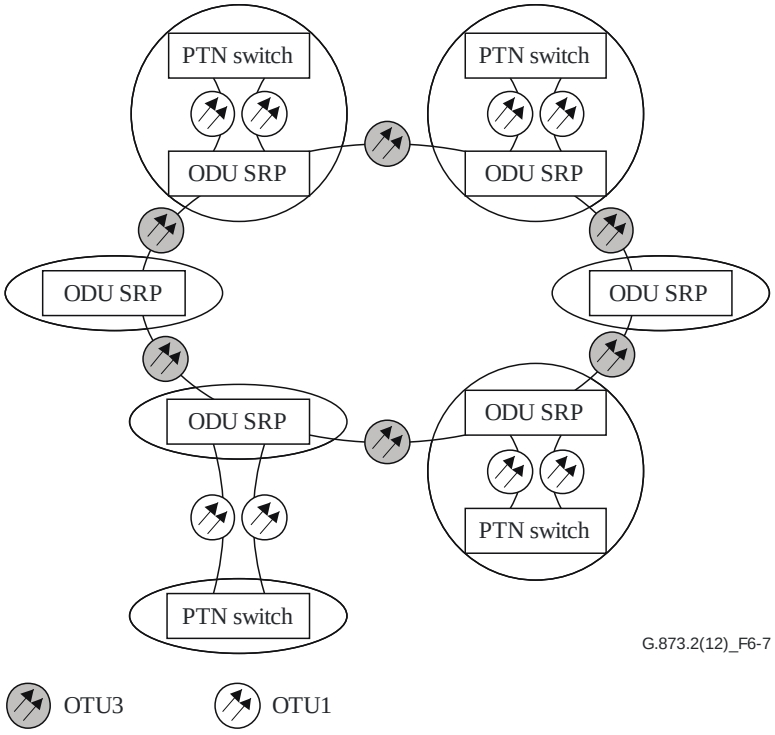


Figure 6-7 – NUT channels supporting ODU connectivity among PTN switches

6.3.2 ODU SRP (steering application)

This application, including its additional requirements and operating characteristics, are described in clause 7.3. Because of the unique characteristics of long-haul optical transport network systems, i.e., very long transmission paths, the approach described for general purpose ODU SRP is insufficient. For some types of failures, a total adaptation of the general purpose ODU SRP would lead to restoration transmission paths that would cross the ring three times. The inherent delays in such an approach will only result in degraded performance.

Therefore, additional details required for implementing the "long-haul application" option demonstrate that using the existing protocol and augmenting the switching action at the ring nodes results in eliminating the problem mentioned above. It should be noted that these problems only manifest themselves in long-haul networks, where the distances between the nodes on the ring exceed 1500 km. While this clause was developed to meet the needs of the long-haul application, the protocol modifications in this clause can be used to meet the needs of other high delay spans within an ODU shared ring protection.

When a ring switch occurs on the long-haul ring network, all normal traffic ODUj signals affected by the failure are bridged at their source nodes onto the protection tributary slots that travel away from the failure. When the affected tributaries reach their final destination nodes, they are switched to their original drop points, as illustrated in Figure 6-8. This is accomplished by using the local node ring maps and the APS-byte protocol. The differences in Figures 6-5 and 6-8 illustrate the differences in the length of the protection tributary slots.

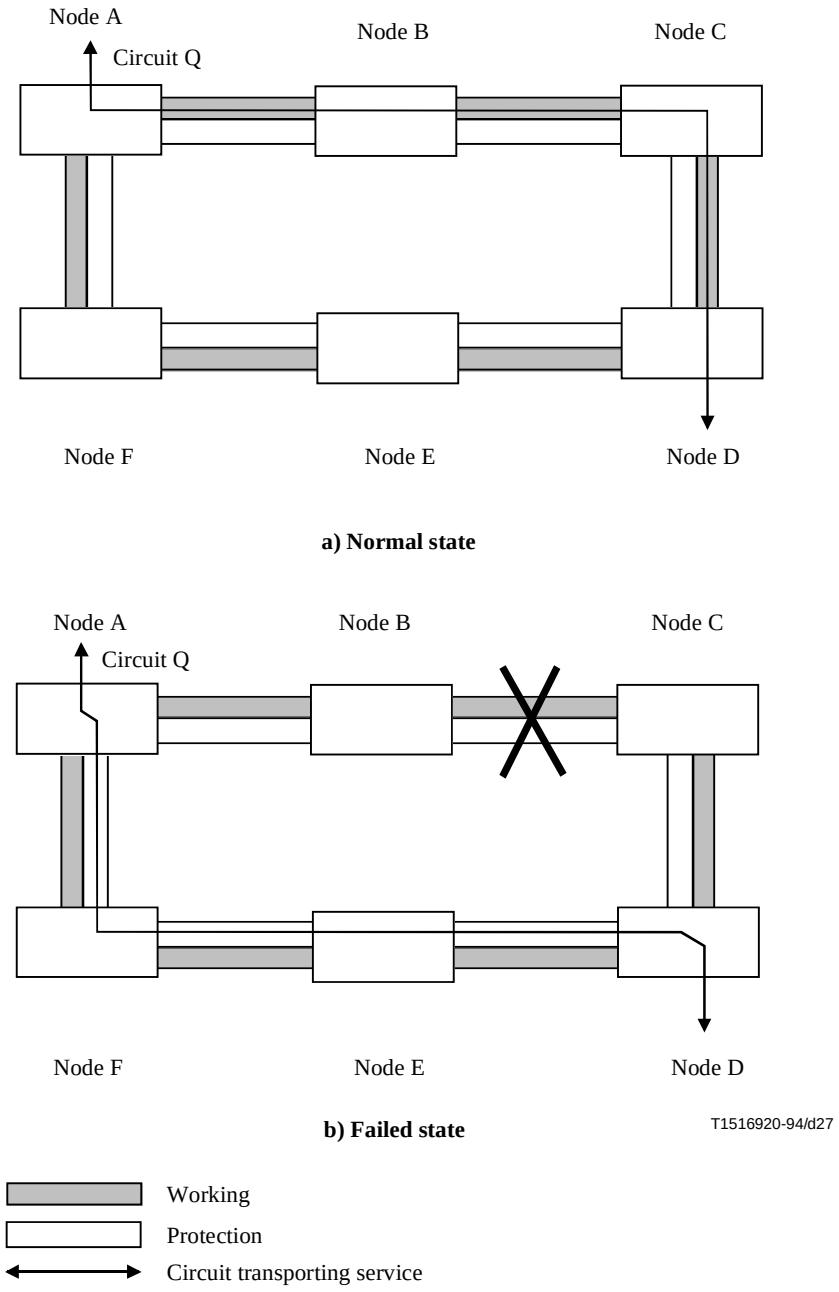


Figure 6-8 – Example of circuit routing in failure state for a ring switch (long-haul application)

For the non-long-haul ring network, the extra traffic remains off the ring network until the failure is cleared. Since only the affected normal traffic ODUj signals are switched for the steering ring network, the pre-empted extra traffic can be re-established on the protection tributary slots not used to restore the normal traffic. The signalling channel used to re-establish the extra traffic can be the general communication channel (GCC) or ODU protection communication channel (PCC).

6.4 Use of extra traffic

During fault-free conditions, it is possible to use the protection tributary slots to carry extra traffic, which has lower priority than the normal traffic on the working tributary slots and is unprotected. The main benefit in using Extra Traffic is the efficiency improvement of the network resources usage.

The extra traffic is set up by provisioning the add- and drop-nodes for its usage. Intermediate nodes along the ring are provisioned so that the extra traffic ODUk signals (which use protection tributary slots) are passed through the node (protection tributary slots that are not carrying extra traffic are terminated at the intermediate nodes).

Nodes that are inserting, dropping, or passing through extra traffic indicate its presence on those spans by inserting the extra traffic code in APS byte 1 bits 6-8. Before capacity is allocated to extra traffic, it has to be verified that the corresponding protection tributary slots are not occupied by protection-switched normal traffic.

When it becomes necessary to restore normal traffic by use of the protection tributary slots (due to a failure on the working path and corresponding protection action or an externally initiated command) the extra traffic is pre-empted and dropped on the spans whose protection tributary slots are required for the protection switch. Extra traffic circuits that have their source removed by this pre-emption shall be squelched with ODU alarm indication signal (ODU-AIS). This is necessary in order to avoid misconnection of extra traffic and switched normal traffic.

When the affected nodes or spans return to the idle state, the extra traffic should be restored.

7 ODU SRP

7.1 Two- and four-fibre ODU SRP types

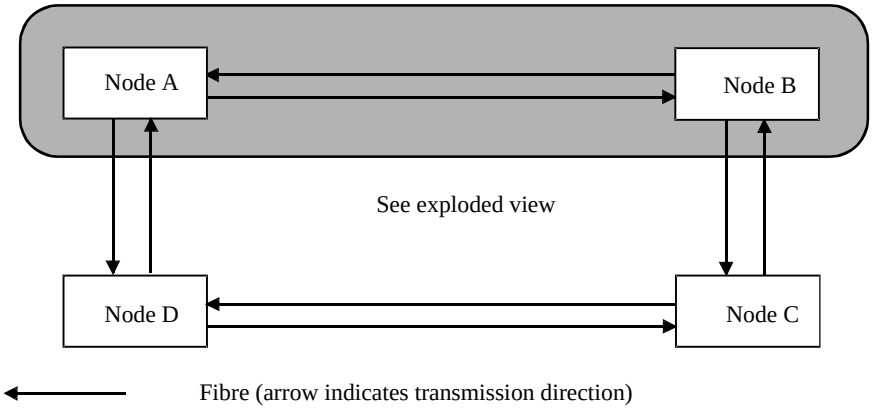
All ODU shared ring protection types support ring switching. In addition, four-fibre ODU SRP types support span switching.

7.1.1 Two-fibre/two-lambda ODU SRP (22SRP-p)

Two-fibre/two-lambda ODU switched rings require only two fibres and two lambdas for each span of the ring. Each lambda carries both working tributary slots and protection tributary slots. On each lambda, half the tributary slots are defined as working tributary slots and half are defined as protection tributary slots. The normal traffic carried on working tributary slots in one lambda is protected by the protection tributary slots travelling in the opposite direction around the ring (see Figure 7-1). This permits the bidirectional transport of normal traffic. Only one set of overhead channels is used on each lambda.

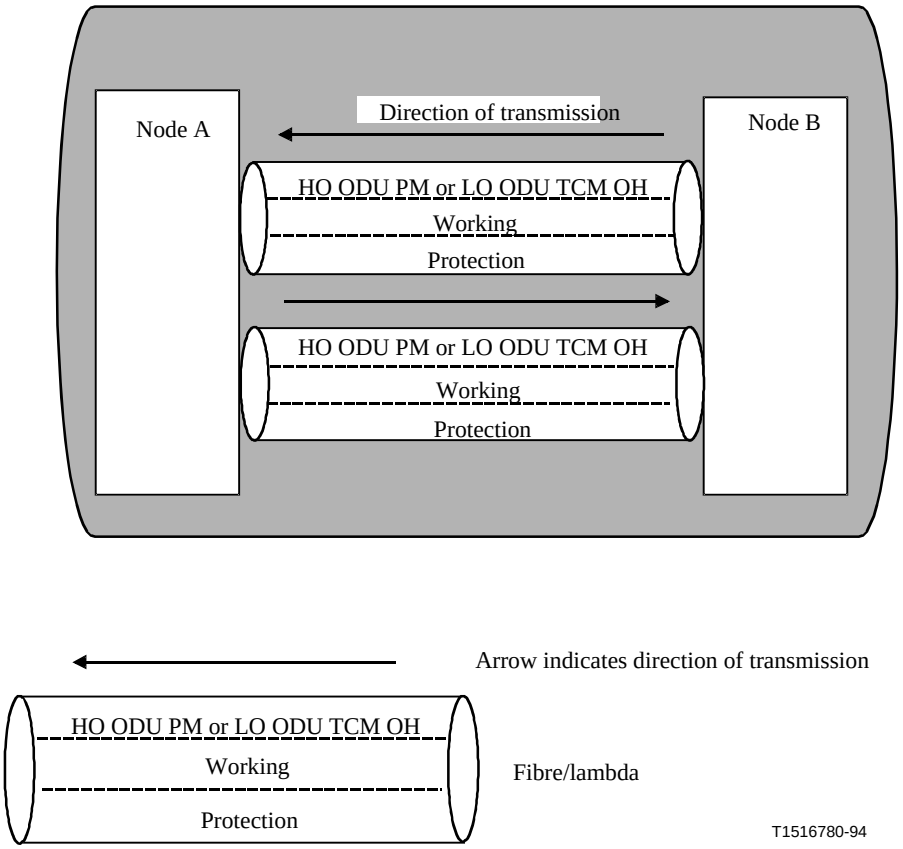
Two-fibre/two-lambda ODU shared ring protection types support ring switching only. When a ring switch is invoked, the normal traffic is switched from the working tributary slots to the protection tributary slots in the opposite direction.

If NUT is supported, selected tributary slots on the working bandwidth and their corresponding protection tributary slots may be provisioned as non-pre-emptible unprotected tributary slots. The remaining working tributary slots are still protected by the corresponding protection tributary slots. The non-pre-emptible unprotected tributary slots will have no ODU SRP protection.



NOTE – Each fibre/lambda carries both working and protection traffic, as shown in the exploded view.

a) View of entire ring



b) Exploded view of the shaded portion of the ring

Figure 7-1 – Two-fibre/two-lambda ODU SRP (22SRP-p)

7.1.2 Four-fibre/four-lambda ODU SRP (44SRP-p)

Four-fibre/four-lambda ODU SRP requires four fibres for each span of the ring. As illustrated in Figure 7-2, working and protection tributary slots are carried over different fibres: two ODUk (HO ODU) paths transmitting in opposite directions carry the working tributary slots while two ODUk (HO ODU) paths, also transmitting in opposite directions, carry the protection tributary slots. This permits the bidirectional transport of normal traffic. The ODUk (HO ODU) path

overhead is dedicated to either working or protection tributary slots since working and protection tributary slots are not transported over the same fibres/lambdas.

Four-fibre/four-lambda ODU shared ring protection supports ring switching as a protection switch, as well as span switching, though not concurrently. Multiple span switches can coexist on the ring since only the protection tributary slots along one span are used for each span switch. Certain multiple failures (those that affect only the working tributary slots of a span such as electronic failures and cable cuts severing only the working tributary slots) can be fully protected using span switching.

If NUT is supported, then on each span, selected tributary slots on the working tributary slots and their corresponding protection tributary slots may be provisioned as non-pre-emptible unprotected tributary slots. The remaining working tributary slots are still protected, for both span and ring switching, by their corresponding protection tributary slots. The effect on a selected non-pre-emptible unprotected tributary slot is as follows:

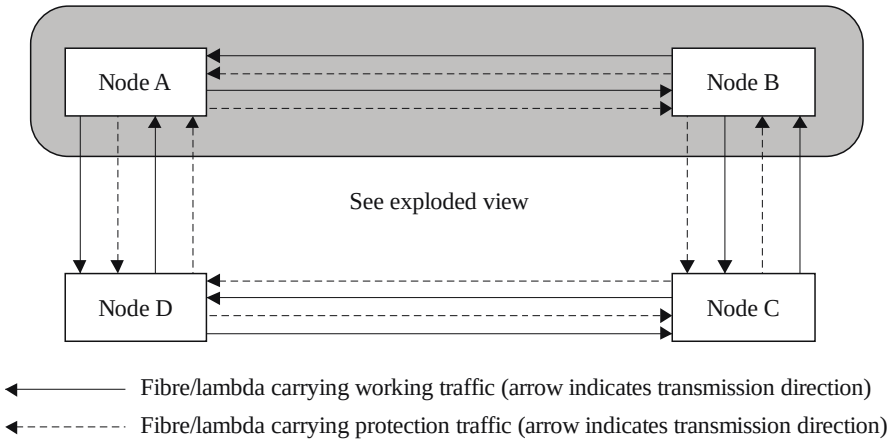
– ring switching is disabled on that tributary slot everywhere on the ring (as in the two-fibre case);

– span switching is disabled for that tributary slot on the provisioned span.

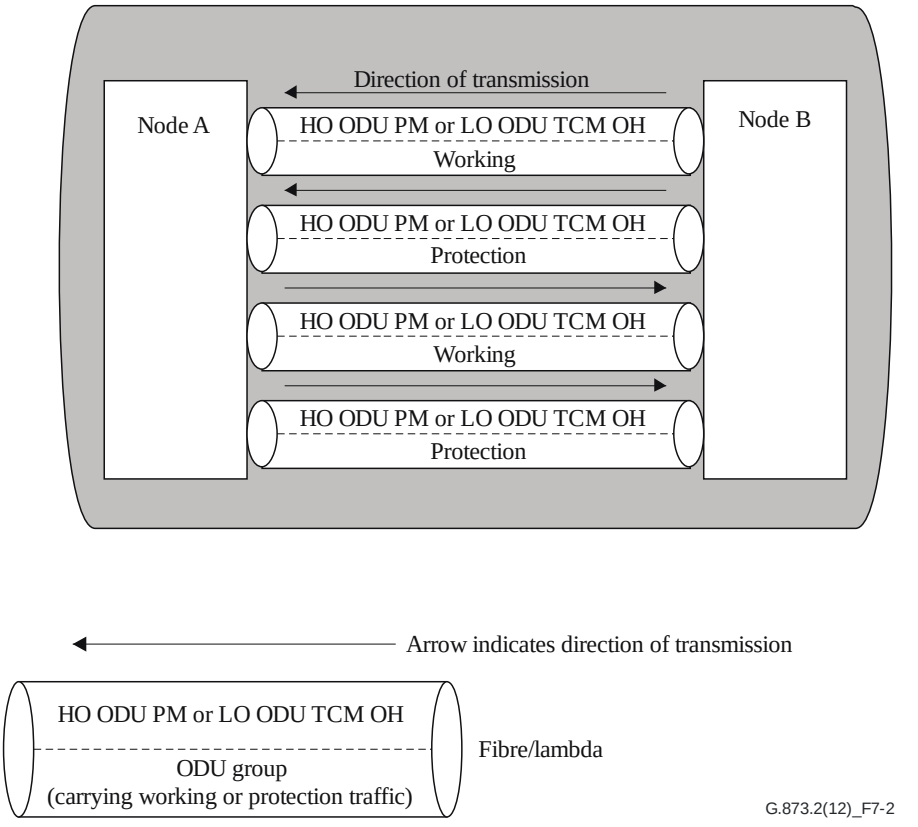
Hence, the NUT tributary slot has no ODU SRP on the provisioned span; on other spans, the same tributary slot (if not provisioned as NUT) has only span switching available to it. Note that if this tributary slot is provisioned as a working tributary slot on other spans, it will have lower survivability than other working tributary slots since ring switching is unavailable to it.

Support of non-pre-emptible unprotected tributary slots provisioning requires that a NUT table be present at each node on the ODU SRP. Figure 7-3 gives a conceptual representation and example of a NUT table. This table contains information to identify the tributary slots that have been provisioned for NUT, and identifies which type of switching (i.e., span or ring switch) is prohibited by the NUT. Since provisioning of working tributary slots for non-pre-emptible unprotected automatically ensures that the corresponding protection tributary slots are also provisioned as non-pre-emptible unprotected, only the working tributary slot ID needs to be stored in the table. The corresponding table for two-fibre operation only needs a column for ring switching.

Four-fibre/four-lambda ODU SRP may have the capability of operating similar to a linear add-drop multiplexer (ADM) chain when not fully connected as a continuous ring (i.e., they can lock out ring switches and use span switches only to protect existing traffic). This configuration may exist because an isolated ring segment has been established before all the other spans have been made fully operational.

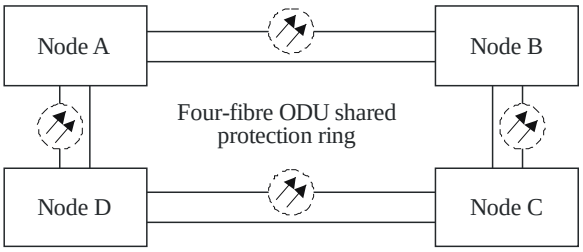


a) View of entire ring



b) Exploded view of the shaded portion of the ring

Figure 7-2 – Four-fibre/four-lambda ODU shared ring protection



- All spans have NUT for TS #1
- The span between B and C has NUT on TS #2

Node A

TS #	Ring switch	Span switch	
		East	West
1	–	–	–
2	–		
3			
4			
5			
. . .			

Node B

TS #	Ring switch	Span switch	
		East	West
1	–	–	–
2	–	–	
3			
4			
5			
. . .			

Node C

TS #	Ring switch	Span switch	
		East	West
1	–	–	–
2	–		–
3			
4			
5			
. . .			

Node D

TS #	Ring switch	Span switch	
		East	West
1	–	–	–
2	–		
3			
4			
5			
. . .			

G.873.2(12)_F7-3

– Indicates that this facility is not available for protection switching.

NOTE – In this example, "West" refers to the counter-clockwise direction of the ring.

Figure 7-3 – Conceptual representation and example of a NUT table

7.1.3 Two-fibre/four-lambda ODU SRP (24SRP-p)

For further study.

7.1.4 Four-fibre/four-lambda ODU SRP (44SRP-1)

For further study.

7.1.5 Two-fibre/four-lambda ODU SRP (24SRP-1)

For further study.

7.2 Wrapping application of ODU SRP

7.2.1 Application architecture (wrapping application)

The optical channel data tributary unit (ODTU) groups that traverse the span between any two adjacent nodes are divided into working tributary slots, protection tributary slots and NUT tributary slots.

In the case of the two-fibre/two-lambda ring, the OTUk can be viewed as a multiplex of N OPUk tributary slots (TSs), where the OPUk TSs are numbered from 1 to N according to the order that they appear in the multiplex. OPUk TSs numbered from 1 to N/2 shall be assigned as working tributary slots, and OPUk TSs numbered from ((N/2) + 1) to N shall be assigned as protection tributary slots. Furthermore, the normal traffic carried on working tributary slot *m* is protected by protection tributary slot ((N/2) + *m*). For example, an OTU3 can be considered a multiplex of 32 OPU3 TSs numbered 1 to 32. OPUk TSss number 1 to 16 would be assigned as working tributary slots, and OPUk-TSs number 17 to 32 would be assigned as protection tributary slots. This assignment applies to both directions of transmission and to all spans, as illustrated in Figure 7-4.

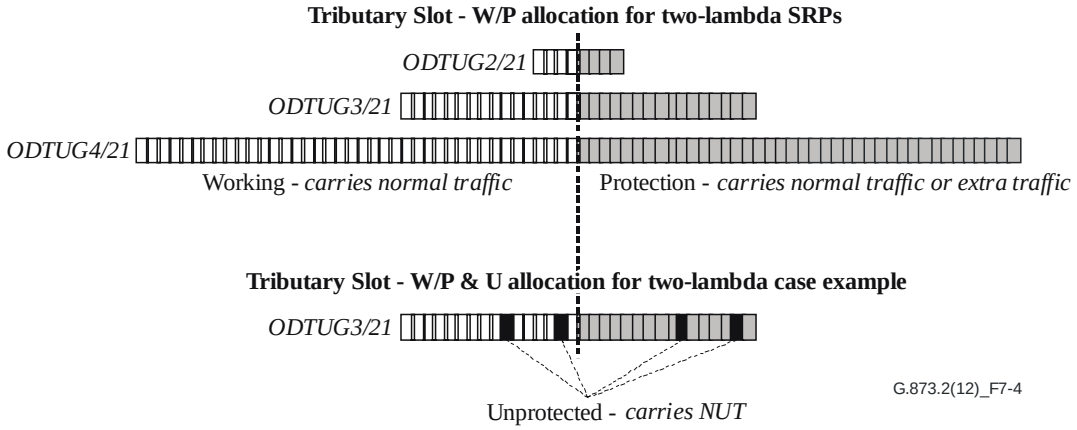


Figure 7-4 – Tributary slot allocation for two-lambda ODU SRP

In the case of the four-fibre ring, each working and protection OTUk is carried on a separate fibre.

In the case of the two-fibre/four-lambda ring, the working and protection OTUk are carried on the same fibre.

The shared protection ring APS protocol shall be carried on the APS bytes in the ODUk (HO ODU) path (multi-frame alignment signal (MFAS) = xxxx x000) or ODUk (LO ODU) tandem connection (MFAS = xxxx x110) overhead. In the case of the four-fibre ring, the APS protocol is only active on the lambdas carrying protection channels. Functions that are required in real time and required to make a protection switch are defined in the SRP APS protocol using those ODU APS bytes.

Each node on the ring shall be assigned an ID that is a number from 0 to 15 (optionally 127), allowing a maximum of 16 (optionally 128) nodes on the ring. The ID is independent of the order that the nodes appear on the ring.

A node on the ring may insert normal or extra traffic into tributary slots in either direction, drop normal or extra traffic from tributary slots from either direction, or pass the ODU signals in tributary slots directly through in order to allow other nodes to be connected. Because ODU SRP can support extra traffic, this capability may apply not only to the normal traffic ODU signals in working tributary slots, but also, as an option, to the extra traffic ODU signals in protection tributary slots. Each node has a ring map that is maintained by local craft or by an OS and contains information about the assignment of tributary slots that the node handles. An example of such a ring map is provided in Figure 7-5 and an example of a squelch table is provided in Figure 7-6.

	Node
1	A
2	J
3	M
4	P
5	B
6	L
7	K
8	G
9	S
10	E
11	F
12	R
13	C
14	D
15	N
16	H
⋮	
127	xx

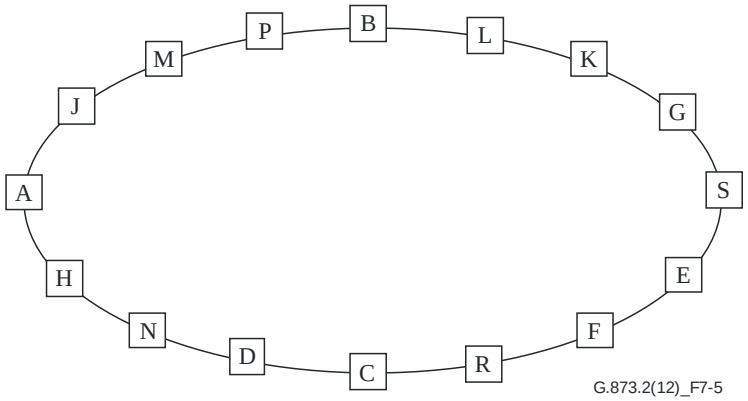


Figure 7-5 – Conceptual representation of a ring topology map

OPUk TS number	← West A	B	Node C	D	East → A
1	ODU				
2	ODU				
3		ODU			
4					
5					
6					

Sample traffic routing for a four node ring

Node A

	West			East		
	Src	Dst	ODU	Src	Dst	ODU
1				A	B	✓
2				A	D	✓
3	A	C	✓	A	C	
4	A	D		A	B	
5	A	B				
6	B	C		C	B	

Node B

	West			East		
	Src	Dst	ODU	Src	Dst	ODU
1	B	A	✓	B	D	
2	D	A	✓	A	D	✓
3	C	A		A	C	
4	B	A		B	C	
5				B	A	
6	B	C		B	C	

Node C

	West			East		
	Src	Dst	ODU	Src	Dst	ODU
1	D	B	✓	B	D	✓
2	D	A	✓	A	D	✓
3	C	A		C	A	
4	C	B		C	D	
5	A	B		B	A	
6	C	B		C	B	

Node D

	West			East		
	Src	Dst	ODU	Src	Dst	ODU
1	D	B				
2	D	A	✓			
3	A	C	✓	C	A	✓
4	D	C		D	A	
5	A	B		B	A	
6	B	C		C	B	

G.873.2(12)_F7-6

Src Node at which an ODUk enters the ring or is sourced
Dst Node at which an ODUk exists the ring or is terminated
✓ Indicates an client ODU organized OPUk TS

NOTE – Marking of OPUk TS for client ODU access is optional. All connections in this example are bi directional.

Figure 7-6 – Conceptual representation of node cross-connect map

When no protection switches are active on the SRP-p ring, each node sources the APS-bytes in each direction indicating no bridge request. In general, the protection tributary slots that are sourced at each node contain an "unallocated" indication in their multiplex structure identifier (MSI) fields (for case of payload type 21), as specified in [ITU-T G.709]. The exception is extra traffic tributary slots that may be added, dropped, or passed through similar to normal traffic.

When no protection switches are active on the SRP-1 ring, each node sources the APS-bytes in each direction indicating no bridge request. In general, the protection ODUk that are sourced at each node contain an ODUk open connection indication (ODUk-OCI), as specified in [ITU-T G.709]. The exception is extra traffic that may be added, dropped, or passed through similar to normal traffic.

A switch shall be initiated by one of the criteria specified in clause 7.2. A failure of the APS protocol or controller shall not trigger a protection switch. It is assumed, however, that the appropriate alarms will be generated.

A two-fibre ring only uses ring switches to restore traffic. A four-fibre ring has the additional option of span switching. Specifically, from the perspective of a node in a four-fibre ring, two protection channels exist: a short path over the span, used in the span switch, and a long path over the long way around the ring, used in a ring switch. With span switching, each span in a four-fibre ring can behave similar to a 1:1 protected linear system. Therefore, failures that only affect the working tributary slots and not the protection tributary slots can be restored using a span switch. Four-fibre rings should use span switching when possible so that multiple span switches can coexist. Therefore, span switching has priority over ring switching for bridge requests of the same type (e.g., signal fail (SF), signal degrade (SD), and forced switch (FS)). Lower priority span switches shall not be maintained in the event of a higher priority ring bridge request.

When a node determines that a switch is required, it sources the appropriate bridge request in the APS-bytes in both directions, i.e., the short path and long path.

In the case of unidirectional failures, signalling on the short path may permit faster switch completion. Since the node across the failed span will typically see the short-path bridge request much sooner than the long-path bridge request status (or bridge request), it can initiate its own bridge requests more quickly. In the case of span bridge requests on four-fibre rings, signalling on the long path informs other nodes on the ring that a span switch exists elsewhere on the ring. This mechanism denies lower priority ring switches.

The destination node is the node that is adjacent to the source node across the failed span. When a node that is not the destination node receives a higher priority bridge request, it enters the appropriate pass-through state. In this way, the switching nodes can maintain direct APS-byte communication on the long path. Note that in the case of a bidirectional failure such as a cable cut, the destination node would have detected the failure itself and sourced a bridge request in the opposite direction around the ring.

When the destination node receives the bridge request, it performs the bridge. If the bridge request is of a ring type, the node bridges the channels that were entering the failed span onto the protection channels in the opposite direction. In addition, for signal fail-ring switches, the node also performs the switch to protection channels.

For example, consider a section of a ring consisting of four nodes, A, B, C, D, where the span between B and C has failed. This situation is illustrated in Figure 7-7. In a two-fibre ring, B will bridge the normal traffic from OPUk tributary slots numbered 1 to N/2 (working) that were being transmitted from B to C onto OPUk tributary slots (N/2) + 1 to N (protection) being transmitted from B to A and around the ring ultimately back to C. This action is referred to as a bridge. C will switch the normal traffic from protection channels received from B by way of A back onto the working channels toward D. This action is referred to as the switch.

If the ring switch in this example is on a four-fibre ring, B will bridge the normal traffic from tributary slots that were being transmitted on the working fibre from B to C onto the tributary slots being transmitted on the protection fibre from B to A. Similarly, C will switch the normal traffic from tributary slots on the protection fibre received from D onto the tributary slots transmitted on the working fibre to D.

The end result for this example is that all the normal traffic on tributary slots that were being sent from B to C across the failed span are now sent from B to C the long way around the ring through nodes A and D. Symmetrical actions will take place to restore the normal traffic on tributary slots that were being sent from C to B.

When the failure has cleared, the nodes sourcing those bridge requests will drop their respective requests and switches. Other nodes on the ring will stop passing through the normal traffic on protection tributary slots and the APS-bytes. In general, normal traffic only reverts from the protection tributary slots back to the working tributary slots. Specifically, in a four-fibre ring, if a ring switch is active on the long-path protection channels, and the short-path protection tributary slots become available, the service will not be switched to the short-path protection tributary slots unless a new bridge request pre-empts the long-path protection tributary slots.

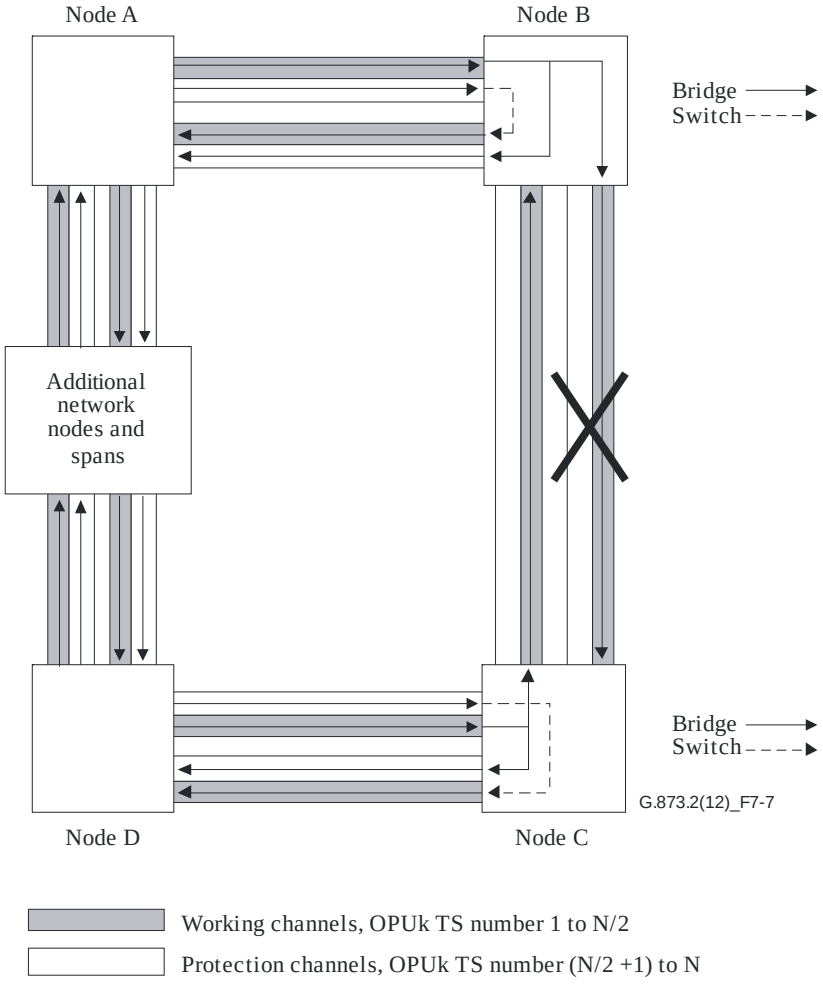
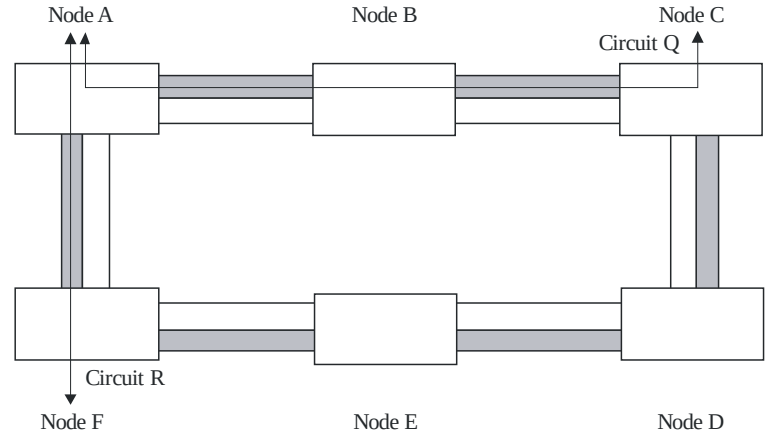


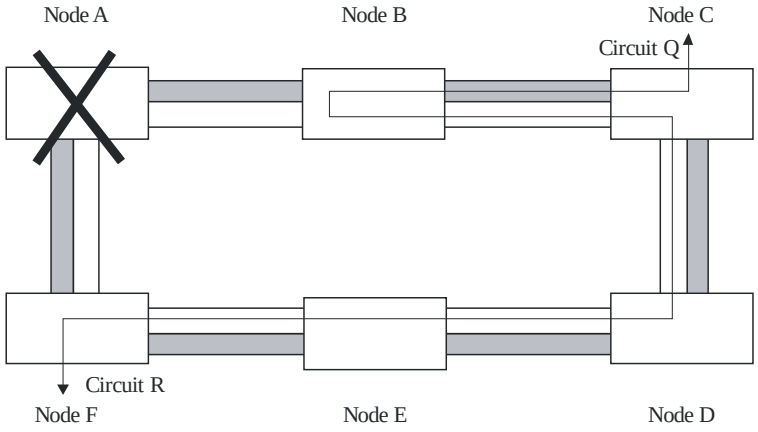
Figure 7-7 – Bridge and switch in a two-lambda ODU SRP-p

Ring and span switches can be pre-empted by bridge requests of higher priority as determined by Table 7-1 in relation to the status info given in clause 7.2.3.1. For example, consider that a span switch is up due to a signal degrade on that span, and a ring switch is required due to a failure on another span that affects both the working and protection tributary slots. A ring bridge request will be generated, the span switch dropped, and the ring switch established.

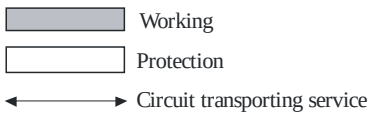
Externally initiated commands that are denied or pre-empted due to a higher priority APS request at that node are not allowed to pend.



a) Normal state before node failure



b) Misconnection after node failure



Circuit	Time-slot assignment	Entity
Q	1W	Working
R	1W	Working

NOTE – Under the "Time-slot assignment" column, the designation "1W" indicates that it is the first time slot in the capacity reserved for working.

Figure 7-8 – Example of misconnection

As soon as a request of higher priority than the no request (NR) priority is received by the node, and only if that request is a ring request other than exercise ring (EXER-R) or requires the usage of the protection tributary slots carrying the extra traffic, then the extra traffic is pre-empted.

If a ring switch exists and a failure of equal priority occurs on another span requiring a ring switch (including the combination of signal fail (ring) (SF-R) and forced switch (ring) (FS-R)), then, if the priority of the bridge request is SF-R or higher, both ring switches shall be established resulting in the ring segmenting into two separate segments. Otherwise, if the priority of the bridge requests is lower than SF-R, the new bridge request shall not be established and the first switch shall be dropped.

In general, proper operation of the ring relies on all nodes having knowledge of the state of the ring, so that nodes do not pre-empt a bridge request unless they have a higher priority bridge request. In order to accommodate this ring state knowledge, signalling over the long path during a bridge request, in addition to the short path, shall be used. For example, although span bridges can be established with only short-path signalling, a bridged indication is sent on the long path in order to inform other nodes of the state of the ring. In addition, management plane and/or control plane messages transported over the GCC can be used to determine the details regarding the condition of the ring.

7.2.1.1 Extra traffic

During fault-free conditions, it is possible to use the protection tributary slots to carry additional pre-emptible unprotected traffic. This additional traffic, which is referred to as extra traffic, has lower priority than the normal traffic on the working tributary slots and has no means for protection. The extra traffic is set up by provisioning the add- and drop-nodes for the traffic. Intermediate nodes along the ring are provisioned so that the extra traffic ODUk signals in protection tributary slots are passed through the node (protection tributary slots that are not carrying extra traffic are terminated at the intermediate nodes). Nodes that are inserting, dropping, or passing through extra traffic indicate its presence on those spans by inserting the extra traffic code in APS byte 1 bits 6-8. Note that NUT is not considered extra traffic, and as such, shall not set the ET code.

When it becomes necessary to bridge the normal traffic onto the protection tributary slots (due to a failure or an externally initiated command) the extra traffic is pre-empted and dropped on the spans whose protection tributary slots are required for the protection switch. Extra traffic circuits that have their source removed by this pre-emption shall be squelched with ODU-AIS. When the affected nodes return to the idle state, the extra traffic is restored.

7.2.1.2 Squelching to avoid misconnected traffic

In order to perform a ring switch, the protection tributary slots are essentially shared among each span of the ring. Also, extra traffic may reside in the protection tributary slots when the protection tributary slots are not currently being used to restore normal traffic transported on the working tributary slots. Thus, each protection tributary slot is subject to use by multiple services (services from the same tributary slot but on different spans, and service from extra traffic). With no extra traffic on the ring, under certain multiple point failures, such as those that cause node(s) isolation, services (from the same time slot but on different spans) may contend for access to the same protection tributary slot. This yields a potential for misconnected traffic. With extra traffic on the ring, even under single point failures, normal traffic on the working tributary slots may contend for access to the same protection tributary slot that carries the extra traffic. This also yields a potential for misconnected traffic.

Without a mechanism to prevent misconnection, the following failure scenario would yield misconnections. Referring to Figure 7-8, a cut in both the spans between nodes A and F and between nodes A and B (isolating node A) causes circuits Q and R to attempt to access time slot #1P on the protection channels.

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 bytes. 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. Potential misconnections shall be squelched by inserting the appropriate ODU-AIS in those tributary slots where misconnected traffic can occur. Specifically, the traffic that is sourced or dropped at the node(s) isolated from the ring by the failure shall be squelched. For rings operating at an ODUj level, this squelching occurs at the switching nodes. ODU level squelching occurs for the normal or extra traffic into or out of the

protection tributary slots (i.e., normal traffic into or out of working tributary slots is never squelched). For rings using ODUi (i,j) access, squelching locations are under study.

For example, consider a segment of a ring consisting of three nodes, A, B, and C where B has failed. In a typical scenario, both A and C will send bridge requests destined for B. When A sees the bridge request from C, and sees that B is between A and C (from the node map) it can deduce that B is isolated from the ring. A and C will use their respective maps to find out which tributary slots carry ODU signals that are added or dropped by B. A and C will squelch these ODU signals before the ring switch is performed by inserting ODU-AIS. Thus, any node on the ring that was connected to B will now receive AIS on those tributary slots.

Each of the ring maps, then, shall contain at minimum:

1) a ring map that contains information regarding the order in which the nodes appear on the ring;
2) a cross-connect map that contains the OPUk tributary slot assignments for traffic that is both terminated at that node and passed-through that node;
3) a squelch table that contains, for each of these OPUk tributary slots, the node addresses at which the traffic enters and exits the ring; and
4) an optional indication of whether the ODUj is being accessed at the ODUi level somewhere on the ring.

An example of such ring maps is given in Figures 7-2 and 7-3. For ODUi access, the map requirements are under study.

An ODU SRP may, as an option, support unidirectional traffic. Unidirectional traffic may be one of the following:

– a simple directed connection sourced in one node and terminated in another node;
– a multiply dropped circuit (such as the drop and continue used in ring interworking (see clause 8);
– a multiply sourced circuit (such as the reverse direction of the drop and continue direction of a ring interworking circuit).

In the event of a node failure, the squelching performed for these circuits is based only on the following:

– (for a simple directed connection) the failure of the source node or the failure of the destination node;
– (for a multiply dropped circuit) the failure of the source node or the failure of the last drop node;
– (for a multiply sourced circuit) the failure of the first source node or the failure of the destination node.

In order to prevent the misconnection of extra traffic, the bridge or switch operations are not executed until the switching nodes are informed that the ET code has been removed from the spans required for the protection switch.

A node that pre-empts extra traffic should squelch the extra traffic ODU on the tributary slots that are pre-empted in the following manner:

– for a node executing a span switch that pre-empts extra traffic on that span, extra traffic is squelched by inserting ODU-AIS on extra traffic tributary slots from that span that are dropped at that node (i.e., on the low-speed side), and inserting ODU-AIS on extra traffic tributary slots from that span that pass through the node (i.e., on the high-speed side), as long as those protection tributary slots are not required for a protection switch.

– for a node executing a ring switch, extra traffic is squelched by inserting ODU-AIS on extra traffic tributary slots that are dropped at that node (i.e., on the low-speed side).
– for a node entering full pass-through, extra traffic is squelched by inserting ODU-AIS on extra traffic tributary slots that are dropped at that node (i.e., on the low-speed side).

7.2.2 Switch initiation criteria

The requests to perform protection switching can be initiated either externally or automatically. Externally initiated commands are entered by way of the operations system (OS) or the craftsperson interface. Clause 7.2.2.1 describes these externally initiated commands available at the OS, craftsperson, or both interfaces. Automatically initiated commands can also be initiated based on ODUk (HO ODU) path or ODUj (LO ODU) tandem connection and equipment performance criteria, received bridge requests, and received bridge request status information. Clause 7.2.2.2 provides the automatically initiated command criteria.

The bridge requests related to span switching (except for lockout of protection) are used only for four-fibre ODU shared ring protections.

The no request (NR) code is transmitted when there is no need to use the protection channels.

7.2.2.1 Externally initiated commands

Externally initiated commands are initiated at an network element (NE) by either the OS or the craftsperson. The externally initiated command may be transmitted to the appropriate NE via the APS bytes, the telecommunication(s) management network (TMN), or over the local craftsperson interface. The bridge requests are evaluated by the priority algorithm in the protection switching controller.

7.2.2.1.1 Commands not signalled on the APS channel

The descriptions of the externally initiated commands are provided below.

clear: This command clears the externally initiated command and wait-to-restore (WTR) at the node to which the command was addressed. The NE-to-NE signalling following removal of the externally initiated commands is performed using the 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 only have traffic that does not need protection. These commands are not time critical (i.e., they do not need to be completed in tens of milliseconds). Thus, they can be transmitted over the management system to each affected NE.

NOTE – When PCC usage is standardized in the future, the ODU PCC byte can be used to transmit them to the affected destination NEs (see clause 7.2.3.2).

lockout of working tributary slots – ring switch: This command prevents normal traffic from working tributary slots over the addressed span from accessing the protection tributary slots for a ring switch. It does this 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 tributary slots. 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 tributary slots for any other span. For example, the node can go into any of the pass-through modes.

lockout of working tributary slots – span switch: This command prevents the normal traffic from the working tributary slots over the addressed span from accessing the protection tributary slots for a span switch. If any normal traffic is already on protection, the span switch is dropped regardless of the condition of the working tributary slots. 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 tributary slots for any other span.

lockout of protection – all spans: This command prevents protection switching on the entire ring. If any normal traffic is using the protection facility on any span, this command causes normal traffic to switch back to the working tributary slots regardless of the condition of the working tributary slots. Note that the APS bytes do not support this command. Thus, these command have to be sent to each of the NEs via the PCC or the management system transmitting them to each individual NE. The lockout of protection – all span request is used by each NE to coordinate activities with the far end.

7.2.2.1.2 Commands using the APS bytes

The following commands are carried over the APS bytes.

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 from working tributary slots to the protection tributary slots 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 tributary slots, unless the protection tributary slots are satisfying a higher priority bridge request.

Forced Switch to protection – Span (FS-S): This command switches the normal traffic from the working tributary slots to the protection tributary slots of that span. This switch occurs regardless of the state of the protection tributary slots, unless the protection tributary slots are satisfying a higher priority bridge request, or a signal failure (or a APS- failure) exists on the protection tributary slots of the span.

Manual Switch to protection – Ring (MS-R): This command performs the ring switch of the normal traffic from the working tributary slots to the protection tributary slots 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 tributary slots are not in an SD condition and are not satisfying an equal or higher priority bridge request (including failure of the protection tributary slots).

Manual Switch to protection – Span (MS-S): This command switches the normal traffic from the working tributary slots to the protection tributary slots for the same span over which the command is initiated. This occurs if the protection tributary slots are not in an SD condition and are not satisfying an equal or higher priority bridge request (including failure of the protection tributary slots).

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

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

NOTE – Undetected failures are a concern since they do not manifest themselves until a switch is made. This situation makes the protection facility unavailable when it is most needed. In a ODU shared ring protection, because the protection facility is shared among all the nodes on the ring, the exerciser function is even more essential. An undetected failure in one span makes ring switching impossible for all the spans on the ring. Thus, the probability of having undetected failures is reduced by exercising the protection switch controller. If a controller failure is detected during an exercise or any diagnostic routine, unless the failure is service affecting, no protection switching request is initiated. An alarm is generated to facilitate prompt repair.

7.2.2.2 Automatically initiated commands

APS requests are also initiated based on HO ODU path or LO ODU tandem connection and equipment performance criteria detected by the NE. All the working and protection tributary slots are monitored regardless of the failure or degradation conditions (i.e., after a switch has been completed, all appropriate performance monitoring is continued). The NE initiates the following bridge requests automatically: signal failure (SF), signal degrade (SD), reverse request (RR), and wait-to-restore (WTR). The bridge requests are transmitted from NE to NE (not from OS to NE).

The SF bridge request is used to protect normal traffic affected by defects, while the SD bridge request is used to protect against signal degradations due to bit errors. The bridge requests are transmitted on both the short and long paths. Each intermediate node verifies the destination node ID of the long-path bridge request and relays the bridge request. The destination node receives the bridge request, performs the activity according to the priority level, and sends the bridged indication.

The WTR bridge request is used to prevent frequent oscillation between the protection tributary slots and the working tributary slots. The intent is to minimize oscillations, since hits are incurred during switching. The WTR bridge request is issued after the clearing of the defect condition on the working tributary slots. The WTR is issued only after an SF or an SD condition and, thus, does not apply for externally initiated commands.

NOTE – There is an issue with interworking the protection scheme with wavelength division multiplexing (WDM) systems. The issue occurs when four-fibre shared protection ring (spring) traffic is carried over a WDM system and, depending upon the order of repair of a failed WDM link, it may cause the protection scheme to "flap" between worker and protection. This issue is currently under study.

The definitions of the automatically initiated bridge requests and their trigger conditions are provided below.

Signal Fail – Span (SF-S): An SF is defined as the presence of the trail signal fail (TSF) condition generated by the ODUkP or ODUkT trail termination function defined in [ITU-T G.798]. The tail-end detects the failure and generates the bridge request. For four-fibre rings, if the failure affects only the working tributary slots, traffic can be restored by switching to the protection tributary slots on the same span. The SF-S bridge request is used to initiate span switching for an SF on the working tributary slots of a four-fibre ring.

Signal Fail – Ring (SF-R): For two-fibre rings, all SFs (as defined previously for span switching) are protected using the ring switch. For four-fibre rings, the ring switch is used only if traffic cannot be restored using span switching. If failures exist on both the working and protection tributary slots 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 four-fibre ring, 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 entity:

– 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 tributary slots are in a SF state (as defined previously for span switching). SF-P is used only for four-fibre rings.

Signal Degrade – Span (SD-S): Signal degrade is defined as the presence of the trail signal degraded (TSD) condition generated by the ODUkP or ODUkT trail termination function defined in [ITU-T G.798]. In four-fibre rings, the working tributary slots on the degraded span can be protected using the protection tributary slots on the same span. This bridge request is used to switch the normal traffic to the protection tributary slots in the same span where the failure is located.

Signal Degrade – Ring (SD-R): For two-fibre rings, any degraded ODUk (HO ODU) path or ODUj (LO ODU) tandem connection is protected using the ring switch (where degradation is defined above under SD-S). For four-fibre rings, an 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 an NE detects a degradation on its protection tributary slots, and there are no higher priority bridge requests existing on the working tributary slots (Degradation is defined above under Signal Degrade – Span). This bridge request is used only for four-fibre rings.

Reverse Request – Span (RR-S): This command is transmitted to the tail-end NE 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 NE 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 tributary slots 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.

7.2.3 Protection switch protocol

The 3-byte ODU APS overhead shall be used for protection switching. See clause 7.2.4 for details on the operational usage of these bytes.

ODU APS shall be transmitted within the ODUk (HO ODU) path or ODUj (LO ODU) tandem connection overhead of the OTUk that is carrying the protection tributary slots.

ODU APS bytes shall be accepted as valid only when identical bytes are received in three consecutive frames.

7.2.3.1 APS Bytes 1 to 3

There are three bytes available in each ODUk frame for APS with an 8-frame multi-frame structure as specified in [ITU-T G.709]. For ODU SRP-1, TCM APS level 6 (110) is used. For ODU SRP-p, Path APS level 0 (000) is used.

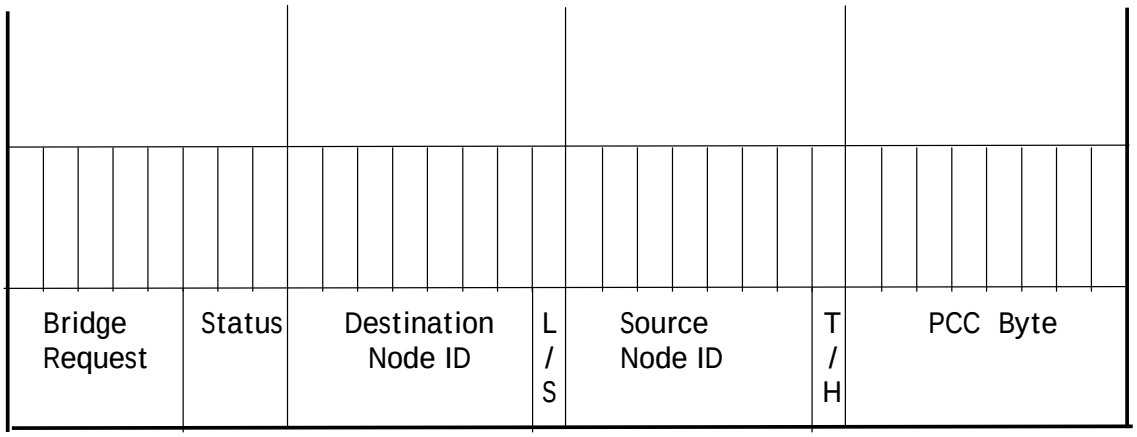


Figure 7-9 – APS/PCC format for ODU SRP signalling

The first five bits indicate the APS request type as follows in Table 7-1:

Table 7-1 – Types of request

Request	Meaning	Order
11111	Lockout of Protection (Span) LP-S	Highest
11110	Signal Fail (Protection) SF-P	↑
11101	Forced Switch (Span) FS-S	
11100	unused	
11011	Forced Switch (Ring) FS-R	
11010	unused	
11001	unused	
11000	Signal Fail (Span) SF-S	
10111	unused	
10110	Signal Fail (Ring) SF-R	
10101	unused	
10100	Signal Degrade (Protection) SD-P	
10011	unused	
10010	Signal Degrade (Span) SD-S	
10001	unused	
10000	Signal Degrade (Ring) SD-R	
01111	Manual Switch (Span) MS-S	
01110	unused	
01101	Manual Switch (Ring) MS-R	
01100	unused	
01011	unused	
01010	Wait-To-Restore WTR	
01001	Exerciser (Span) EXER-S	

Table 7-1 – Types of request

Request	Meaning	Order
01000	unused	
00111	Exerciser (Ring) EXER-R	
00110	unused	
00101	unused	
00100	Reverse Request (Span) RR-S	
00011	unused	
00010	Reverse Request (Ring) RR-R	
00001	unused	↓
00000	No Request NR	Lowest

Additional fields in the APS bytes are as follows:

Status:
Indicates the status of the node sending the request. Codes:

1xx reserved for future applications

011 Extra Traffic on protection channels

010 Bridged and Switched (Br&Sw)

001 Bridged (Br)

000 Idle

Destination Node ID:

The destination node ID is set to the value of the ID of the node for which the APS bytes are destined. The destination node ID is always that of an adjacent node (except for default APS bytes):

L/S:
Indicates whether the bridge request is a short path or a long path request. Codes:

0 Short path code (S)

1 Long path code (L)

Source Node ID:

The source node ID is set to the value of the ID of the node that sources the APS bytes (exception: default APS bytes):

T/H:
Indicates whether the source node acts as a tail end node or a head end node for the sent bridge request.

0 is head end node (H)

1 is tail end node (T)

This is used to be able to detect whether a signalled long-path ring bridge request is also locally present at that node. See also the detailed rules for using this code and when to evaluate it as additional information.

APS bytes will be inserted and recovered for the TCM level where monitoring occurs for the ring. Nodes in pass-through state need to be able to forward APS bytes from one adjacent span into the other adjacent span (TCM level 6 proposed) TCM levels.

In addition to the matrix connections for the normal and extra traffic signals as configured, each node must be able to make the following matrix connections:

- Bridge/Select an added/dropped normal traffic signal to/from the protection channel in the same direction (span switch)
- Bridge/Select a through connected normal traffic signal to/from the protection channel in the same direction (span switch)
- Bridge/Select an added/dropped normal traffic signal to/from the protection channel in the opposite direction (ring switch)
- Bridge/Select a through connected normal traffic signal to/from the protection channel in the opposite direction (ring switch, not necessary for the steering method)
- Multiple added/dropped circuits will require additional bridging and service selection
- Through-connect the protection channel between east and west (ring switch)
- Squelch ET signals when any portion of the path has been used for another purpose

These circuits might also include nodes with through connections if the ring has more nodes than the current traffic topology would require.

7.2.3.2 PCC byte

One byte is available for protection communication with an 8-frame multi-frame structure as specified in [ITU-T G.709]. For ODU SRP-1, TCM PCC level 6 (110) is used. For ODU SRP-p, Path PCC level 0 (000) is used.

The use of the byte is for further study.

7.2.4 Protection algorithm operation

This clause is structured as follows:

First, a number of general APS algorithm rules are given, followed by detailed rules. Clause 7.2.4.1 covers the three classes of ring node APS states, and the steady-state behaviour of the node in these states. Clause 7.2.4.2 describes the transition rules among the different ring node APS states.

These rules apply conceptually to a single ODU shared ring protection APS controller operating at a node, and describes choosing switching and signalling actions for both sides of the node based on all incoming APS-byte signalling from both directions, detected failures on both sides, local equipment failures, and externally initiated commands. In general, this conceptual controller considers all incoming information, chooses the highest priority input, and then takes action based on the chosen highest priority input.

Figure 7-10 illustrates the conceptual operation of an ODU shared ring protection APS controller.

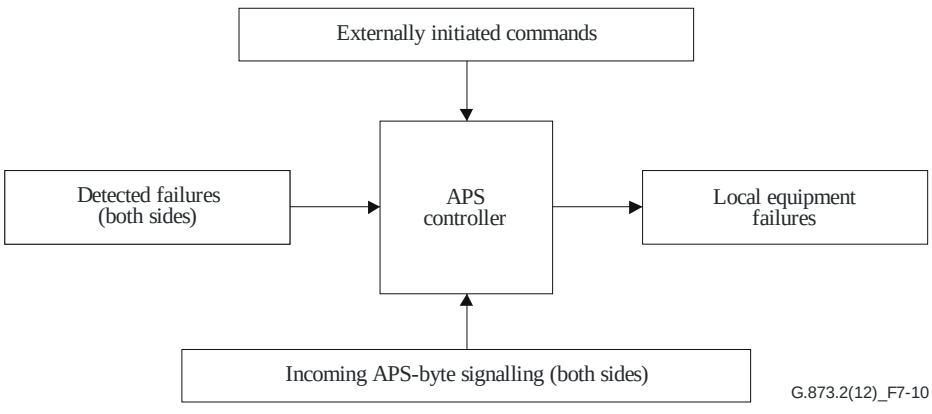


Figure 7-10 – Conceptual ODU shared ring protection APS controller

The following set of general rules apply:

Rule G #1 – BRIDGE REQUEST VALIDATION (where bridge request and bridge request status definitions are as follows):

Rule G #1a: (Bridge request) The information contained in APS byte 1 bits 1-5 shall be considered as a bridge request if:

– these bits indicate one of the ring bridge request codes and APS byte 2 bit 8 indicates a long-path code; or

– these bits indicate one of the ring bridge request codes and APS byte 2 bit 8 indicates a short-path code; or

– these bits indicate one of the span bridge request codes and APS byte 2 bit 8 indicates a short-path code.

Rule G #1b: (bridge request status) The information contained in APS byte 1 bits 1-5 shall be considered as a bridge request status if:

– these bits indicate one of the span bridge request codes and APS byte 2 bit 8 indicates a long path code.

Rule G #1.c: When a four-fibre ring node is in an SF-R or SD-R condition, and the SF-R or SD-R request cannot be signalled because it is not allowed to coexist with other higher priority APS requests at that node, then the node shall consider the detected or received protection entity condition as a second input to the APS controller.

The relationship among bridge request codes, bridge request status information, and APS-byte indications is shown in Table 7-2.

Table 7-2 – Relationships between APS byte2 bit 8 and APS byte1 bits 1-5

APS byte 2 bit 8code	APS byte1 bits 1-5	
	Ring bridge code	Span bridge code
Long path	Bridge request	Bridge request status
Short path	Bridge request	Bridge request

7.2.4.1 Ring node APS state

There are three classes of ring node states: the idle state, the switching state, and the pass-through state.

7.2.4.1.1 Idle state

A node is in the idle state when it is not sourcing or receiving any APS requests or bridge request status and it is receiving Idle or ET codes from both directions.

Rule I #1 – IDLE STATE SOURCED APS-BYTES:

Rule I #1a: Any node in the idle state not inserting, dropping, or passing through extra traffic shall source the APS-bytes in both directions as given in Table 7-3.

Table 7-3 – APS byte 1,2 and 3 values sourced in the idle state

Byte position	Value
APS byte 1 [1-5]	00000 (No Request code)
APS byte 2 [1-7]	Destination node ID
APS byte 3 [1-7]	Source node ID
APS byte 2 [8]	0 (short path code)
APS byte 1 [6-8]	000 (idle code)

Rule I #1b: Any node in the idle state inserting, dropping, or passing through extra traffic shall source the APS-bytes shown in Table 7-3 with the exception that APS byte 1 bits 6-8 transmitted over any span that contains extra traffic shall have the value 011 (ET code).

Until the node has knowledge of the ring map, it shall behave as per Rule I-S #3. Signalling in the start-up state is for further study.

Rule I #2 – IDLE STATE RECEIVED APS-BYTES: Any node in the idle state shall terminate APS in both directions.

7.2.4.1.2 Switching state

It is understood that a node not in the idle or pass-through states is in the switching state. This includes the default signalling status, e.g., node start-up, where there is no ring map available.

Rule S #1 – SWITCHING STATE SOURCED APS-BYTES:

Rule S #1a: Any node in the switching state shall source APS-bytes as shown in Table 7-4:

Table 7-4 – APS byte 1,2 and 3 values sourced by a node in the switching state

Byte position	Value
APS byte 1 [1-5]	Bridge Request (Status) code
APS byte 2 [1-7]	Destination node ID
APS byte 3 [1-7]	Source node ID
APS byte 2 [8]	0/1 (short-/long-path code)
APS byte1 [6-8]	Status code

Rule S #1b: Any node in the switching state (for either span or ring bridge requests) shall source a bridge request on the short path and a bridge request (or bridge request status) on the long path. Both the bridge request and the bridge request status have the same priority (or one of them is an RR), and protect the same span. Exceptions to this can occur when there are more than one switch requests active at a node. The exceptions are as follows:

– The isolated node cases described in Rules S #1c and S #1d.

– The case of a span bridge request on each side of the node, the node shall source a bridge request on each short path, where the status bits indicate the state of the bridge and switch for the corresponding span.

– The case of a ring bridge request pre-empting a span bridge request on an adjacent span as described in Rule S-S #2b.

– Cases where SF-P and SD-P coexist with a ring switch on the same span. Table 7-5 defines the signalling for these cases.

Table 7-5 – SD-P and SF-P coexisting with ring switches on the same span

Highest priority ring request	Short-path conditions		Priority signalled on short path
	Working	Protection	
FS-R	clear, SD, or SF	SF	SF-P
FS-R	clear, SD, or SF	SD	SD-P
FS-R	clear, SD, or SF	SF-P or SD-P (APS-byte)	RR-S
SF-R(APS-byte)	clear	SF	SF-P
SF-R(APS-byte)	clear or SD	SD	SD-P
SD-R(APS-byte)	clear	SD	SD-P
MS-R or EXER-R	clear	SF	SF-P
MS-R or EXER-R	clear	SD	SD-P
MS-R or EXER-R	clear	SF-Por SD-P (APS-byte)	RR-S

Rule S #1c: Whenever a node in the switching state terminates a new short-path APS-byte bridge request from an adjacent node, of equal or higher priority than the bridge request it is currently executing, over the same span, it shall source a bridge request of the same priority on the corresponding long path. Whenever a node receives ring bridge requests on both short paths from its adjacent nodes, the long-path bridge request shall be signalled rather than the short-path reverse requests. This rule takes precedence over Rule S #1b in case of multiple bridge requests at the same node (see Figure 7-11 a).

Rule S #1d: Whenever a node detects a condition requiring a ring switch or an externally initiated command for a ring switch applied at that node, it shall always source over the short path a short-path ring bridge request as long as the ring bridge request is not pre-empted by a higher priority bridge request (see Figure 7-11 b). This rule takes precedence over Rule S #1c. Note that whenever a node receives in one direction a short-path ring bridge request on one side and detects one of the above-mentioned conditions on the other side, it shall signal the bridge request associated with that condition (see Figure 7-11 c).

Rule S #1e: A node in the switching state shall insert the ET code in APS byte 1 bits 6-8 on spans that are carrying extra traffic.

Rule S #2 – SWITCHING STATE RECEIVED APS-BYTES: Any node in the switching state shall terminate APS in both directions.

Rule S #3 – UNIDIRECTIONAL BRIDGE REQUEST ACKNOWLEDGMENT: As soon as it receives a bridge request or bridge request status, the node to which it is addressed shall acknowledge the bridge request by changing APS byte 1 bits 1-5 to the RR code on the short path, and to the received bridge request priority on the long path.

Rule S #4 – ALLOWED COEXISTING COMPLETED PROTECTION SWITCHES:

Rule S #4a: The following switches are allowed to coexist:

– SD-P with any span switch;
– LP-S or SF-P with any span switch for other spans;
– SF-P or SD-P with any ring switch on the same span;
– LP-S with SD-P;
– LP-S with LP-S;
– SD-P with SD-P;

– FS-R with FS-R (ring split into multiple subrings);
– SF-R with SF-R (ring split into multiple subrings);
– FS-R with SF-R (ring split into multiple subrings);
– Any span switch with any other span switch.

Rule S #4b: When multiple equal priority bridge requests over different spans of SD-R, MS-R, or EXER-R exist at the same time, no bridge or switch shall be executed and existing switches and bridges shall be dropped. (Note that in case of multiple SD-R failures, all failures will be reported or alarmed. However, this behaviour can be considered as expected by the user.) The nodes shall signal the ring bridge request in APS byte 1, bits 1-5 and APS byte 1 bits 6-8 shall be set to Idle.

Rule S #5 – LOSS OF RING BRIDGE REQUEST: If a node executing a ring bridge and switch no longer receives a valid ring bridge request on the long path, it shall drop its ring bridge and switch, and shall signal and act based on its highest priority input.

Rule S #6 – LOSS OF SPAN BRIDGE REQUEST: If a node executing a span bridge and switch no longer receives a valid span bridge request (on the short path), it shall drop its span bridge and switch, and shall signal and act based on its highest priority input.

Rule S #7 – EXTRA TRAFFIC: A node in the switching state shall not pass through extra traffic, unless it is in the switching state due to an LP-S, SF-P, or SD-P request. A node in the switching state due to a WTR for a span switch, or any span request, except LP-S, SF-P, SD-P, or EXER-S, shall not source or terminate extra traffic on the short path of that bridge request. A node in the switching state due to WTR for a ring switch, or any ring request, except EXER-R, shall not source or terminate extra traffic.

Rule S #8 – WTR TERMINATION: Whenever a node in the WTR state drops its bridge and switch before the WTR timer expires, it shall immediately terminate the WTR and act based on its highest priority input.

Rule S #9 – A node in a ring switching state that receives the external command LOW-R for the affected span shall drop its bridge and switch and shall signal NR, SF-P, or SD-P. Upon the reception of NR in combination with either Idle or ET code or bridge request status from the span away from the LOW-R span, the node shall re-insert extra traffic that was pre-empted on that span.

Rule S #10 a: A span switching node shall insert the tail end node and head end node indication in accordance with usage of the RR-S signalling. If an RR-S span bridge request message is sent, it shall carry the head end node indication, and the same is true for a span bridge request status message sent for the same span. If a span switching node does not send RR-S, it shall send its span bridge request and span bridge request status messages with the tail end node indication.

Rule S #10 b: A ring switching node which is either serving a locally applied external ring switch command or has locally detected failures which result or combine into a ring switch request for a span, shall insert the tail end node indication into its long-path ring bridge request message associated with this span. If a short-path ring bridge request message for the same span is sent, it shall have the same tail end node indication. When a span bridge request is sent on the short path, the tail-end node indication shall be sent for all span bridge requests other than RR-S. In these cases the node is acting as a tail-end node. In all other cases the ring switching node acts as a head end node and shall insert the head end node indication into long-path and short-path bridge request/bridge request status messages associated with this span.

Rule S #11 – A node shall ignore a long-path ring switch request with head end node indication addressed to it for the purpose of determining its highest priority input.

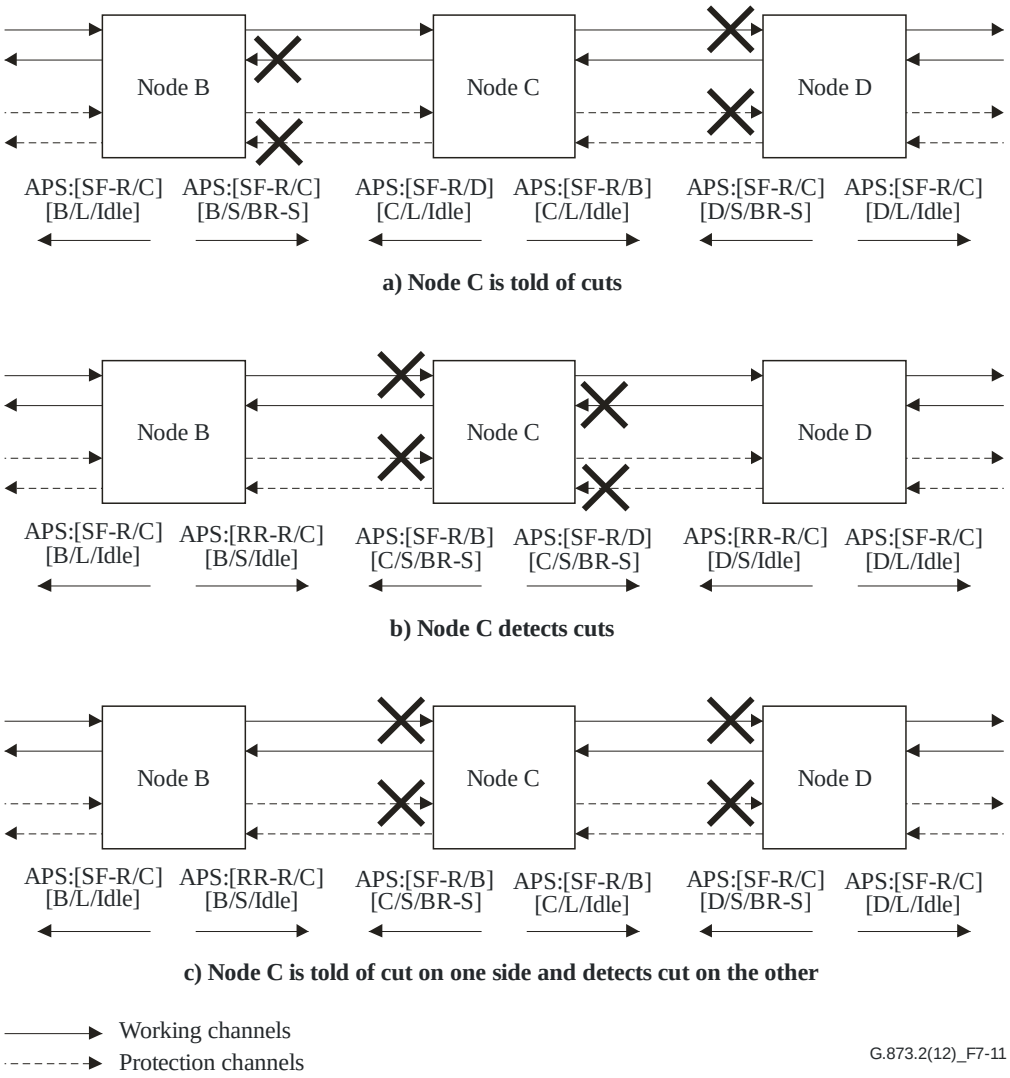


Figure 7-11 – Isolated node signalling (signalling states prior to nodes B and D establishing a ring bridge and switch)

7.2.4.1.3 Pass-through state

A node is in the pass-through state when its highest priority APS request is a bridge request or bridge request status not destined to or sourced by the node itself. The pass-through can be either unidirectional or bidirectional, depending on its nature. There are three types of pass-through: unidirectional full pass-through, bidirectional full pass-through, and APS-byte pass-through (see clause 3 for the definition of the different kinds of pass-through).

Rule P #1 – PASS-THROUGH STATE SOURCED AND RECEIVED APS-BYTES: When a node is in pass-through, it transmits on one side, all or part of the APS bytes, which it receives from the other side. A node in the APS-byte pass-through state shall source the ET code in bits 6-8 of APS byte 1 on spans that are carrying extra traffic. An APS-byte pass-through node receiving the ET code shall source Idle in the opposite direction if no extra traffic exists on the opposite span. A node in unidirectional full pass-through shall continue sourcing the previously sourced APS-bytes in the opposite direction, with the exception that APS byte 1 bits 6-8 shall reflect the appropriate status code.

Rule P #2 – REMAINING IN THE PASS-THROUGH STATE DURING SIGNALLING TRANSITIONS: When a node that is in a pass-through state receives a long-path ring bridge request destined to itself, and another long-path ring bridge request of the same priority destined to another node, the node shall not transit to another state. (This rule is necessary for the clearing sequence of the node failure condition. See Figure I.5.)

Rule P #3 – EXTRA TRAFFIC: A node in full pass-through shall not source or terminate extra traffic. A node that is in the APS-byte pass-through state can source, terminate, and pass-through extra traffic.

7.2.4.2 Ring node APS state transition rules

Clause 7.2.4.1 described the three ring node states. This clause describes the transition rules among these different states. Note that, as in linear APS, the following basic rules apply:

Rule Basic #1 – STATE TRANSITION TRIGGERS: All state transitions are triggered by an incoming APS-byte change, a WTR expiration, an externally initiated command, or locally detected ODUk (HO ODU) path or ODUj (LO ODU) tandem connection or equipment performance criteria.

Rule Basic #2 – APS-BYTE VALIDATION: Before accepting the APS-bytes as valid, the value shall be received identically in three successive frames.

Rule Basic #3 – APS byte 1 BITS 6-8 UPDATE: All bridge and switch actions shall be reflected by updating APS byte 1 bits 6-8, unless the span is carrying extra traffic. A node shall signal the ET code on any span that is carrying extra traffic.

Rule Basic #4 – APS requests due to a locally detected failure, an externally initiated command, or received APS-bytes shall pre-empt APS requests in the prioritized order given in Table 7-1, unless the bridge requests are allowed to coexist. Actions resulting from incoming bridge requests shall take priority over actions resulting from incoming bridge request status signalling regardless of the priority of each. Bridge request status signalling shall never pre-empt a bridge request.

7.2.4.2.1 Transitions between the idle and pass-through states

Rule I-P #1 – TRANSITION FROM THE IDLE STATE TO THE PASS-THROUGH STATE:

Rule I-P #1a: The transition from the idle state to the full or APS-byte pass-through states shall be triggered by a valid APS-byte change, in any direction, from the NR code to any other bridge request code, as long as the new bridge request is not destined for the node itself. Both directions move then into full or APS-byte pass-through, according to Rule I-P #1b.

Rule I-P #1b: For any span bridge request status or the EXER-R bridge request, the intermediate nodes on the long path shall go into APS-byte pass-through. Actions taken at an intermediate node upon receiving a valid ring bridge request other than EXER-R are:

– for NEs without extra traffic, when the node in the idle state receives a valid ring bridge request in any direction that is not destined for the node itself, the node shall enter the bidirectional full pass-through state;

– for NEs with extra traffic, when the node in the idle state receives a valid ring bridge request in any direction that is not destined for the node itself, the node shall drop extra traffic bidirectionally, and shall enter unidirectional full pass-through, in the direction of the bridge request only. Upon receiving the crossing APS-bytes, the node shall enter bidirectional full pass-through.

Rule I-P #2 – TRANSITION FROM THE PASS-THROUGH STATE TO THE IDLE STATE: A node shall revert from any pass-through state to the idle state when it detects NR codes in APS Byte1 bits 1-5and Idle or ET codes in APS byte 1 bits 6-8, from both directions. Both directions revert simultaneously from the pass-through state to the idle state. Extra traffic that was pre-empted shall be re-inserted and the ET code sourced as defined in Rule I #1b.

7.2.4.2.2 Transitions between the idle and switching states

Rule I-S #1 – TRANSITION FROM THE IDLE STATE TO THE SWITCHING STATE:

Rule I-S #1a: Transition of an NE from the idle state to the switching state shall be triggered by one of the following conditions:

– a valid APS-byte change from the NR code to any ring bridge request code received on either the long path or the short path and destined to that NE;

– a valid APS-byte change from the NR code to any span bridge request code received on the short path and destined to that NE;

– an externally initiated command for that NE;

– the detection of a failure at that NE.

Rule I-S #1b: Actions taken at a switching NE upon receiving a valid bridge request are (Note that in order to execute a ring bridge and switch, the bridge request shall be received on the long path. See Rule I-S #1c):

– for FS-R bridge requests, the node shall check if there is a need for squelching and squelch accordingly, execute a bridge and insert the bridged code in APS byte 1 bits 6-8 in both directions. Upon receiving a bridged code in APS byte 1 bits 6-8 on the bridge request path, the NE shall execute a switch and update APS byte 2 bits 6-8 on both paths accordingly;

– for SF-R bridge requests, the node shall check if there is any need for squelching and squelch accordingly, execute a bridge and switch, and insert in APS byte 1 bits 6-8 the bridged and switched code on both the long and the short path;

– for all other bridge requests, except SD-P, EXER-S, EXER-R, SF-P, and LP-S, the node shall execute a bridge and insert the bridged code in APS byte 2 bits 6-8 in both directions. Upon receiving a bridged code in byte APS byte 2 bits 6-8 on the bridge request path, the NE shall execute a switch and update APS byte 2 bits 6-8 on both paths accordingly;

– for SD-P, EXER-S, EXER-R, SF-P, and LP-S, the node shall signal as for any other bridge request, but shall not execute the bridge or switch. See clause 7.1.2;

– extra traffic shall be dropped immediately on all spans for a ring switch, or on the span whose protection channels are required for a span switch;

– no bridge or switch shall be executed while the ET code is received on the span whose protection channels are required by that bridge and switch.

Rule I-S #1c: A span switch shall be put up or brought down only with short-path bridge requests. A ring switch shall be put up or brought down only with long-path bridge requests.

Rule I-S #2 – TRANSITION FROM THE SWITCHING STATE TO THE IDLE STATE: A node shall revert from the switching state to the idle state when it detects NR codes in APS byte 1 bits 1-5 and Idle or ET codes in APS byte 1 bits 6-8 from both directions. The transition from the switching state to the idle state shall be a three-step transition.

– Step 1: When a WTR time expires or an externally initiated command is cleared at a node, and the node receives an RR from the short span, the node shall drop its switch, and signal the NR code in APS byte 1 bits 1-5, and the bridged code in APS byte 1 bits 6-8. (Note that this step may be executed in transitions from the switching state to the pass-through state.)

– Step 2: Upon reception of the NR code, and of the indication that the switch has been dropped, the head-end node shall drop its bridge and its switch, and source the Idle code in both directions. The indication that the switch has been dropped is received on the short path for span bridge requests, and on the long path for ring bridge requests.

– Step 3: Once the tail-end detects incoming Idle codes, it shall also drop its bridge and switch and source the idle code in both directions. Extra traffic that was pre-empted shall be re-inserted and the ET code sourced as defined in Rule I #1b. An SF-P code due to a signal fail – protection that was pre-empted, shall be re-inserted.

– Step 4: Once the head-end detects incoming Idle or ET codes from both directions, it shall revert to the idle state. Extra traffic that was pre-empted shall be re-inserted and the ET code shall be sourced as defined in Rule I #1b. An SF-P code due to a signal fail – protection that was pre-empted shall be re-inserted.

– Note that there are cases in which no bridge or switch is to be executed due to other conditions on the ring. In these cases, the NE that initiated the request (i.e., tail-end) shall signal the NR code. Upon reception of the NR code, the head-end shall also source the Idle code.

Rule I-S #3 – A node shall transmit the default APS code until it is capable of proper APS signalling in accordance with the current state of the ring. The default APS code shall be used to indicate that the node cannot properly signal APS bytes, and therefore cannot properly execute protection switching.

Rule I-S #4 – A ring (span) switching node receiving the default APS code on the short (long) path shall not change its signalling or take any action associated with that path until proper APS codes are received. A ring (span) switching node receiving default APS code on the long (short) path shall drop its bridge and switch.

Rule I-S #5 – A switching node that is not bridged or switched that receives long-path ring bridge requests destined to itself from both of its neighbours shall take no action based on these bridge requests.

Rule I-S #6 – If a switching node receives from both directions the APS bytes that it is sourcing, and receives no other APS request, it shall transition to the idle state. Otherwise, the switching node shall signal according to its highest priority input.

Rule I-S #7 – When a node receives a RR code over the span which it is protecting, and when that same node is sending a RR code, it shall drop its bridge and switch as described in Rule I-S #2, except for bridge request status or bridge requests of signal failure and signal degrade priority. For signal failure and signal degrade, the node shall drop the switch and the bridge after the expiration of the WTR time according to Rule S-S #3.

7.2.4.2.3 Transitions between switching states

This clause first provides a set of requirements and objectives with which each ring node shall comply to be able to perform a switch without creating misconnections, and then provides the set of rules necessary to coordinate a transition between switching states.

7.2.4.2.3.1 Ring map and squelch table information

Each node on a ring shall maintain a ring map describing the ring connectivity, and a local squelch table indicating the source and destination of all added, dropped, and pass-through ODUs.

7.2.4.2.3.2 Squelching

ODU squelching shall be performed at the switching nodes by inserting ODU-AIS.

The switching node shall, by comparing APS-byte addresses (crossing APS-bytes) to the information contained in the ring map, identify which nodes are missing. From this information and the information in the squelch table, it shall identify which ODUs are added and dropped at these nodes and shall squelch them bidirectionally.

7.2.4.2.3.3 Transition rules

The following transition rules apply:

Rule S-S #1 – TRANSITION FROM THE SWITCHING STATE TO THE SWITCHING STATE:

Rule S-S #1a: When an NE that is currently executing an SF-R switch receives another SF-R or FS-R bridge request over the long path not destined to that NE, the NE shall check if there is any need for squelching and squelch accordingly. The NE shall stop squelching when the bridge and switch are dropped.

Rule S-S #1b: When an NE that is currently executing an FS-R switch receives another FS-R or SF-R bridge request over the long path not destined to that NE, the NE shall check if there is any need for squelching and squelch accordingly. The NE shall stop squelching when the bridge and switch are dropped.

Rule S-S #1c: When an NE that is currently executing any ring switch receives a higher priority ring APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) for the same span, it shall upgrade the priority of the ring switch it is executing to the priority of the received ring bridge request.

Rule S-S #1d: When an NE that is currently executing any span switch receives a higher priority span APS request (due to a locally detected failure, an externally initiated command, or a span bridge request destined to it) for the same span, it shall upgrade the priority of the span switch it is executing to the priority of the received span bridge request.

Rule S-S #1e: When a NE that is currently executing an EXER-R request receives a higher priority ring APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) for the same span, it shall remove any extra traffic. The node shall then execute the new ring APS request as detailed in Rule I-S #1.

Rule S-S #1f: When a NE that is currently executing an EXER-S request receives a higher priority span APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) for the same span, with the exception of LP-S, SF-P, and SD-P, it shall remove any extra traffic from the short path. It shall then signal the new span bridge request with the Idle code in APS byte 1 bits 6-8 on the short path, and the new span bridge request on the long path. If there is extra traffic on the long path, the ET code shall be signalled in APS byte 1 bits 6-8. The node shall then execute the new span APS request as detailed in Rule I-S #1.

Rule S-S #2 – SWITCH PRE-EMPTION:

Rule S-S #2a: When an NE that is currently executing a span switch receives a ring APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) destined to it of greater priority for the same span, it shall:

– drop the span bridge and switch immediately;

– execute the ring APS request (as detailed in Rule I-S #1).

Rule S-S #2b: When a node that is currently executing a span switch receives a ring APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) destined to it for its adjacent span of greater priority than the span switch it is executing, it shall drop the span switch, signal NR in APS byte 1 bits 1-5 and bridged in APS byte 1 bits 6-8 in the direction of the span APS request, and signal the ring request in APS byte 1 bits 1-5 and idle in APS byte 1 bits 6-8 in the direction of the ring APS request.

Rule S-S #2c: When a node that is currently executing a span switch receives a long-path ring bridge request for a non-adjacent span of greater priority than the span switch it is executing, it shall drop the span switch and signal NR in APS byte 1 bits 1-5 and bridged in APS byte 1 bits 6-8 in both directions.

Rule S-S #2d: If a span switching node that is bridged and switched receives a NR and an indication that the switch has been dropped for that span, the node shall drop its bridge and switch, and, if the node's highest priority input is:

– a span bridge request status destined to the node itself, or NR, then the node shall source NR in APS byte 1 bits 1-5 and idle in APS byte 1 bits 6-8 in both directions;

– a span APS request (due to a locally detected failure, an externally initiated command, or a span bridge request destined to it) for an adjacent span, then the node shall signal in accordance with that request;

– a ring APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) for an adjacent span, then the node shall execute the ring bridge request;

– a long-path ring APS request destined to another node, then the node shall signal in accordance with either Rule S-P #1a or S-P #1b, depending upon whether or not the bridged indication is being received;

– a span bridge request status destined to another node, then the node shall signal in accordance with either Rule S-P #1c or S-P #1d, depending upon whether or not the bridged indication is being received;

– a span APS request (due to a locally detected failure or externally initiated command) for the same span, the node shall signal the span bridge request in APS byte 1 bits 1-5 and Idle in APS byte 1 bits 6-8.

Rule S-S #2e: If a span switching node that is bridged receives a NR and an indication that the switch has been dropped for that span, the node shall drop its bridge, and, if the node's highest priority input is:

– a span bridge request status destined to the node itself, or NR, then the node shall source NR in APS byte 1 bits 1-5 and Idle in APS byte 1 bits 6-8 in both directions;

– a span APS request (due to a locally detected failure, an externally initiated command, or a span bridge request destined to it) for an adjacent span, then the node shall signal in accordance with that request;

– a ring APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) for an adjacent span then the node shall execute that request;

– a long-path ring bridge request destined to another node, then the node shall signal in accordance with either Rule S-P #1a or S-P #1b, depending up whether or not the bridged indication is being received;

– a span bridge request status destined to another node, then the node shall signal in accordance with either Rule S-P #1c or S-P #1d, depending on whether or not the bridged indication is being received;

– a span APS request (due to a locally detected failure or externally initiated command) for the same span, the node shall signal the span bridge request in APS byte 1 bits 1-5 and idle in APS byte 1 bits 6-8.

Rule S-S #2f: When an NE that is currently executing a ring switch receives a span or ring APS request (due to a locally detected failure, an externally initiated command, or a span or ring bridge request destined to it) of greater priority for an adjacent span than the ring switch it is executing, it shall:

– drop the ring bridge and switch immediately;

– execute the higher priority APS request (as detailed in Rule I-S #1).

Rule S-S #2g: When an NE that is currently executing a ring switch receives a span APS request (due to a locally detected failure, an externally initiated command, or a span bridge request destined to it) of greater priority for the same span, it shall:

– drop the ring bridge and switch immediately;

– execute the span APS request.

Rule S-S #2h: For a four-fibre ring: If a ring switching node receives an APS request of higher priority than the ring APS request it is executing, and the two requests are not allowed to coexist, the node shall drop the lower priority request and consider its detected or received protection entity condition in addition to the higher priority request. If the detected or received request for the protection entity is allowed to coexist with the higher priority APS request, and if either the higher priority APS request is for a span switch on the adjacent span to the detected or received protection channel request, or if the higher priority APS request is for a ring switch for the same span as the detected or received protection channel request, then the node shall respond to both the protection channel request and the higher priority APS request on the respective spans. This rule takes precedence over Rule S-S #1c and Rule S-S #2f.

Rule S-S #3 – RING AND SPAN SWITCH CLEARING (NO PRE-EMPTION):

Rule S-S #3a: When a failure condition clears at a node, the node shall enter WTR and remain in WTR for the appropriate time-out interval, unless:

1) a different bridge request of higher priority than WTR is received; or

2) another failure is detected; or

3) an externally initiated command becomes active.

The node shall send out a WTR code on both the long and short paths.

Rule S-S #3b: When a node that is executing a switch in response to an incoming SD-S, SD-R, SF-S, or SF-R bridge request (not due to a locally detected failure) receives a WTR code (unidirectional failure case), it shall send out RR on the short path and WTR on the long path.

Rule S-S #4 – SPAN SWITCH TIME-OUT: For a two fibre/four-lambda or four-fibre/four-lambda ring, when it is not possible to execute an SD-S or SF-S bridge request because no acknowledgment is received on the short path (time-out, whose duration is an equipment issue), or because the protection channels become unavailable, including degradation or failure of the protection entity or LOW-S, the appropriate ring switch shall be attempted.

Rule S-S #5 – A switching node that receives ring bridge requests destined for itself from both of its neighbours shall drop its bridge and switch.

Rule S-S #6 – When an NE that is currently receiving an SF-P bridge request or is sourcing an SF-P SF-P bridge request because of a signal fail – protection receives an externally initiated ring bridge command or detects a failure of the working entity for the same span, it shall assume the priority of the ring bridge request.

7.2.4.2.4 Transitions between switching and pass-through states

Rule S-P #1 – SWITCH PRE-EMPTION RULES (switching state to pass-through state):

Rule S-P #1a: If a span switching node that is not bridged or switched is receiving a bridged code for that span, and its highest priority input is a long-path ring bridge request destined to another node, then the node shall signal NR in APS byte 1 bits 1-5 and idle in APS byte 1 bits 6-8 in both directions.

Rule S-P #1b: If a span switching node that is not bridged or switched receives an indication that the bridge has been dropped for that span, and its highest priority input is a long-path ring bridge request destined to another node, then:

– for NEs without extra traffic, the node shall enter bidirectional full pass-through;

– for NEs with extra traffic, the node shall drop extra traffic bidirectionally, and shall enter unidirectional full pass-through, in the direction of the bridge request only. Upon receiving the crossing APS-bytes, the node shall enter bidirectional full pass-through.

Rule S-P #1c: If a span switching node that is not bridged or switched is receiving a bridged code for that span, and its highest priority input is a span bridge request status destined to another node, then the node shall signal NR in APS byte 1 bits 1-5 and Idle in APS byte 1 bits 6-8 in both directions.

Rule S-P #1d: If a span switching node that is not bridged or switched receives an indication that the bridge has been dropped for that span, and its highest priority input is a span bridge request status destined to another node, then the node shall enter APS-byte pass-through. It shall then reinsert any extra traffic that had been pre-empted.

Rule S-P #1e: When a node that is currently executing a ring switch receives a long-path ring bridge request for a non-adjacent span of greater priority than the ring switch it is executing, it shall drop its bridge and switch immediately, then the node shall enter bidirectional full pass-through.

Rule S-P #1f: When a node that is currently executing a ring switch has as its highest priority input long-path ring bridge requests not destined to itself from both directions, it shall drop its bridge and switch immediately, then the node shall enter bidirectional full pass-through.

Rule S-P #1g: If a ring switching node that is not bridged or switched has as its highest priority input a span bridge request status destined to another node, then the node shall enter APS-byte pass-through. It shall then reinsert any extra traffic that had been pre-empted.

Rule S-P #2 – PASS-THROUGH TO SWITCHING TRANSITIONS:

Rule S-P #2a: The transition of a node from full pass-through to switching shall be triggered by:

1) an equal, higher priority, or allowed coexisting externally initiated command;

2) the detection of an equal, higher priority, or allowed coexisting failure;

3) the receipt of an equal, higher priority, or allowed coexisting bridge request destined to that NE;

4) the detection of an APS byte sourced by that NE.

Rule S-P #2b: The transition of a node from APS-byte pass-through to switching shall be triggered by:

1) any externally initiated command;

2) the detection of any failure;

3) the receipt of any bridge request destined to that NE.

Rule S-P #2c: If a node that was in the full pass-through state is now sourcing a span bridge request due to Rule S-P #2a, the node shall insert ODU-AIS on the protection channels on the span adjacent to the affected span, until the node receives an indication that the ring switch has been dropped.

Rule S-P #3 – If a node that was in the pass-through state due to a SF-R or FS-R request on the ring, and the node is now sourcing a SF-R or FS-R bridge request (due to Rule S-P #2a), the node shall:

1) determine if there is any need for squelching and squelch accordingly; and

2) execute the ring bridge and switch.

Rule S-P #4 – If a pass-through node receives from at least one direction an APS byte that has itself as the source ID, it shall source Idle in both directions.

7.2.4.2.5 Transitions between pass-through states

This clause provides the set of rules necessary to change from a APS-byte pass-through state to a full pass-through state, and vice versa.

The following transition rules apply:

Rule P-P #1 – TRANSITION FROM APS-BYTE PASS-THROUGH TO FULL PASS-THROUGH:

– For NEs without extra traffic, a node in APS-byte pass-through receives a long-path ring bridge request other than EXER-R not destined to itself, the node shall enter bidirectional full pass-through.

– For NEs with extra traffic, the node shall drop extra traffic bidirectionally, and shall enter unidirectional full pass-through in the direction of the bridge request only. Upon receiving the crossing APS-bytes, the node shall enter bidirectional full pass-through.

Rule P-P #2 – TRANSITION FROM FULL PASS-THROUGH TO APS-BYTE PASS-THROUGH: A node in bidirectional full pass-through that receives a span bridge request status not destined to itself from both directions shall enter APS-byte pass-through.

7.2.5 Examples

Appendix I describes how the above-mentioned rules apply in a set of basic examples.

7.3 Steering application of ODU shared ring protection

For further study.

8 Interworking architectures

This clause describes the interworking between multiple instances of protection architectures within the same network layer intersecting at one or more network nodes (e.g., two or more rings exchanging traffic within a single office).

8.1 Single node interconnection

Single node interconnection is an architecture between two rings where one node in each ring is interconnected.

This architecture (shown in Figure 8-1) has a single point of failure at the point where the rings are interconnected. Interconnection protection can be provided by optical multiplex section protection or OTUk protection SNC with inherent monitoring (ODUk SNC/I) of the interconnecting span, but no protection is available due to failure of either interconnecting node. Alternatively, nodes D and W are a single node, supporting both rings.

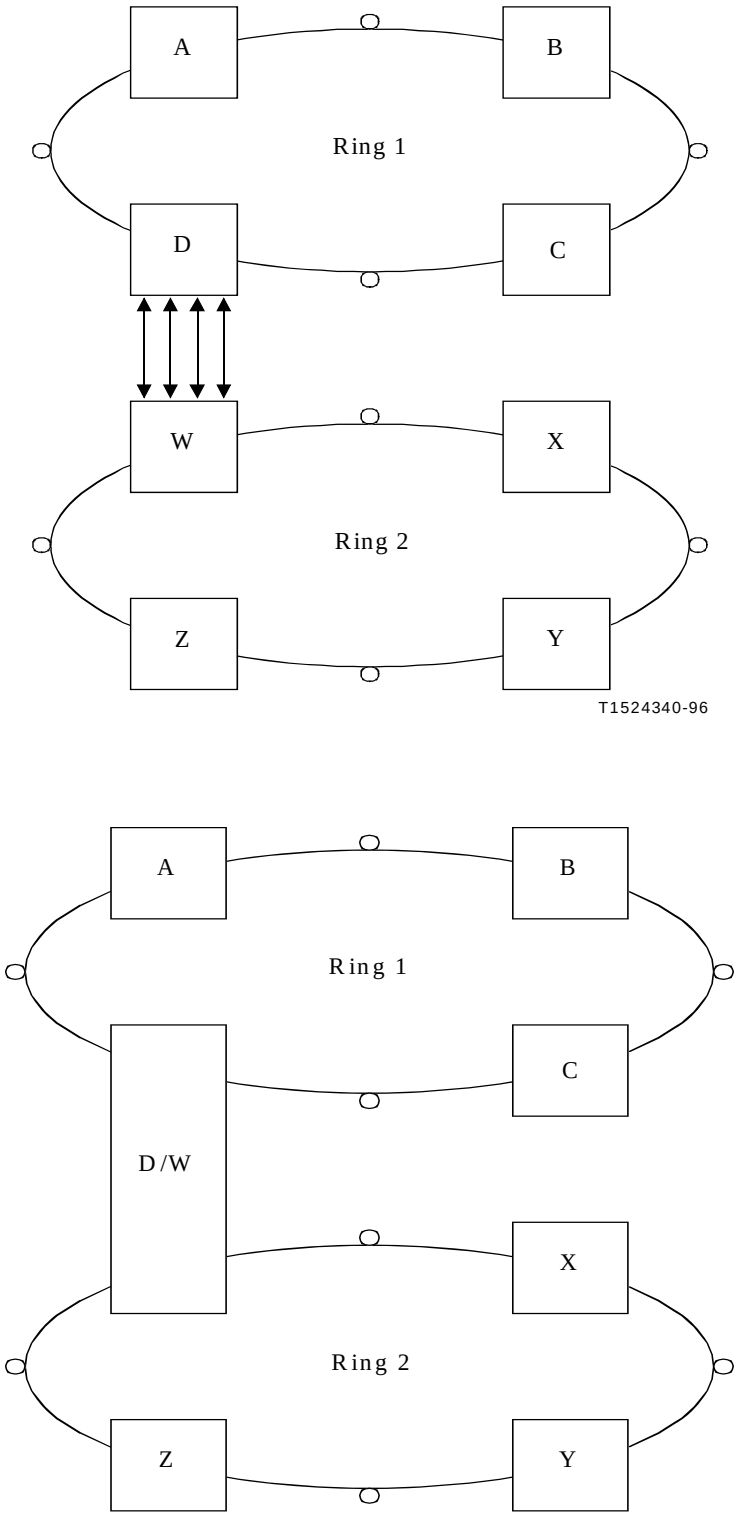


Figure 8-1 – Example of single node interconnection type I and II

8.2 Dual node interconnection

8.2.1 Generalized architecture

Dual node interconnection is an architecture between two rings where two nodes in each ring are interconnected. This is illustrated in Figure 8-2. The two interconnections between the two rings can be arranged to provide protection of the traffic crossing from one ring to the other. A special form of dual node interconnection is referred to by the term "ring interworking". Ring interworking is a network topology whereby two rings are interconnected at two nodes on each ring, and the topology operates such that a failure at either of these two nodes will not cause loss of any working traffic.

This is illustrated in Figure 8-3. In this figure, there is an ODU that enters and exits the top ring from Node A, and also enters and exits the bottom ring from Node Z. Using the following notation:

- T_A = the transmit signal at Node A;
- R_A = the receive signal at Node A;
- T_{I1} = the transmit signal at one of the interconnection nodes;
- R_{I1} = the receive signal at one of the interconnection nodes;
- T_{I2} = the transmit signal at the other interconnection node;
- R_{I2} = the receive signal at the other interconnection node.

In ring interworking, the interfaces between the two set of interconnecting nodes is such that:

- $R_{I1} = R_{I2} = T_A$;
- $T_{I1} = T_{I2}$; and
- $R_A = T_{I1}$ or T_{I2}.

In other words, the signal transmitted from Node A towards Node Z is present at both interconnection interfaces. Similarly, the signal transmitted from Node Z back to Node A is also present at both interconnection interfaces. Eventually only one copy of the duplicated signals at the interconnection interfaces is chosen at either Node A or Node Z. Specific examples of ring interworking architectures are described below. Alternatively, nodes D and W are a single node and nodes C and X are a single node, supporting both rings.

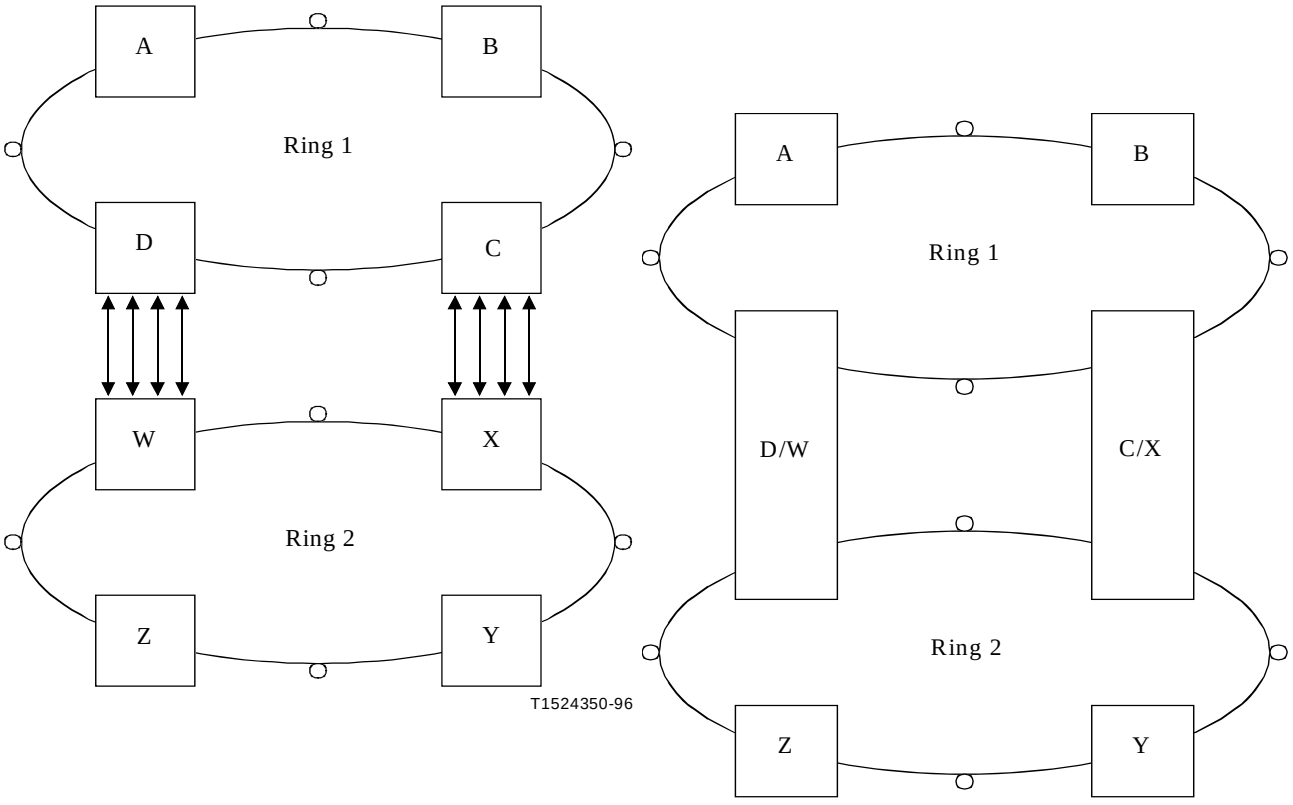
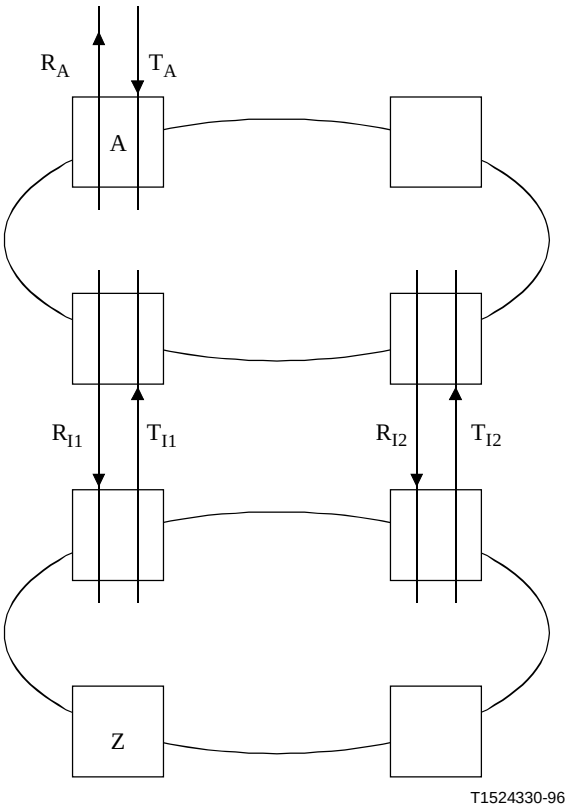


Figure 8-2 – Example of dual node interconnection type I and II



Failure free state (from perspective of top ring)

$R_{I1} = R_{I2} = T_A$

$R_A = T_{I1}$ or T_{I2}

$T_{I1} = T_{I2}$

Figure 8-3 – Generalized ring interworking

8.2.2 Ring interworking with an ODU-shared protection ring

8.2.2.1 Architecture

Figure 8-4 shows the nominal failure-free state of a simple ODU shared ring protection and illustrates a particular tributary handed-off at two ring interconnection nodes and to be terminated at the node A. The two ring interconnection nodes are referred to as the primary node and the secondary node. These interconnection nodes need not be adjacent. Starting from the top in Figure 8-4, a bidirectional tributary from the (uppermost) termination node A is assigned counter-clockwise towards the bottom on the ring. Although there is symmetry in the hand-off to the other ring, the primary node would normally be the one "closest" to the terminating node without respect to ring orientation. Primary and secondary nodes are defined on a per tributary basis. The ODU shared ring protection nodes can interface with any architecture at the interconnection nodes so long as the interface requirements illustrated in Figure 8-4 are met.

This architecture includes recovery from the following failure scenarios:

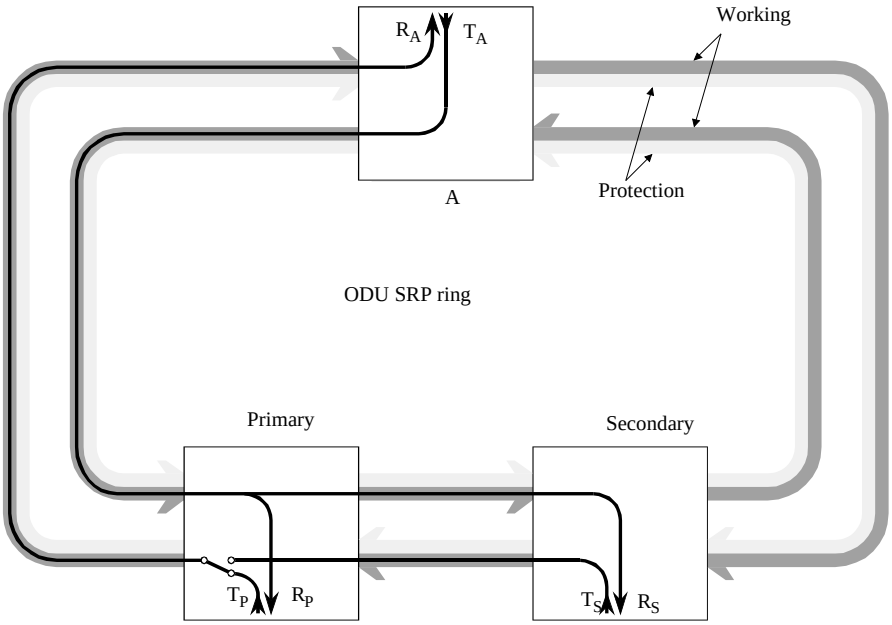
1) Within the ODU shared ring protection, any failure outside of the termination, primary, or secondary nodes are handled in standard fashion. The ODU shared ring protection is assumed to behave as described in clause 7 above. The nature of the failure – whether an electronics failure, a cable cut, or even a node failure – has no impact on the configuration of the termination, primary, or secondary nodes. A cable cut failure is illustrated in Figure 8-5.

2) A failure of the primary node in the ODU shared ring protection results in a secondary connection of the tributary. Normally such a tributary would be squelched, but for this architecture this particular tributary remains un-squelched. All other (undesired) crossed traffic is squelched. Failure of the primary node is illustrated in Figure 8-6. The ring interworking behaviour for this case remains the same even if a disaster is large enough (e.g., central office lost) to cause a failure of both the primary node on one ring and its interconnected node on the other ring.

3) For a failure of the secondary node, the tributary at the terminating node (see Node A in Figure 8-7) is unaffected, since it receives its tributary from the primary node. Because of the ring signalling, the primary node knows that the secondary node has failed. The primary node chooses its tributary from the traffic entering it from the other ring. The secondary node has a failed tributary R_S sent to the second ring. The failure of this signal may unavoidably lead to a switch in the second ring depending on its ring type.

4) For a failure of either of the signals coming in from the other ring (i.e., T_{I1} or T_{I2}), the primary node in the ODU SRP chooses the signal that is not failed. Figure 8-8 illustrates a failure of the hand-off to the secondary node. Here the primary node remains switched to its own good hand-off. Figure 8-9 illustrates a failure of the hand-off to the primary node. In this case, the primary node switches to choose a good tributary from the secondary node.

5) This architecture also protects against a single failure in each of the two rings (i.e., the ODU-shared protection ring and the other ring), provided that these failures are not terminating node failures, or these failures do not combine to affect both interconnections between the rings.

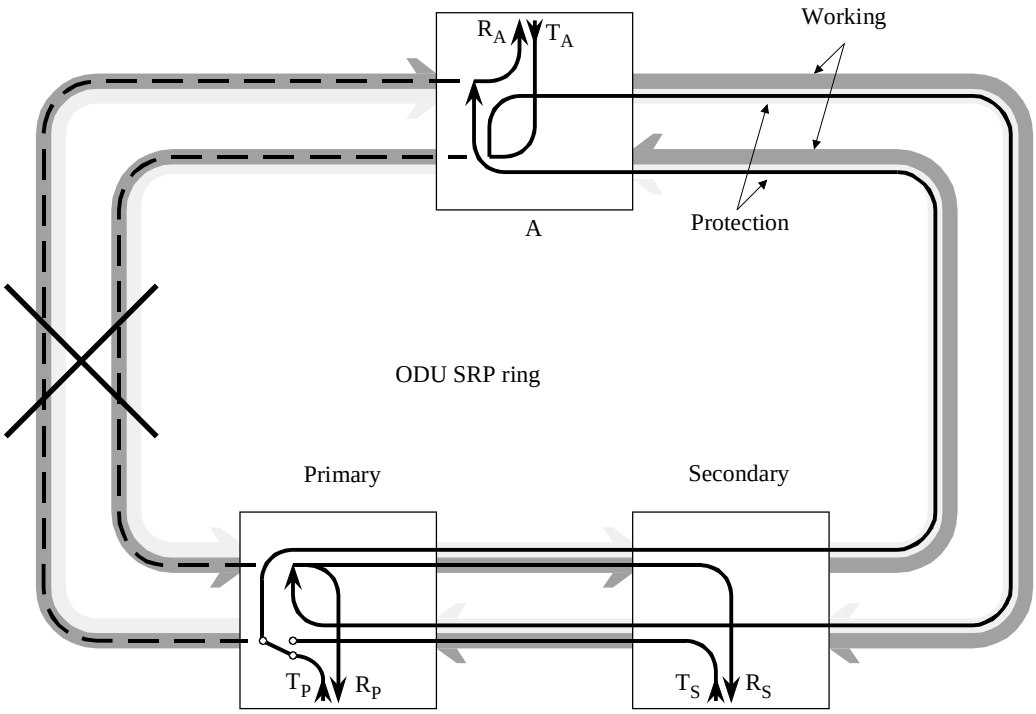


Nominal failure free state of A-Z tributary in ODU SRP ring:

$R_P = R_S = T_A$

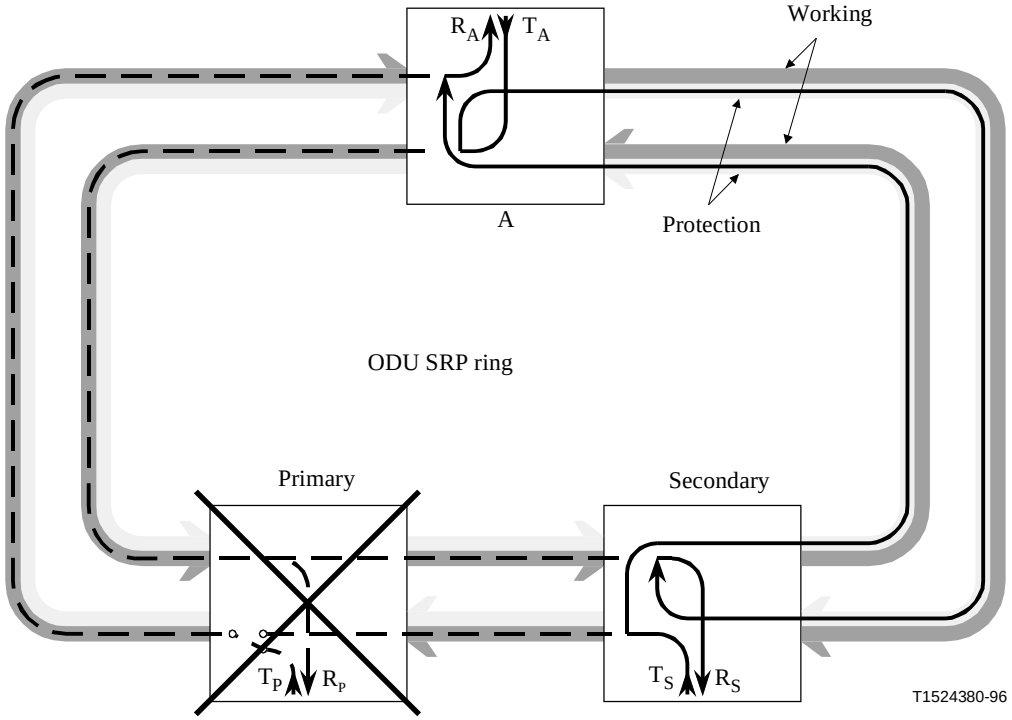
$R_A = T_P = (T_S)$

Figure 8-4 – Ring interworking with an ODU SRP ring



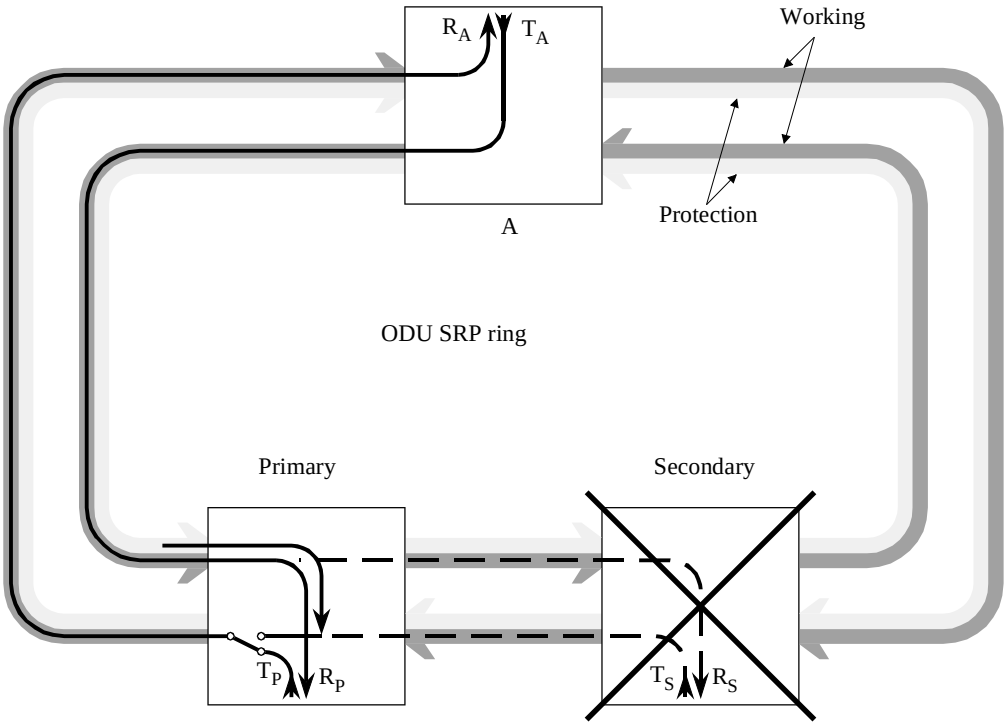
$R_P = R_S = T_A$
$R_A = T_P = (T_S)$

Figure 8-5 – Signal response to any ring failure outside of termination, primary, or secondary nodes (cable cut between primary and Node A shown)



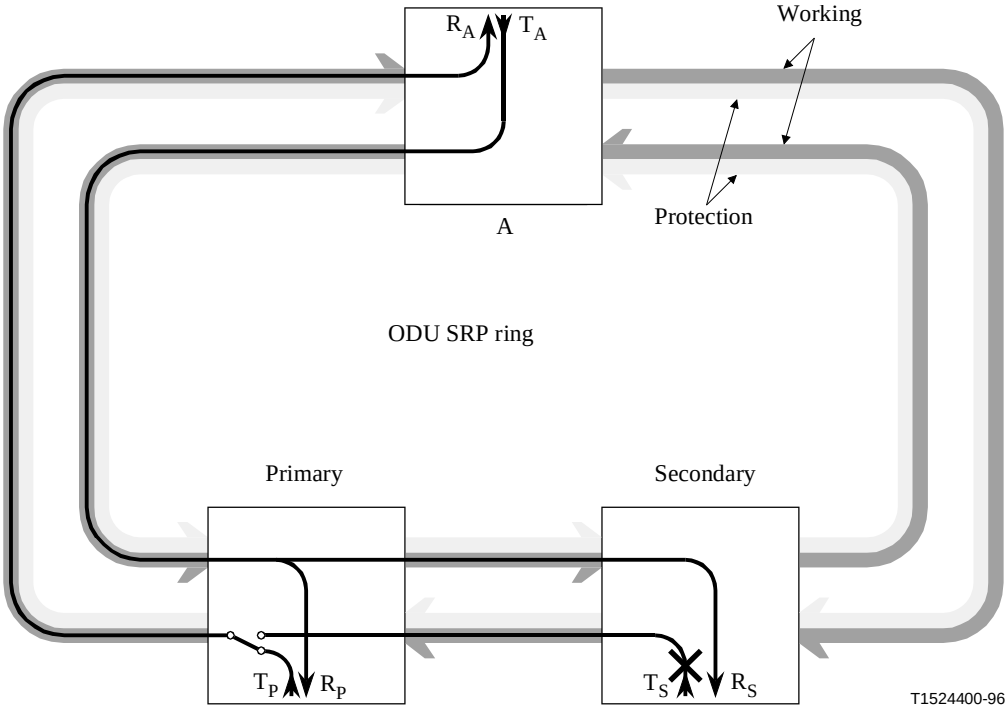
$R_A = T_S$
$R_S = T_A$
$R_P = T_P = 0$

Figure 8-6 – Signal response to complete primary node failure



$R_A = T_P$
$R_P = T_A$
$R_S = T_S = 0$

Figure 8-7 – Signal response to complete secondary node failure



$R_A = T_P$
$R_P = R_S = T_A$
$T_S = 0$

Figure 8-8 – Failure of the transmit hand-off at the secondary node

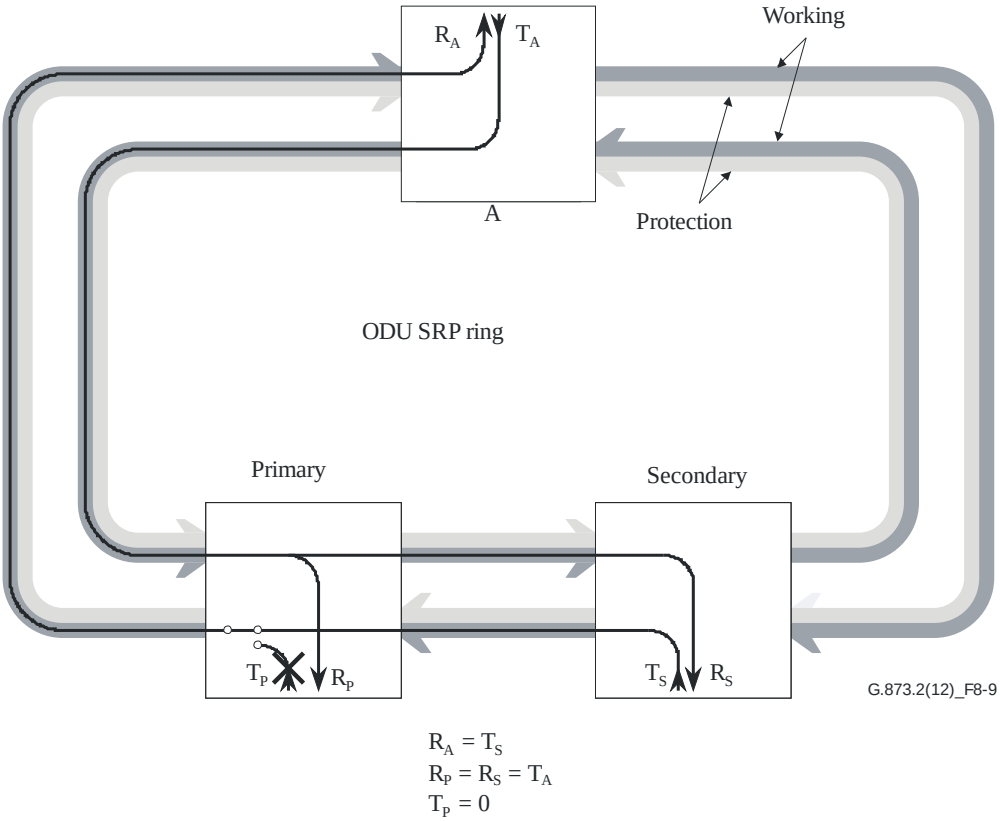


Figure 8-9 – Failure of the transmit hand-off at the primary node

8.2.2.1.1 Routing with all traffic on working channels

For the unidirectional signal transmitted from the node A, the primary node dual feeds that signal both towards its own interface and towards the ODUk (HO ODU) to the secondary node. This function is often referred to as drop-and-continue. In the other direction, the primary node selects, via a service selector, between the hand-offs to the primary and secondary nodes from the other ring, and transmits that selection to the upper terminating node. The interconnections are at the OTM optical level. The same tributary slots assignment on the ODUk (HO ODU) used between the secondary and primary nodes is the same as that used between the primary and terminating nodes. Figures 8-10 and 8-11 give two ring interworking examples. Interworking of an MS-shared protection ring with a lower order SNCP ring may require further study. With the switching criteria from clause 8.2.2.3 and squelching logic from clause 8.2.2.4, this interconnection architecture provides protection against the failure of one or both interconnecting nodes (each on different rings, but on the same interconnect), or the connection between the two interconnecting nodes. Furthermore, the interconnection architecture does not require inter-ring signalling.

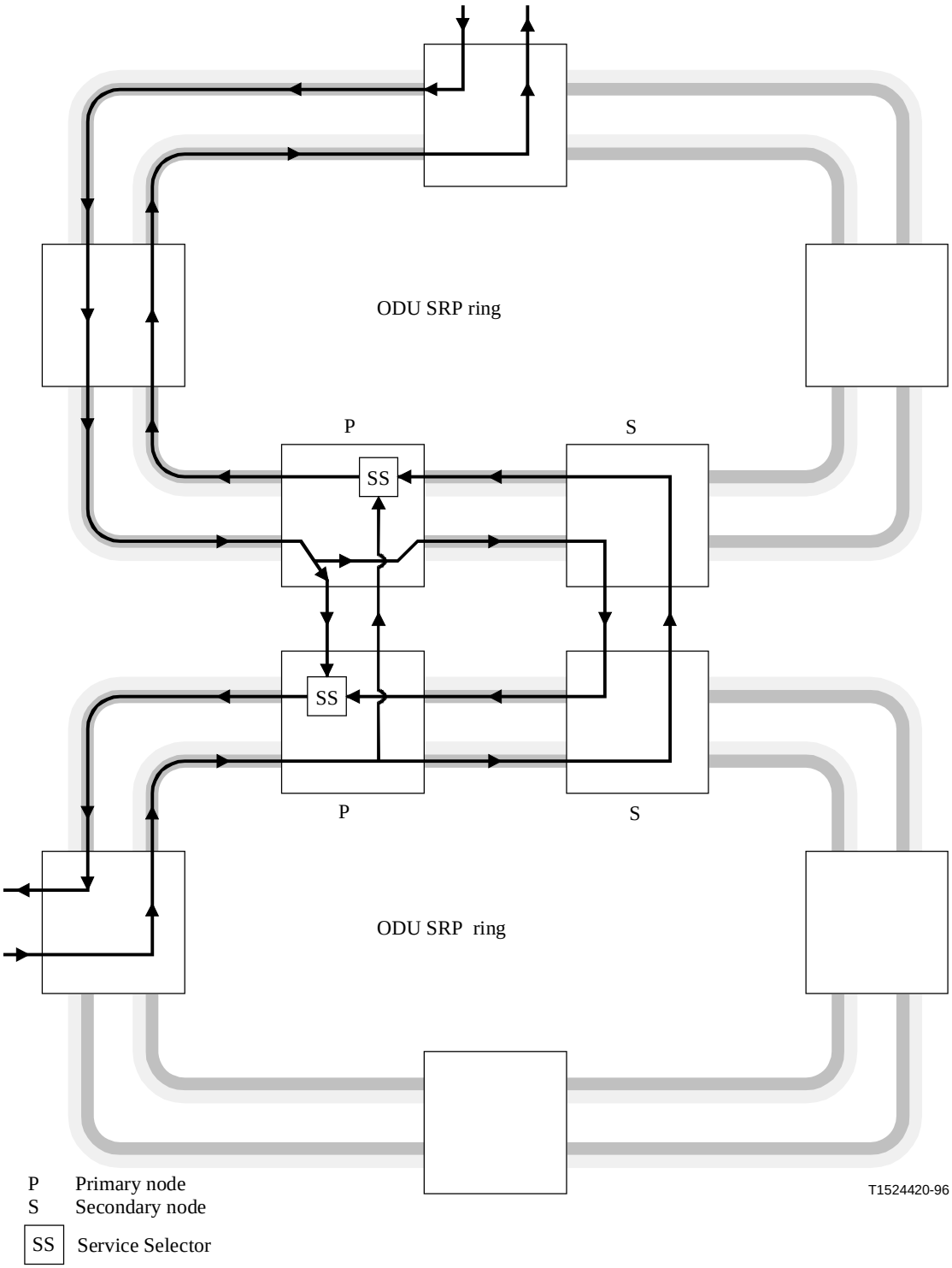


Figure 8-10 – Ring interworking between two ODU shared ring protection rings

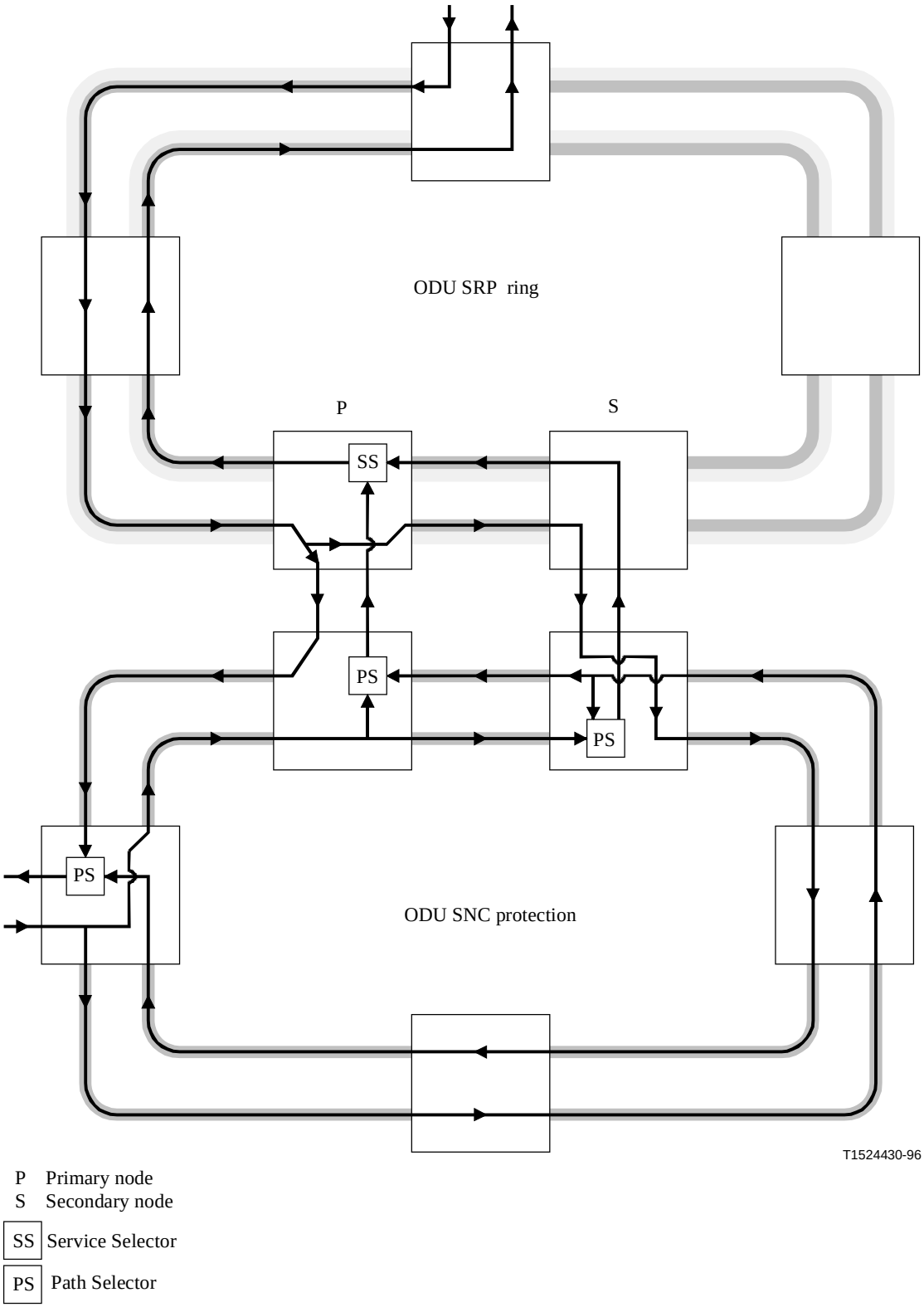


Figure 8-11 – Ring interworking between an ODU SRP ring and an ODU SNCP ring

8.2.2.1.2 Routing with continue traffic on protection channels between primary and secondary nodes

This clause describes general considerations associated with using protection bandwidth for ring interconnection. Further details of ring interworking using protection bandwidth are under study.

This alternative method to ring interworking takes advantage of the protection bandwidth between primary and secondary ring interworking nodes to address the capacity issue that arises when drop-and-continue in conjunction with a service selector is used for ring interconnection on an ODU shared ring protection ring. This is illustrated in Figure 8-12. The issue is one of early bandwidth exhaust between primary and secondary nodes when using only working bandwidth for drop-and-continue in conjunction with a service selector.

The problem can be illustrated by referring to Figure 8-10, which shows two interconnected ODU shared ring protection rings. The two interconnecting ring nodes in each ODU shared ring protection ring use the working bandwidth for the extra circuit between them that allows for dual node ring interworking, i.e., the combination of the "continue" portion of the drop-and-continue (from the primary to the secondary node), along with the duplicate feed from the other ring (from the secondary node to the service selector in the primary node). This extra circuit is called the secondary circuit.

By taking advantage of the protection bandwidth between the interconnection nodes on the ODU shared ring protection ring, less working bandwidth would be consumed as compared to the method of using only working bandwidth for ring interconnection. For example, either one, or both, of the secondary circuits in Figure 8-10 can use the protection bandwidth between the primary and secondary nodes, instead of using the working bandwidth. The protection bandwidth between the primary and secondary nodes on an ODU shared ring protection ring can be used even if the other interconnected ring is an ODU SNCP ring (see Figure 8-11).

The following options for ring interworking using combinations of working and protection bandwidth between interconnecting ring nodes (i.e., between primary and secondary nodes) are possible:

a) ring interconnection using working bandwidth only;

b) ring interconnection using working bandwidth in one ring and protection bandwidth in the other; and

c) ring interconnection using protection bandwidth in both rings.

These ring interworking options may be used on interconnected rings with either same-side or opposite-side routing. Same-side routing is illustrated in Figure 8-10, while opposite-side routing is illustrated in Figure 8-6. Note that same-side routing requires two extra, or secondary circuits, i.e., one per ring, for dual node interworking (see Figure 8-10), while opposite-side routing requires only one extra, or secondary circuit (see Figure 8-13). In the bottom ring shown in Figure 8-13, the traffic already passes through both the primary and secondary nodes for opposite-side ring interworking; this is known as the service circuit. For opposite-side routing, extra bandwidth for a secondary circuit is only used in one ring (e.g., the top ring shown in Figure 8-13).

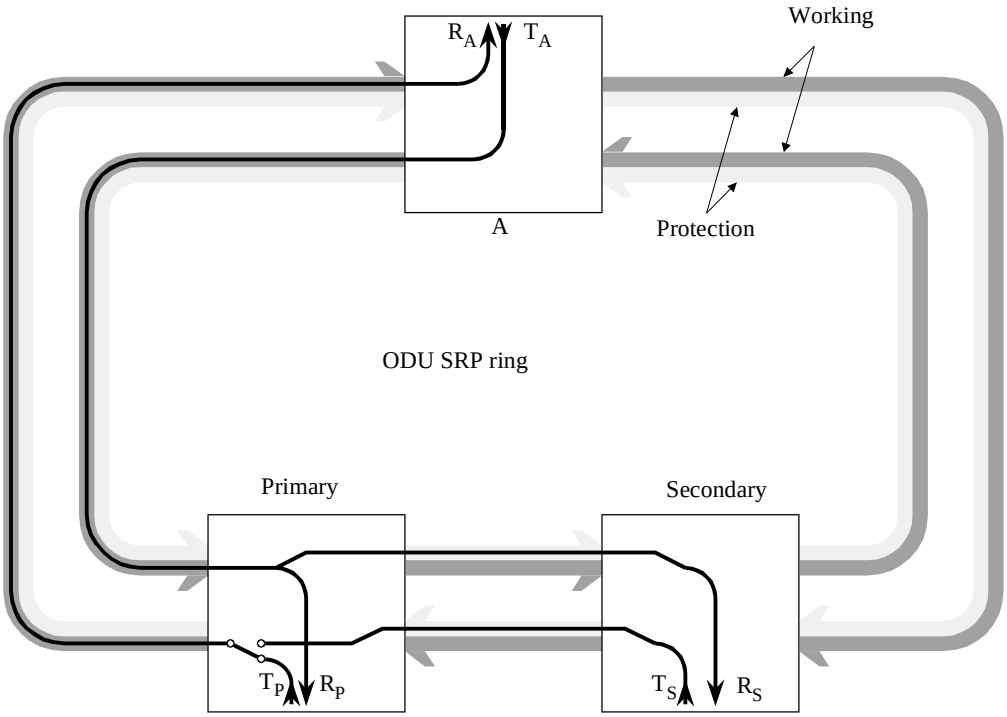
The option of using only working bandwidth provides the highest level of survivability. If reduced survivability can be tolerated, certain options that take advantage of protection bandwidth between interconnecting ring nodes may be used, including:

a) same-side ring interworking with one secondary circuit on working and one secondary circuit on protection;

b) same-side ring interworking with both secondary circuits on protection;

c) opposite-side ring interworking with the service circuit on working and the secondary circuit on protection.

Assigning the service circuit to protection bandwidth in opposite-side ring interworking is not recommended.



Nominal failure free state of A-Z tributary in ODU SRP ring:

$R_P = R_S = T_A$

$R_A = T_P = (T_S)$

Tributary assignment for secondary connection = Protection tributary for working path

Figure 8-12 – Ring interworking using protection capacity

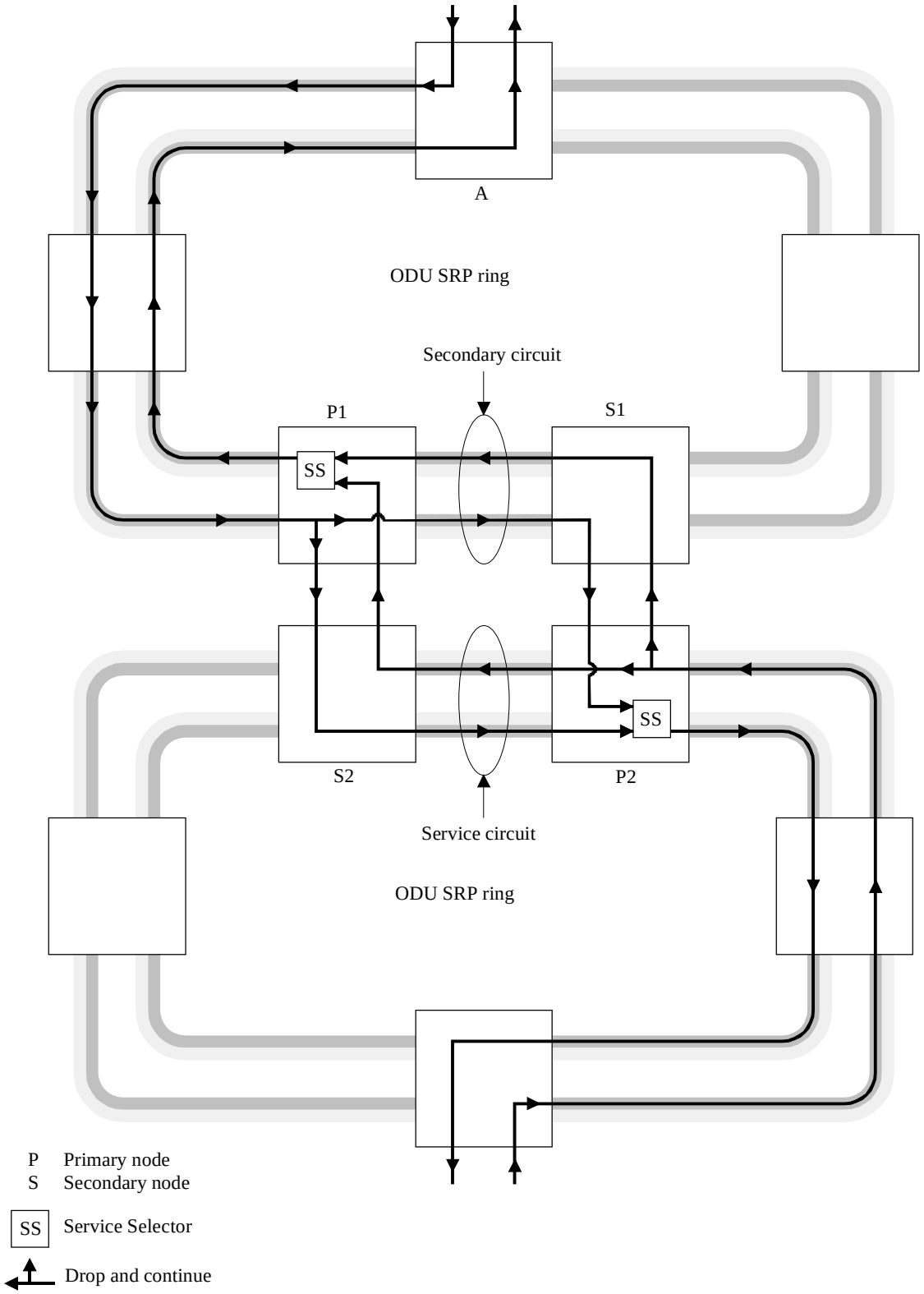


Figure 8-13 – Ring interworking between two ODU-shared protection rings, with opposite-side routing

8.2.2.2 Functional model

Figure 8-14 illustrates the functional model associated with a primary node in an ODU-shared protection ring. In this example, an OTUk signal is connected at the tributary side of the ODU XC equipment and two OTUk signals are connected at both west and east line sides.

An ODUj out of the ODUk signal has a 1 + 1 unidirectionally switched sub-network connection with non-intrusive monitoring (SNC/N) protection relationship with an ODUj out of the west ODUk signal; the selected ODUj signal is connected to the east ODUk signal. In the other direction, the associated ODUk at the east OTUk signal is dual-fed to both the tributary OTUk and west OTUk signals. The ODUj out of the tributary OTUk is also connected to the interface with an ODUj non-intrusive monitoring (NIM) function. Similarly, the ODUj out of the west OTUk is connected also to an ODUj NIM function.

Figure 8-15 illustrates the matrix connections within the ODU_C that realise the "service selector". For ODUj SNC/N five matrix connections are required: (1) ... (5).

NOTE – The ODU_C interfaces A, B, C, D, E in Figure 8-15 represent the same interfaces in Figure 8-14.

A ODUj out of the ODUk signal has a 1 + 1 SNC protection relation with a ODUj out of the west ODUk signal; the selected ODUj signal is connected to the east ODUk signal. In the other direction the associated ODUk at the east OTUk signal is dual-fed to both the tributary OTUk and west OTUk signals.

For the case of SNC/N protection (Figure 8-15), the ODUj out of the tributary OTUk is also connected to the interface with a ODUj non-intrusive monitoring (NIM) function. Similarly, the ODUj out of the west OTUk is connected also to the ODUj NIM function.

Figure 8-15 illustrates the matrix connections within the ODU_C that realise the "service selector". For ODUj SNC/N five matrix connections are required: (1) ... (5).

NOTE – The ODU_C interfaces A, B, C, D, E in Figure 8-15 represent the same interfaces in Figure 8-14.

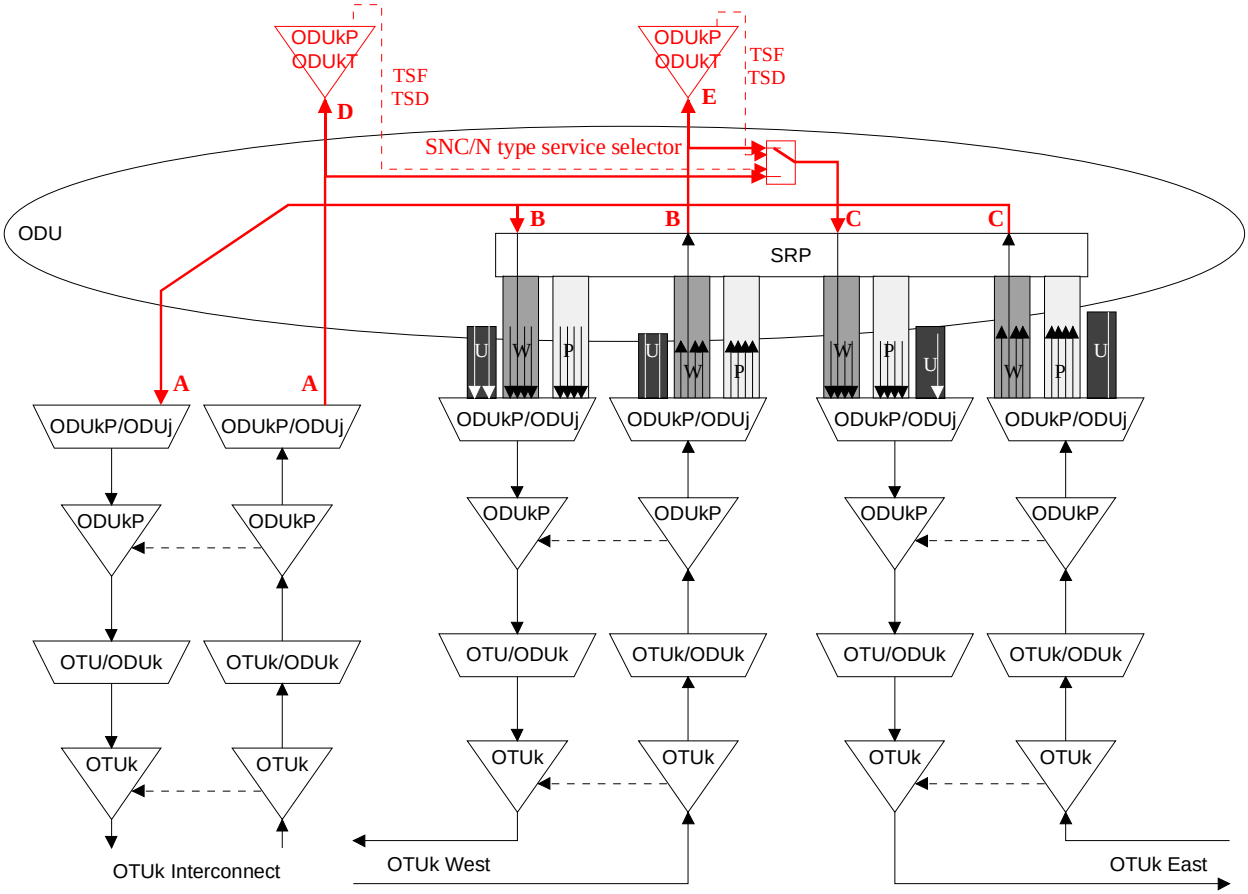


Figure 8-14 – Example of functional model for network element with service selector of type SNC/N

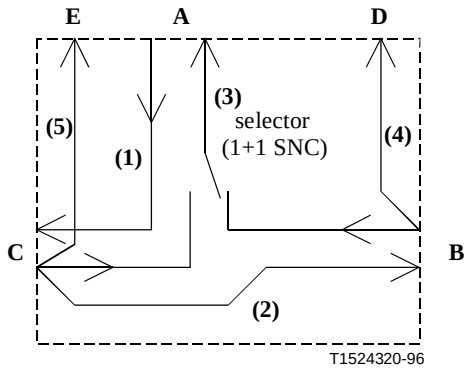


Figure 8-15 – Service selector's ODU_C connectivity

Figure 8-16 illustrates the functional model associated with an interconnecting node in an SNC protected ring or subnetwork. In this example, an OTUk signal is connected at the tributary side of the ODU XC equipment and two OTUk signals are connected at both west and east line sides.

An ODUj out of the east ODUk signal has a 1+1 unidirectionally switched SNC/N protection relation with an ODUj out of the west ODUk signal; the selected ODUj signal is connected to the OTUk signal. In the other direction the associated ODUj in the OTUk signal is connected to the east OTUk signal. The received ODUj in the east OTUk signal is also connected to the west OTUk signal. The ODUj signals out of the east and west OTUk signals are also connected to interfaces with an ODUj NIM function.

Figure 8-17 illustrates the matrix connections within the ODU_C that realise the "path selector". For the case of SNC/N five matrix connections are required: (1) ... (5).

NOTE – The ODU_C interfaces A, B, C, D, E in Figure 8-17 represent the same interfaces in Figures 8-16.

Figures 8-16 and 8-17 are presented below.

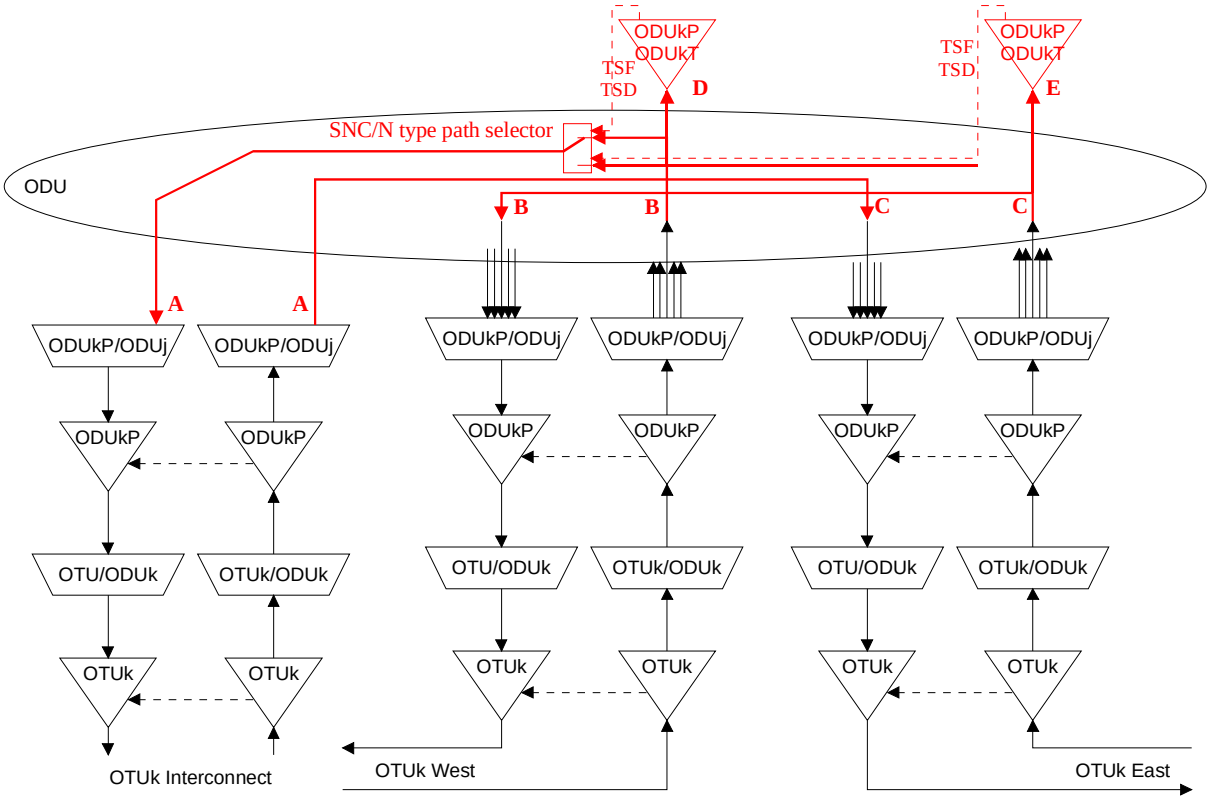


Figure 8-16 – Example of functional model for network element with path selector of type SNC/N

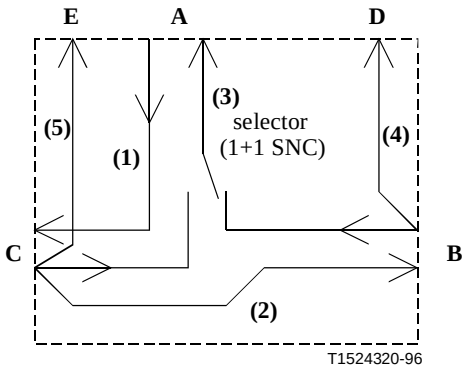


Figure 8-17 – Path selector's ODU_C connectivity

8.2.2.3 Switching criteria and operation

At the primary node, a service selector is used to select the better of two incoming tributaries, i.e., the tributary from the interconnecting line or the tributary from the secondary node. The service selectors trigger on ODU layer criteria as specified in [ITU-T G.798]. The switching hierarchy must select the least impacted signal under multiple failures occurring at different levels on the same ODU.

The service selector shall be capable of revertive or non-revertive operation. To have a known failure-free state, it may be desirable to have the service selector be revertive. In the case of conditions of identical severity arriving on both incoming ODUs, the service selector shall select the preferred route in the case of revertive operation, or the current (i.e., active or currently selected) route in the case of non-revertive operation. This may be subject to a hold-off time.

8.2.2.4 Squelching logic

For the case of the failure of the primary node, the connection of the signal between the termination A and the secondary node is maintained. This is called a secondary connection.

An ODU shared ring protection ring providing the sort of ring interworking described here must be provisionable on a per-ODU basis to allow a secondary connection or to squelch the traffic in the case of a node failure as required for the particular application and circuit. The squelching for a ring interworking circuit is simply based on the failure of either of the endpoints for the interconnected circuit, because a switching node should squelch the channel (as shown in Figure 8-4) if and only if node A fails or the secondary node fails. If the secondary node fails and the primary node is the switching node, observe that the primary node squelches bidirectionally with respect to the signal towards the secondary node, but that the bidirectional connection from the primary node toward node A is maintained.

The rules for squelching logic when interworking using protection capacity are for further study.

Annex A

Network objectives

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

The network objectives are given as follows:

(i) switching time

While there is the generic requirement for switch completion time for SRP, the actual completion time is dependent on total fibre length, due to propagation time, and number of ring nodes for forwarding delay. Thus, the following requirement shall be fulfilled with respect to switching time validation.

In the absence of additional traffic on the ring, all nodes in the empty state (i.e., no failure is detected, no activity of the automatic or external command, and only an "NR"APS request is received) and with a fibre length of less than 1200 km, a single-span failure (ring and ring span) switching completion time should be less than 50 ms for 16 nodes. In other cases, in order to provide time to remove the extra traffic, ignore or be compatible with an existing APS request, switching completion time can be more than 50 ms (with a more specific interval of time required to be studied).

(ii) holdoff time

In order to coordinate timing of protection switches at multiple layers or across cascaded protection domains, a hold-off timer may be required. This holdoff timer allows either a server layer protection switch to have a chance to fix the problem before switching at a client layer, or to allow an upstream protection domain to switch before a downstream domain. Each protection group should have a provisionable hold-off timer. When a new defect or more severe defect occurs (new SD or SF, or SD becoming SF),this event will not be reported immediately to protection switching if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the hold-off timer expires, it will be checked to determine whether a defect still exists on the trail that started the timer. If it does, that defect will be reported to protection switching. The defect need not be the same one that started the timer.

(iii) transmission delay

The transmission delay depends on the physical length of the trail and the processing functions within the trail. Limitations on the transmission delay may be imposed if the target switch completion time for bidirectional protection switching operation is to be met.

(iv) degree of protection

For a single point failure, the ring will restore all traffic that is passing through the failed location as if no failure had occurred. The ring shall restore as much traffic as possible, even under conditions of multiple bridge requests of the same priority (including the combination of FS-R and SF-R).

(v) switching type

This can provide bi-directional protection switching.

Appendix I

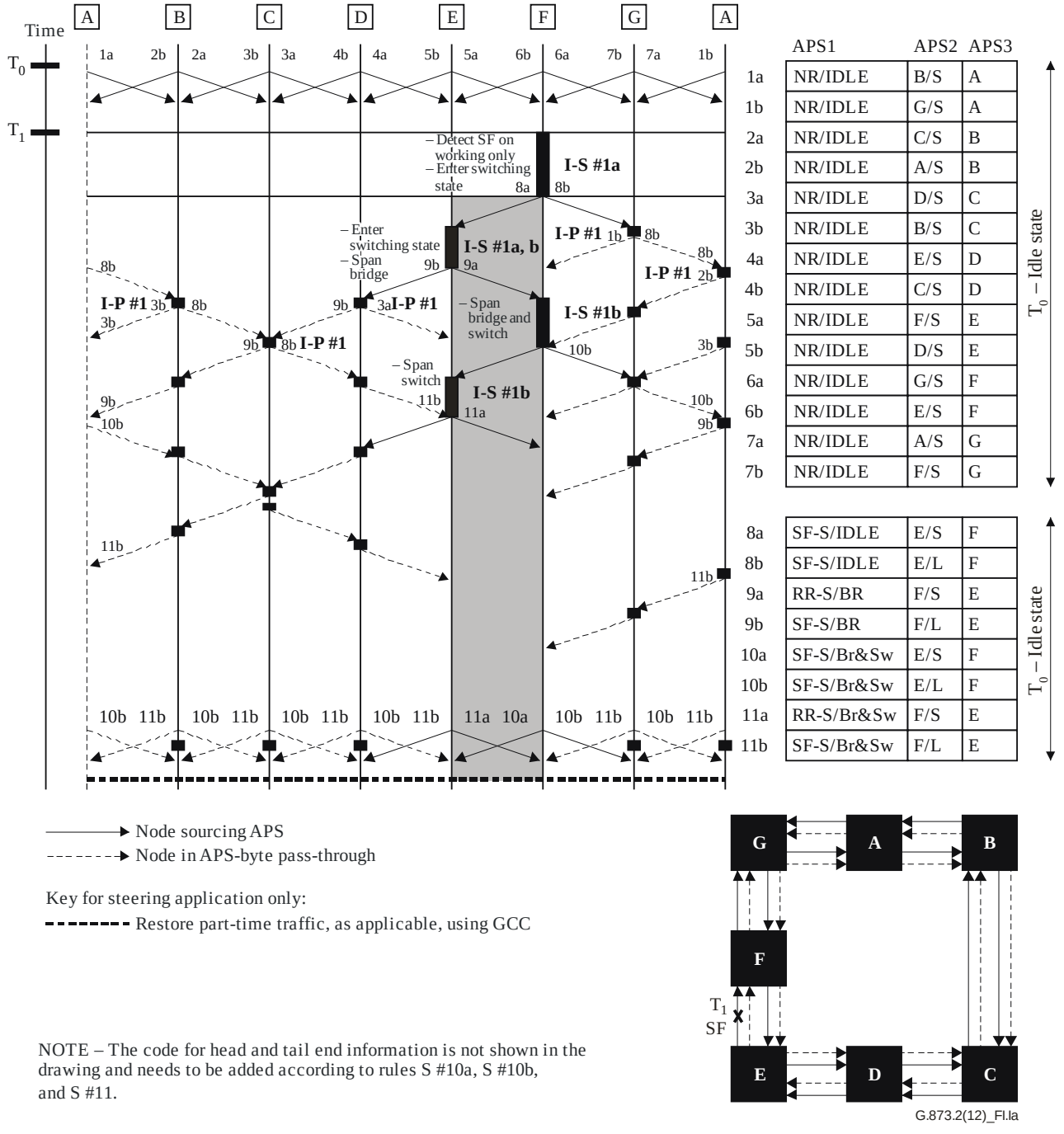
Examples of protection switching in an ODU SRP

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

This appendix provides examples showing how the state transition rules are used to execute a ring switch.

I.1 Unidirectional signal fail (span) in a four-fibre ring

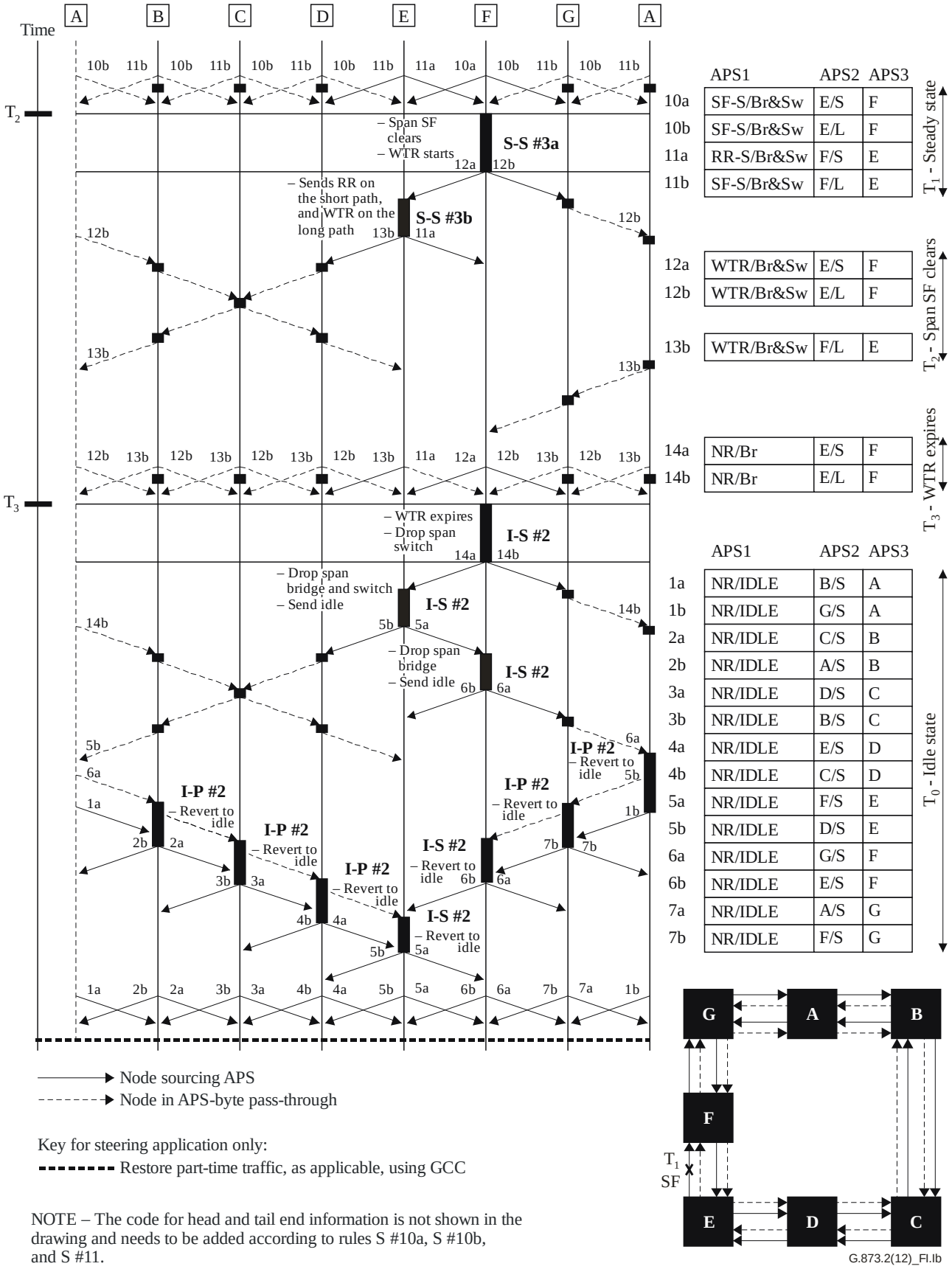
See Figure I.1.



	APS1	APS2	APS3	
1a	NR/IDLE	B/S	A	T_0 – Idle state
1b	NR/IDLE	G/S	A	
2a	NR/IDLE	C/S	B	
2b	NR/IDLE	A/S	B	
3a	NR/IDLE	D/S	C	
3b	NR/IDLE	B/S	C	
4a	NR/IDLE	E/S	D	
4b	NR/IDLE	C/S	D	
5a	NR/IDLE	F/S	E	
5b	NR/IDLE	D/S	E	
6a	NR/IDLE	G/S	F	
6b	NR/IDLE	E/S	F	
7a	NR/IDLE	A/S	G	
7b	NR/IDLE	F/S	G	
8a	SF-S/IDLE	E/S	F	T_0 – Idle state
8b	SF-S/IDLE	E/L	F	
9a	RR-S/BR	F/S	E	
9b	SF-S/BR	F/L	E	
10a	SF-S/Br&Sw	E/S	F	
10b	SF-S/Br&Sw	E/L	F	
11a	RR-S/Br&Sw	F/S	E	
11b	SF-S/Br&Sw	F/L	E	

NOTE – The code for head and tail end information is not shown in the drawing and needs to be added according to rules S #10a, S #10b, and S #11.

Figure I.1 – Four-fibre/four-lambda ODU SRP – Unidirectional failure (span) on working from E to F



NOTE – The code for head and tail end information is not shown in the drawing and needs to be added according to rules S #10a, S #10b, and S #11.

Figure I.1 – Four-fibre/four-lambda ODU SRP – Unidirectional failure (span) on working from E to F *(concluded)*

In this example, a span switch is executed and cleared for an SF condition over the working channels in a four-fibre ring. The initial state of the ring is the idle state. At time T_1, node F detects an SF condition on its working channels. It becomes a switching node (Rule I-S #1) and sends bridge requests in both directions (Rule S #1). Node G, and all successive intermediate nodes on the long path, enter APS-byte pass-through (Rule I-P #1). Node E, upon reception of the bridge request from Node F on the short path, executes a span bridge and transmits an SF span bridge request on the long path, and a RR on the short path (Rules S #3, S #1, and I-S #1b). Node F, upon reception of the bridge acknowledgment from node E on the short path, executes a span bridge and switch, and updates its APS-byte signalling (Rule I-S #1b). Node E, upon reception of the bridge and switch acknowledgment from node F on the short path, completes the switch. Signalling reaches steady state.

For steering applications, the switching activities take place at the intermediate nodes. On all protection TS not being used to protect working channels, extra traffic is restored using the GCC.

At time T_2, the span SF condition clears, and node F enters the WTR state, and signals its new state in both directions (Rule S-S #3a). Node E, upon reception of the WTR bridge request from node F on the short path, sends out RR on the short path and WTR on the long path (Rule S-S #3b.) At time T_3, the WTR interval expires. Node F drops the span switch, and sends out NR codes (Rule I-S #2.) Node E, upon reception of the NR code from node F on the short path, drops its bridge and switch, and sources the idle code (Rule I-S #2). Node F, upon reception of the Idle code on the short path, drops its bridge and also sources the idle code. All nodes then cascade back to idle state.

I.2 Unidirectional signal fail (ring)

See Figure I.2.

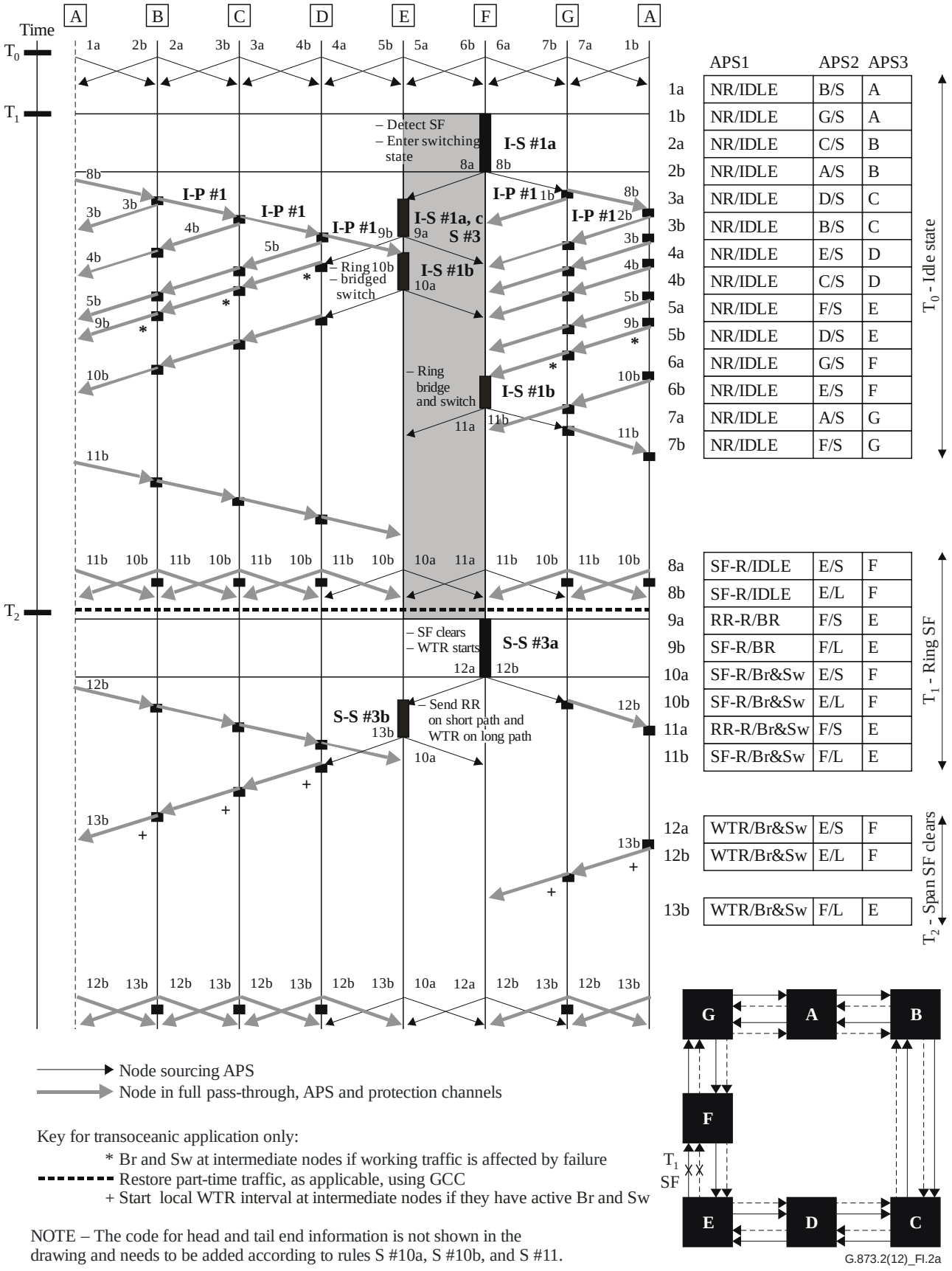


Figure I.2 – Two- or four-fibre/four-lambda ODU SRP – Unidirectional SF (ring)

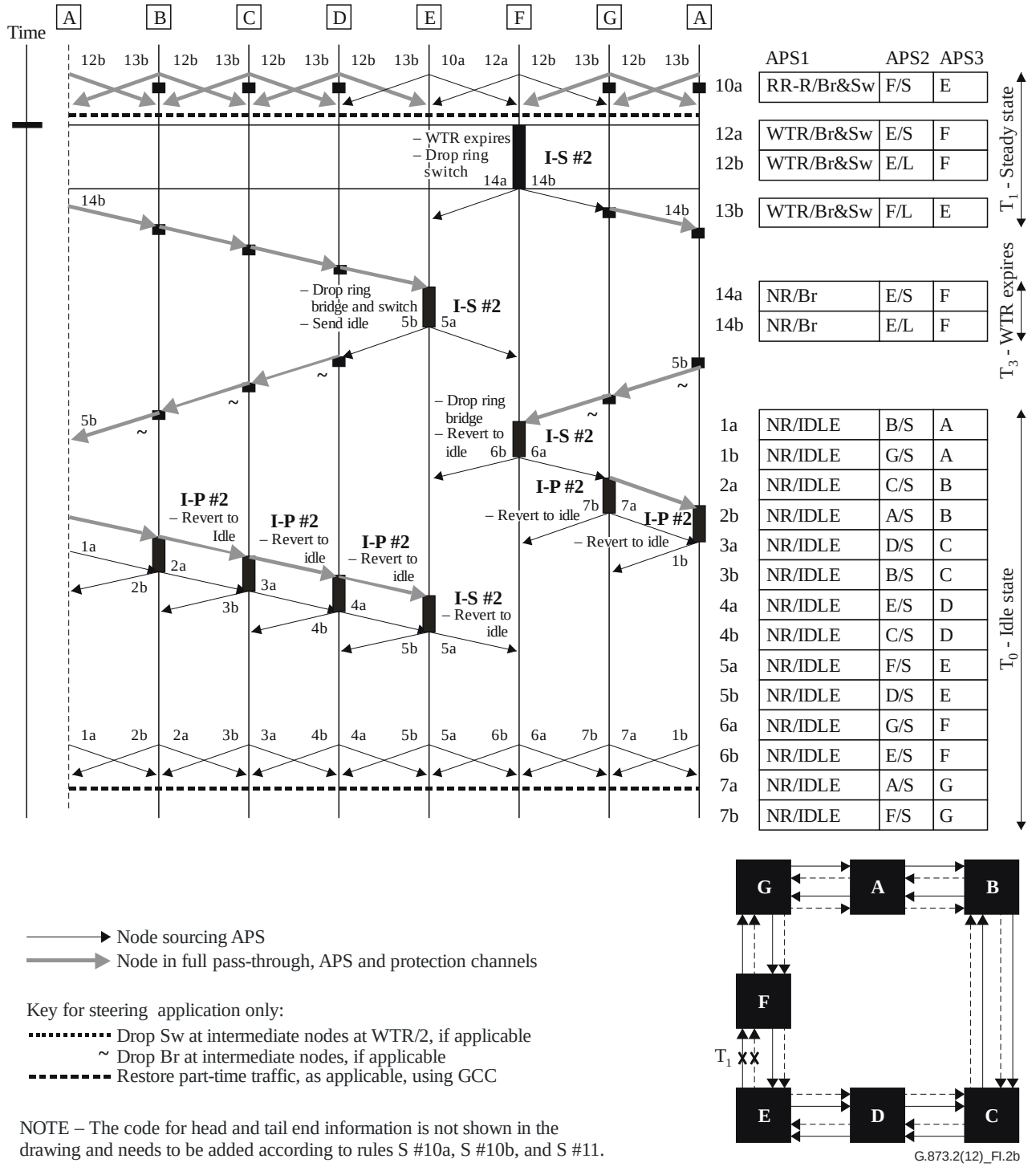


Figure I.2 – Two- or four-fibre/four-lambda ODU SRP – Unidirectional SF (ring) *(concluded)*

This example covers the case of a unidirectional SF condition in a two-fibre ring, and the case of a unidirectional SF condition on both working and protection channels in a four-fibre ring.

The initial state of the ring is the idle state. At time T_1, node F detects an SF condition on its working and protection channels. It becomes a switching node (Rule I-S #1) and sends bridge requests in both directions (Rule S #1). Node G, and all successive intermediate nodes on the long path, enter full pass-through (Rule I-P #1). Node E, upon reception of the bridge request from node F on the short path, transmits an SF ring bridge request on the long path, and a RR on the short path (Rules S #3, and I-S #1a). Node E, upon reception of the bridge request from node F on the long path, executes a ring bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Node F, upon reception of the acknowledgment from node E on the long path, executes a ring bridge and switch, and updates its APS-byte signalling (Rule I-S #1b). Signalling reaches steady state.

For steering applications, the switching activities take place at the intermediate nodes. On all TS protection channels not being used to protect working channels, extra traffic is restored using the GCC.

At time T_2, the ring SF condition clears, and node F enters the WTR state, and signals its new state in both directions (Rule S-S #3a). Node E, upon reception of the WTR bridge request from node F on the short path, sends out RR on the short path and WTR on the long path (Rule S-S #3b). At time T_3, the WTR interval expires. Node F drops the ring switch, and sends out NR codes (Rule I-S #2). Node E, upon reception of the NR code from node F on the long path, drops its bridge and switch, and sources the idle code (Rule I-S #2). Node F, upon reception of the Idle code on the long path, drops its bridge and also sources the idle code. All nodes then cascade back to the idle state.

I.3 Bidirectional signal fail (ring)

See Figure I.3.

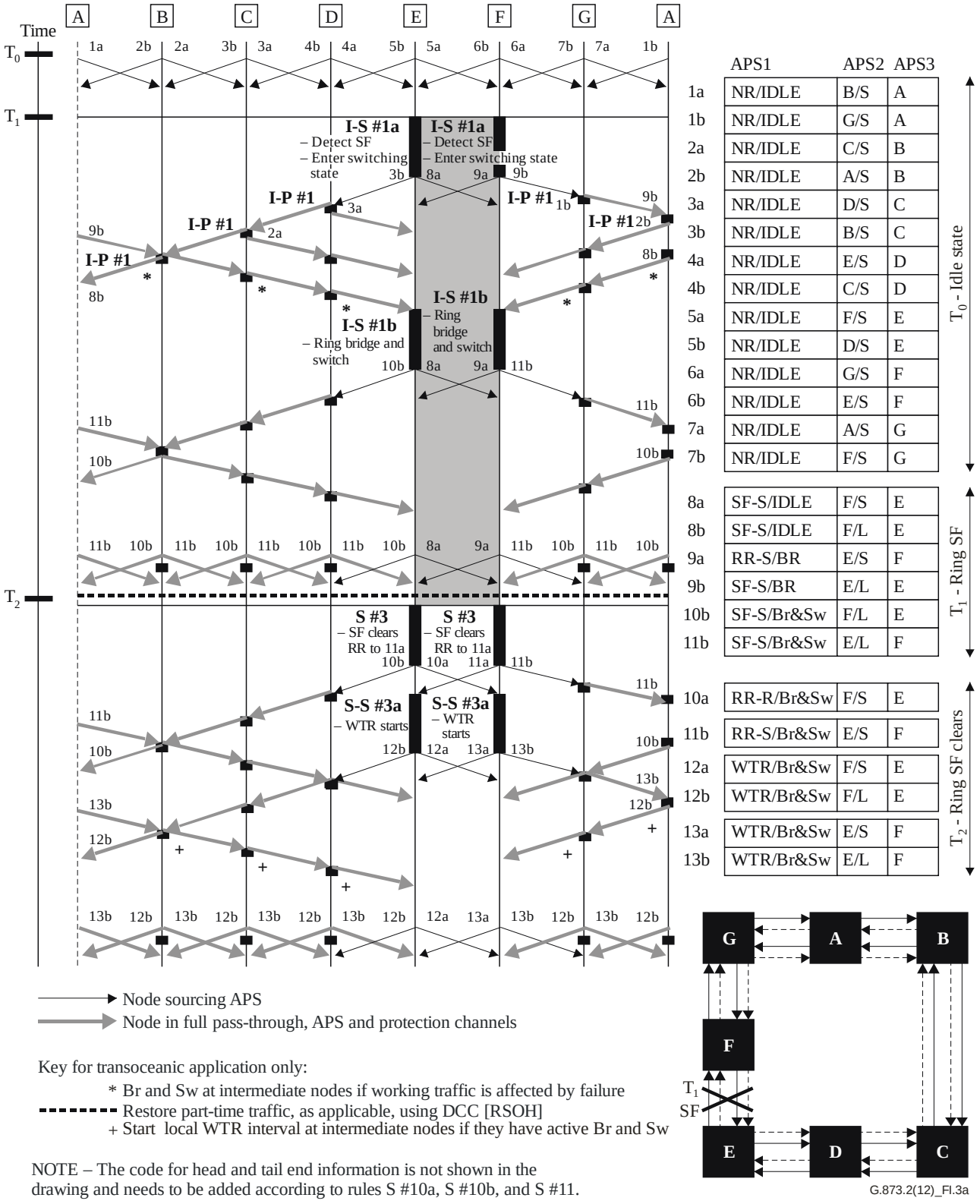


Figure I.3 – Two- or four-fibre/four-lambda ODU SRP – Bidirectional SF (ring)

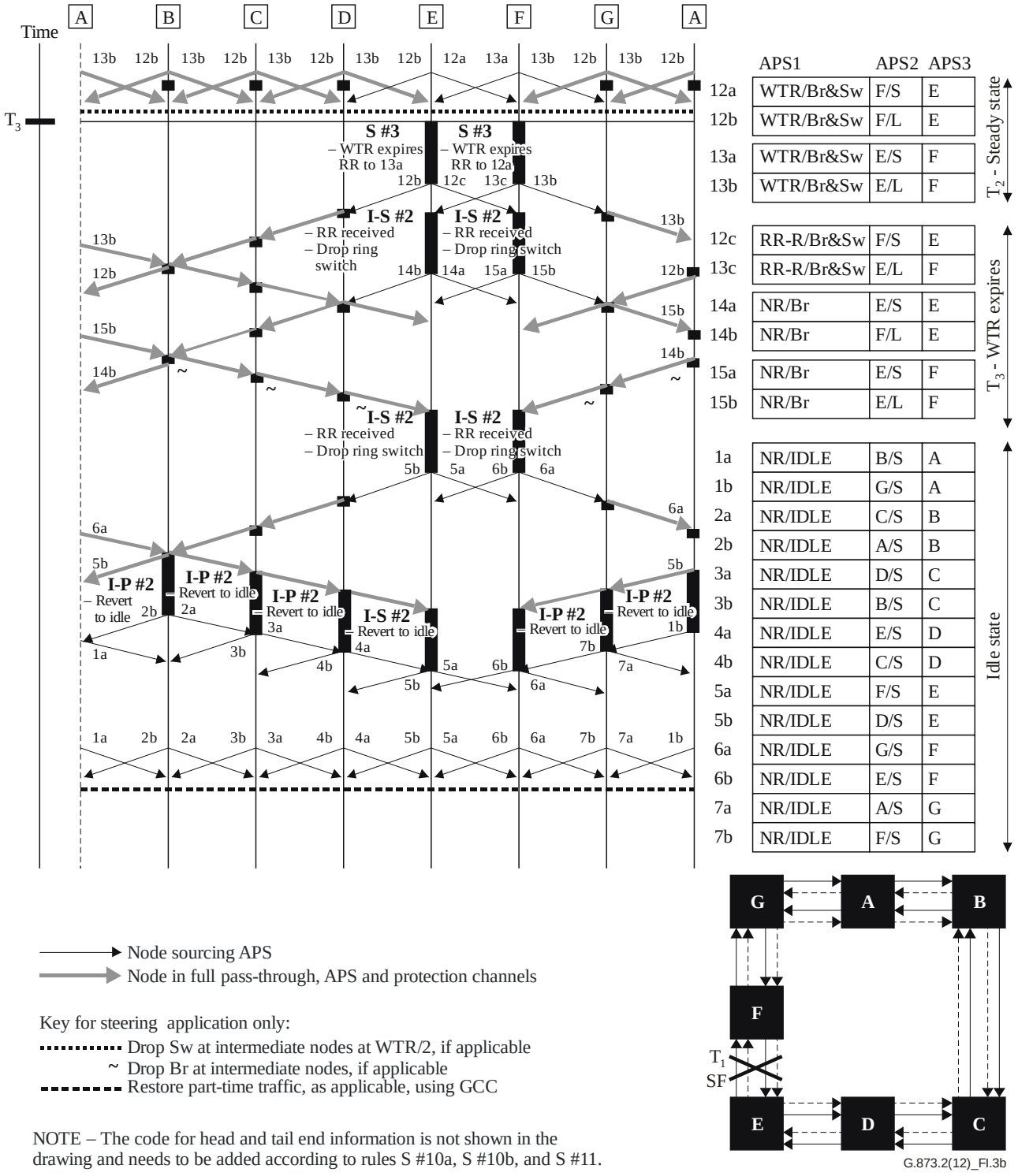


Figure I.3 – Two- or four-fibre/four-lambda ODU SRP MS shared protection ring – Bidirectional SF (ring) *(concluded)*

This example covers the case of a bidirectional SF condition in a two-fibre ring, and the case of a bidirectional SF condition on both working and protection channels in a four-fibre ring.

The initial state of the ring is the idle state. At time T_1, nodes E and F detect an SF condition on their working and protection channels. They become switching nodes (Rule I-S #1) and send bridge requests in both directions (Rule S #1). Nodes D and G, and all successive intermediate nodes on the long path, enter full pass-through (Rule I-P #1). Node E, upon reception of the bridge request from node F on the long path, executes a ring bridge and switch, and updates APS byte 1 bits 6-8

(Rule I-S #1b). Node F, upon reception of the bridge request from node E on the long path, executes a ring bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Signalling reaches steady-state.

For steering applications, switching activities take place at the intermediate nodes. On all TS protection channels not being used to protect working channels, extra traffic is restored using the GCC.

At time T_2 when the SF-R condition clears, the APS-byte values that nodes E and F receive indicate to both nodes E and F that they are head-ends of a unidirectional SF condition on the span, which pre-empts WTR. For this condition, the SF-R priority must be signalled on the long path and RR-R on the short path (Rule S #3). These actions cause crossing RR-R on the short path between nodes E and F. The WTR period for both head-ends (due to simultaneous clearing) is entered after they receive a crossing RR-R from the node that was its tail-end. At time T_3, the WTR intervals expire. Both nodes react as head-ends to the WTR by sourcing the WTR priority on the long path and RR-R on the short path. Upon receiving the crossing RR-R, nodes E and F drop their ring switch and send NR codes (Rule I-S #2). Node E, upon reception of the NR code from node F on the long path, drops its bridge and sources the Idle code (Rule I-S #2). Node F, upon reception of the NR code from E on the long path, drops its bridge and sources the idle code (Rule I-S #2). All nodes then cascade back to the idle state.

I.4 Unidirectional signal degrade (ring)

See Figure I.4.

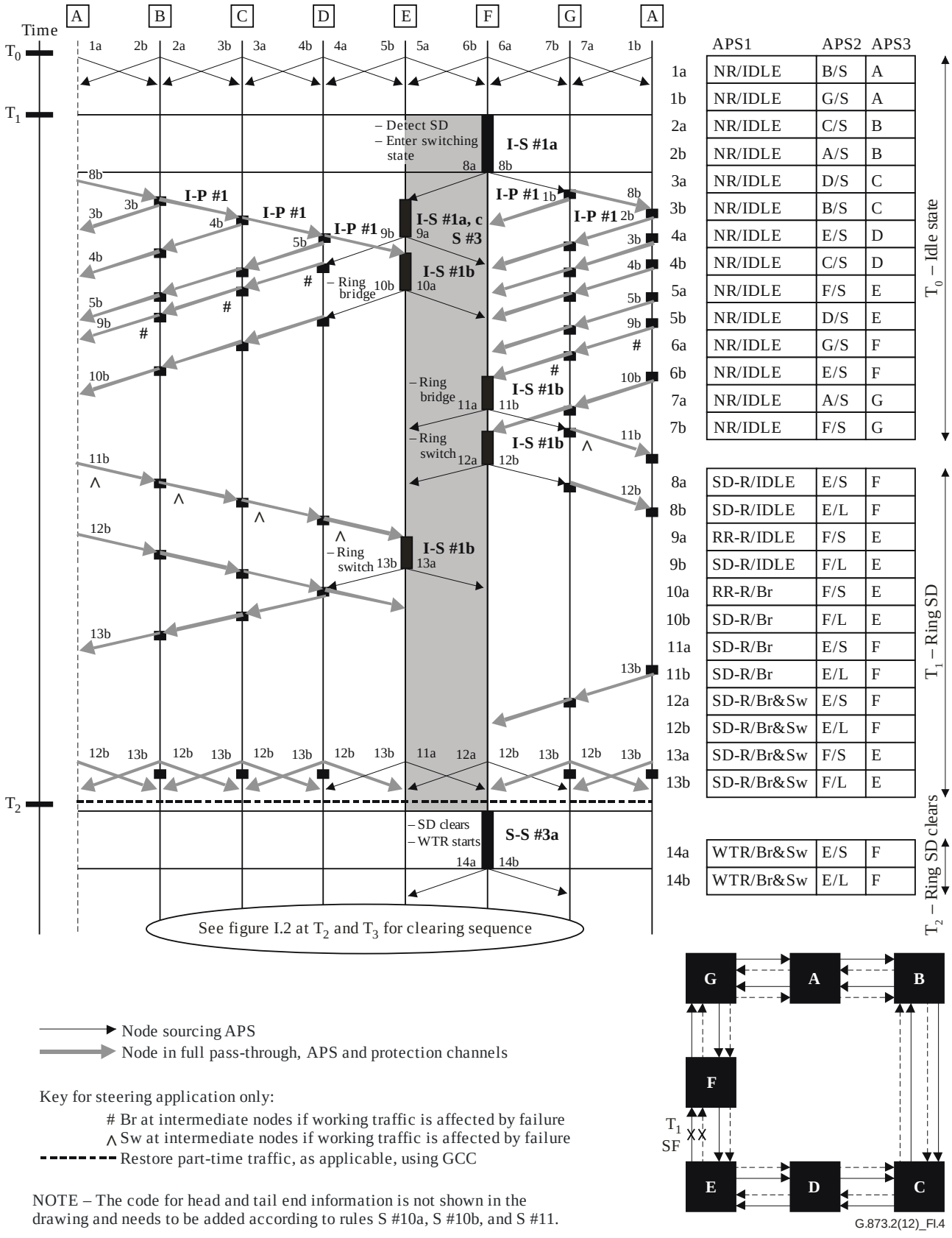


Figure I.4 – Two- or four-fibre/four-lambda ODU SRP – Unidirectional SD (ring)

In this example, a ring switch is executed and cleared for a ring SD condition in a two-fibre ring, and for a ring SD condition over the working and protection channels in a four-fibre ring.

The initial state of the ring is the idle state. At time T_1, node F detects a ring SD condition. It becomes a switching node (Rule I-S #1) and sends bridge requests in both directions (Rule S #1). Node G, and all successive intermediate nodes on the long path, enter full pass-through (Rule I-P #1). Node E, upon reception of the bridge request from node F on the short path, transmits an SD ring bridge request on the long path, and a RR on the short path (Rule S #3). Node E, upon reception of the bridge request from node F on the long path, executes a ring bridge and updates APS byte 1 bits 6-8 (Rule I-S #1b). Node F, upon reception of the bridge acknowledgment from node E on the long path, executes a ring switch, and updates its APS-byte signalling (Rule I-S #1b). Node E, upon reception on the long path of the bridge acknowledgment from node F, completes the switch. Signalling reaches steady state.

For steering applications, switching activities take place at the intermediate nodes. On all TS protection channels not being used to protect working channels, extra traffic is restored using the GCC.

Clearing is identical to the clearing of a unidirectional SF-R condition.

I.5 Node failure

See Figure I.5.

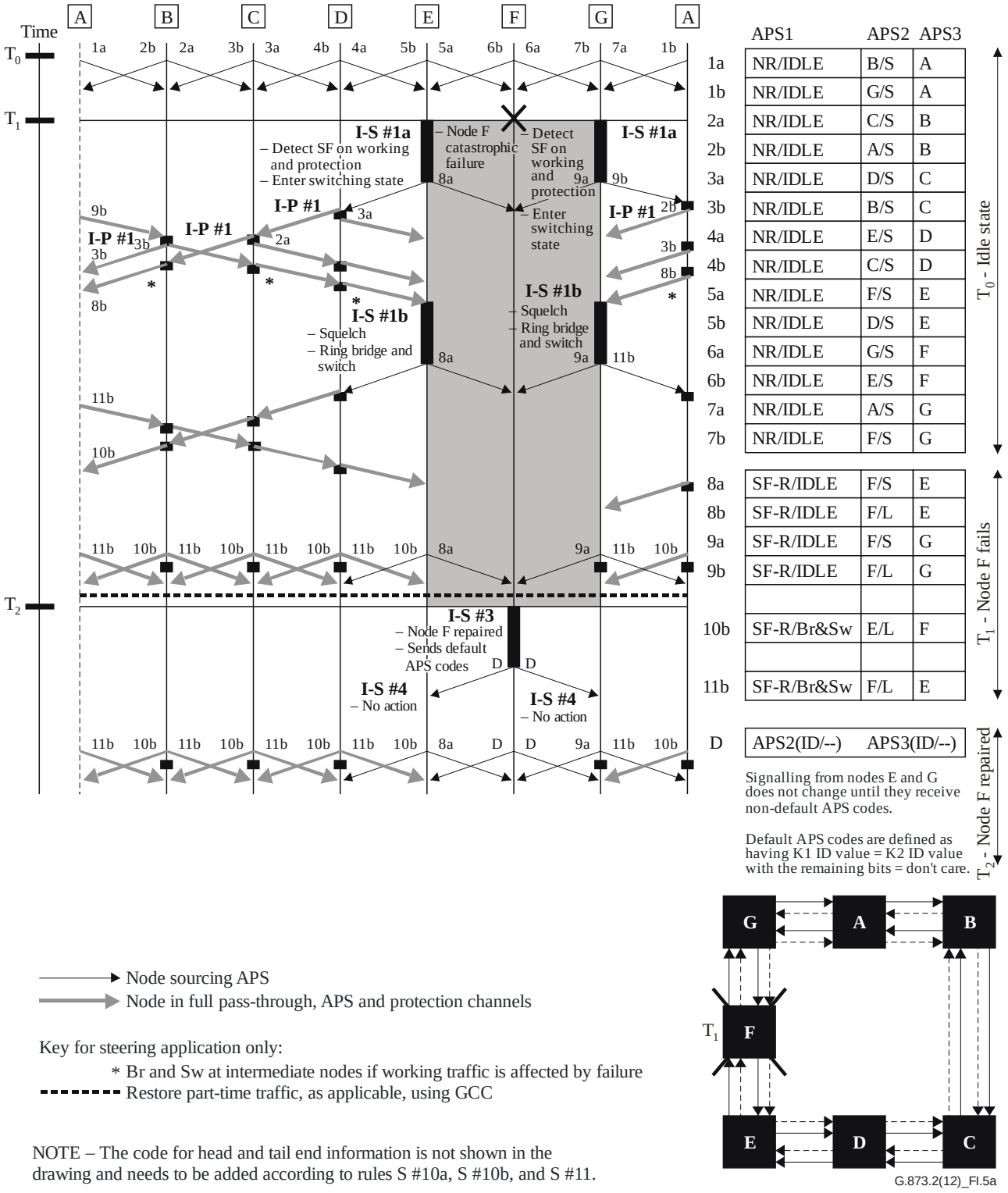


Figure I.5 – Four-fibre/four-lambda ODU SRP – Node failure

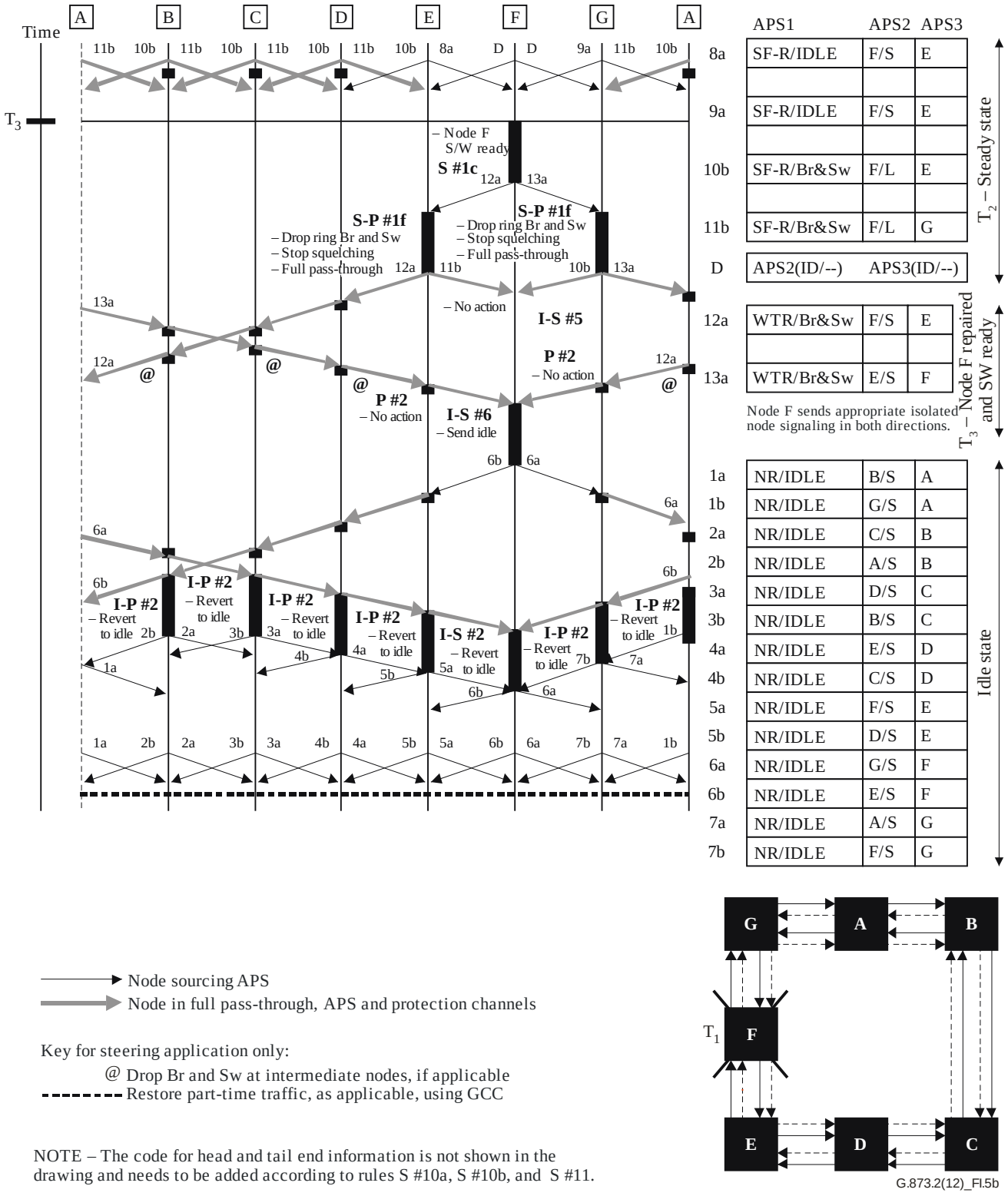


Figure I.5 – Four-fibre/four-lambda ODU SRP – Node failure *(concluded)*

This example covers the case of a node failure in both two- and four-fibre rings. Node failure here means that all transmission, both incoming and outgoing, to and from the node, has failed, affecting both working and protection channels, and the node itself has lost all provisioned information.

The initial state of the ring is the idle state. At time T_1, both nodes E and G detect an SF condition on their working and protection channels. They become switching nodes (Rule I-S #1) and source bridge requests on both the short and long paths (Rule S #1). Nodes A and D, and all successive intermediate nodes on the long path enter full pass-through (Rule I-P #1). Node E, upon reception of the bridge request from node G on the long path, squelches all potentially misconnected traffic, executes a ring bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Node G, upon reception of the bridge request from node E on the long path, squelches all potentially misconnected traffic, executes a ring bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Signalling reaches steady state.

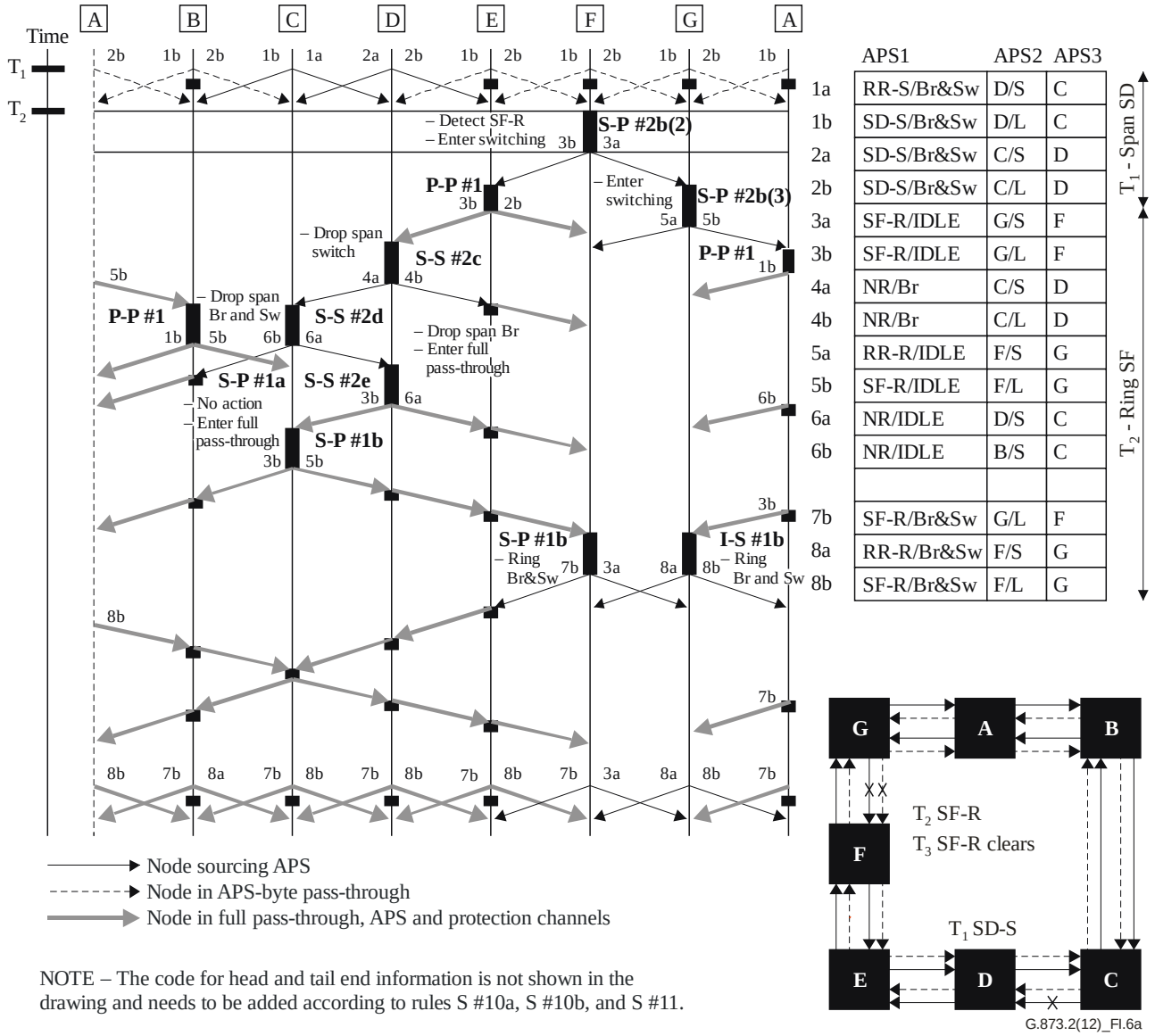
For steering applications, switching activities take place at the intermediate nodes. On all TS protection channels not being used to protect working channels, extra traffic is restored using the GCC.

At time T_2, the failed node has recovered physically but has not fully recovered its provisioning information, preventing the recovering node from proper APS-byte signalling. Until the recovering node is capable of proper APS-byte signalling in accordance with the current state of the ring, default APS codes are transmitted (Rule I-S #3). Nodes E and G detect the physical clearing of the signal from node F, but also receive default APS codes. As long as nodes E and G receive the default APS codes, they do not declare the defect cleared (Rule I-S #4). Signalling reaches steady state.

At time T_3, node F has fully recovered and signals appropriately. Nodes E and G receive non-default APS codes and declare the defect cleared. The WTR intervals at nodes E and G are pre-empted by the higher priority long-path bridge requests, causing nodes E and G to drop their ring bridge and switch, stop squelching and go into full pass-through (Rule S-P #1f). After Nodes E and G go into full pass-through, Node F receives long path bridge requests destined to itself from both E and G and takes no action (Rule I-S #5). When Node F receives the same signals which it is sending, it then signals the idle code in both directions (Rule I-S #6). All nodes then cascade back to the idle state.

I.6 Unidirectional SF-R pre-empting a unidirectional SD-S on non-adjacent spans

See Figure I.6.



NOTE – The code for head and tail end information is not shown in the drawing and needs to be added according to rules S #10a, S #10b, and S #11.

Figure I.6 – Four-fibre/four-lambda ODU SRP – Unidirectional SF-R pre-empting a unidirectional SD-S on non-adjacent spans

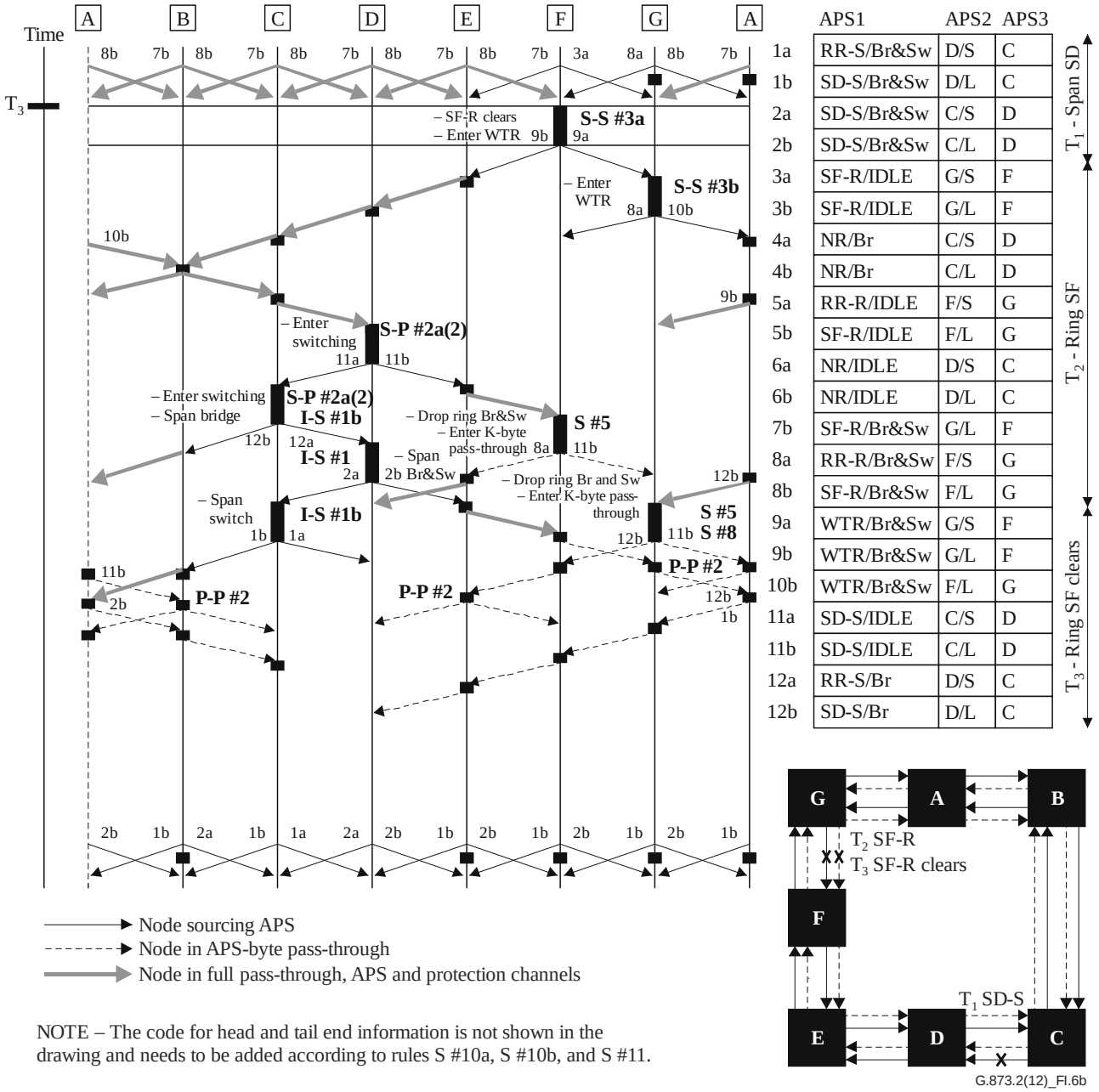


Figure I.6 – Four-fibre/four-lambda ODU SRP – Unidirectional SF-R pre-empting a unidirectional SD-S on non-adjacent spans *(concluded)*

This example covers the case of a unidirectional SF-R condition on a four-fibre ring pre-empting a unidirectional SD-S condition that had previously existed on a non-adjacent span.

The initial state of the ring is the idle state. At time T_1, node D detects an SD-S condition on its working channels from node C. The signalling proceeds in as shown in Figure I.1, except that:

1) the switching nodes become nodes C and D, not nodes E and F; and

2) the bridge request becomes SD-S, not SF-S.

Signalling reaches steady-state.

At time T_2, Node F detects an SF condition on its working and protection channels from Node G. Node F becomes a switching node (Rule S-P #2b) and sources bridge requests in both directions (Rule S #1). Node G, upon seeing the short-path ring request from node F, also becomes a switching node (Rule S-P #2b). Node G sources RR back on the short path, and SF-R on the long path (Rule S #3). Intermediate nodes A, B, and E change from APS-byte pass-through to full pass-through (Rule P-P #1). Node D, upon seeing a higher priority ring bridge request, drops its span switch, updates APS byte 1 bits 6-8, and sources NR in both directions (Rule S-S #2c). Node C, upon seeing a NR and dropped switch from node D, drops its bridge and switch, updates APS byte 1 bits 6-8, and acts on its highest priority input (Rule S-S #2d, first point) to source NR. Node C eventually sees a ring bridge request destined to node F, but this does not change Node C's signalling (Rule S-P #1a). Node D, upon seeing a dropped switch at node C, drops its bridge and acts on its highest priority input (Rule S-S #2e) to enter full pass-through. Node C, upon seeing the dropped bridge from node D, acts on its highest priority input (Rule S-P #1b) to enter full pass-through. With all the intermediate nodes in full pass-through, nodes F and G finally receive long-path ring bridge requests. Nodes F and G each execute a bridge and switch (Rule I-S #1b, second point) and update APS byte 1 bits 6-8. Signalling reaches steady state.

At time T_3, the SF condition on the working and protection channels from node E to node F clears. Node F enters WTR (Rule S-S #3a). Node G, upon seeing the WTR bridge request from node F, also enters WTR (Rule S-S #3b). Node D, upon seeing two WTR bridge requests which are lower priority than its locally detected SD condition, becomes a switching node [Rule S-P #2a, point 2)], and signals appropriately. Node C, upon seeing a higher priority span bridge request destined to it, also becomes a switching node [Rule S-P #2a, point 2)], executes a span bridge, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Node F loses its long path ring bridge request due to the span bridge request status from Node D. Node F drops its bridge and switch (Rule S #5), terminates its WTR signalling, and enters APS-byte pass-through (Rule S #8). Similarly, when Node G loses its long-path ring bridge request, it drops its bridge and switch (Rule S #5), terminates its WTR signalling, and enters bidirectional APS-byte pass-through. Node D, upon seeing a bridged code on the short path from node C, executes a span bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Node C, upon seeing a bridged and switched code from node D, completes the process by executing a span switch and updating APS byte 1 bits 6-8 (Rule I-S #1b). Intermediate nodes A, E, and B then move from full pass-through to APS-byte pass-through. Signalling reaches the same steady state as found at time T_1.

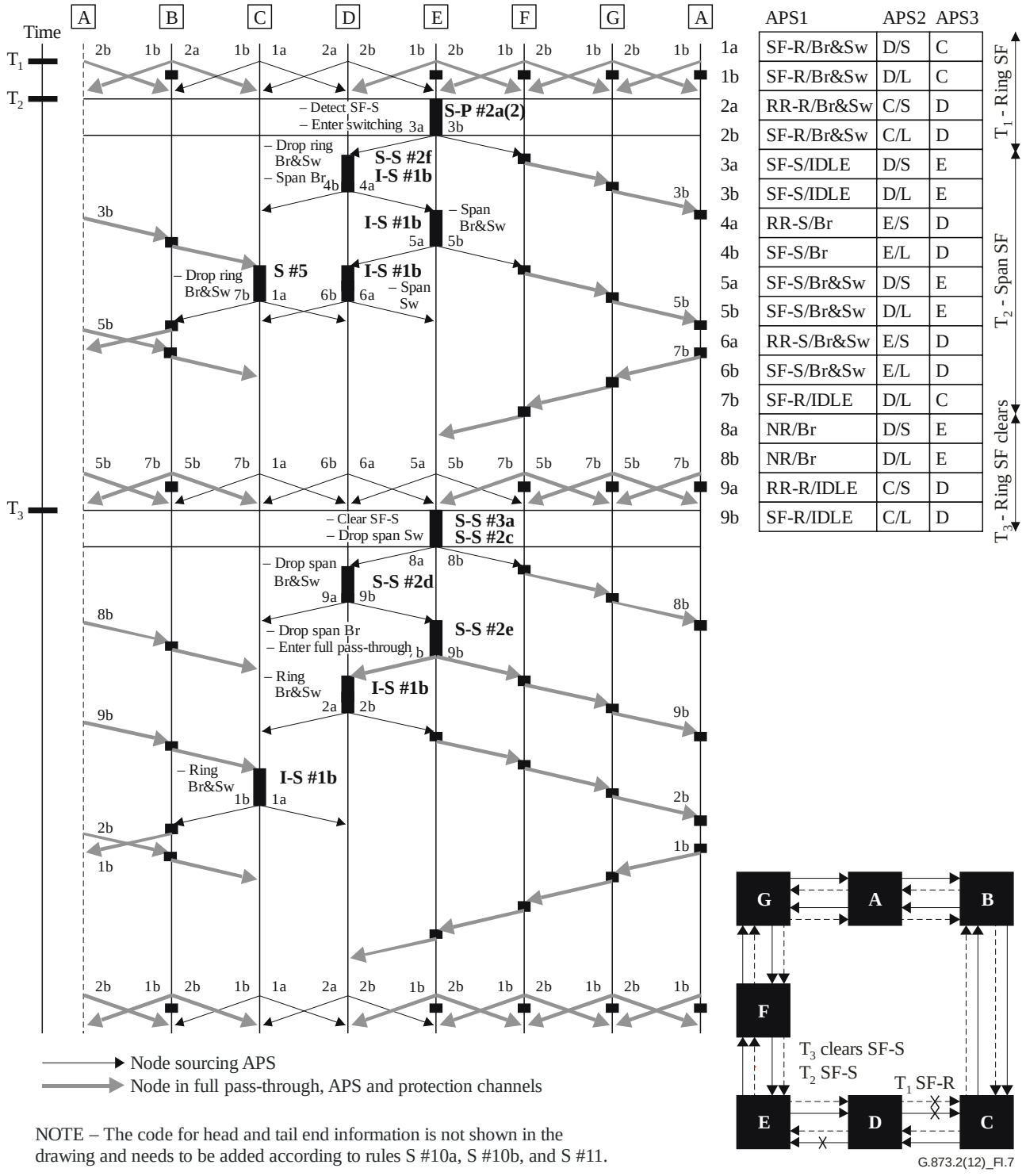
At time T_4 (not shown), the span SD condition on the working channels from node C to node D clears. The signalling proceeds in a manner as shown at time T2 in Figure I.1, except that:

1) the switching nodes become nodes C and D, not nodes E and F; and

2) the bridge request becomes SD-S, not SF-S.

I.7 Unidirectional SF-S pre-empting a unidirectional SF-R on adjacent spans – SF-S and SF-R detected at non-adjacent nodes

See Figure I.7.



NOTE – The code for head and tail end information is not shown in the drawing and needs to be added according to rules S #10a, S #10b, and S #11.

Figure I.7 – Four-fibre/four-lambda ODU SRP ring – Unidirectional SF-S pre-empting a unidirectional SF-R on adjacent spans

This example covers the case of a unidirectional SF-S condition on a four-fibre ring pre-empting a unidirectional SF-R condition that had previously existed on an adjacent span.

The initial state of the ring is the idle state. At time T_1, node C detects an SF condition on its working and protection channels from node D. The signalling proceeds in a manner as shown in Figure I.2 (at time T_1 in the figure), except that the switching nodes become nodes C and D, not nodes E and F. Signalling reaches steady state.

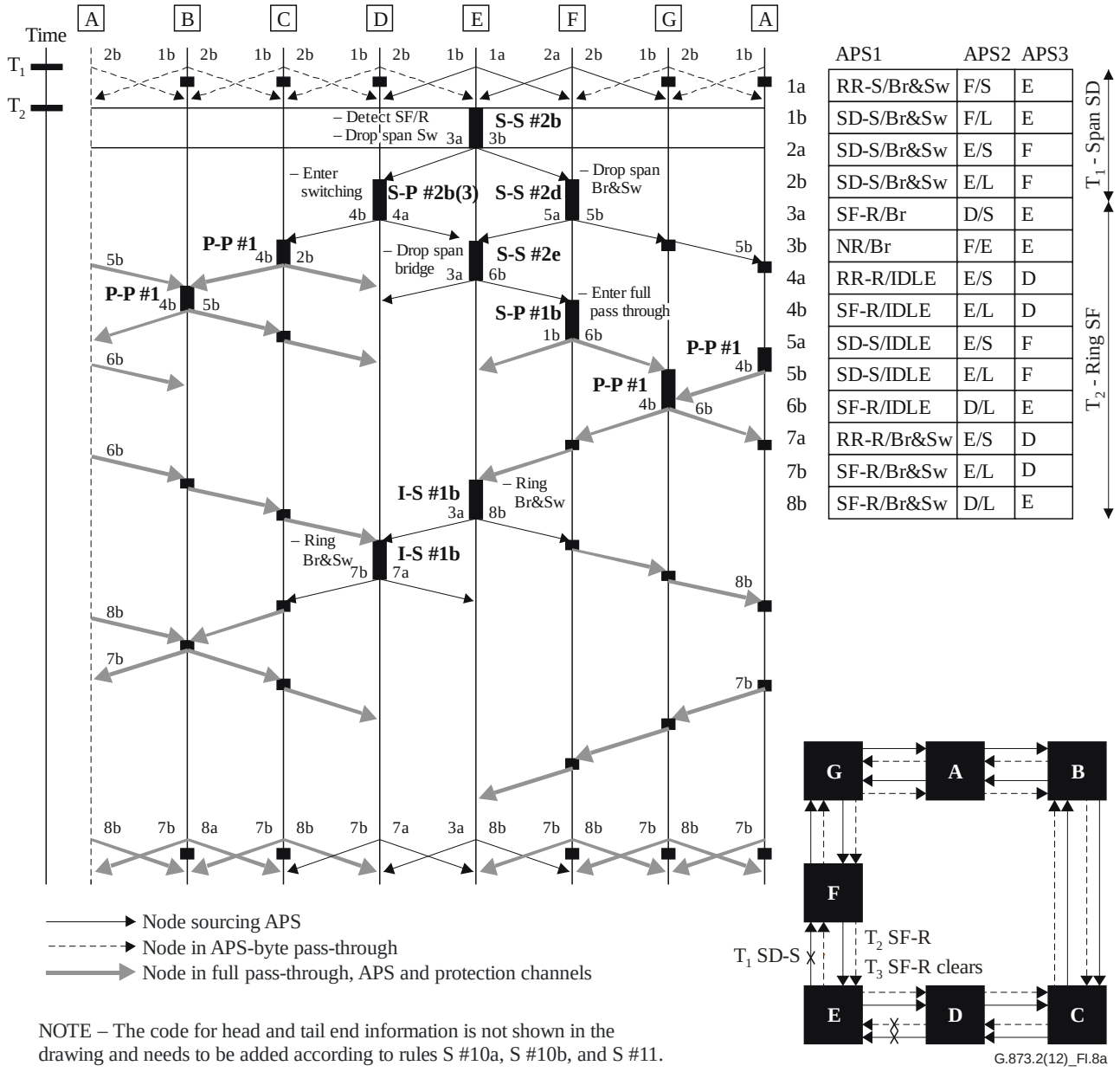
At time T_2, Node E detects an SF condition on its working channels from node D. Node E becomes a switching node [Rule S-P #2a, point 2)] and sources a span bridge request towards node D and a span bridge request status towards node F (Rules S #1, G #1). Node C, upon seeing this span bridge request status, drops its ring bridge and switch because it is no longer receiving a long-path ring bridge request (Rule S #5). Node C updates its APS byte 1 bits 6-8, and sources SF-R in APS byte 1 because that is its highest priority input (Rule S #5). Node D, upon seeing the higher priority span bridge request from node E, drops its ring bridge and switch, executes a span bridge towards node E (Rule S-S #2f), and signals accordingly (Rule I-S #1b, third point, and Rule S #3). Node E, upon seeing the bridged code from node D, executes a span bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b, third point). Node D, upon seeing the bridged code from node E, executes a switch, and updates APS byte 1 bits 6-8 accordingly (Rule I-S #1b, third point). Signalling reaches steady state.

At time T_3, the SF condition on the working channels from node D to node E clears. Node E would enter WTR, but it detects another failure (Rule S-S #3a). Node E, upon seeing the SF-R bridge request destined to node D (for a span which is non-adjacent), drops its span switch, signals NR in APS byte 1, and Bridged in APS byte 2 (Rule S-S #2c). Node D, upon seeing the NR and bridged codes from node E, drops its span bridge and switch, and acts on the input from node C to signal a ring bridge request back to node C (Rule S-S #2d). Node E, upon seeing that node D has dropped its switch, drops its bridge (Rule S-S #2e). Node E also sees a long-path ring bridge request destined to node D, so node E also enters full pass-through (Rule S-S #2e, fourth point). Node D, upon seeing a long-path ring bridge request from node C, executes a ring bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Node C, upon seeing a long-path ring bridge request from node D, also executes a ring bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Signalling reaches the same steady state found at time T_1.

At time T_4 (not shown), the SF condition on the working and protection channels from node D to node C clears. The signalling proceeds in the manner as shown in Figure I.2 (at time T_2 in the figure), except that the switching nodes become nodes C and D, not nodes E and F.

I.8 Unidirectional SF-R pre-empting a unidirectional SD-S on adjacent spans

See Figure I.8.



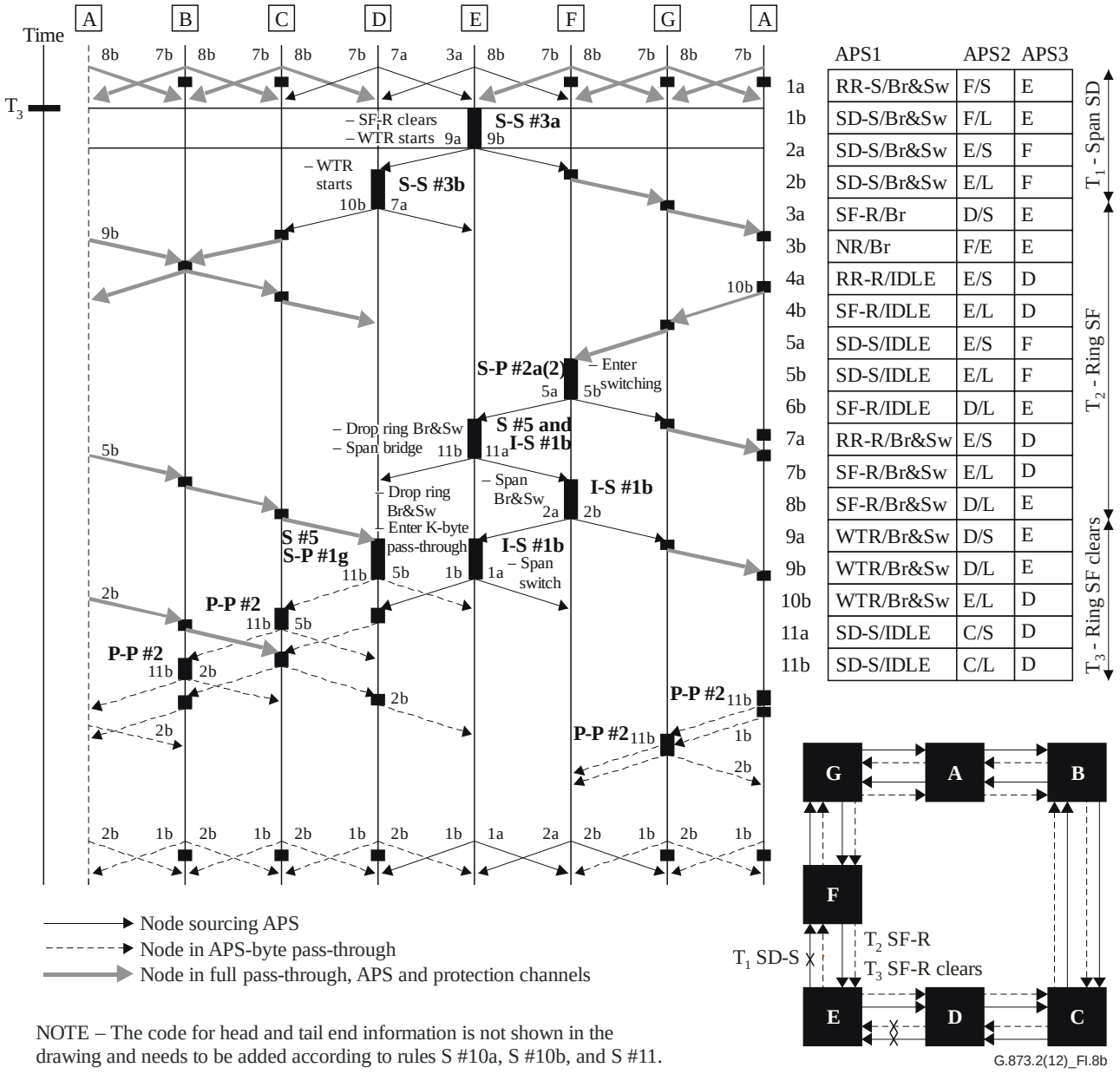
	APS1	APS2	APS3
1a	RR-S/Br&Sw	F/S	E
1b	SD-S/Br&Sw	F/L	E
2a	SD-S/Br&Sw	E/S	F
2b	SD-S/Br&Sw	E/L	F
3a	SF-R/Br	D/S	E
3b	NR/Br	F/E	E
4a	RR-R/IDLE	E/S	D
4b	SF-R/IDLE	E/L	D
5a	SD-S/IDLE	E/S	F
5b	SD-S/IDLE	E/L	F
6b	SF-R/IDLE	D/L	E
7a	RR-R/Br&Sw	E/S	D
7b	SF-R/Br&Sw	E/L	D
8b	SF-R/Br&Sw	D/L	E

T_1 - Span SD

T_2 - Ring SF

NOTE – The code for head and tail end information is not shown in the drawing and needs to be added according to rules S #10a, S #10b, and S #11.

Figure I.8 – Four-fibre/four-lambda ODU SRP – Unidirectional SF-R pre-empting a unidirectional SD-S on non-adjacent spans



NOTE – The code for head and tail end information is not shown in the drawing and needs to be added according to rules S #10a, S #10b, and S #11.

Figure I.8 – Four-fibre/four-lambda ODU SRP – Unidirectional SF-R pre-empting a unidirectional SD-S on non-adjacent spans *(concluded)*

This example covers the case of a unidirectional SF-R condition on a four-fibre ring pre-empting a unidirectional SD-S condition that had previously existed on an adjacent span.

The initial state of the ring is the idle state. At time T_1, node F detects an SD condition on its working channels from node E. The signalling proceeds in the manner as shown in Figure I.1 (at time T_1 in the figure), except that the bridge request becomes SD-S, not SF-S. Signalling reaches steady state.

At time T_2, node E detects an SF condition on its working and protection channels from node D. Node E drops its span switch, sources a SF-R bridge request (in APS byte 1) and Bridged (in APS byte 1) towards Node D, and sources NR (in APS byte 1) and bridged (in APS byte 1) towards Node F (Rule S-S #2b). Node D becomes a switching node [Rule S-P #2b, point 3)]. Node D sources RR on the short path, and a SF-R bridge request on the long path (Rule S #3). This long-path ring bridge request changes nodes C, B, and A from APS-byte pass-through to full pass-through (Rule P-P #1). Node F, upon seeing a NR and dropped switch from node E, drops its bridge and switch, updates APS byte 1 bits 6-8, and acts on its highest priority input (Rule S-S #2d,

last point) to source a SD-S bridge request towards node E. Node E, upon seeing a dropped switch at node F, drops its bridge, updates APS byte 1 bits 6-8, and acts on its highest priority input (Rule S-S #2e, third point) to source ring bridge requests in both directions. Node F, upon seeing the dropped bridge from Node E, acts on its highest priority input (Rule S-P #1b) to enter full pass-through. This permits a long-path ring bridge request to reach node G, and node G changes from APS-byte pass-through to full pass-through (Rule P-P #1). With all the intermediate nodes in full pass-through, nodes E and D finally receive long-path ring bridge requests. Nodes E and D each execute a bridge and switch (Rule I-S #1b, second point) and update APS byte 1 bits 6-8. Signalling reaches steady state.

At time T_3, the SF condition on the working and protection channels from node D to node E clears. Node E starts its WTR period, and signals so (Rule S-S #3a). Node D, upon seeing the WTR bridge request from node E, also starts its WTR period, and signals so (Rule S-S #3b). Node F, upon seeing WTR bridge requests from both directions, acts on the fact that its local SD-S condition is higher priority, and becomes a span switching node [Rule S-P #2a, point 2)]. Node E, upon seeing the span bridge request from node F, loses its long-path ring bridge request from Node D. Node E therefore drops its ring bridge and switch (Rule S #5), and acts on the span bridge request from node F by executing a span bridge (Rule I-S #1b, third point). Node F, upon seeing the bridged code from node F, executes a span bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b, third point). Node E, upon seeing the bridged and switched codes from node F, completes the process by executing a span switch and updating APS byte 1 bits 6-8 (Rule I-S #1b, third point). Meanwhile, node D, upon seeing the span bridge request from node F, loses its long-path ring bridge request from node E. Node D therefore drops its ring bridge and switch (Rule S #5), and acts on the span bridge request status destined to node E by entering APS-byte pass-through (Rule S-P #1g). Intermediate full pass-through nodes A, B, C and G eventually receive a span bridge request status not destined to them from both directions, so they move into APS-byte pass-through. Signalling reaches the same steady state found at time T_1.

At time T_4 (not shown), the SD condition on the working channels from node E to node F clears. The signalling proceeds in a manner as shown in Figure I.1 (at time T_2 in the figure), except that the bridge request becomes SD-S, not SF-S.

I.9 Unidirectional SF-R coexisting with a unidirectional SF-R on non-adjacent spans

See Figure I.9.

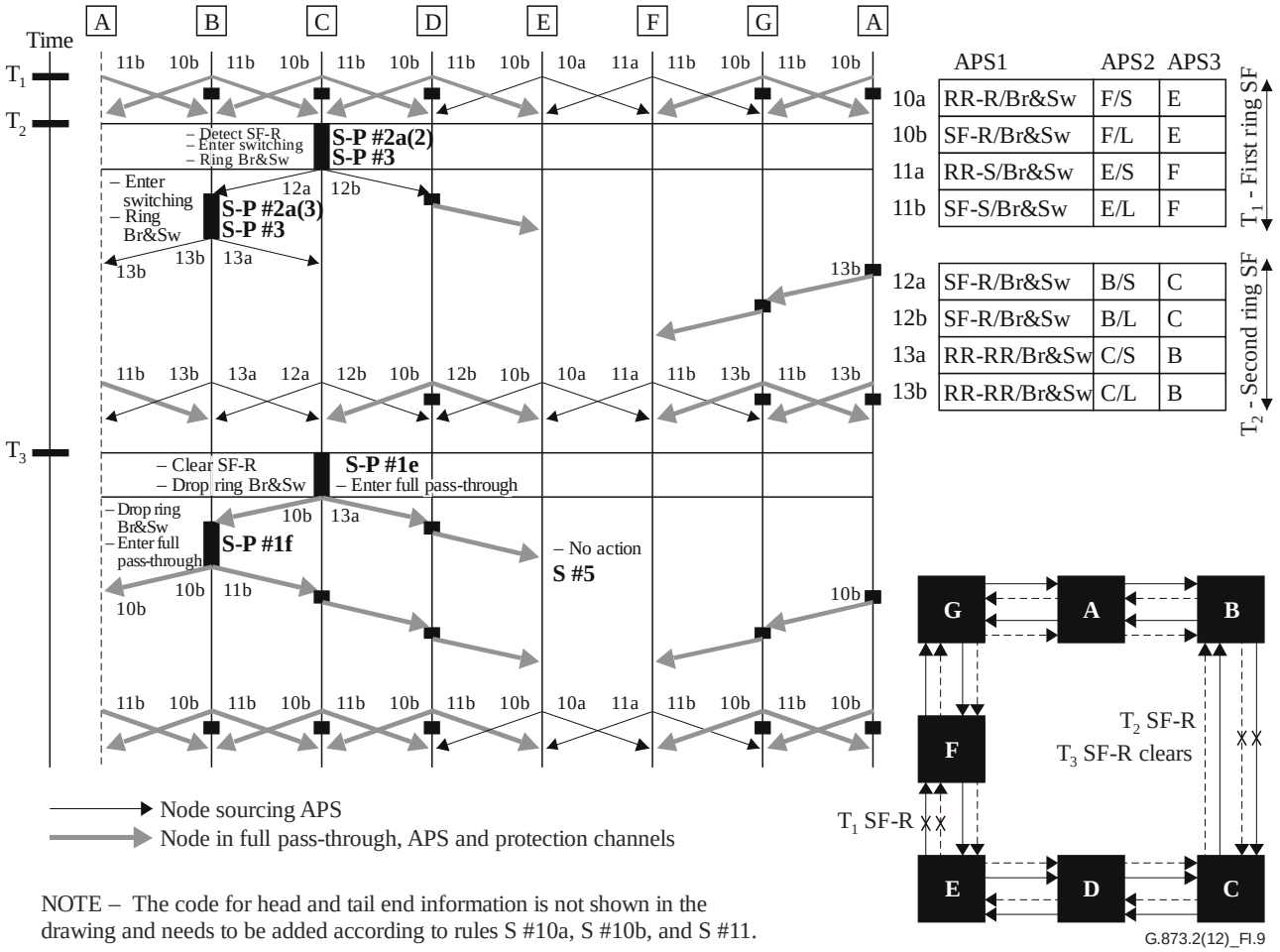


Figure I.9 – Four-fibre/four-lambda ODU SRP – Unidirectional SF-R plus unidirectional SF-R on non-adjacent spans

This example covers the case of a unidirectional SF-R condition on a four-fibre ring coexisting with another unidirectional SF-R condition that had previously existed on a non-adjacent span.

The initial state of the ring is the idle state. At time T_1, node F detects an SF condition on its working and protection channels. The signalling proceeds in a manner as shown in Figure I.2 (at time T_1 in the figure). The signalling reaches steady state.

At time T_2, node C detects an SF condition on its working and protection channels. Node C becomes a switching node [Rule S-P #2a, point 2)], squelches traffic if necessary, executes a ring bridge and switch, and sources ring bridge requests in both directions (S-P #3). Node B, upon seeing the bridge request from node C, becomes a switching node [Rule S-P #2a, point 3)]. Node B also squelches traffic if necessary, executes a ring bridge and switch, and sources ring bridge requests in both directions (S-P #3). The long-path ring bridge request from nodes B and C do not affect the bridges and switches at nodes E and F, because multiple SF-R switches are allowed to coexist (Rule S #4a, Rule S #5). The signalling reaches steady state.

For steering applications, there is some additional signalling that occurs. As shown in Figure I.10, at time T_2, node C detects an SF condition on its working and protection channels. Node C becomes a switching node [Rule S-P #2a, point 2)], drops extra traffic if present, maintains ring bridges and switches on the tributaries affected by the first failure, and sources ring bridge requests in both directions (Rule S-P #3 in steering clause 7.3). Node B, upon seeing the bridge request from Node C, becomes a switching node [Rule S-P #2a, point 3)]. Node B also drops extra traffic if present, maintains ring bridges and switches on the tributaries affected by the first failure, and sources ring bridge requests in both directions (Rule S-P #3 in Steering clause 7.3). Node E (F),

upon seeing the ring bridge request from node C (B), drops extra traffic if present, maintains ring bridges and switches on the tributaries affected by the first failure, and updates APS byte 1 bits 6-8 to the idle code [Rule S-S #1a, point 2), in Steering clause 7.3]. Node C (B), upon seeing the ring bridge request and an idle code from node E (F), updates APS byte 1 bits 6-8 to bridged and switched [Rule S-S #1a, point 2), in steering clause 7.3]. Node E (F), upon seeing the ring bridge request and the bridged and switched code from node C (B), updates APS byte 1 bits 6-8 to bridged and switched [Rule S-S #1a, point 3), in steering clause 7.3]. Signalling reaches the same steady state as described for Figure I.9.

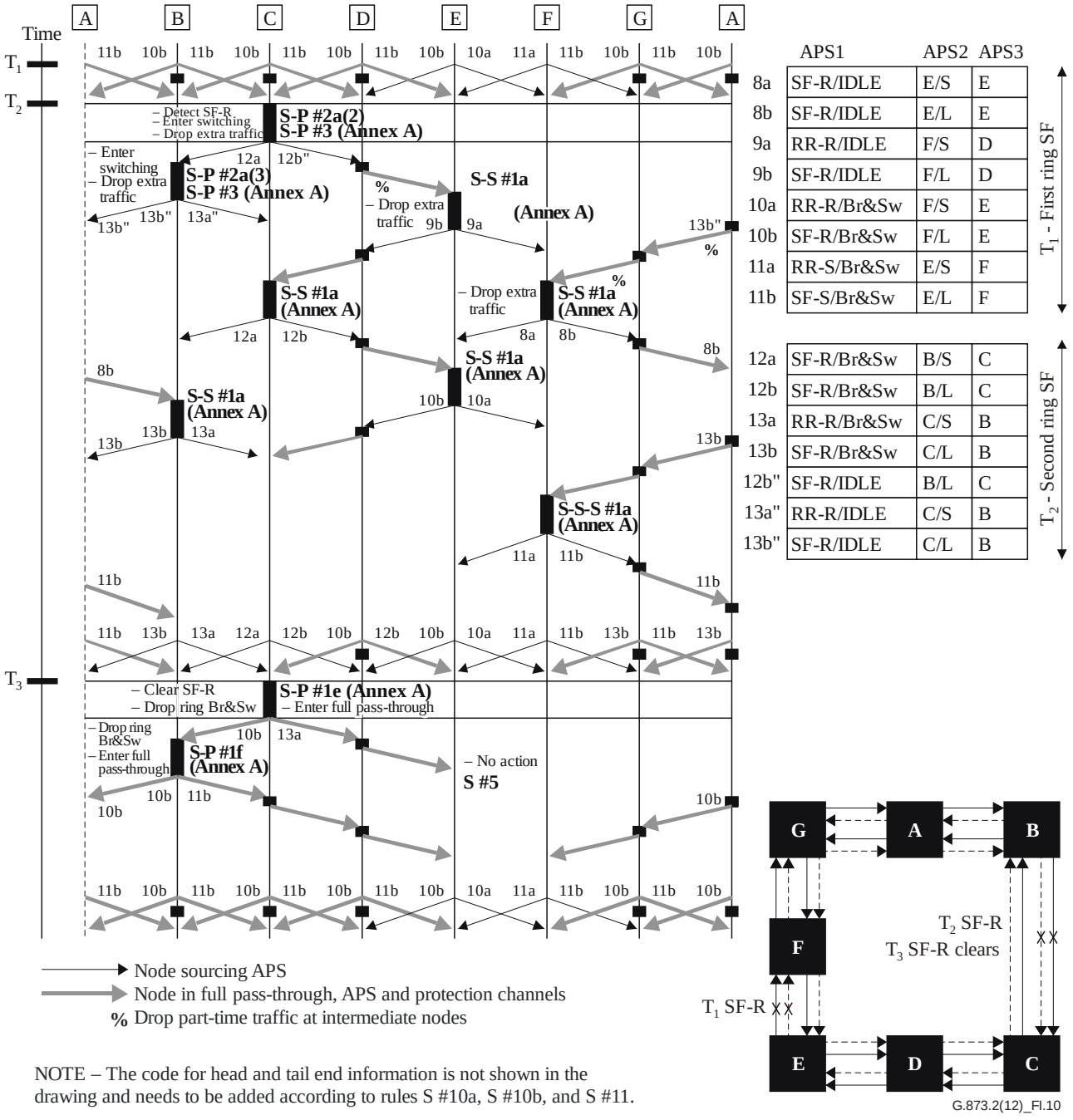
At time T_3, the SF condition on the working and protection channels from node B to node C clears. Node C sees from node D a ring bridge request for a non-adjacent span. This is a higher priority than its local (WTR) condition, so node C drops its bridge and switch and enters full pass-through (Rule S-P #1e). This permits the short-path ring RR signal from node B to reach node E. Node E still considers this to be a valid ring bridge request, so Node E retains its ring bridge and switch (Rule S #5). Node B, upon receiving both ring bridge requests that are not destined to it, drops its bridge and switch and enters full pass-through (Rule S-P #1f). Signalling reaches the same steady state as found at time T_1.

For steering applications, the signalling is identical, but the nodes have additional actions to perform. As shown in Figure I.10, at time T_3, the SF condition on the working and protection channels from node B to node C clears. Node C sees from node D a ring bridge request for a non-adjacent span, due to the first SF-R between nodes E and F. This is a higher priority than its local (WTR) condition, so node C maintains ring bridges and switches on the tributaries affected by the first failure, and enters full pass-through [Rule S-P #1e, point 1), in Steering clause 7.3]. This permits the short-path ring RR signal from node B to reach node E. Node E still considers this to be a valid ring bridge request, so node E retains its ring bridge and switch (Rule S #5). Node B sees ring bridge requests that are not destined to it, due to the first SF-R between nodes E and F. Node B maintains ring bridges and switches on the tributaries affected by the first failure, and enters full pass-through [Rule S-P #1f, point 1), in steering clause 7.3]. Signalling reaches the same steady state as described for Figure I.9.

At time T_4 (not shown), the SF condition on the working and protection channels from node E to node F clears. The signalling proceeds in a manner as shown in Figure I.2 (at time T_3 in the figure).

I.10 Node failure on a ring with extra traffic capability

Figure I.11 covers the case of extra traffic squelching on a ring after a node failure on either a two- or four-fibre ring. Node failure here means that all transmissions, including both incoming and outgoing, to and from the node, have failed, affecting both working and protection channels, and the node itself has lost all provisioned information.



NOTE – The code for head and tail end information is not shown in the drawing and needs to be added according to rules S #10a, S #10b, and S #11.

Figure I.10 – Four-fibre/four-lambda ODU SRP – Unidirectional SF-R plus unidirectional SF-R on non-adjacent spans (steering application)

The initial state of the ring is the idle state. Extra traffic is supported on the protection channels around the ring. At time T_1, both nodes E and G detect an SF condition on their working and protection channels. Nodes E and G drop extra traffic bidirectionally, become switching nodes (Rule I-S #1a, S #7), and source bridge requests on the long and short paths. All intermediate nodes will drop extra traffic bidirectionally, and enter into unidirectional full pass-through (Rule I-P #1). The nodes enter bidirectional full pass-through upon receiving crossing APS-bytes. Node E, upon reception of the bridge request from G on the long path, squelches all potentially misconnected traffic, executes a ring bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Node G, upon reception of the bridge request from E on the long path squelches all potentially misconnected traffic, executes a ring bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Signalling reaches steady state.

At time T_2, the failed node has recovered and the recovery sequence proceeds as per normal node recovery. Extra traffic is un-squelched when the node receives NR and idle or ET code from both directions.

I.11 Unidirectional SF-S pre-empting a unidirectional SF-R on adjacent spans – SF-S and SF-R detected at adjacent nodes

See Figure I.11.

This example covers the case of a unidirectional SF-S condition on a four-fibre ring pre-empting a unidirectional SF-R condition that had previously existed on an adjacent span.

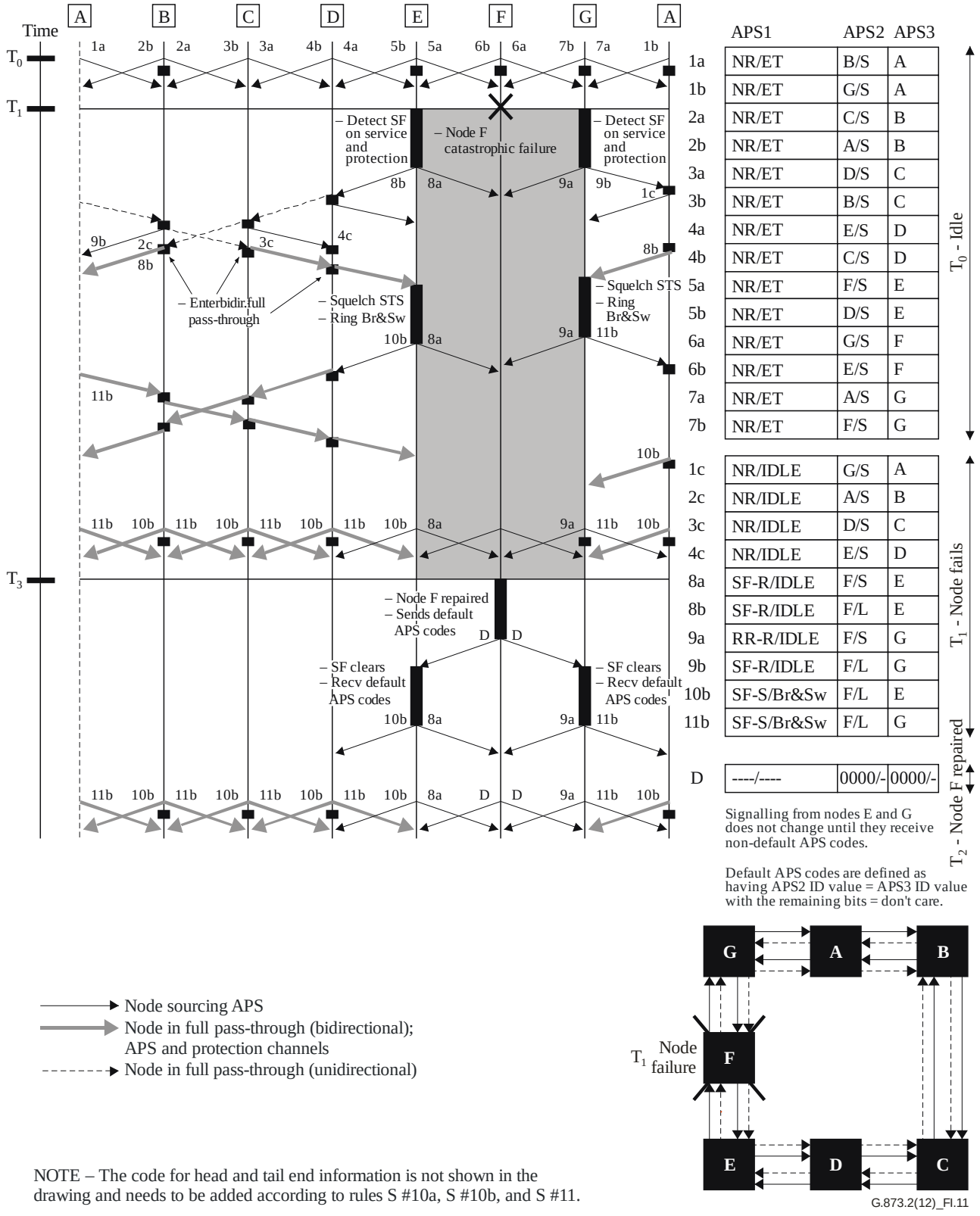


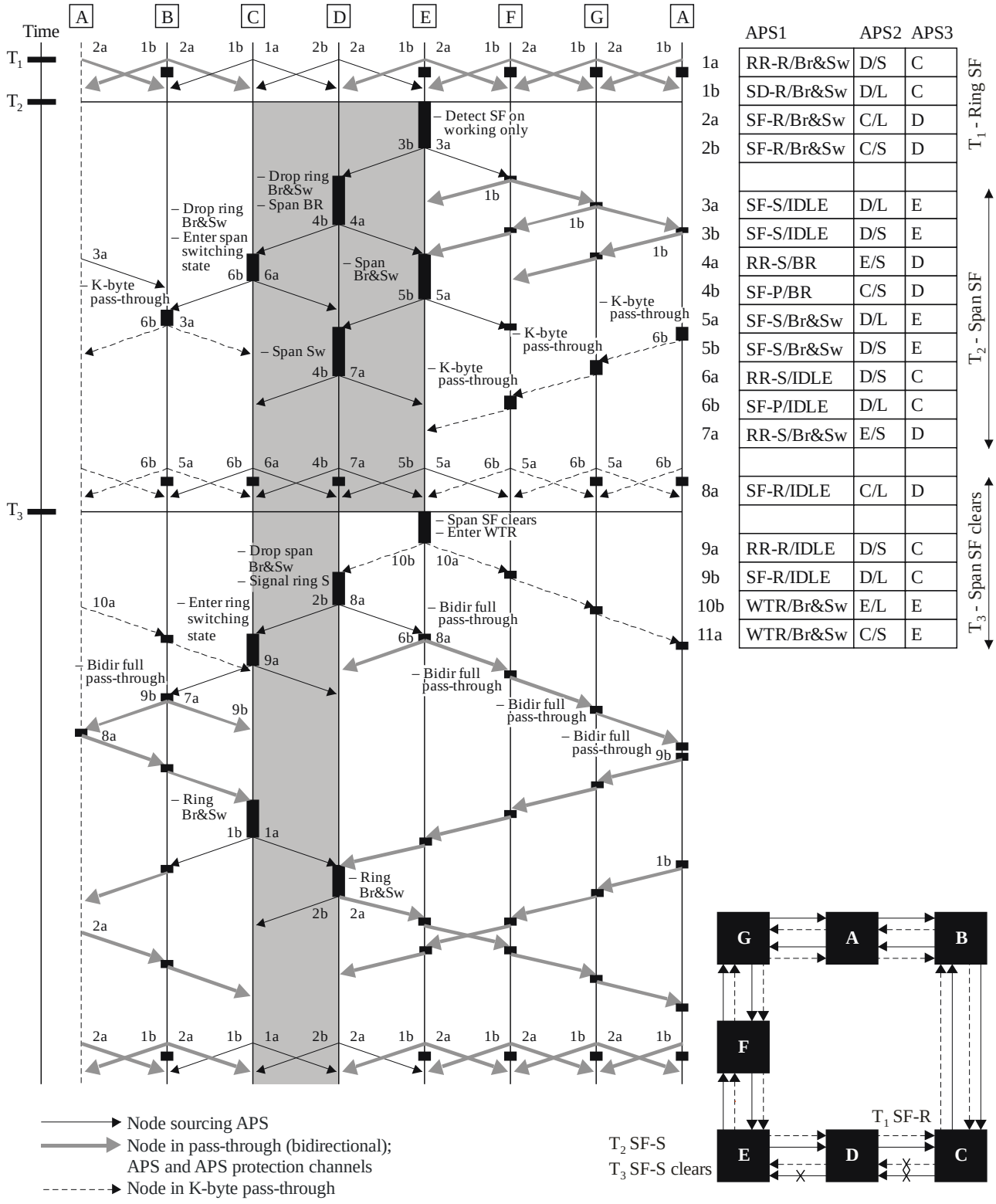
Figure I.11 – Four-fibre/four-lambda ODU SRP – Node failure on a ring with extra traffic

The initial state of the ring is the idle state. At time T_1, node D detects an SF condition on its working and protection channels from node C. The signalling proceeds in a manner as shown in Figure I.2 (at time T_1 in the figure), except that the switching nodes become nodes C and D, not nodes E and F. Signalling reaches steady state.

At time T_2, node E detects a SF condition on its working channel from node D. Node E becomes a switching node (Rule S-P #2a) and sources a span bridge request towards node D and a span bridge request status towards node F destined for node D (Rules S #1, G #1). Node D, upon seeing the higher priority span bridge request from node E, drops its ring bridge and switch, and signals based on its highest allowed coexisting APS requests (Rules G #1c, S-S #2h). Node D's highest priority input allowed to coexist is SF-S request from node E, and SF-P detected from node C (Rule S-S #2 h). It executes a span bridge towards node E (Rule S-S #2f), and signals accordingly (Rules I-S #1b, S #3). Node D also signals SF-P and bridged towards node C, since SF-P and SF-S are allowed to coexist (Rules S #4 a, S-S #2 h). Node C, upon losing the ring bridge request and seeing SF-P destined for it on the short path, becomes a span switching node, and responds to the span request accordingly (Rules S-P #2 b, S #1b). Node E, upon seeing the bridged code from Node D, executes a span bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Node D, upon seeing the bridged code from node E, executes a switch, and updates APS byte 1 bits 6-8 accordingly (Rule I-S #1b). Intermediate nodes enter APS-byte pass-through when crossing APS-bytes are detected (Rule P-P #2). Signalling reaches steady state.

At time T_3, the SF condition on the working channels from node D to node E clears. Node E enters WTR and signals accordingly (Rule S-S #3a). Node D, upon seeing the WTR code from node E, drops its span bridge and switch, and acts on all its inputs, which is a detected SF-R and a lower priority WTR request from node E. Node D signals a ring bridge request toward node C on both the long and short path (Rule S-S #2d). Node E, upon seeing a ring bridge request destined to another node, enters bidirectional full pass-through (Rule S-P #1e). Node C, upon losing the span bridge request and seeing a long-path ring bridge request from node D, executes a ring bridge and switch, and updates APS byte 1 bits 6-8 (Rules S #6, I-S #1b). Node D, upon seeing a long-path ring bridge request from node C, also executes a ring bridge and switch, and updates APS byte 1 bits 6-8 (Rule I-S #1b). Signalling reaches the same steady state found at time T_1.

At time T_4 (not shown), the SF condition on the working and protection channels from node C to node D clears. The signalling proceeds in the manner as shown at time T_2 in Figure I.2, except that the switching nodes become nodes C and D, not nodes E and F.



	APS1	APS2	APS3	
1a	RR-R/Br&Sw	D/S	C	T_1 - Ring SF
1b	SD-R/Br&Sw	D/L	C	
2a	SF-R/Br&Sw	C/L	D	
2b	SF-R/Br&Sw	C/S	D	
3a	SF-S/IDLE	D/L	E	T_2 - Span SF
3b	SF-S/IDLE	D/S	E	
4a	RR-S/BR	E/S	D	
4b	SF-P/BR	C/S	D	
5a	SF-S/Br&Sw	D/L	E	
5b	SF-S/Br&Sw	D/S	E	
6a	RR-S/IDLE	D/S	C	
6b	SF-P/IDLE	D/L	C	
7a	RR-S/Br&Sw	E/S	D	
8a	SF-R/IDLE	C/L	D	T_3 - Span SF clears
9a	RR-R/IDLE	D/S	C	
9b	SF-R/IDLE	D/L	C	
10b	WTR/Br&Sw	E/L	E	
11a	WTR/Br&Sw	C/S	E	

NOTE – The code for head and tail end information is not shown in the drawing and needs to be added according to rules S #10a, S #10b, and S #11.

G.873.2(12)_FI.12

Figure I.12 – Four-fibre/four-lambda ODU SRP – Unidirectional SF-S pre-empting a unidirectional SF-R on adjacent spans – SF-S and SF-R detected on adjacent nodes

Appendix II

Generalized squelching logic

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

This appendix provides the generalized squelching logic for circuits that are not of a simple bidirectional nature. Generalized squelching logic can be derived from the notions of squelching for basic unidirectional circuits, squelching for multiply dropped unidirectional circuits, and squelching for multiply sourced unidirectional circuits. Bidirectional switching and the HO ODU path or LO ODU tandem connection shared protection ring switching protocols described in other portions of this Recommendation are not impacted by this generalization. The extension of squelching logic formally allows a greater variety of services to be provisioned within the context of this Recommendation.

For clarity, the squelching requirements of this appendix will be discussed from the standpoint of an observer at a switching node. For simplicity, the figures show just the switching node on one side of the node failure.

II.1 Squelching for unidirectional (and bidirectional) circuits

The following two rules are required for squelching simple unidirectional circuits:

1) Assume, with respect to the switching node, that the failure is in the direction of the unidirectional circuit. Squelch the circuit (insert AIS into the circuit's corresponding protection channel as it is bridged in the direction away from the failure) if and only if the node failure scenario includes the exit node for the unidirectional circuit. See Figure II.1.

2) Assume, with respect to the switching node, that the failure is in the opposite direction from the direction of the unidirectional circuit. Squelch the circuit (insert AIS into the working channel) if and only if the node failure scenario includes the entry node for the unidirectional circuit. See Figure II.2.

Note that the combination of these two rules give the current rule for bidirectional squelching of a bidirectional circuit at a switching node if the circuit is terminated at a failed node. See Figure II.3.

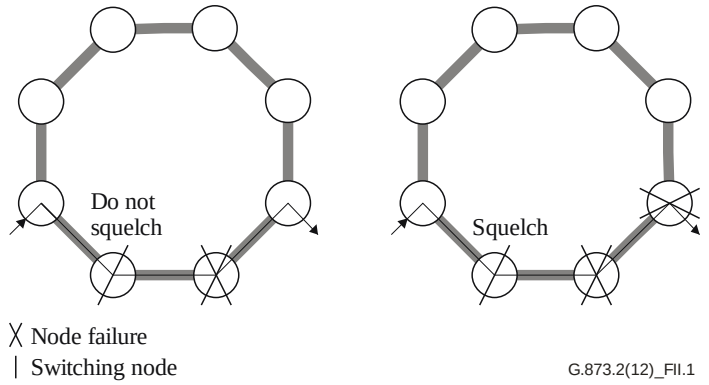


Figure II.1 – Unidirectional circuit squelching example where the failure is in the direction of the unidirectional circuit

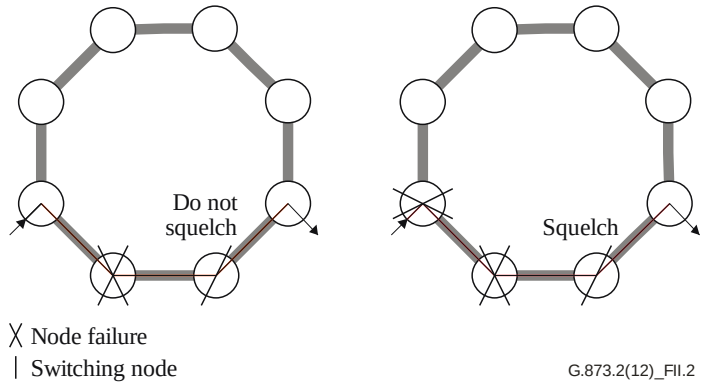


Figure II.2 – Unidirectional circuit squelching example where the failure is in the opposite direction from the unidirectional circuit

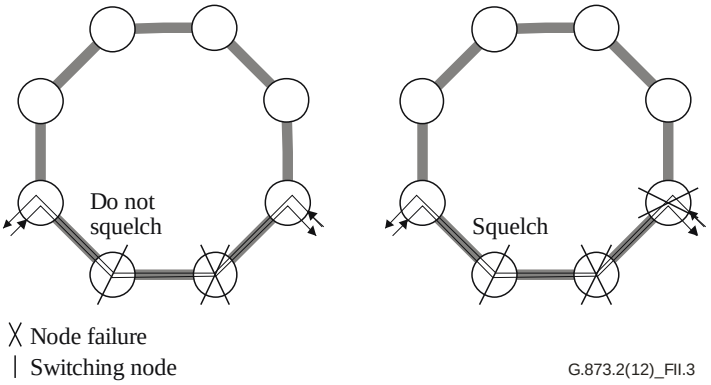


Figure II.3 – Bidirectional circuit squelching example

II.2 Squelching of multiply dropped and multiply sourced unidirectional circuits

II.2.1 Multiply dropped unidirectional circuits

A multiply dropped unidirectional circuit is shown in Figure II.4. Intuitively, in the presence of failures, the squelching logic should allow a circuit to be delivered to as many drops as possible. The corresponding squelching rules are similar to those for simple unidirectional circuits:

1) Assume, with respect to the switching node, that the failure is in the direction of the multiply dropped unidirectional circuit. Squelch the circuit (insert AIS into the circuit's corresponding protection channel as it is bridged in the direction away from the failure) if and only if the node failure scenario includes the exit node for the multiply dropped unidirectional circuit. See Figure II.5.

2) Assume, with respect to the switching node, that the failure is in the opposite direction from the direction from the multiply dropped unidirectional circuit. Squelch the circuit (insert AIS into the working channel) if and only if the node failure scenario includes the entry node for the multiply dropped unidirectional circuit. See Figure II.6.

A unidirectional broadcast is treated as two independent unidirectional circuits for squelching purposes.

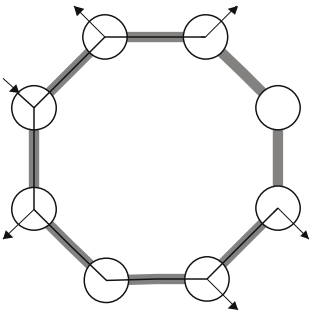


Figure II.4 – Multiply dropped unidirectional circuit example

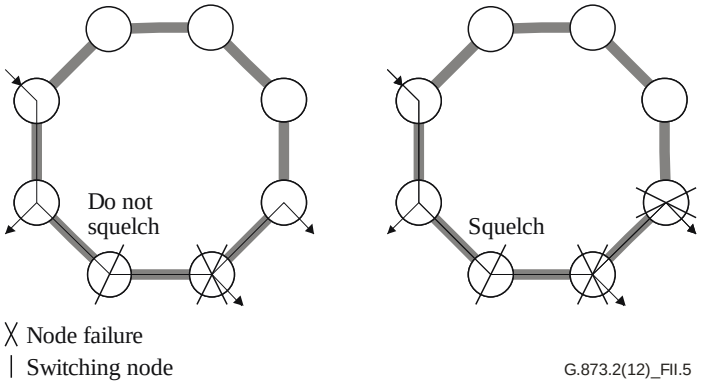


Figure II.5 – Multiply dropped unidirectional circuit squelching example where the failure is in the direction of the unidirectional circuit

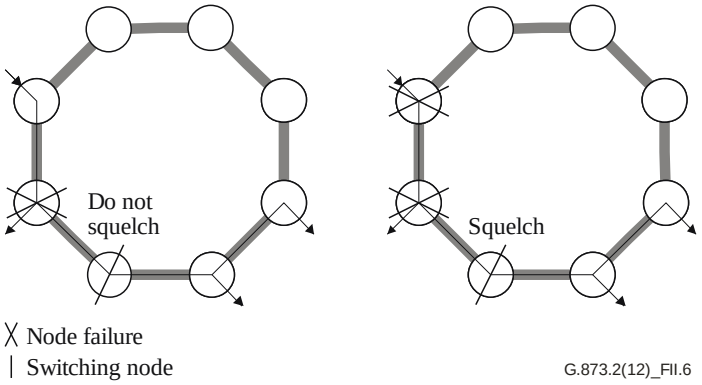


Figure II.6 – Multiply dropped unidirectional circuit squelching example where the failure is in the opposite direction from the unidirectional circuit

II.2.2 Multiply sourced unidirectional circuits

A multiply sourced unidirectional circuit is illustrated in Figure II.7. The following discussion is independent of which source is actually transmitted to the end node, or how that decision is made or implemented. The objective of the squelching logic is, in the presence of failures, to deliver the circuit to the drop node as long there is at least one source. The corresponding squelching rules are similar to those for simple unidirectional circuits:

1) Assume, with respect to the switch node, that the failure is in the direction of the multiply sourced unidirectional circuit. Squelch the circuit (insert AIS into the circuit's corresponding protection channel as it is bridged in the direction away from the failure) if and only if the node failure scenario includes the exit node for the multiply sourced unidirectional circuit. See Figure II.8.

2) Assume, with respect to the switching node, that the failure is in the opposite direction from the direction of the multiply sourced unidirectional circuit. Squelch the circuit (insert AIS into the working channel) if and only if the node failure scenario includes the entry node (i.e., the first source node) for the multiply sourced unidirectional circuit. See Figure II.9.

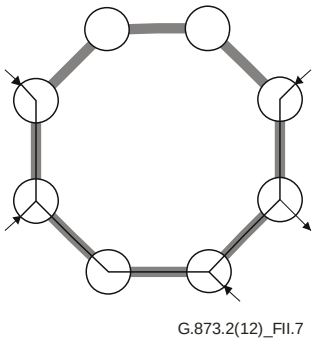


Figure II.7 – Multiply sourced unidirectional circuit example

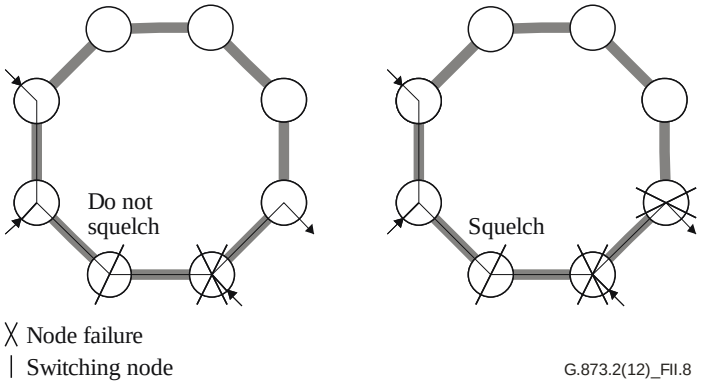


Figure II.8 – Multiply sourced unidirectional circuit squelching example where the failure is in the direction of the unidirectional circuit

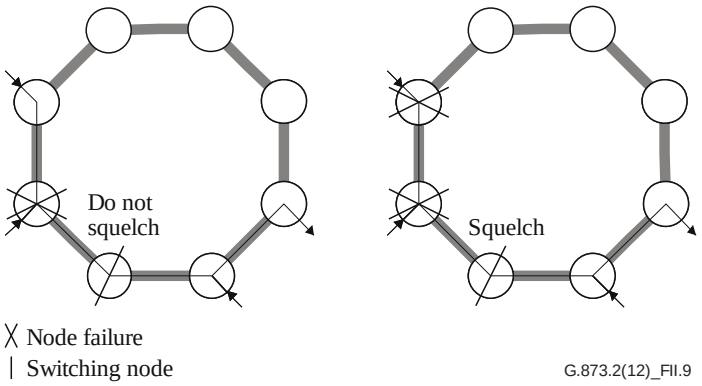


Figure II.9 – Multiply sourced unidirectional circuit squelching example where the failure is in the opposite direction from the unidirectional circuit

II.2.3 Application to ring interworking

For the ring interworking described in clause 8, the bidirectional interworking circuit is a multiply dropped circuit with two drops (drop and continue), and is a multiply sourced circuit with two sources in the other direction. The squelching for ring interworking is precisely the combination of the squelching for multiply dropped and multiply sourced circuits given above. More generally, the squelching rules discussed here extend to unidirectional circuits with combinations of multiple drops, multiple sources, or multiple broadcasts.

Appendix III

Ring configuration examples

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

This appendix describes some ring configuration examples.

III.1 2-fibre/2-lambda, 2-fibre/4-lambda and 4-fibre/4-lambda SRP-p Ring (22SRP-p, 24SRP-p, 44SRP-p) configurations example

The first step is to set up the optical transmission section/optical multiplexer section (OTSn/OMSn) trails and/or optical physical section (OPSn) trails between adjacent nodes in the ring. The second step is to set up the HO ODU trails between adjacent ODU SRP-p enabled ring nodes. Then add the LO ODU signals protected by the ODU SRP-p ring.

Figure III.1 illustrates the concept of a series of bidirectional HO ODU trails #A to #F (green) between adjacent ODU SRP-p enabled XC ring nodes over which bidirectional LO ODU connections #a to #f are supported. These LO ODU connections may have different bandwidths (≥ 1.25G); in the figure this is illustrated by means of the weight of the solid/dotted lines.

Extra traffic may be present as well and consists then of any low priority, pre-emptible signals along the same route as the logical ring of normal traffic signals. Figure III.1 does not illustrate such extra traffic.

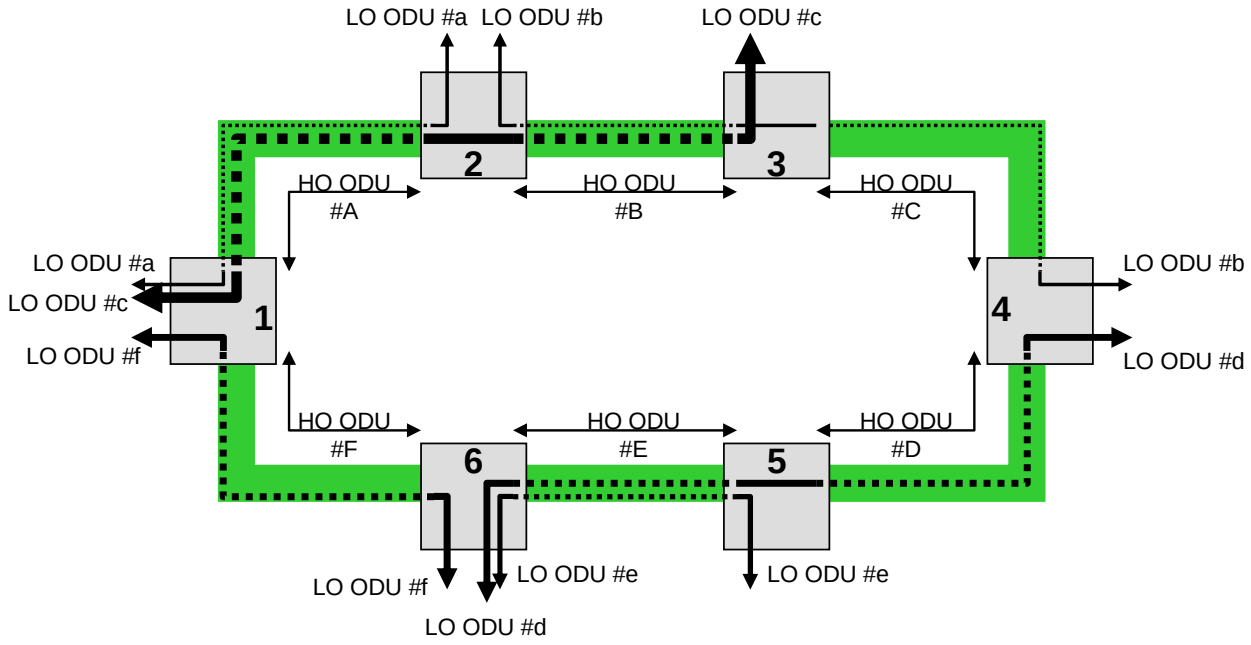


Figure III.1 – Example of HO ODU trails for SRP-p and LO ODU normal traffic signals

Every HO ODUk is monitored to provide the protection switching SF/SD conditions. ODUkP_TT functions at the end of the HO ODU trails perform this monitoring task (see Figures III.2 and III.3). The LO ODU signals carried in the HO ODUs are not monitored for the purpose of ODU SRP-p; a connectivity fault for an LO ODU in a ring node will not be protected by the ODU SRP-p.

An ODU SRP-p ring may be using 2 or 4 fibres.

– For the case of 2 fibres, these fibres may carry either one or two bidirectional HO ODUk signal(s) between two adjacent nodes in the ring.

– For the case of 4 fibres, these fibres carry two bidirectional HO ODUk signals between two adjacent nodes in the ring.

The APS controllers for ODU SRP-p ring switching are located as follows:

– APS controllers are located at each ring node.

– APS will be inserted and recovered at the HO ODU PM level where monitoring occurs for the ring.

– APS bytes are exchanged over the Protection HO ODUk for the case of a 4-lambda ODU SRP-p (see Figure III.3) and over the HO ODUk for the case of a 2-lambda ODU SRP-p (see Figure III.2).

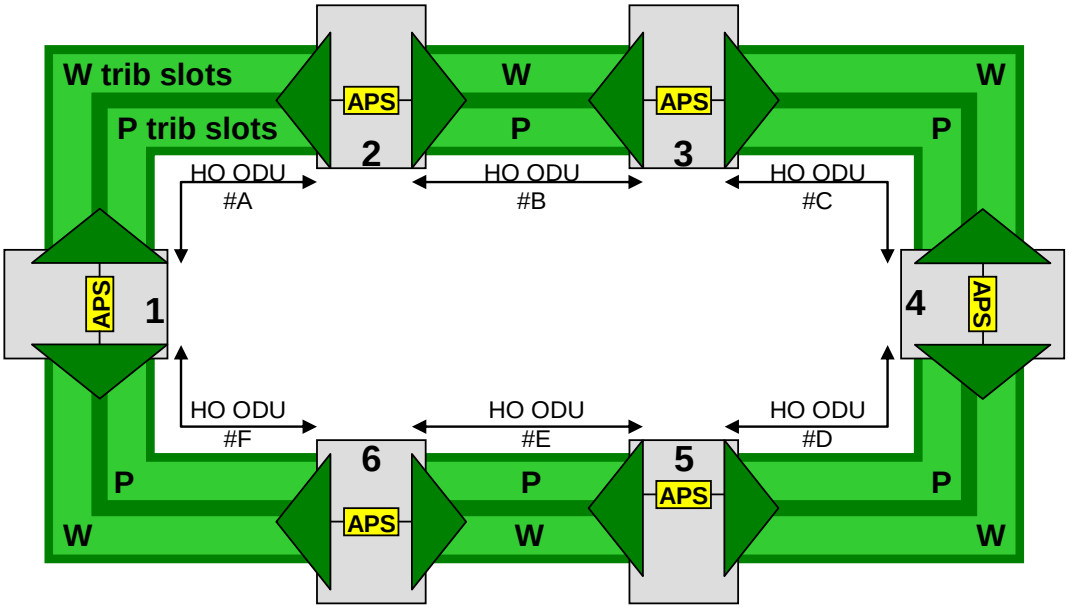


Figure III.2 – Location of APS controllers for 22SRP-p switching

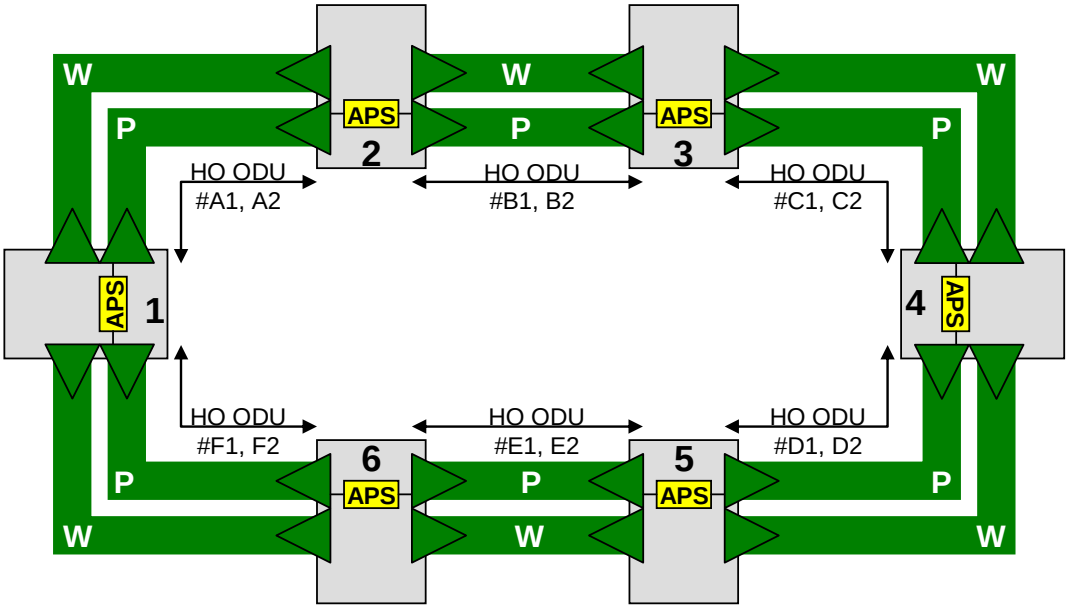


Figure III.3 – Location of APS controllers for 24SRP-p and 44SRP-p switching

III.2 2 fibres/4 lambda, 4-fibre/4-lambda SRP-1 Ring (24SRP-1, 44SRP-1) configuration example

The first step is to set up the OTSn/OMSn trails and/or OPSn trails between adjacent nodes in the ring. Then add the LO ODU signals protected by the ODU SRP-1 ring. The addition of a LO ODUk includes the set up of the associated working and protection OCh and OTUk[V] connections in the ring.

Extra traffic may be present as well and consists then of any low priority, pre-emptible signals along the same route as the logical ring of normal traffic signals.

III.3 ODU SRP group protection example

There are a many wavelengths in a fibre in an OTN network, which may result in a large number of ODU SRP-p and ODU SRP-1 protection instances within the ring. Figure III.4 presents an example of a ring with two ODU SRP-p and two ODU SRP-1 instances, both using 4-lambda SRP architecture.

The illustrated ring contains 16 lambdas of which 8 are carrying ODU signals in the clockwise direction and 8 in the counter-clockwise direction.

In a 2-fibre ring each fibre will carry 8 lambdas (resulting in W and P being member of the same shared risk link groups).

In a 4-fibre ring each fibre will carry 4 lambdas and W and P connections are in different shared ring link groups.

The two ODU SRP-1 instances carry e.g., LO ODU2s (#13, #35, #61b) over W4/P4 and LO ODU3s (#12, #24, #61a) over W3/P3.

One of the two ODU SRP-p instances (W1/P1) carries a number of LO ODU signals (#a, #b, #c, #d, #e, #f), with different bandwidths.

Each ring node contains multiple ODU SRP APS processes as illustrated in Figure III.4.

An objective of ring protection is to minimize the number of APS instances within the ring. From the HO ODU SRP perspective there is a reduction of APS processes obtained as there is only one APS process for the group of LO ODUs transported over the HO ODU. But per ring there are still a number of APS processes active; i.e., one per ODU SRP instance. A further reduction of the number of APS instances can be obtained when SRP Group protection is deployed.

All HO ODU and LO ODU signals in the ring experience the same set of link faults, and it is as such possible to deploy a single APS process for the whole multi-lambda ring.

SRP Group protection can be triggered on the basis of SFG/SDG specifications in clause 11.1.2 of [ITU-T G.808.1] and clause 11.3.1 of [ITU-T G.808.1]. I.e., combine the SF and SD indications of each HO ODU PM end point and LO ODU TCM endpoint into a SF/SD Group signal and use this to trigger protection for all the HO and LO ODU SRP instances. Alternatively, one SF/SD indication out of the set of all ODU SRP-p and SRP-1 instances is used to trigger protection for all members of the group.

ODU SRP Group protection is possible for all ODU SRP-p instances. One of the HO ODU lambdas will be selected to support the HO ODU SRP Group APS channel.

ODU SRP Group protection is also possible for all ODU SRP-1 instances if those instances have their LO ODU TCM trails starting/ending in the same ring nodes. This condition is not met in the example of Figure III.4.

ODU SRP Group protection is also possible for all ODU SRP-p and SRP-1 instances if all ODU SRP-1 instances have their LO ODU TCM trails starting/ending in all ring nodes. See Figure III.5.

The latter implies that the ODU SRP-1 rings are architecturally similar to the ODU SRP-p rings. The ODU TCM trails terminate at the same locations as the ODU PM trails. The main difference between ODU SRP-p and ODU SRP-1 rings is then the number of LO ODU signals that can be carried by the lambda. In ODU SRP-1 rings this number is 1, while in ODU SRP-p rings this number is $n > 1$.

For this latter case it is possible to deploy a single ODU SRP-p/SRP-1 Group APS channel as illustrated in Figure III.6. The APS channel is supported in this example by the Protection #1 (P1) HO ODU connections.

For the case the ODU SRP-1 instances have maintenance end points in every ring node it may be possible to deploy the OTUk SM overhead (instead of one level of ODUk TCM OH) to monitor the LO ODU link connections between two adjacent ring nodes. The OTUk SM OH can be used (instead of ODUk TCM OH) when there are no 3R Regenerator functions located between two adjacent ring nodes.

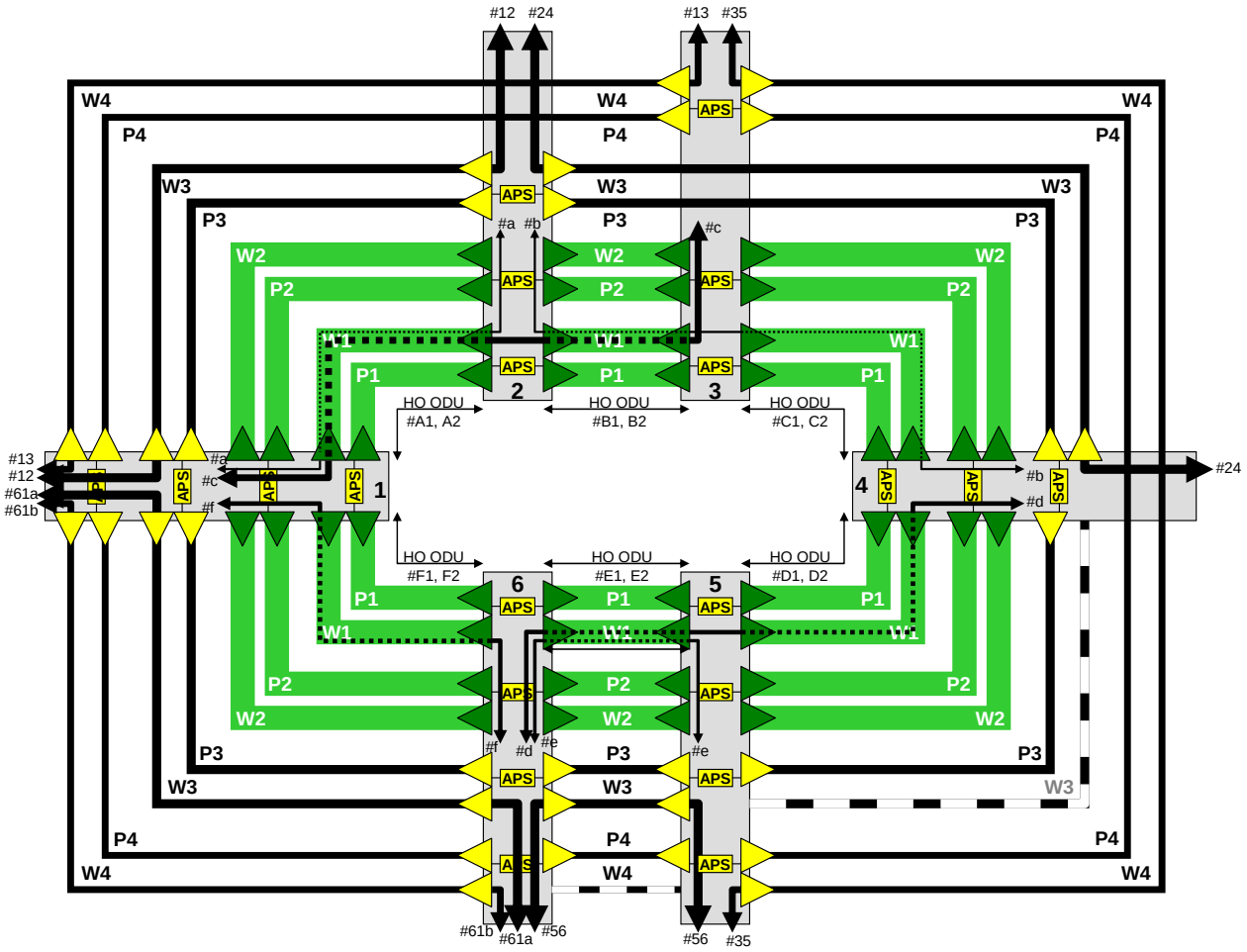


Figure III.4 – 4-lambda SRP-p and SRP-1 example with ODU SRP APS processes in selected ring nodes

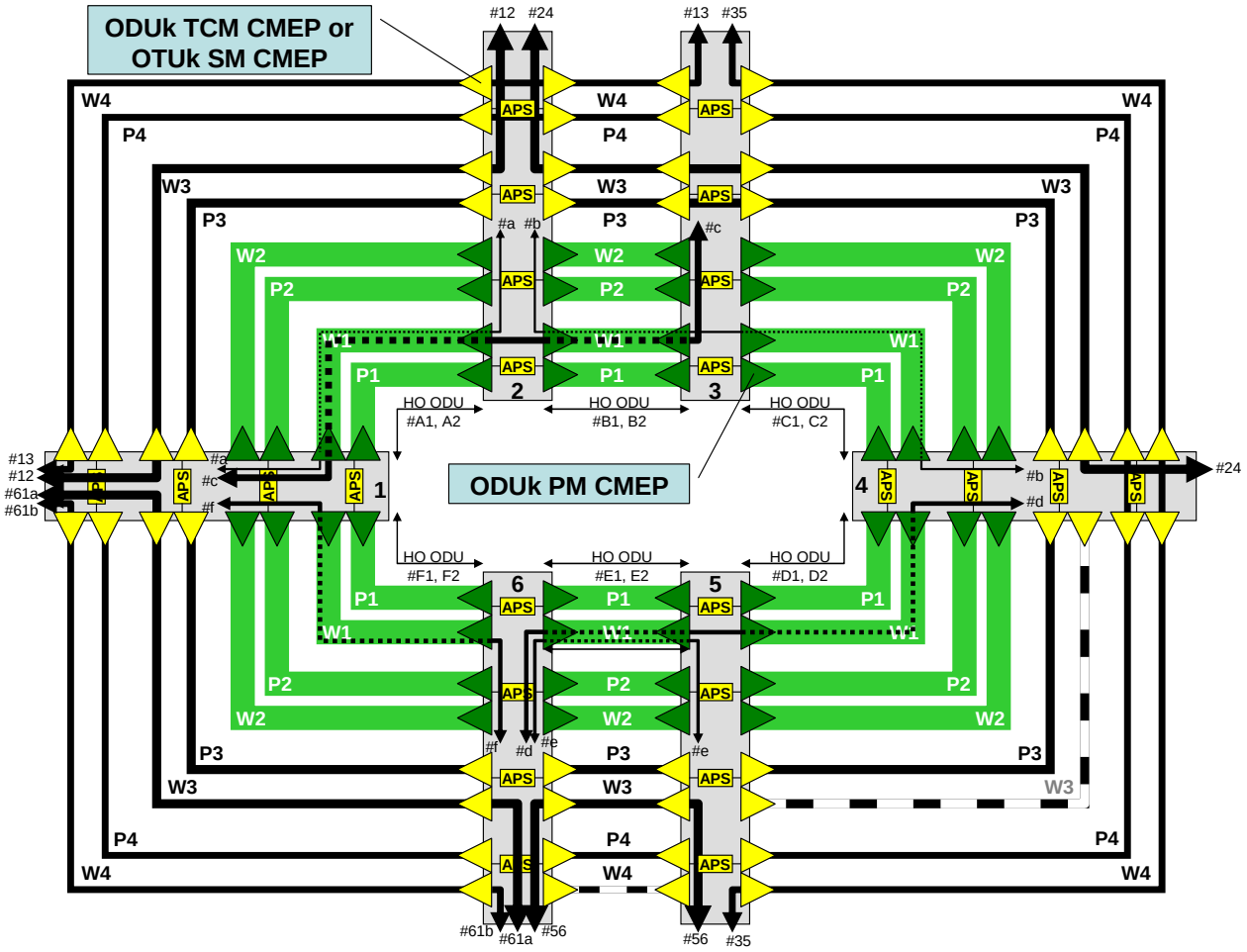


Figure III.5 – 4-lambda SRP-p and SRP-1 example with ODU SRP APS processes in every ring node

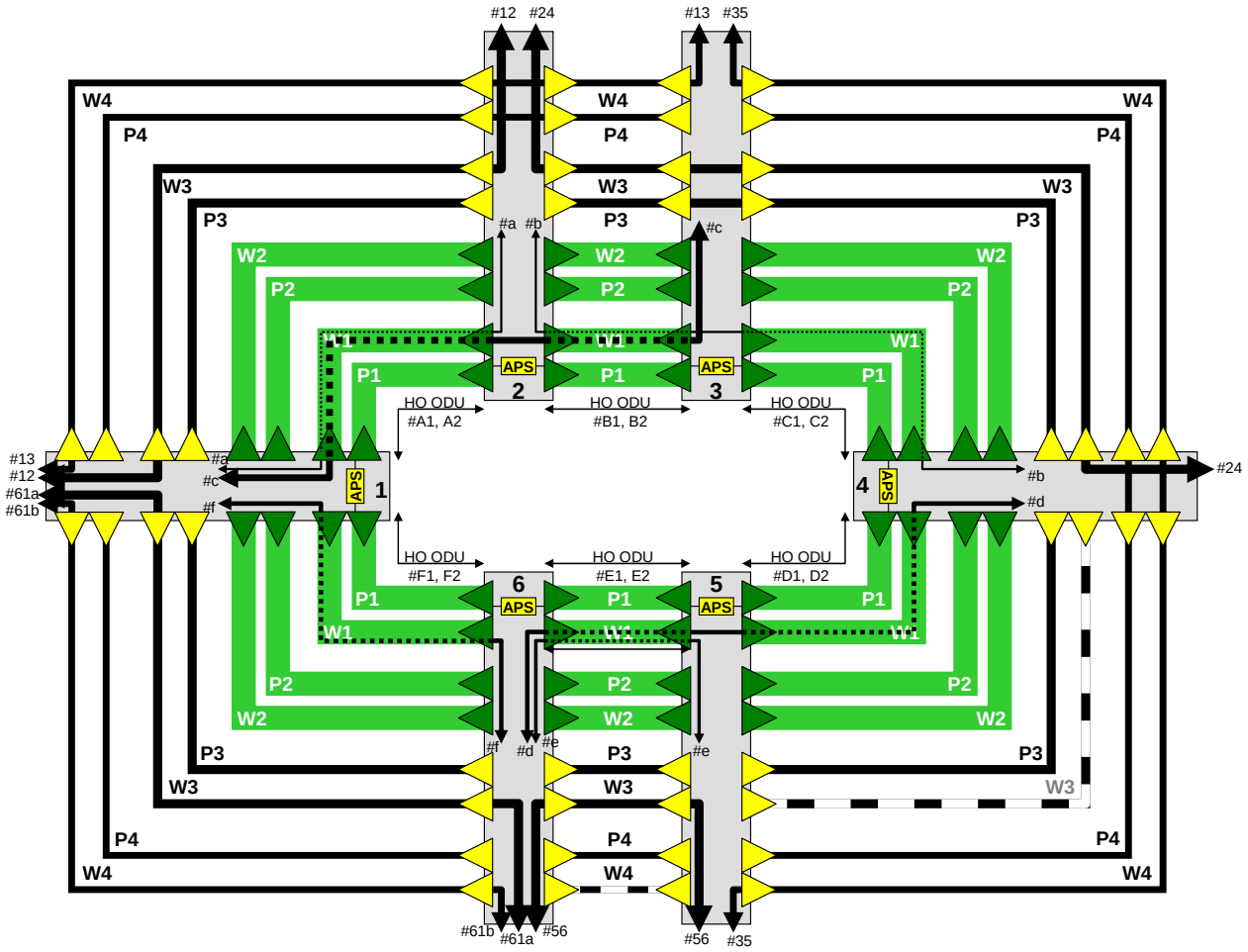


Figure III.6 – 4-lambda SRP-p and SRP-1 Group protection example with single ODU SRP Group APS process per ring node

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013