INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

G.841

(07/95)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

DIGITAL NETWORKS

TYPES AND CHARACTERISTICS OF SDH NETWORK PROTECTION ARCHITECTURES

ITU-T Recommendation G.841

(Previously "CCITT Recommendation")

FOREWORD

The ITU-T (Telecommunication Standardization Sector) is a permanent organ of the International Telecommunication Union (ITU). The 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 Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1 (Helsinki, March 1-12, 1993).

ITU-T Recommendation G.841 was prepared by ITU-T Study Group 15 (1993-1996) and was approved under the WTSC Resolution No. 1 procedure on the 10th of July 1995.

____

NOTE

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

CONTENTS

SUMMARY

This Recommendation provides the necessary equipment-level specifications to implement different choices of protection architectures for Synchronous Digital Hierarchy (SDH) networks. Protected entities may range from a single SDH multiplex section (e.g. linear multiplex section protection), to a portion of an SDH end-to-end path (e.g. subnetwork connection protection), or to an entire SDH end-to-end path (e.g. HO/LO linear VC trail protection). Physical implementations of these protection architectures may include rings, or linear chains of nodes. Each protection classification includes guidelines on network objectives, architecture, application functionality, switching criteria, protocols, and algorithms.

Recommendation G.841

TYPES AND CHARACTERISTICS OF SDH NETWORK PROTECTION ARCHITECTURES

(Geneva, 1995)

1 Scope

This Recommendation describes the various protection mechanisms for Synchronous Digital Hierarchy (SDH) networks, their objectives and their applications.

Protection schemes are classified as:

- SDH trail protection (at the section or path layer);
- SDH subnetwork connection protection (with inherent monitoring, non-intrusive monitoring, and sub-layer monitoring).

Protection interworking (including switching hierarchy) and interconnection scenarii are under development in a separate Recommendation.

OAM&P, performance, and satellite/radio aspects are for further study. Synchronization architecture and protection of synchronization are not described here. It is not necessary to have all protection mechanisms described within this Recommendation available on the same SDH equipment.

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; all 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.

- ITU-T Recommendation G.707 (1993), *Synchronous digital hierarchy bit rates.*
- ITU-T Recommendation G.708 (1993), *Network node interface for the synchronous digital hierarchy.*
- ITU-T Recommendation G.709 (1993), *Synchronous multiplexing structure.*
- CCITT Recommendation G.774 (1992), *Synchronous Digital Hierarchy (SDH) management information model for the network element view*.
- CCITT Recommendation G.782 (1990), *Types and general characteristics of Synchronous Digital Hierarchy (SDH) multiplexing equipment.*
- CCITT Recommendation G.783 (1990), *Characteristics of synchronous Digital Hierarchy (SDH) multiplexing equipment functional blocks.*
- ITU-T Recommendation G.784 (1994), *Synchronous Digital Hierarchy (SDH) management.*
- ITU-T Recommendation G.803 (1993), *Architectures of transport networks based on the Synchronous Digital Hierarchy* (SDH).

3 Terms and definitions

For the purposes of this Recommendation, the following definitions apply:

3.1` **APS controller:** That part of a node that is responsible for generating and terminating information carried in the APS protocol and implementing the APS algorithm.

3.2 **Add-Drop Multiplex (ADM):** Network elements that provide access to all, or some subset of the constituent signals contained within an STM-N signal. The constituent signals are added to (inserted), and/or dropped from (extracted) the STM-N signal as it passes through the ADM. See 3.5/G.782.

3.3 add traffic: Traffic inserted into working channels on the ring at a ring node.

3.4 Administrative Unit (AU): See Recommendation G.708.

3.5 Alarm Indication Signal (AIS): A code sent downstream in a digital network as an indication that an upstream failure has been detected and alarmed. It is associated with multiple transport layers.

3.6 AU-AIS: See Recommendation G.783.

3.7 AU pointer: See Recommendation G.709.

3.8 auto-provisioning: The assignment of values to parameters within a network element, without those values being specifically entered externally by a user.

3.9 bidirectional connection: See Recommendation G.803. An illustration is given in Figure 3-2.

3.10 bidirectional ring: In a bidirectional ring, normal routing of the working traffic is such that both directions of a bidirectional connection travel along the ring through the same nodes, but in opposite directions.

3.11 Bit Interleaved Parity N (BIP-N): See Recommendation G.708.

3.12 bridge: The action of transmitting identical traffic on both the working and protection channels.

3.13 bridge request: A message sent from a tail-end node to the head-end node requesting that the head-end perform a bridge of the working channels onto the protection channels.

3.14 bridge request status: A message sent from a tail-end node to all other nodes within the protection system indicating that the tail-end has requested a bridge.

3.15 container: See Recommendation G.708.

3.16 controller failure: The condition during which a node is no longer able to correctly operate the APS protocol, but still generates a correctly formatted SDH frame.

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

3.18 Data Communications Channel (DCC): See Recommendation G.784.

3.19 dedicated protection: A protection architecture that provides capacity dedicated to the protection of traffic-carrying capacity (1 + 1). See Recommendation G.803.

3.20 default APS code: This term refers to the APS bytes transmitted with the source node ID equal to the destination node ID.

3.21 diverse routing: Bidirectional working traffic (i.e. go and return) is transported on the different physical facilities under non-failure conditions. Such routing may apply to individual trails or subnetwork connections. This is illustrated in Figure 3-2.

3.22 drop traffic: Traffic extracted from working channels on the ring at a ring node.

3.23 dual-ended switching: A protection switching method which takes switching action at both ends of the protected entity (e.g. “connection,” “path”), even in the case of a unidirectional failure. See Recommendation G.803.

3.24 extra traffic: Traffic that is carried over the protection channels when that capacity is not used for the protection of working traffic. Extra traffic is not protected. Whenever the protection channels are required to protect the working traffic, the extra traffic is preempted.

3.25 full pass-through: The action of transmitting the same K1, K2, and protection channels that are being received. Full pass-through is bidirectional.

3.26 head-end: The node executing a bridge. Note that a node functions as a head-end and a tail-end for a bidirectional switch for the same span.

3.27 **higher order virtual container:** See Recommendation G.708.

3.28 **hold-off time:** The time between declaration of signal degrade or signal fail, and the initialization of the protection switching algorithm.

3.29 **idle:** A node that is not generating, detecting, or passing-through bridge requests or bridge request status information.

3.30 **isolated node**: A single node that is isolated from a traffic perspective by ring switches on each of its two spans by its adjacent nodes.

3.31 **K-byte pass-through:** The action of transmitting the same K1 and K2 bytes that are being received. Protection channels are not passed through. K-byte pass-through is bidirectional.

3.32 **long path:** The path segment away from the span for which the bridge request is initiated. Typically there are other intermediate nodes along this path segment.

3.33 **Loss of Frame (LOF):** See Recommendation G.783.

3.34 **Loss of Signal (LOS):** See Recommendation G.783 for SDH systems, and Recommendation G.775 for PDH systems.

3.35 **lower order virtual container:** See Recommendation G.708.

3.36 **lower order VC access:** The termination of a higher order VC for the purpose of adding, dropping, or cross-connecting any individual lower order VC or VC group.

3.37 **misconnection:** A condition in which traffic destined for a given node is incorrectly routed to another node and no corrective action has been taken.

3.38 **most significant bit**: The "leftmost" bit position, or first transmitted bit position in a byte.

3.39 **Multiplex Section (MS):** See Recommendation G.803.

3.40 **Multiplex Section Alarm Indication Signal (MS-AIS):** See Recommendation G.783.

3.41 **Multiplex Section Remote Defect Indication (MS-RDI)**: Formerly known as multiplex section far end remote failure. See Recommendation G.709.

3.42 **network connection protection:** A scheme that protects the largest possible subnetwork connection of a trail.

3.43 **Network Node Interface (NNI):** See Recommendation G.708.

3.44 **pass-through:** The action of transmitting the same information that is being received for any given direction of transmission.

3.45 **path:** See Recommendation G.803.

3.46 **path overhead:** See Recommendation G.708.

3.47 **protection channels:** The channels allocated to transport the working traffic during a switch event. When there is a switch event, traffic on the affected working channels is bridged onto on the protection channels.

3.48 **regenerator section:** See Recommendation G.803.

3.49 **remote error indication:** Formerly far-end block error. See Recommendation G.709.

3.50 **restoral threshold:** For automatically initiated commands, a hysteresis method is used when switching from the protection channels back to the working channels. This method specifies a BER threshold for the multiplex section that is carrying the working channels. This threshold is commonly referred to as "restoral threshold." The restoral threshold is set to a lower BER than the signal degrade threshold.

3.51 **restoration:** See Recommendation G.803.

3.52 **ring:** A collection of nodes forming a closed loop whereby each node is connected to two adjacent nodes via a duplex communications facility. A ring provides redundant bandwidth or redundant network equipment, or both, so distributed services can be automatically restored following a failure or degradation in the network. Thus a ring can be self-healing.

3.53 **ring failure:** A failure for which restoration can only be accomplished by a ring switch.

3.54 **ring interworking:** A network topology where two rings are connected at two points and operate such that failure at either of these two points will not cause loss of any traffic, except possibly that dropped or inserted at the point of failure.

3.55 **ring switching:** Protection mechanism that applies to both two-fibre and four-fibre rings. During a ring switch, the traffic from the affected span is carried over the protection channels on the long path.

3.56 **section overhead:** See Recommendation G.708.

3.57 **segmented ring:** A ring that is separated into two or more segments, either externally using Forced Switches (FS-R), or automatically as a result of Signal Failed-Ring switches (SF-R).

3.58 **shared protection:** A protection architecture using m protection entities shared among n working entities (m:n). The protection entities may also be used to carry extra traffic when not used for protection. See Recommendation G.803.

3.59 **short path:** The path segment over the span for which the bridge request is initiated. This span is always the one to which both the head-end and tail-end are connected. The short path bridge request is the bridge request sent over the span for which the bridge request is initiated.

3.60 **single-ended switching:** A protection switching method which takes switching action only at the affected end of the protected entity (e.g. "trail," "subnetwork connection"), in the case of a unidirectional failure. See Recommendation G.803.

3.61 **single point failure:** Failure located at a single physical point in a ring. The failure may affect one or more fibres. A single point failure may be detected by any number of NEs.

3.62 **span:** The set of multiplex sections between two adjacent nodes on a ring.

3.63 **span switching:** Protection mechanism similar to 1:1 linear APS that applies only to four-fibre rings where working and protection channels are contained in separate fibres and the failure only affects the working channels. During a span switch, the working traffic is carried over the protection channels on the same span as the failure.

3.64 **squelched traffic:** An all "1"s signal resulting from the squelching process.

3.65 **squelching:** The process of inserting AU-AIS in order to prevent misconnections.

3.66 **subnetwork connection:** See Recommendation G.803.

3.67 **subnetwork connection protection:** A working subnetwork connection is replaced by a protection subnetwork connection if the working subnetwork connection fails, or if its performance falls below a required level.

3.68 **survivable network**: A network that is capable of restoring traffic in the event of a failure. The degree of survivability is determined by the network's ability to survive single line system failures, multiple line system failures, and equipment failures.

3.69 **switch:** The action of selecting traffic from the protection channels rather than the working channels.

3.70 **switch completion time:** The interval from the decision to switch to the completion of the bridge and switch operation at a switching node initiating the bridge request.

3.71 **switching node:** The node that performs the bridge or switch function for a protection event. In the case of a multiplex section switched ring network architecture, this node also performs any necessary squelching of misconnected traffic for VC-3/4 or higher rate paths.

3.72 **synchronous:** The essential characteristic of time scales or signals such that their corresponding significant instants occur at precisely the same average rate.

3.73 **Synchronous Transport Module level N (STM-N)**: See Recommendation G.707.

3.74 **tail-end:** The node that is requesting the bridge. Note that a node functions as a head-end and a tail-end for a bidirectional switch for the same span.

3.75 **Timeslot Interchange (TSI):** For the purposes of this Recommendation, TSI is the capability of changing the timeslot position of through-connected traffic (i.e. traffic that is not added or dropped from the node).

3.76 **trail:** See Recommendation G.803.

3.77 **trail protection:** A working trail is replaced by a protection trail if the working trail fails, or if its performance falls below a required level.

3.78 **transport:** Facilities associated with the carriage of STM-1 or higher level signals.

3.79 **undetected failure:** Any equipment defect which is not detected by equipment maintenance functions, hence does not initiate a protection switch or provide the appropriate OA&M notification. These types of failures do not manifest themselves until a protection switch is attempted.

3.80 **unidirectional connection:** See Recommendation G.803. An illustration is given in Figure 3-1.

3.81 **unidirectional ring:** In a unidirectional ring (path switched or multiplex section switched), normal routing of the working traffic is such that both directions of a bidirectional connection travel around the ring in the same direction (e.g. clockwise). Specifically, each bidirectional connection uses capacity along the entire circumference of the ring.

3.82 **uniform routing:** Bidirectional working traffic (i.e. go and return) is transported on the same physical facilities under non-failure conditions. Such routing may apply to individual trails or subnetwork connections. This is illustrated in Figure 3-2.

3.83 **Virtual Container (VC):** See Recommendation G.708.

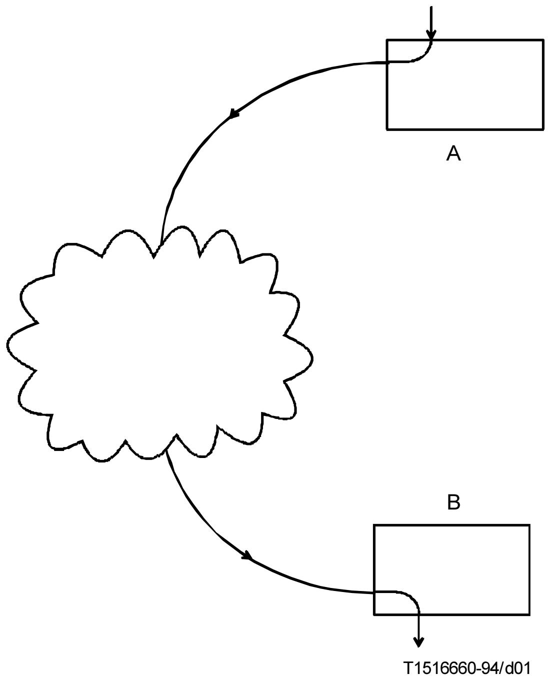
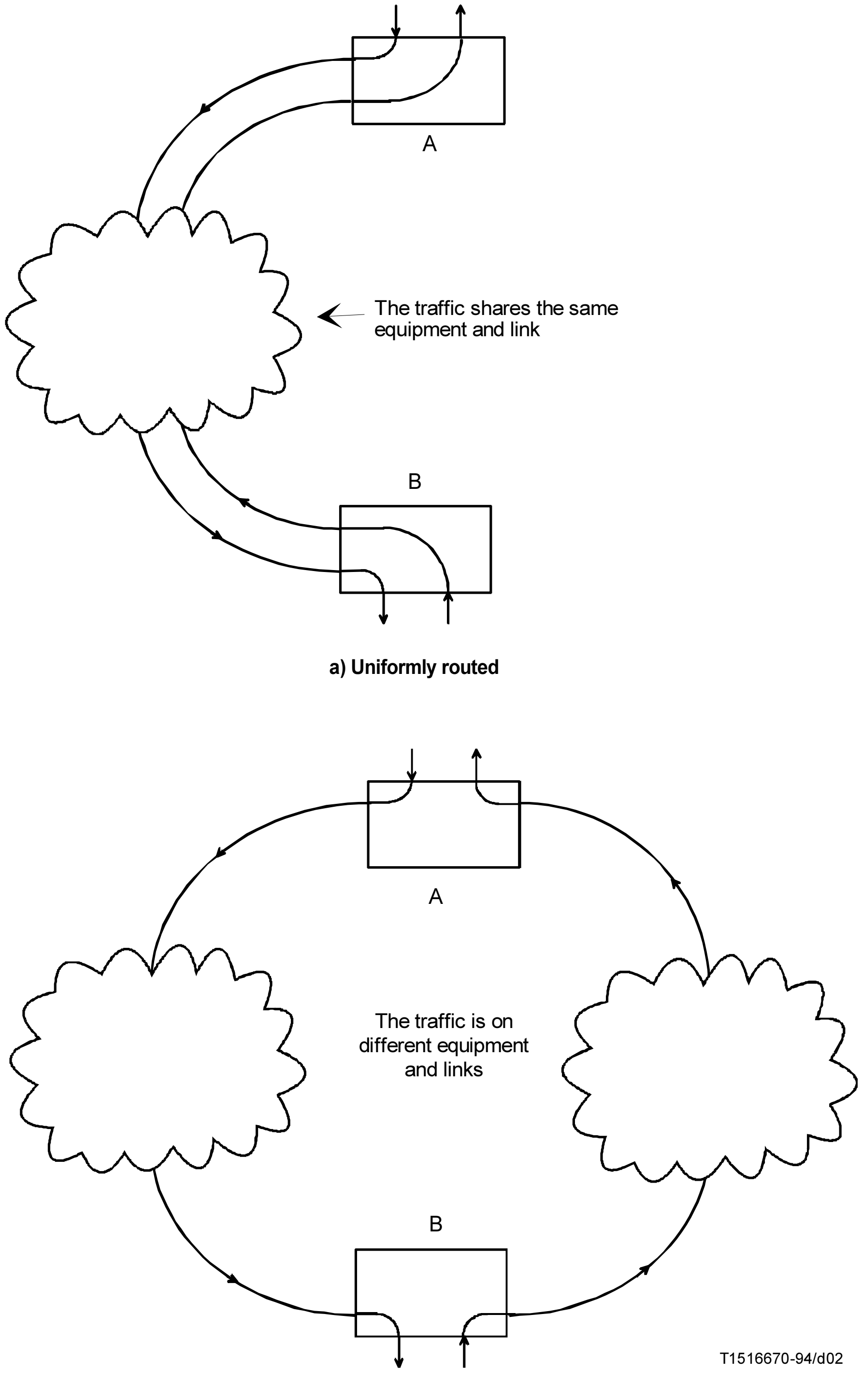


FIGURE 3-1/G.841

Unidirectional connection

3.84 working channels: The channels over which working traffic is transported when there are no switch events. An APS system performs restoration for the working channels only.

3.85 working traffic: Traffic transversing a ring normally carried in working channels, except in the event of a ring or span protection switch, in which case it is restored on the protection channels.


A
The traffic shares the same equipment and link
B
A
The traffic is on different equipment and links
B
T1516670-94/d02

a) Uniformly routed

b) Diversely routed

FIGURE 3-2/G.841

Uniformly routed and diversely routed bidirectional connection

4 Abbreviations

For the purpose of this Recommendation, the following abbreviations are used:

ADM	Add Drop Multiplex
AIS	Alarm Indication Signal
AP	Access Point
APS	Automatic Protection Switching
AU	Administrative Unit
AUG	Administrative Unit Group
AU-AIS	Administrative Unit Alarm Indication Signal
AU-LOP	Administrative Unit Loss of Pointer
BER	Bit Error Ratio
BIP-N	Bit Interleaved Parity N
Br	Bridge(d)
CP	Connection Point
DCC	Data Communications Channel
DCN	Data Communications Network
EXER-R	Exerciser-Ring
EXER-S	Exerciser-Span
FS-P	Forced Switch to Protection
FS-R	Forced Switched Working to Protection-Ring
FS-S	Forced Switched Working to Protection-Span
FS-W	Forced Switch to Working
HO	Higher Order
HOVC	Higher Order Virtual Container
HP-DEG	Higher Order Path Degraded
HP-EXC	Higher Order Path Excessive Errors
HP-SSF	Higher Order Path Server Signal Fail
HP-TIM	Higher Order Path Trace Identifier Mismatch
HP-UNEQ	Higher Order Path Unequipped
ID	Identification
LO	Lower Order
LOF	Loss of Frame
LOVC	Lower Order Virtual Container
LP	Lockout of Protection
LP-DEG	Lower Order Path Degraded
LP-EXC	Lower Order Path Excessive Errors
LP-S	Lockout of Protection-Span
LP-SSF	Lower Order Path Server Signal Fail
LP-TIM	Lower Order Path Trace Identifier Mismatch
LP-UNEQ	Lower Order Path Unequipped
LOS	Loss of Signal
MS	Multiplex Section
MSA	Multiplex Section Adaptation

MSP	Multiplex Section Protection
MSPA	Multiplex Section Protection Adaptation
MSPT	Multiplex Section Protection Termination
MST	Multiplex Section Termination
MS-P	Manual Switch to Protection
MS-R	Manual Switch-Ring
MS-S	Manual Switch-Span
MS-W	Manual Switch to Working
NE	Network Element
NNI	Network Node Interface
NR	No Request
OAM&P	Operations, Administration, Maintenance and Provisioning
OS	Operation System(s)
POH	Path OverHead
RR-R	Reverse Request-Ring
RR-S	Reverse Request-Span
RSOH	Regenerator Section OverHead
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SD-P	Signal Degrade of the Protection Channels
SD-R	Signal Degrade-Ring
SD-S	Signal Degrade-Span
SF	Signal Fail
SF-R	Signal Fail-Ring
SF-S	Signal Fail-Span
SNC	SubNetwork Connection
SNC/I	SubNetwork Connection Protection with Inherent Monitoring
SNC/N	SubNetwork Connection Protection with Non-intrusive Monitoring
SSF	Server Signal Fail
STM-N	Synchronous Transport Module Level N
Sw	Switch(ed)
TCP	Termination Connection Point
TMN	Telecommunications Management Network
TSI	Time Slot Interchange
TU	Tributary Unit
VC	Virtual Container
WTR	Wait to restore

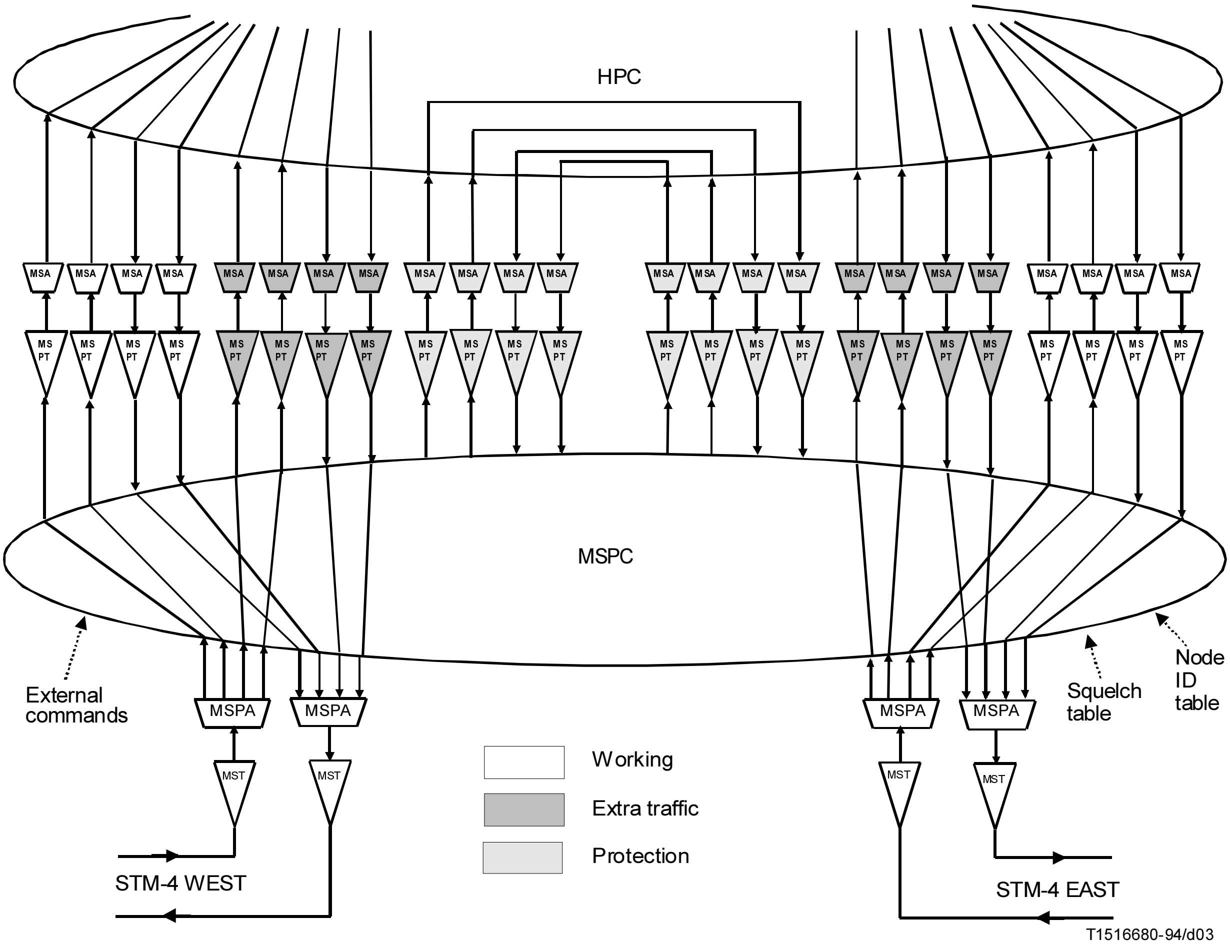
5 Protection classifications

This clause describes in general terms the types of protection architectures described within this Recommendation. There are basically two types of protection switching: SDH trail protection and SDH subnetwork connection protection.

MS shared protection rings is a SDH trail protection. Figure 5-1 illustrates the model of a two-fibre MS shared protection ring with a 4 AUG capacity, including the transmit and receive subnetwork connection. Figure 5-2 shows the same model reacting to a complete cable cut on one side. Figure 5-3 shows the same model reacting as a pass-through node.

Figure 5-4 shows the generic functional model for 1 + 1 VC trail protection. Figure 5-5 shows the generic functional model for 1:1 revertive VC trail protection and Figure 5-6 shows the generic functional model for 1:1 non-revertive VC trail protection.

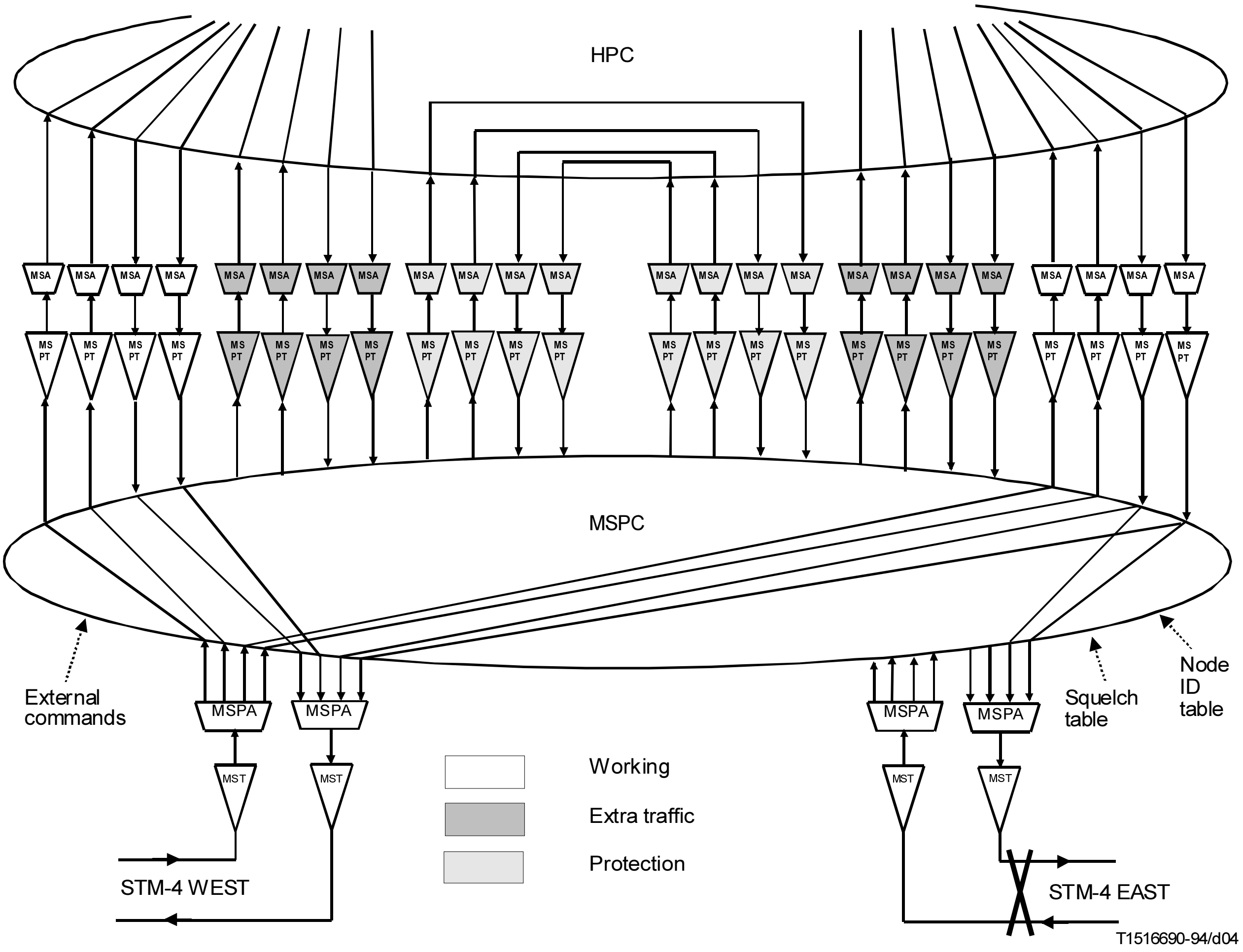
Figure 5-7 shows the functional model for subnetwork connection protection with inherent monitoring (SNC/I). Figure 5-8 shows the functional model for subnetwork connection with non-intrusive monitoring (SNC/N).



HPC Higher order Path Connection
MSA Multiplex Section Adaptation
MSPA Multiplex Section Protection Adaptation
MSPC Multiplex Section Protection Connection
MSPT Multiplex Section Protection Termination
MST Multiplex Section Termination

FIGURE 5-1/G.841

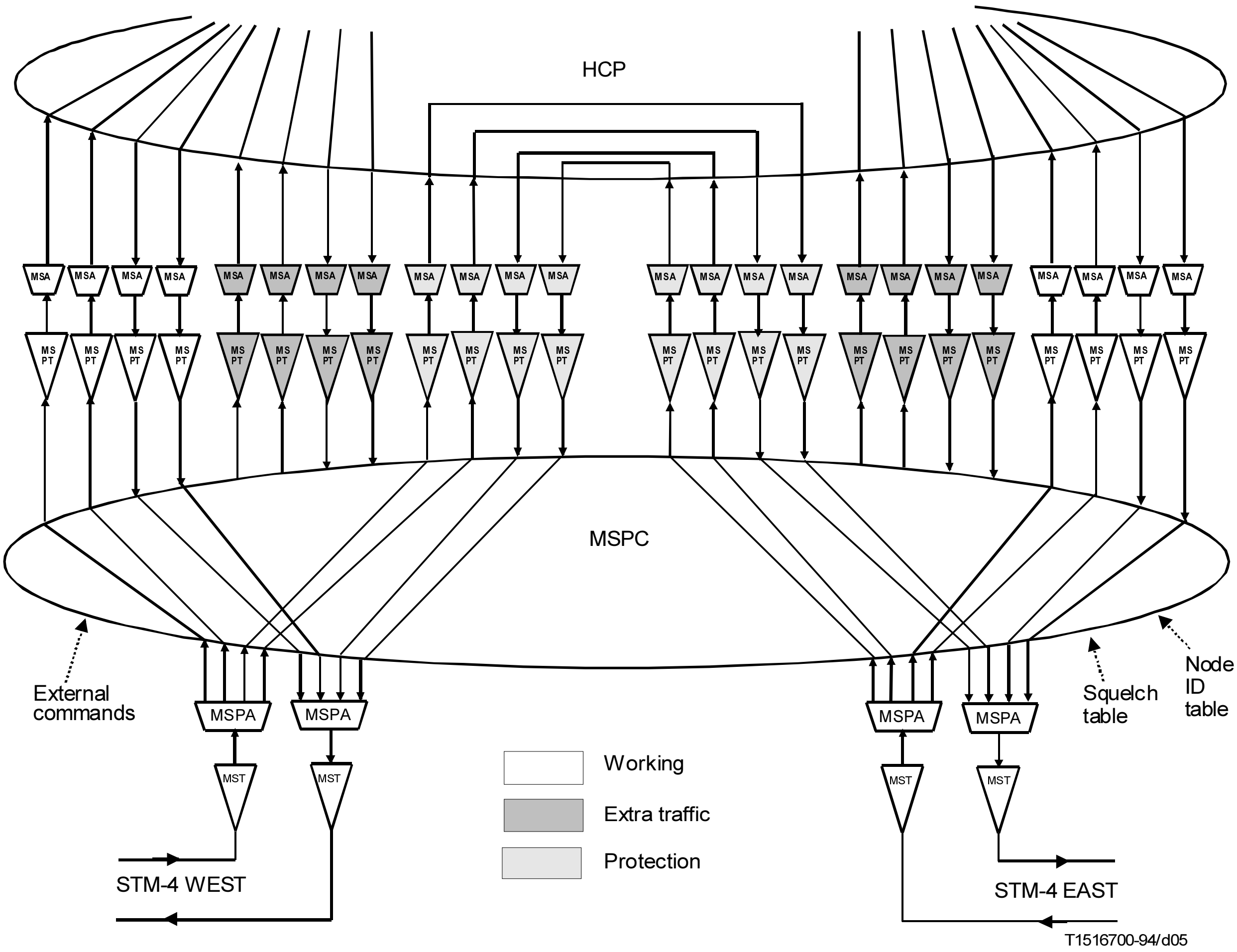
Functional model for a two-fibre MS shared protection ring – Normal state with extra traffic



HPC	Higher order Path Connection
MSA	Multiplex Section Adaptation
MSPA	Multiplex Section Protection Adaptation
MSPC	Multiplex Section Protection Connection
MSPT	Multiplex Section Protection Termination
MST	Multiplex Section Termination

FIGURE 5-2/G.841

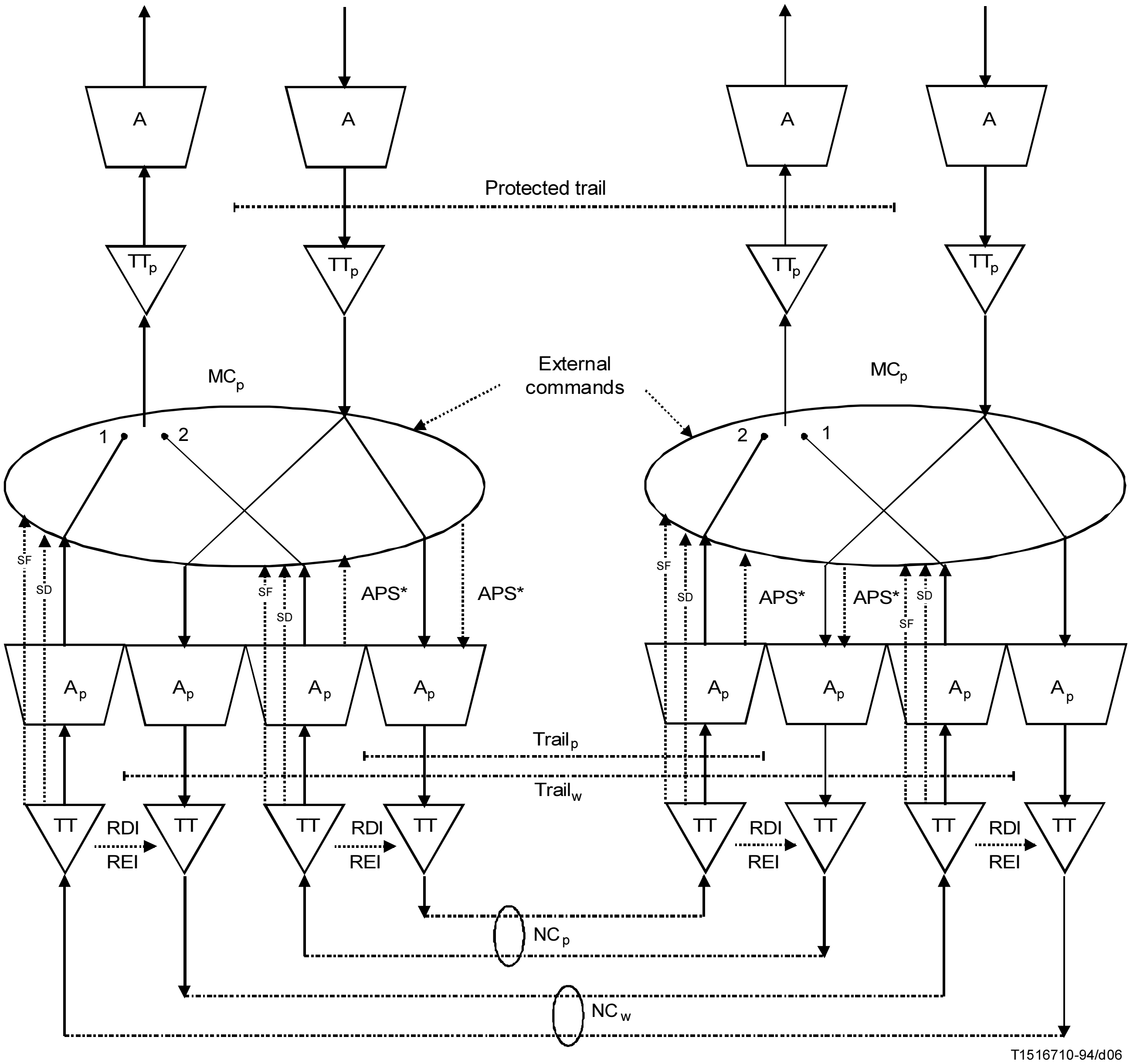
Functional model for a two-fibre MS shared protection ring – Failure on east side



HPC	Higher order Path Connection
MSA	Multiplex Section Adaptation
MSPA	Multiplex Section Protection Adaptation
MSPC	Multiplex Section Protection Connection
MSPT	Multiplex Section Protection Termination
MST	Multiplex Section Termination

FIGURE 5-3/G.841

Functional model for a two-fibre MS shared protection ring – Pass-through state



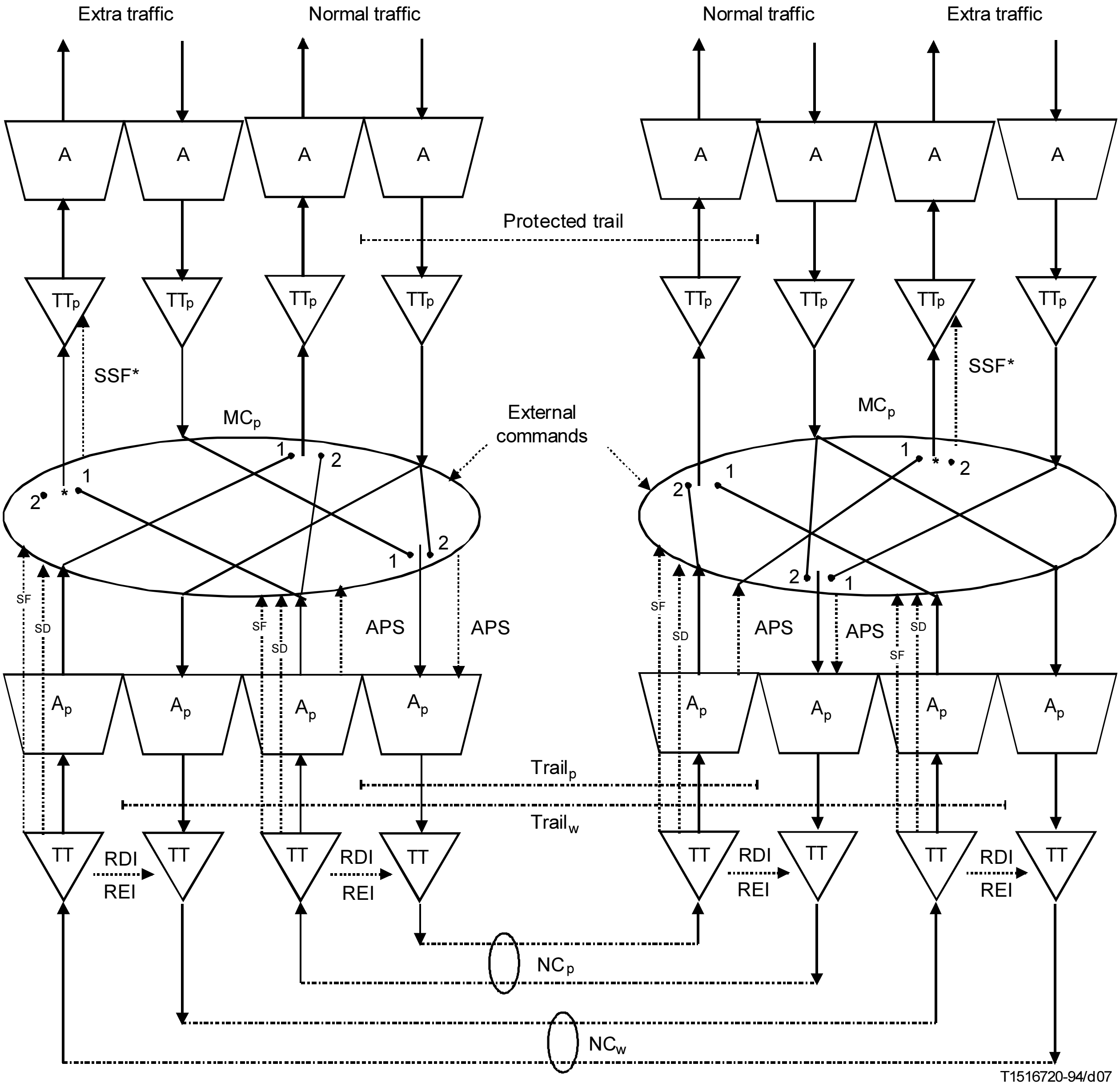
* Required for dual ended switching.
Not required for single ended switching.

A	Adaptation	SD	Signal Degrade
A_p	Protection Adaptation	SF	Signal Fail
MC_p	Protection Matrix Connection	SSF	Server Signal Fail
NC_p	Protection Network Connection	$Trail_p$	Protection Trail
NC_w	Working Network Connection	$Trail_w$	Working Trail
RDI	Remote Defect Indication	TT	Trail Termination
REI	Remote Error Indication	TT_p	Protection Trail Termination

States: 1 Normal state
2 Failure state

FIGURE 5-4/G.841

Functional model for generic 1 + 1 linear trail protection



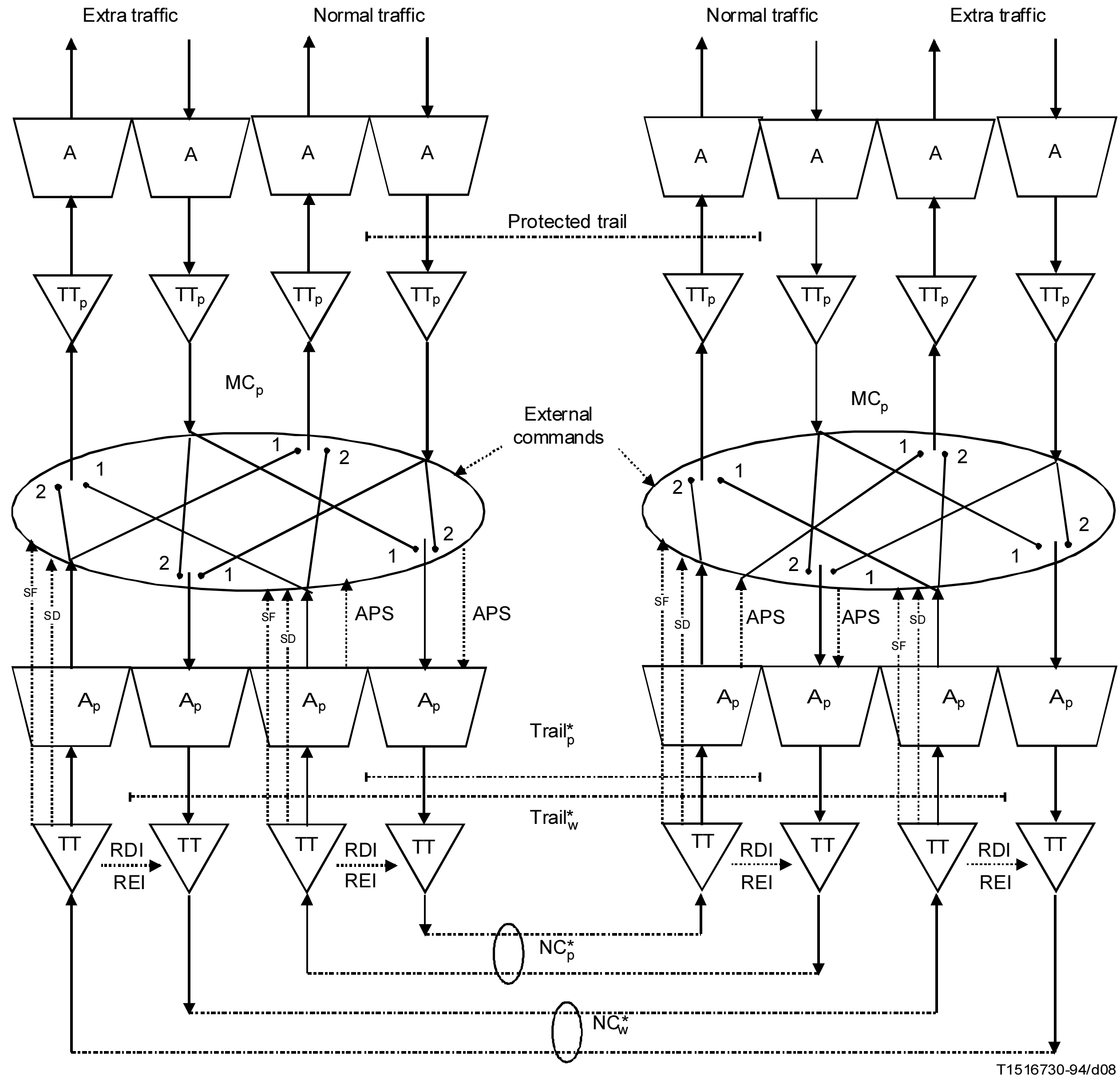
* SSF active on open connection [Failure state (2)]. This is for further study.

A	Adaptation	SD	Signal Degrade
A_p	Protection Adaptation	SF	Signal Fail
MC_p	Protection Matrix Connection	SSF	Server Signal Fail
NC_p	Protection Network Connection	$Trail_p$	Protection Trail
NC_w	Working Network Connection	$Trail_w$	Working Trail
RDI	Remote Defect Indication	TT	Trail Termination
REI	Remote Error Indication	TT_p	Protection Trail Termination

States: 1 Normal state
2 Failure state

FIGURE 5-5/G.841

Functional model for generic 1 : 1 linear trail protection – Revertive operation



T1516730-94/d08

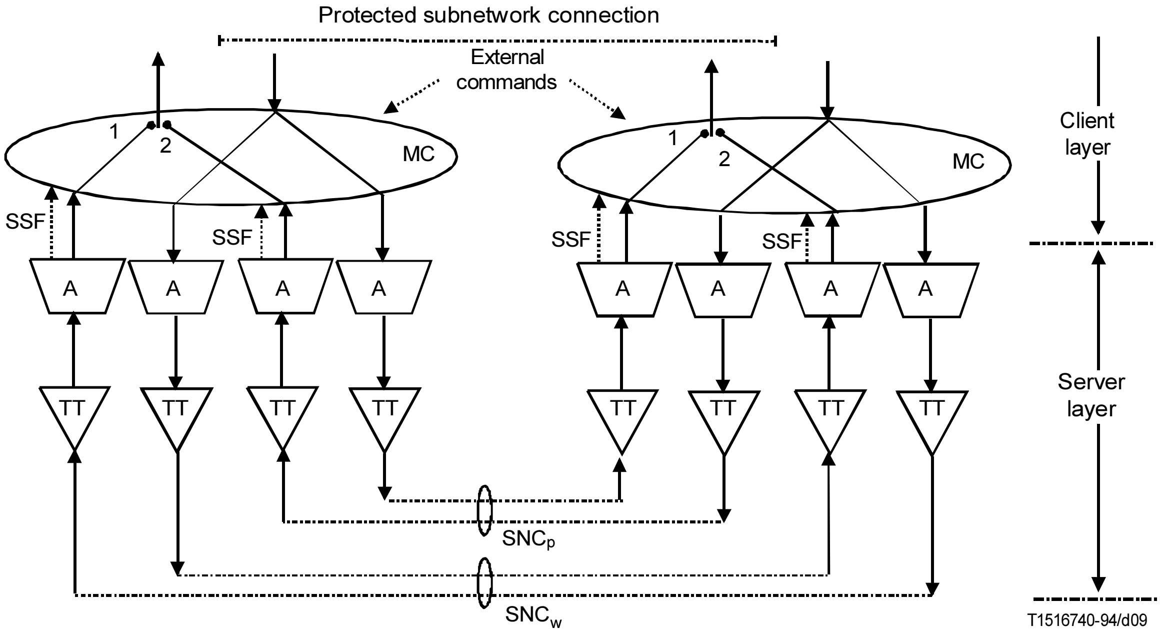
* On failure state (2), $Trail_p$ becomes $Trail_w$,$Trail_w$ becomes $Trail_p$, NC_p becomes NC_w and NC_w becomes NC_p .

A	Adaptation	SD	Signal Degrade
A_p	Protection Adaptation	SF	Signal Fail
MC_p	Protection Matrix Connection	SSF	Server Signal Fail
NC_p	Protection Network Connection	$Trail_p$	Protection Trail
NC_w	Working Network Connection	$Trail_w$	Working Trail
RDI	Remote Defect Indication	TT	Trail Termination
REI	Remote Error Indication	TT_p	Protection Trail Termination

States: 1 Normal state
2 Failure state

FIGURE 5-6/G.841

Functional model for generic 1 : 1 linear trail protection – Non-revertive operation

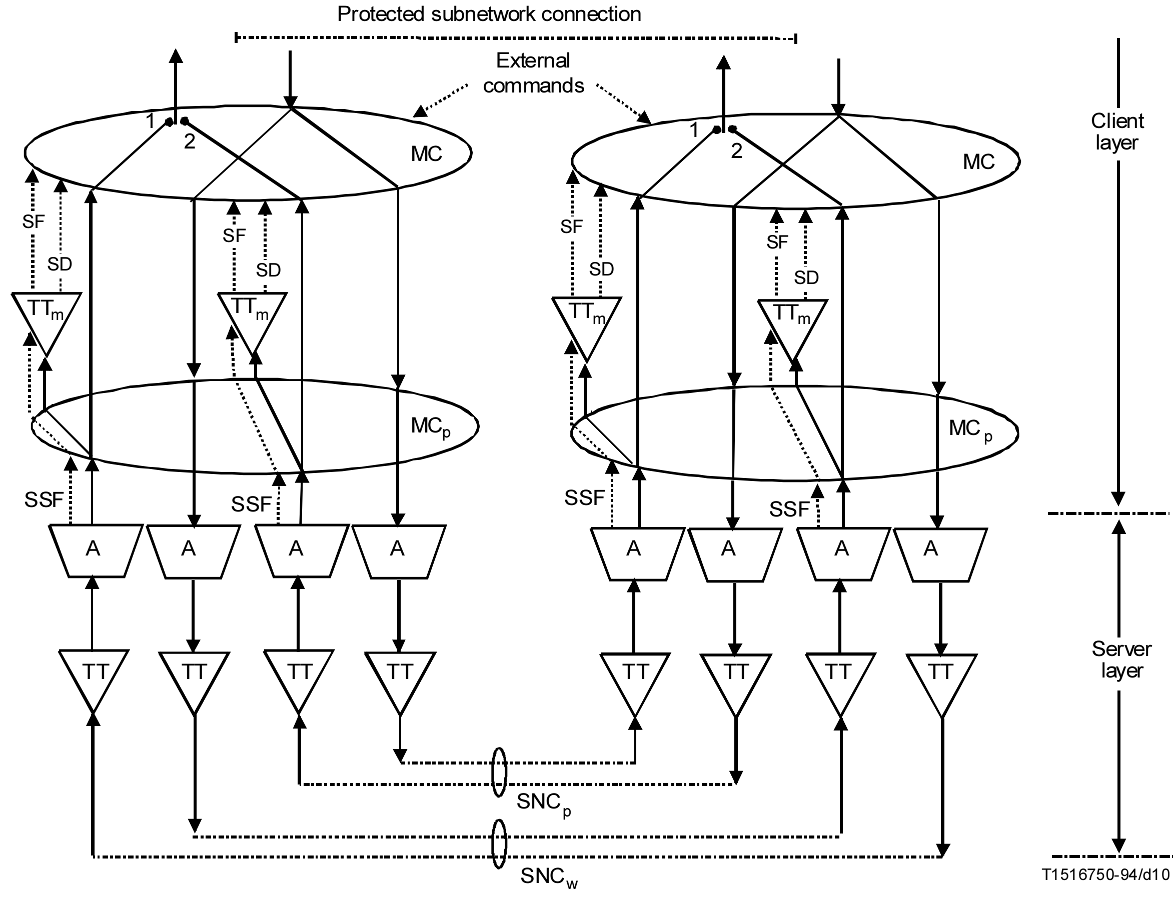


A	Adaptation
MC	Matrix Connection
SNC_p	Protection Subnetwork Connection
SNC_w	Working Subnetwork Connection
SSF	Server Signal Fail
TT	Trail Termination

States: 1 Normal state
2 Failure state

FIGURE 5-7/G.841

Functional model for Subnetwork Connection Protection with Inherent Monitoring (SNC/I) by means of a server signal fail



A	Adaptation
MC	Matrix Connection
MC_p	Protection Matrix Connection
SD	Signal Degrade
SF	Signal Fail
SNC_p	Protection Subnetwork Connection
SNC_w	Working Subnetwork Connection
SSF	Server Signal Fail
TT	Trail Termination
TT_m	Non-intrusive Monitor

States: 1 Normal state
2 Failure state

FIGURE 5-8/G.841

Functional model for Subnetwork Connection Protection with Non-intrusive Monitoring (SNC/N)

6 Applications considerations

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

6.1 MS shared protection rings

MS shared protection rings can be categorized into two types: two-fibre and four-fibre. The ring APS protocol accommodates both types.

For MS shared protection rings, the working channels carry service to be protected while the protection channels are reserved for protection of this service. Working traffic is transported bidirectionally over spans: an incoming tributary travels in one direction of the working channels while its associated outgoing tributary travels in the opposite direction but over the same spans.

The pair of tributaries (incoming and outgoing) only uses capacity along the spans between the nodes where the pair is added and dropped. Thus, as illustrated in Figure 6-1, the pattern that these pairs of tributaries are placed on the ring impacts the maximum load that can be placed on MS shared protection rings. The sum of the tributaries that traverse a span cannot exceed the maximum capacity of that particular span.

Depending upon the tributary pattern, the maximum load that can be placed on a (bidirectional) MS shared protection ring can exceed the maximum load that can be placed on the equivalent type of unidirectional ring (e.g. MS dedicated protection, or SNC protection) with the same optical rate and the same number of fibres. This gives the bidirectional ring a capacity advantage over unidirectional rings, except whenever the tributaries are all destined for only one node on the ring, in which case they are equivalent.

One advantage of MS shared protection rings is that service can be routed on the ring in either one of the two different directions, the long way around the ring or the short way. Although the short way will usually be preferred, occasionally routing service over the long way permits some load balancing capabilities.

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

During a ring switch, working channels transmitted toward the failed span are switched at one switching node to the protection channels transmitted in the opposite direction (away from the failure). This bridged traffic travels the long way around the ring on the protection channels to the other switching node where the protection channels are switched back onto the working channels. In the other direction, the working channels are bridged and switched in the same manner. Figure 6-2 illustrates a ring switch in response to a cable cut.

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

6.2 MS shared protection rings (transoceanic application)

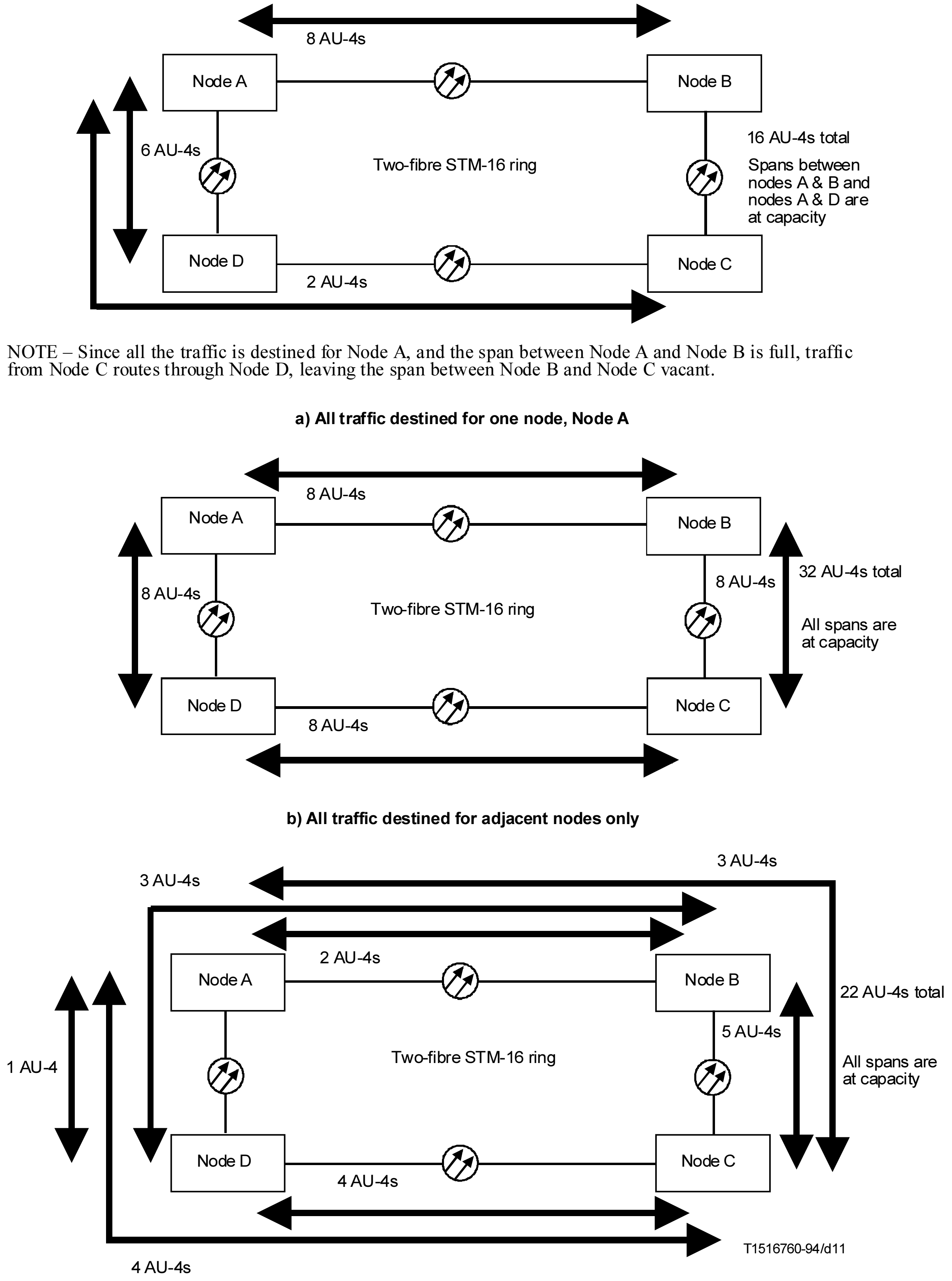
This application, including its additional requirements and operating characteristics, is described in Annex A.

6.3 MS dedicated protection rings

An MS dedicated protection ring consists of two counter-rotating rings, each transmitting in opposite directions relative to each other. In this case, only one ring carries working traffic to be protected while the other is reserved for protection of this working traffic.

The maximum demand that can be placed on the ring is limited to the capacity of a span. The pattern of the demand placed on the ring does not impact the capacity of unidirectional rings. In other words, the sum of the demand from all the nodes cannot exceed the capacity of a single span.

MS dedicated protection rings would also require using the APS bytes, K1 and K2, for protection switching.



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.

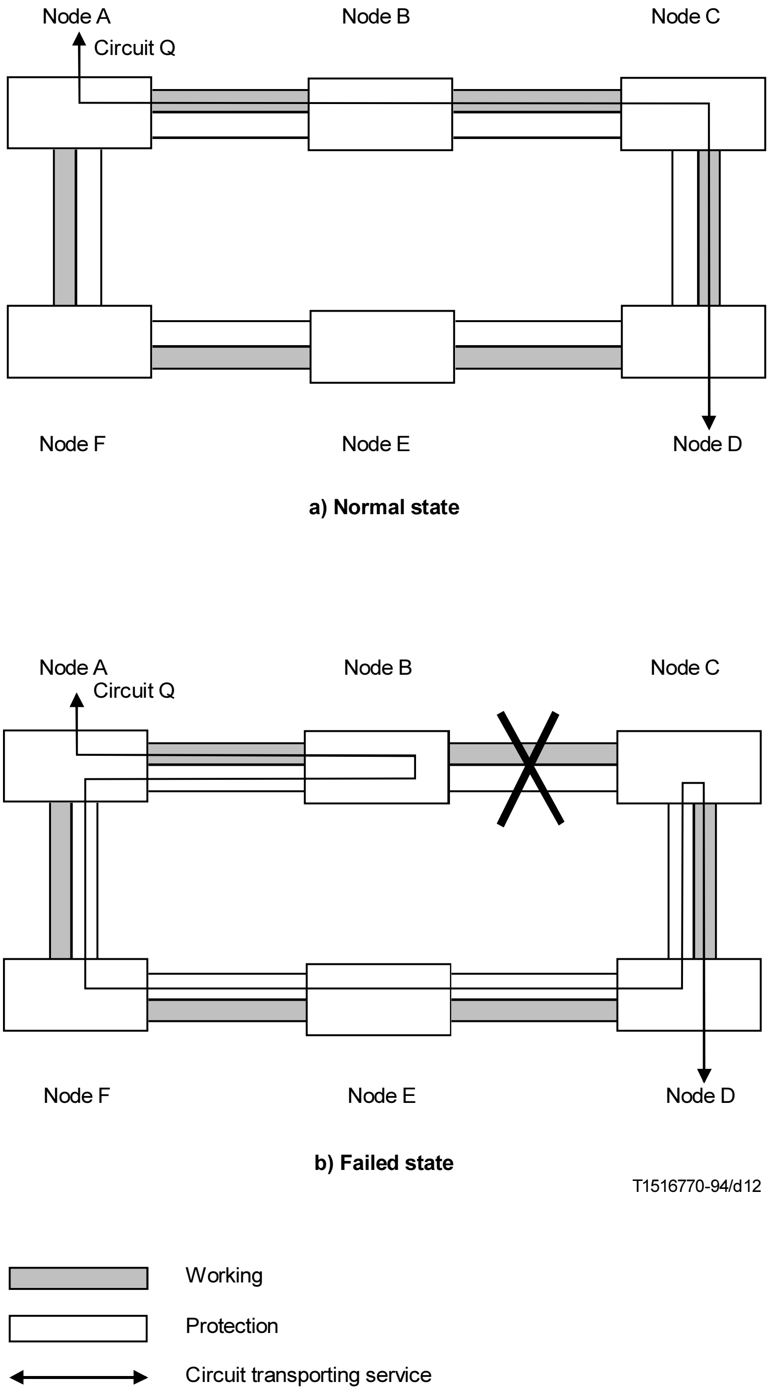
a) All traffic destined for one node, Node A

b) All traffic destined for adjacent nodes only

c) Mixed traffic pattern

FIGURE 6-1/G.841

Effects of demand pattern on capacity of bidirectional MS shared protection rings



a) Normal state

b) Failed state

FIGURE 6-2/G.841

Example of circuit routing in failure state for a ring switch

6.4 Single-ended and dual-ended switching

Possible advantages of single-ended switching include:

1) Single-ended switching is a simple scheme to implement and does not require a protocol.

2) Single-ended switching can be faster than dual-ended switching because it does not require a protocol.

3) Under multiple failure conditions there is a greater chance of restoring traffic by protection switching if single-ended switching is used, than if dual-ended switching is used.

Possible advantages of dual-ended switching when uniform routing is used include:

1) With dual-ended operation, the same equipment is used for both directions of transmission after a failure. The number of breaks due to single failures will be less than if the path is delivered using the different equipment.

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

3) Dual-ended switching is easier to manage because both directions of transmission use the same equipments along the full length of the trail.

4) Dual-ended switching maintains equal delays for both directions of transmission. This may be important where there is a significant imbalance in the length of the trails, e.g. transoceanic links where one trail is via a satellite link and the other via a cable link.

5) Dual-ended switching also has the ability to carry extra traffic on the protection path.

6.5 Linear VC trail protection

Linear VC trail protection is a dedicated protection mechanism that can be used on any physical structure (i.e. meshed, ring, or mixed). It may be applied in any path layer in a layered network.

It is an end-to-end protection mechanism, and switches on server failures and client level information, including path performance information. It need not be used on all VCs within a multiplex section.

Linear VC trail protection can operate in a single-ended or dual-ended manner. Dual-ended switching has the ability to carry extra traffic on the protection path.

6.6 Subnetwork connection protection

Subnetwork connection protection is a dedicated protection mechanism that can be used on any physical structure (i.e. meshed, rings, or mixed). It may be applied at any path layer in a layered network.

It can be used to protect a portion of a path (e.g. that portion where two separate path segments are available), or the full end-to-end path. It switches on server failures (using inherent monitoring) or it switches using client layer information (using non-intrusive monitoring).

It need not be used on all VCs within a multiplex section. SNC protection operates in a single-ended manner. The ability to perform dual-ended switching and the carriage of extra traffic is for further study.

6.7 Linear multiplex section protection

Linear multiplex section protection can be a dedicated or shared protection mechanism. It protects the multiplex section layer, and applies to point-to-point physical networks. One protection multiplex section can be used to protect a number (N) of working multiplex sections. It cannot protect against node failures. It can operate in a single-ended or dual-ended manner, and it can carry extra traffic on the protection multiplex section.

7 SDH trail protection

This clause describes the detailed equipment characteristics required to support SDH trail protection applications.

7.1 Linear multiplex section protection

For more information on this architecture, please refer to Annex A/G.783.

7.2 MS shared protection rings

7.2.1 Application architecture

All MS shared protection rings support ring switching. In addition, four-fibre MS shared protection rings support span switching.

7.2.1.1 Two-fibre MS shared protection rings

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

Two-fibre MS shared protection rings support ring switching only. When a ring switch is invoked, the time slots that carry the working channels are switched to the time slots that carry the protection channels in the opposite direction.

7.2.1.2 Four-fibre MS shared protection rings

Four-fibre MS shared protection rings require four fibres for each span of the ring. As illustrated in Figure 7-2, working and protection channels are carried over different fibres: two multiplex sections transmitting in opposite directions carry the working channels while two multiplex sections, also transmitting in opposite directions, carry the protection channels. This permits the bidirectional transport of working traffic. The multiplex section overhead is dedicated to either working or protection channels since working and protection channels are not transported over the same fibres.

Four-fibre MS shared protection rings support 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 channels along one span are used for each span switch. Certain multiple failures (those that affect only the working channels of a span such as electronic failures and cable cuts severing only the working channels) can be fully protected using span switching.

Four-fibre MS shared protection rings may have the capability of operating similar to a linear ADM chain when not fully connected as a continuous ring (i.e. they can lockout 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.

7.2.2 Network objectives

The following network objectives apply:

1) *Switch time* – On rings with no extra traffic, no previous bridge requests, and less than 1200 km of fibre, the switch completion time shall be less than 50 milliseconds.

2) *Transmission delay* – There is no network objective on transmission delay.

3) *Hold-off times* – There is no network objective on hold-off times.

4) *Extent of protection*

   a) For a single point failure, the ring will restore all traffic that would be passing through the failed location had no failure occurred.

   b) The ring shall restore all traffic possible, even under conditions of multiple bridge requests of the same priority (including the combination of Forced Switch – Ring and Signal Fail – Ring).

5) *Switching types* – Dual-ended switching shall be provided.

6) *APS protocol and algorithm*

   a) The switching protocol shall be able to accommodate up to 16 nodes on a ring.

   b) In order to provide an additional degree of protection for the four-fibre ring, a mechanism to perform span switching shall be provided in the APS protocol.

   c) The APS protocol shall be optimal for the AU-3/4 level of operation.

   d) The APS protocol and associated OAM&P functions shall accommodate the ability to modify and upgrade the ring. In particular, adding and deleting nodes from the ring shall be accommodated.

   e) A deterministic process shall be used to avoid misconnecting traffic.

   f) All spans on a ring shall have equal priority. Therefore, no higher priority spans will exist which would allow ring bridge requests for that span to override (automatically) other span switches of the same type (e.g. Signal Fail, Signal Degrade, or Forced Switch).

   g) The state of ring (i.e. in the normal or protected state) shall be known at each node.

   h) A span bridge request shall have higher priority than a ring bridge request of the same type.

   i) If a ring switch exists and a failure of equal priority occurs on another span requiring a ring switch (including the combination of Forced Switch – Ring and Signal Fail – Ring), then, if the priority of the bridge request is Signal Fail (Ring) or higher, both ring switches shall be established resulting in the ring segmenting into two separate segments.

   j) AUG squelching shall be done at the switching nodes.

7) *Operation modes*

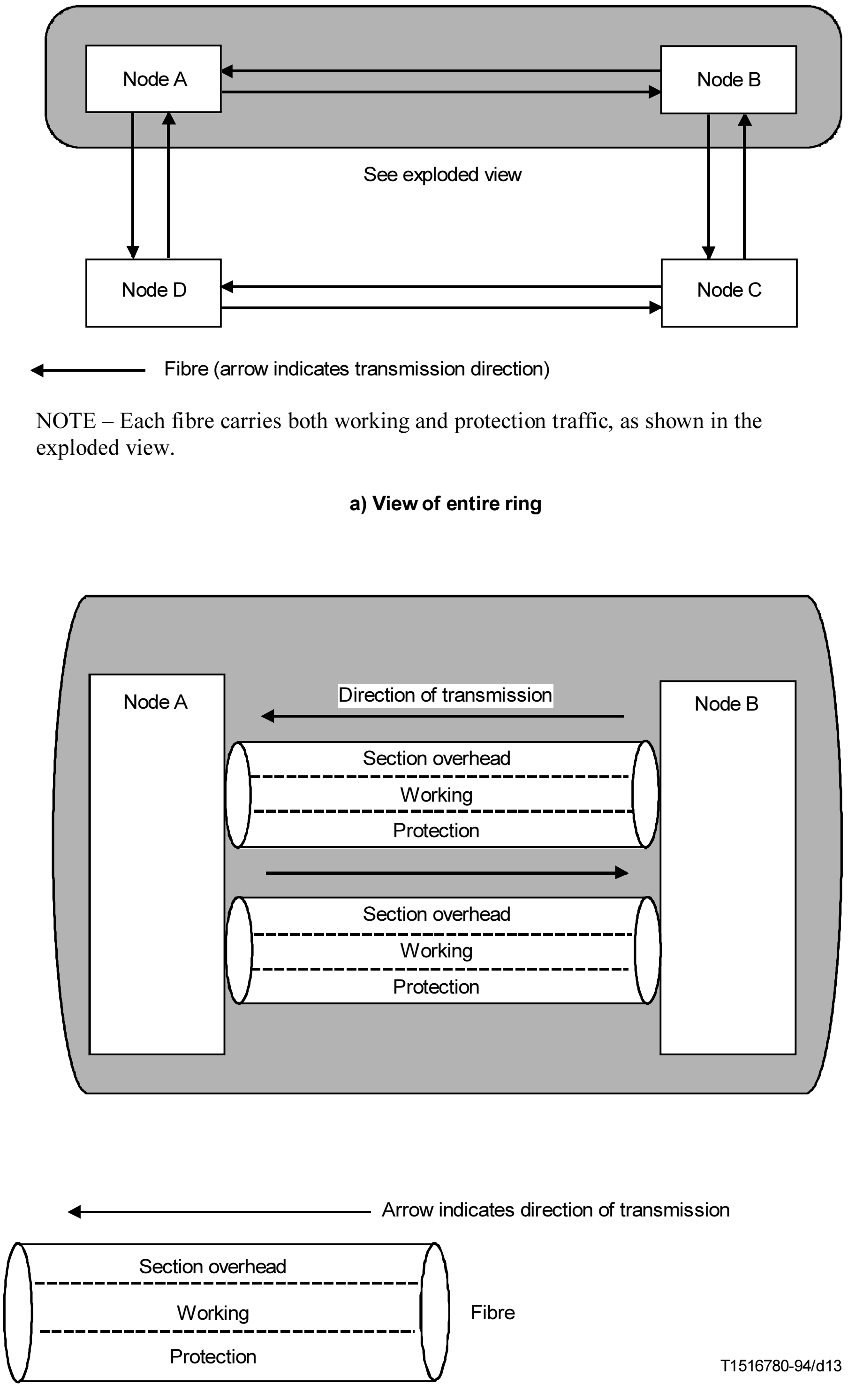
   a) Revertive switching shall be provided. A switch shall revert only to the working channels and not to a different set of protection channels.

   b) The ring APS signalling shall provide protection switching for both two-fibre and four-fibre bidirectional MS shared protection rings.

8) *Manual control* – The following externally initiated commands shall be supported: Lockout of Protection – Span, Forced Switch – Span, Forced Switch – Ring, Manual Switch – Span, Manual Switch – Ring, Exerciser – Span, and Exerciser – Ring.

9) *Switch initiation criteria* – The following automatically initiated commands shall be supported: Signal Failure – Protection, Signal Failure – Span, Signal Failure – Ring, Signal Degrade – Span, Signal Degrade – Ring, Signal Degrade – Protection, Reverse Request – Span, Reverse Request – Ring, Wait-To-Restore, and No Request.

10) *Ring utilization criteria* – Timeslot interchange will allow better utilization of bandwidth of the ring. If Timeslot Interchange (TSI) is allowed, the traffic having a timeslot interchange through the failed location may or may not be restored. It is for further study whether TSI shall be allowed, and if allowed, whether traffic having timeslot interchange through the failed location will be restored.



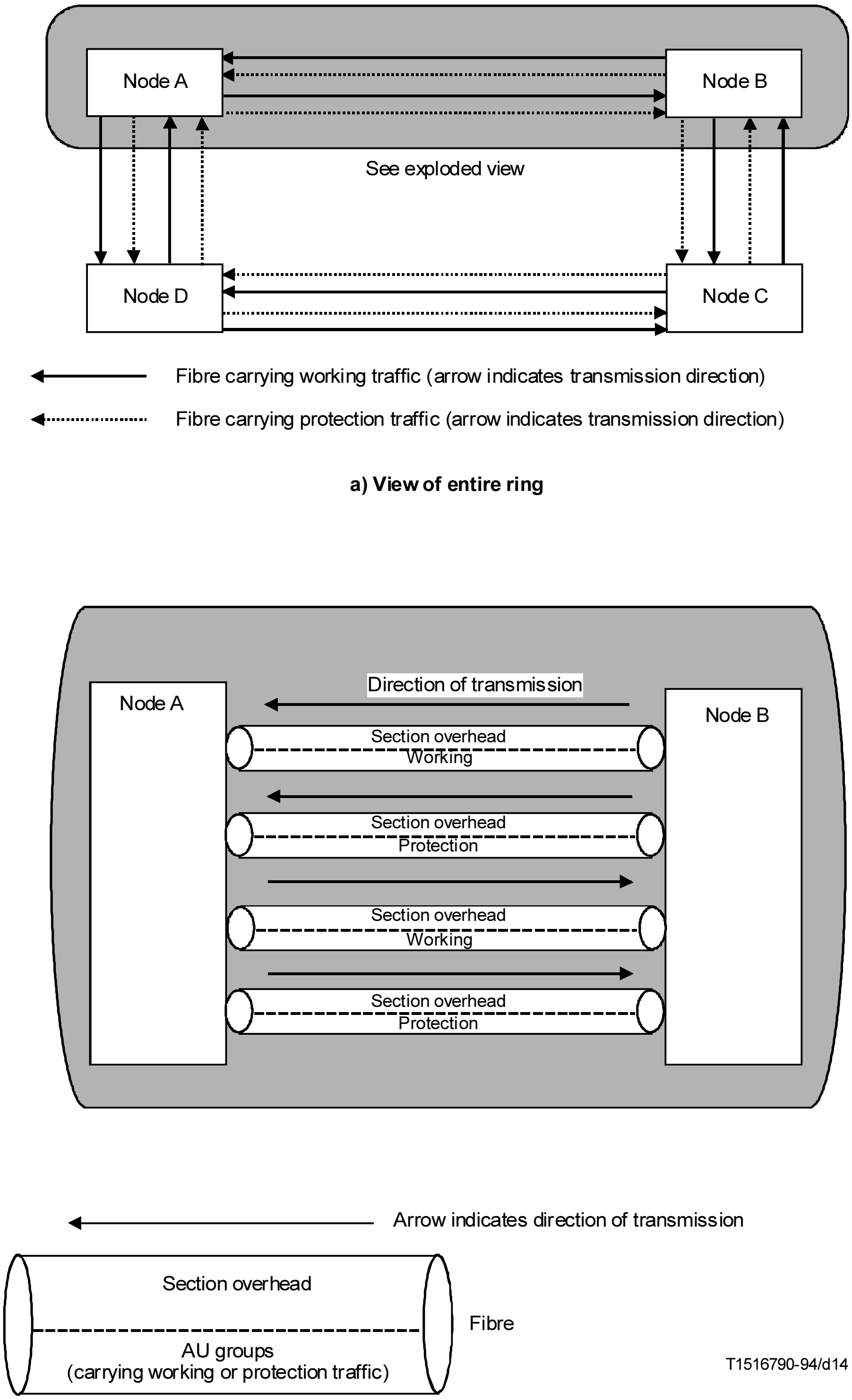
NOTE – Each fibre carries both working and protection traffic, as shown in the exploded view.

a) View of entire ring

b) Exploded view of the shaded portion of the ring

FIGURE 7-1/G.841

Two-fibre MS shared protection ring


Node A
Node B
Node C
Node D
See exploded view
Fibre carrying working traffic (arrow indicates transmission direction)
Fibre carrying protection traffic (arrow indicates transmission direction)
Direction of transmission
Section overhead
Working
Section overhead
Protection
Section overhead
Working
Section overhead
Protection
Arrow indicates direction of transmission
Section overhead
AU groups
(carrying working or protection traffic)
Fibre
T1516790-94/d14

a) View of entire ring

b) Exploded view of the shaded portion of the ring

FIGURE 7-2/G.841

Four-fibre MS shared protection ring

7.2.3 Application architecture

The AU groups that traverse the span between any two adjacent nodes are divided into working channels and protection channels. In the case of the two-fibre ring, the STM-N can be viewed as a multiplex of N AU-4s, where the AU-4s are numbered from 1 to N according to the order that they appear in the multiplex. AU-4s numbered from 1 to N/2 shall be assigned as working channels, and AU-4s numbered from (N/2) + 1 to N shall be assigned as protection channels. Furthermore, working channel m is protected by protection channel (N/2) + m. For example, an STM-4 can be considered a multiplex of four AU-4s numbered one to four. AU-4s number one and two would be assigned as working channels, and AU-4s number three and four would be assigned as protection channels. This assignment applies to both directions of transmission and to all spans.

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

The ring APS protocol shall be carried on bytes K1 and K2 in the multiplex section overhead. In the case of the four-fibre ring, the APS protocol is only active on the fibres carrying protection channels. Functions that are required in real time and required to make a protection switch are defined in the ring APS protocol using bytes K1 and K2. Other operations channels, including the regenerator section and multiplex section Data Communications Channels, may also provide protection switching functions that are not time critical (for example, functions that need not be completed within 50 milliseconds).

Each node on the ring shall be assigned an ID that is a number from zero to fifteen, allowing a maximum of sixteen 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 channels in either direction, drop channels from either direction, or pass channels directly through to allow other nodes to be connected. This issue of the document supports only AU access. Each node has a ring map that is maintained by local craft or by an OS and contains information about the assignment of channels that the node handles. An example of such a ring map is provided in Figures 7-3 and 7-4.

	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

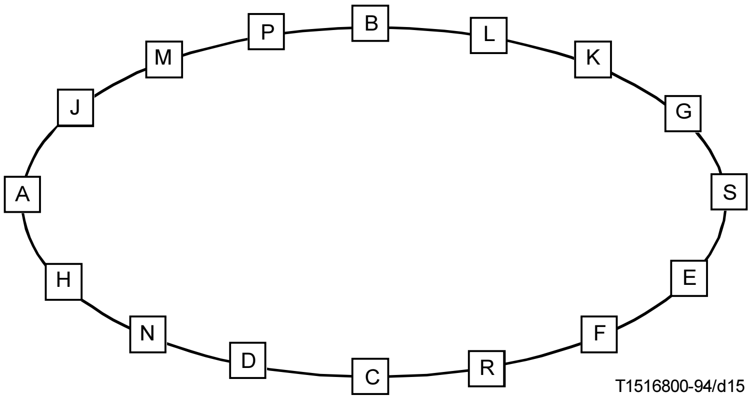
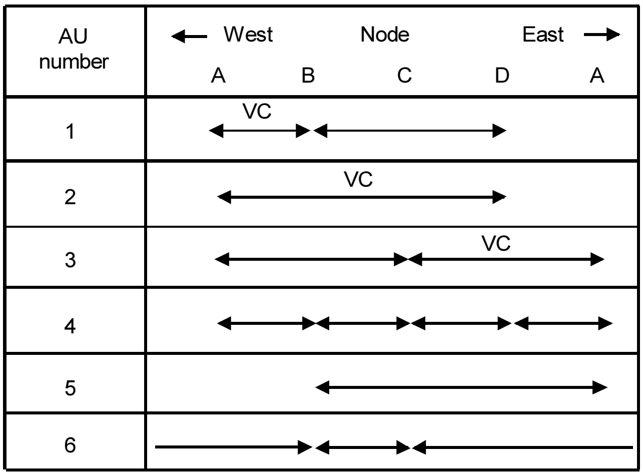


FIGURE 7-3/G.841

Conceptual representation of a ring topology map



Sample traffic routing for a four-node ring.

Node A

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

Node B

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

Node C

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

Node D

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

T1516810-94/d16

Src Node at which an HO VC enters the ring or is sourced
Dst Node at which an HO VC exists the ring or is terminated
✓ Indicates an LO VC organized AU

NOTE – Marking of AUs for LO VC access is optional. All connections in this example are bidirectional.

FIGURE 7-4/G.841

Conceptual representation of node cross-connect map

When no protection switches are active on the ring, each node sources the K-bytes in each direction indicating no bridge request. In general, the protection channels that are sourced at each node contain Path Unequipped, as specified in Recommendation G.709. This point is for further study. The exception is extra traffic that may be added, dropped, or passed through similar to working traffic. Identification of extra traffic in the ring APS protocol is for further study.

A switch shall be initiated by one of the criteria specified in 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 channels and not the protection channels 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, Signal Degrade, Forced Switch). 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 K-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, 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 nodes receives a higher priority bridge request, it enters the appropriate pass-through state. In this way, the switching nodes can maintain direct K-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 7-5. In a two-fibre ring, B will bridge the AU-4 channels numbered 1 to N/2 (working) that were being transmitted from B to C onto AU-4 channels (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 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 channels that were being transmitted on the working fibre from B to C onto the channels being transmitted on the protection fibre from B to A. Similarly, C will switch the channels on the protection fibre received from D onto the channels transmitted on the working fibre to D.

The end result for this example is that all the channels 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 channels 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 protection channels and the K-bytes. In general, traffic only reverts from the protection channels back to the working channels. Specifically, in a four-fibre ring, if a ring switch is active on the long-path protection channels, and the short-path protection channels become available, the service will not be switched to the short-path protection channels unless a new bridge request preempts the long-path protection channels.

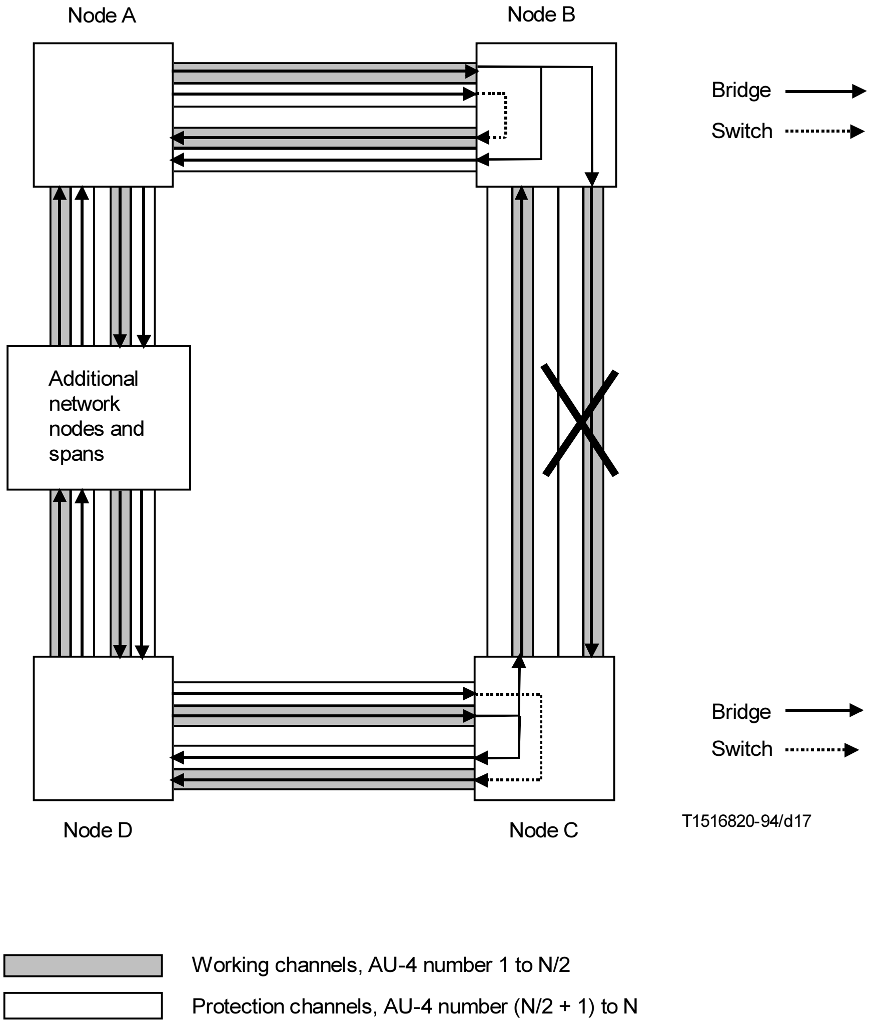

Node A
Node B
Bridge
Switch
Additional network nodes and spans
Bridge
Switch
Node D
Node C
T1516820-94/d17
Working channels, AU-4 number 1 to N/2
Protection channels, AU-4 number (N/2 + 1) to N

FIGURE 7-5/G.841

Bridge and switch in a two-fibre MS shared protection ring

Ring and span switches can be preempted by bridge requests of higher priority as determined by Table 7-1. 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 channels. A ring bridge request will be generated, the span switch dropped, and the ring switch established.

If a ring switch exists and a failure of equal priority occurs on another span requiring a ring switch, then, if the priority of the bridge request is Signal Fail (Ring) 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 Signal Fail (Ring), 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 preempt 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 bridge indication is sent on the long path in order to inform other nodes of the state of the ring. In addition, OAM&P messages transported over the DCC can be used to determine the details regarding the condition of the ring.

In order to perform a ring switch, the protection channels are essentially shared among each span of the ring. Also, extra traffic may reside in the protection channels when the protection channels are not currently being used to restore working traffic transported on the working channels. Thus, each protection channel time slot is subject to use by multiple services (services from the same time 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 channel time slot. This yields a potential for misconnected traffic. With extra traffic on the ring, even under single point failures, a service on the working channels may contend for access to the same protection channel time 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. In Figure 7-6, 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 K1 and K2 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 AU-AIS in those time slots where misconnected traffic could occur. For rings operating at an AU-4 level, this squelching occurs at the switching nodes. For rings using lower order VC 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 channels are added or dropped by B. A and C will squelch these channels before the ring switch is performed by inserting AU-AIS. Thus, any node on the ring that was connected to B will now receive AIS on those channels.

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

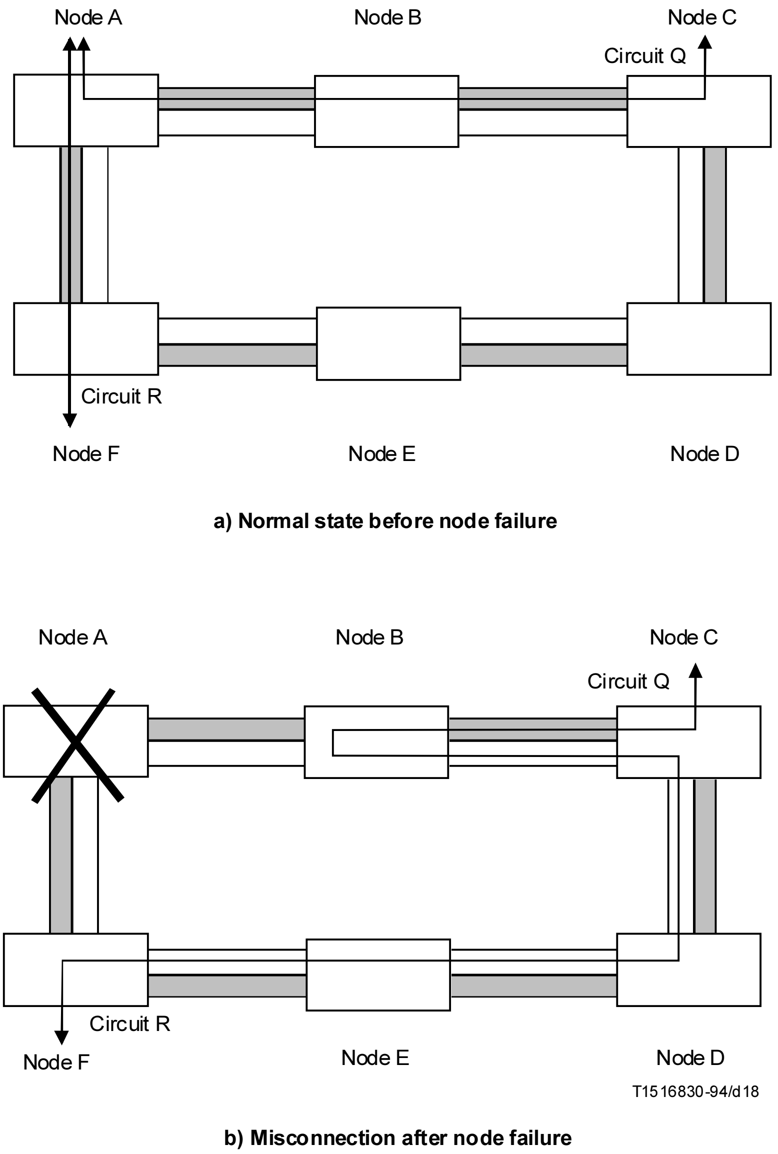
1) information regarding the order in which the nodes appear on the ring,

2) the AU-4 time slot assignments for traffic that is both terminated at that node and passed-through that node,

3) for each of these AU-4 time slots, the node addresses at which the traffic enters and exits the ring; and

4) an optional indication of whether the AU is being accessed at the lower order VC level somewhere on the ring.

An example of such ring maps is given in Figures 7-3 and 7-4. For lower order VC access and extra traffic, the map requirements are under study.



a) Normal state before node failure

b) Misconnection after node failure

Circuit	Timeslot Assignment	Channel
Q	1W	Working
R	1W	Working

▨ Working

□ Protection

↔ Circuit transporting service

NOTE – Under the "Timeslot Assignment" column, the designation "1W" indicates that it is the first timeslot in the capacity reserved for working traffic.

FIGURE 7-6/G.841

Example of misconnection

7.2.4 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. Subclause 7.2.4.1 describes these externally initiated commands available at the OS, craftsperson, or both interfaces. Automatically initiated commands can also be initiated based on multiplex section and equipment performance criteria. Subclause 7.2.4.2 provides the automatically initiated command criteria.

The bridge requests related to span switching (except for Lockout of Protection) are used only for four-fibre MS shared protection rings.

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

7.2.4.1 Externally initiated commands

External bridge requests are initiated at an NE by either the OS or the craftsperson. The external bridge request may be transmitted to the appropriate NE via the APS bytes, the TMN, or over the local craft interface. The bridge requests are evaluated by the priority algorithm in the protection switching controller.

7.2.4.1.1 Commands not signalled on the APS channel

The descriptions of the externally initiated commands are provided below.

7.2.4.1.1.1 clear: This command clears the externally initiated command and 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 have only traffic that does not need protection The commands are not time critical (i.e. not needed to be completed in tens of milliseconds). Thus, they can be transmitted over the DCC.

7.2.4.1.1.2 Lockout of working channels – ring switch: This command prevents the working channels over the addressed span from accessing the protection channels for a ring switch by disabling the node’s capability to request a ring protection switch of any kind. If any working traffic is already on protection, the ring bridge is dropped regardless of the condition of the working channels. If no other bridge requests are active on the ring, the NR code is transmitted. This command has no impact on the use of protection channels for any other span. For example, the node can go into any of the pass-through modes.

7.2.4.1.1.3 Lockout of working channels – span switch: This command prevents the working channels over the addressed span from accessing the protection channels for a span switch. If any working traffic is already on protection, the span switch is dropped regardless of the condition of the working channels. If no other bridge requests are active on the ring, the NR code is transmitted. This command has no impact on the use of protection channels for any other span.

7.2.4.1.1.4 Lockout of protection – all spans: This command prevents protection switching on the entire ring. If any working traffic is using the protection facility on any span, this command causes working traffic to switch back to the working channels regardless of the condition of the working channels. Note that the K1 and K2 bytes do not support this command. Thus, the command has to be sent to each of the NEs and the Lockout of Protection – Span request is used by each NE to coordinate activities with the far end.

7.2.4.1.2 Commands using the APS bytes

The following commands are carried over the APS bytes:

7.2.4.1.2.1 Lockout of Protection – Span (LP-S): This command prevents the usage of the span for any protection activity. If any working traffic is already using the protection on this span, this command causes this traffic to switch back to the working channels. Thus, all ring switching that uses the protection capacity of the locked-out span is prevented (and preempted), and span switching is prevented only on the locked-out span.

7.2.4.1.2.2 Forced switched Working to Protection – Ring (FS-R): This command performs the ring switch from working channels to the protection channels 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 channels, unless the protection channels are satisfying a higher priority bridge request.

7.2.4.1.2.3 Forced Switched Working to Protection – Span (FS-S): This command switches the traffic from the working channels to the protection channels of that span. This switch occurs regardless of the state of the protection channels, unless the protection channels are satisfying a higher priority bridge request, or a signal failure (or a K-byte failure) exists on the protection channels of the span.

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

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

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

7.2.4.1.2.7 Exercise – Span (EXER-S): This command exercises span protection of the requested channel without completing the actual bridge and switch. The command is issued and the responses are checked, but no working 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 MS shared protection ring, 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.

7.2.4.2 Automatically initiated commands

APS requests are also initiated based on multiplex section and equipment performance criteria detected by the NE. All the working and protection channels 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 working traffic affected by a hard failure, while the SD bridge request is used to protect against a soft failure. 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 channels and the working channels. 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 channels. The WTR is issued only after an SF or an SD condition and, thus, does not apply for externally initiated bridge requests.

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

7.2.4.2.1 Signal Fail – Span (SF-S): An SF is defined in Recommendation G.783. The tail end detects the failure and generates the bridge request. For four-fibre rings, if the failure affects only the working channels, traffic can be restored by switching to the protection channels on the same span. The SF-S bridge request is used to initiate span switching for an SF on the working channels of a four-fibre ring.

7.2.4.2.2 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 channels within a span, it is necessary to initiate a ring bridge request. Hence, this command is used to request ring switching for signal failures.

7.2.4.2.3 Signal Fail – Protection (SF-P): This command is used to indicate to an adjacent node that the protection channels are in a Signal Fail state. A signal failure of the protection channels is equivalent to a lockout of protection for the span that is affected by the failure. Hence, the K1 byte that is transmitted to the adjacent node is the same code as that of a Lockout of Protection - Span. SF-P is used only for four-fibre rings.

7.2.4.2.4 Signal Degrade – Span (SD-S): Signal Degrade is defined in Recommendation G.783. In four-fibre rings, the working channels on the degraded span can be protected using the protection channels on the same span. This bridge request is used to switch the working traffic to the protection channels in the same span where the failure is located.

7.2.4.2.5 Signal Degrade – Ring (SD-R): For two-fibre rings, any degraded multiplex section is protected using the ring switch. (Degradation is defined above under Signal Degrade - Span.) For four-fibre rings, this bridge request is used when the working channels are degraded and the protection channels on the same span are degraded or not available.

7.2.4.2.6 Signal Degrade – Protection (SD-P): This command is used when an NE detects a degradation on its protection channels, and there are no higher priority bridge requests existing on the working channels. (Degradation is defined above under Signal Degrade - Span.) This bridge request is used only for four-fibre rings.

7.2.4.2.7 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.

7.2.4.2.8 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.

7.2.4.2.9 Wait to Restore (WTR): This command is issued when working channels meet the restoral threshold after an SD or SF condition. It is used to maintain the state during the WTR period unless it is preempted by a higher priority bridge request.

7.2.5 Protection switch protocol

Two APS bytes, K1 and K2, shall be used for protection switching. See 7.2.6 for details on the operational usage of these bytes.

Bytes K1 and K2 shall be transmitted within the multiplex section overhead of the STM-N that is carrying the protection channels. Note, however, that bits 6-8 of byte K2 are used on all STM-N line signals to signal MS-RDI and MS-AIS.

7.2.5.1 Byte K1

These bits shall be assigned as per Table 7-1. K1 bits 1-4 carry bridge request codes, listed in descending order of priority in Table 7-1. K1 bits 5-8 carry the destination node ID for the bridge request code indicated in K1 bits 1-4.

TABLE 7-1/G.841

Byte K1 functions

Bridge request code (bits 1-4)				Destination node identification (bits 5-8)			
Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8
1111	Lockout of Protection (Span) LP-S or Signal Fail (Protection) SF-P			The Destination Node ID is set to the value of the ID of the node for which that K1 byte is destined. The destination node ID is always that of an adjacent node (except for default APS bytes).			
1110	Forced Switch (Span) FS-S						
1101	Forced Switch (Ring) FS-R						
1100	Signal Fail (Span) SF-S						
1011	Signal Fail (Ring) SF-R						
1010	Signal Degrade (Protection) SD-P						
1001	Signal Degrade (Span) SD-S						
1000	Signal Degrade (Ring) SD-R						
0111	Manual Switch (Span) MS-S						
0110	Manual Switch (Ring) MS-R						
0101	Wait-To-Restore WTR						
0100	Exerciser (Span) EXER-S						
0011	Exerciser (Ring) EXER-R						
0010	Reverse Request (Span) RR-S						
0001	Reverse Request (Ring) RR-R						
0000	No Request-NR						
NOTE – Reverse Request assumes the priority of the bridge request to which it is responding.							

7.2.5.2 Byte K2

Byte K2 shall be assigned as shown in Table 7-2.

TABLE 7-2/G.841

Byte K2 functions

Source node identification (bits 1-4)				Long/ Short	Status (bits 6-8)		
Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8
Source node ID is set to the node's own ID. Long/Short (bit 5) 0 = short-path code (S) 1 = long-path code (L)					Status: 111 MS-AIS 110 MS-RDI 101 Reserved for future use 100 Reserved for future use 011 Reserved for future use 010 Bridged and Switched (Br&Sw) 001 Bridged (Br) 000 Idle		

7.2.6 Protection algorithm operation

This subclause is structured as follows:

First, a number of general APS algorithm rules are given. Detailed rules then follow. The first subclause covers the three classes of ring node APS states, and the steady-state behaviour of the node in these states. The second subclause describes the transition rules among the different ring node APS states.

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

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

The following set of general rules apply:

Rule G #1 – BRIDGE REQUEST VALIDATION (Bridge Request and Bridge Request Status Definitions):

Rule G #1a – (Bridge Request).

The information contained in byte K1 bits 1-4 shall be considered as a Bridge Request if:

- these bits indicate one of the ring bridge request codes and byte K2 bit 5 indicates a long-path code; or
- these bits indicate one of the ring bridge request codes and byte k2 bit 5 indicates a short-path code; or
- these bits indicate one of the span bridge request codes and byte K2 bit 5 indicates a short-path code.

Rule G #1b – (Bridge Request Status).

The information contained in byte K1 bits 1-4 shall be considered as a Bridge Request Status if:

- these bits indicate one of the span bridge request codes and byte K2 bit 5 indicates a long-path code.

The relationship among bridge request codes, bridge request status codes, and K-byte indications is shown in Table 7-3.

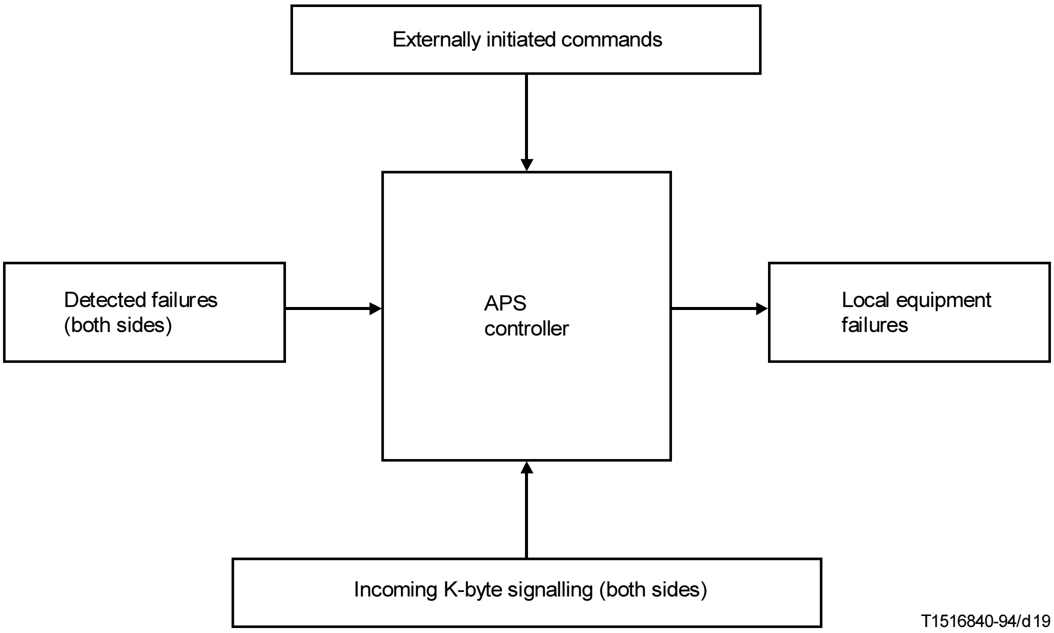

Externally initiated commands
Detected failures (both sides)
APS controller
Local equipment failures
Incoming K-byte signalling (both sides)
T1516840-94/d19

FIGURE 7-7/G.841

Conceptual MS shared protection ring APS controller

TABLE 7-3/G.841

Relationships between K2 bit 5 and K1 bits 1-4

	K1 bits 1-4	
K2 bit 5 code	Ring bridge code	Span bridge code
Long path	Bridge request	Bridge request status
Short path	Bridge request	Bridge request

Note that the MS-RDI and MS-AIS signals terminate at multiplex section terminating elements as specified in Recommendation G.783.

7.2.6.1 Ring node APS state

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

7.2.6.1.1 Idle state

A node is in the idle state when it is not generating, detecting, or passing through bridge requests or bridge request status codes.

Rule I #1 – IDLE STATE SOURCED K BYTES: Any node in the idle state shall source the K-bytes in both directions as given in Table 7-4.

TABLE 7-4/G.841

Byte K1 and K2 values sourced in the idle state

K1 [1-4]	=	0000 (No Request code)
K1 [5-8]	=	destination NODE ID
K2 [1-4]	=	source NODE ID
K2 [5]	=	0 (short-path code)
K2 [6-8]	=	000 (idle 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 K-BYTES: Any node in the idle state shall terminate K1 and K2 in both directions.

7.2.6.1.2 Switching state

A node is in a switching state when it is either sourcing a bridge request (automatically or externally), or terminating a bridge request.

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

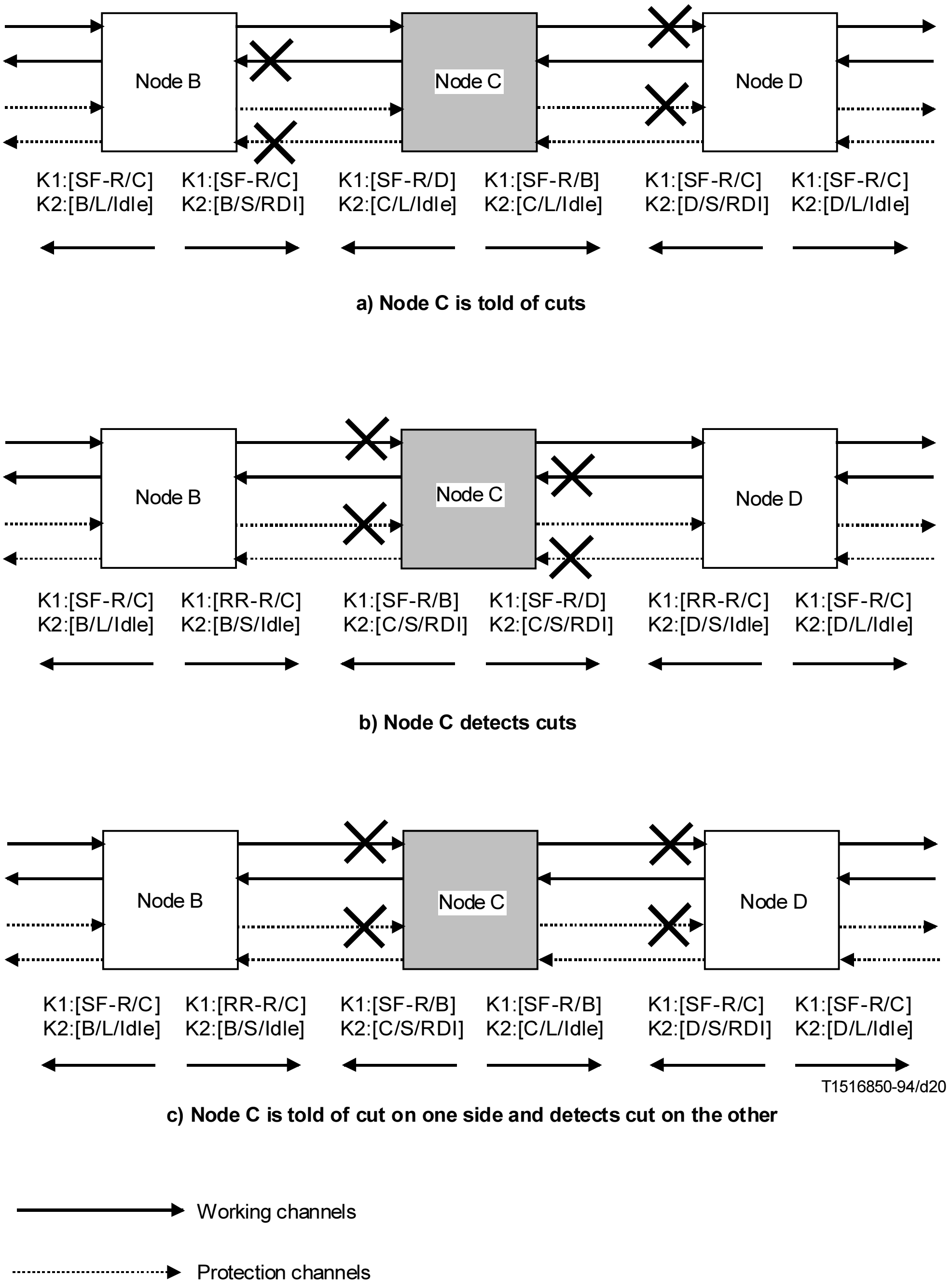
Rule S #1a – Any node in the switching state shall source K-bytes as shown in Table 7-5.

TABLE 7-5/G.841

Byte K1 and K2 values sourced by a node in the switching state

K1 [1-4]	=	BRIDGE REQUEST code
K1 [5-8]	=	destination NODE ID
K2 [1-4]	=	source NODE ID
K2 [5]	=	0/1 (short/long path code)
K2 [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 on the long path. Both bridge requests have the same priority (or one of them is a Reverse Request), and protect the same span. The exceptions are the isolated node case, the case of a span bridge request on each side of the node, the case of a ring request preempting a span bridge request on an adjacent span, and the case where a ring bridge exists on a locked out span. See Figure 7-8 for the isolated node signalling cases.


Node B
Node C
Node D
K1:[SF-R/C] K2:[B/L/Idle]
K1:[SF-R/C] K2:[B/S/RDI]
K1:[SF-R/D] K2:[C/L/Idle]
K1:[SF-R/B] K2:[C/L/Idle]
K1:[SF-R/C] K2:[D/S/RDI]
K1:[SF-R/C] K2:[D/L/Idle]
Node B
Node C
Node D
K1:[SF-R/C] K2:[B/L/Idle]
K1:[RR-R/C] K2:[B/S/Idle]
K1:[SF-R/B] K2:[C/S/RDI]
K1:[SF-R/D] K2:[C/S/RDI]
K1:[RR-R/C] K2:[D/S/Idle]
K1:[SF-R/C] K2:[D/L/Idle]
Node B
Node C
Node D
K1:[SF-R/C] K2:[B/L/Idle]
K1:[RR-R/C] K2:[B/S/Idle]
K1:[SF-R/B] K2:[C/S/RDI]
K1:[SF-R/B] K2:[C/L/Idle]
K1:[SF-R/C] K2:[D/S/RDI]
K1:[SF-R/C] K2:[D/L/Idle]
T1516850-94/d20
Working channels
Protection channels

a) Node C is told of cuts

b) Node C detects cuts

c) Node C is told of cut on one side and detects cut on the other

FIGURE 7-8/G.841

Isolated node signalling (signalling states prior to nodes B and D establishing a ring bridge and switch)

Rule S #1c – Whenever a node in the switching state terminates a new short-path K-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, indicating that both signals it is sending are failed (SF), the long-path bridge request shall take precedence over 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 7-8 a)].

Rule S #1d – Whenever a node detects an incoming failure on the working and on the protection channels, it shall always source over the short path a short-path ring bridge request, even in the case of multiple failures, as long as the ring bridge request is not preempted by a higher priority bridge request. [see Figure 7-8 b).] This rule takes precedence over Rule S #1c. Note that whenever a node receives in one direction a ring bridge request on the short path, (indicating that the signal it is sending has failed) and detects on the other side an incoming failure on the working and on the protection channels, it shall signal the detected failure over both the short and the long paths [see Figure 7-8 c)].

Rule S #2 – SWITCHING STATE RECEIVED K-BYTES: Any node in the switching state shall terminate K1 and K2 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 K1 bits 1-4 to the Reverse Request 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:

- LP-S or SD-P with any span switch;
- LP-S or SD-P with any ring switch on the same span;
- LP-S with SD-P;
- LP-S with LP-S;
- 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 byte K1, and byte K2 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. Note that Reverse Requests and other allowed coexisting ring bridge requests with a short-path code are considered valid ring bridge requests.

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.

7.2.6.1.3 Pass-through state

A node is in the pass-through state when it transmits on one side, all or part of the K1 and K2 bytes, and possibly the protection channels, which it receives on the other side. There are two types of pass-through: full pass-through and K-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 K-BYTES: When a node is in pass-through, it transmits on one side, all or part of the K1 and K2 bytes which it receives from the other side. The part of K1 and K2 that is passed through is dependent upon the state transition rules.

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.) Further clarification of this rule is for further study.

7.2.6.2 Ring node APS state transition rules

The previous subclause described the three ring node states. This subclause 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 K-byte change, a WTR expiration, an externally initiated bridge request, or a locally detected failure.

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

Rule Basic #3 – K2 BITS 6-8 UPDATE: All bridge and switch actions shall be reflected by updating byte K2 bits 6-8, unless an MS-RDI condition exists. An MS-RDI condition shall cause the MS-RDI code to override all other codes in byte K2 bits 6-8 on the failed span (except for MS-AIS) regardless of the state of the Bridge and Switch.

Ring Map Types – Each node on a ring shall maintain a ring map describing the ring connectivity and a local cross-connect map indicating the source and destination of all added, dropped, and passed-through AU-3/4s. In addition, nodes on a ring that will support lower order VC access in the future should include an indication in the ring map of which pass-through AU-3/4s have lower order VC access.

AU-3/4 Squelching – AU-3/4 squelching shall be performed at the switching nodes by inserting AU-AIS. The switching node shall, by comparing K-byte addresses (crossing K-bytes) to the information contained in the ring map, identify which nodes are missing. From this information and the cross-connection map, it shall identify which AU-3/4s are added and dropped at these nodes and shall squelch them bidirectionally.

In addition, nodes on rings that will support lower order VC access in the future should bidirectionally squelch all AU-3/4s with lower order VC access (as indicated in the ring map). Upon receiving the Bridged and Switched code from the far-end switching node, nodes on rings that will support lower order VC access in the future should stop squelching AU-3/4s that have lower order VC access. LOVC access is for further study.

Rule Basic #4 – Bridge requests (due to a locally detected failure, an externally initiated command, or received K-bytes) shall preempt bridge requests in the prioritized order given in Table 7-1, unless the bridge requests are allowed to coexist. Bridge requests shall preempt bridge request status signalling regardless of the priority of each. Bridge request status signalling shall never preempt a bridge request.

7.2.6.2.1 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 K-byte pass-through states shall be triggered by a valid K-byte change, in any direction, from the No Request 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 K-byte pass-through, according to Rule I-P #1b.

Rule I-P #1b – For any ring bridge request, the intermediate nodes on the long path shall go into full pass-through. For any span bridge request status, the intermediate node on the long path shall go into K-byte 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 No Request codes in K1 bits 1-4 and Idle codes in K2 bits 6-8, from both directions. Both directions revert simultaneously from the pass-through state to the idle state.

7.2.6.2.2 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 K-byte change from the No Request (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 K-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 any need for squelching and squelch accordingly, execute a bridge and insert the Bridged code in K2 bits 6-8 in both directions (with MS-RDI and MS-AIS exceptions). Upon receiving a Bridged code in byte K2 bits 6-8 on the bridge request path, the NE shall execute a switch and update K2 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 byte K2 bits 6-8 the Bridged and Switched code on both the long and the short path (with MS-RDI and MS-AIS exceptions).
- for all other bridge requests, except SD-P, EXER, and LP-S, the node shall execute a bridge and insert the Bridged code in byte K2 bits 6-8 in both directions (with MS-RDI and MS-AIS exceptions). Upon receiving a Bridged code in byte K2 bits 6-8 on the bridge request path, the NE shall execute a switch and update K2 bits 6-8 on both paths accordingly.
- for SD-P, EXER, and LP-S, the node shall signal as for any other bridge request, but shall not execute the bridge or switch. See 7.2.1.2.

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 byte K1 bits 1-4 and idle codes in byte K2 bits 6-8 from both directions. The transition from the switching state to the idle state shall be a three-step transition.

- Step 1 – The node (tail-end) originating the bridge request first drops its switch, and signals the No Request code in byte K1 bits 1-4, and the Bridged code in byte K2 bits 6-8.

– Step 2 – Upon reception of the No Request 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.

Note that there are cases in which no bridge or switch is to be dropped (e.g. for SD-P, LP-S, EXER, or switches that could no be executed due to other conditions on the ring). In these cases, the NE that initiated the request (ie. tail-end) shall signal the No Request code. Upon reception of the No Request 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, 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 node receiving 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 – A node receiving the APS bytes which it is sourcing in both directions shall transition to the idle state.

Rule I-S #7 – When a node receives a Reverse Request code over the span which it is protecting, and when that same node is sending a Reverse Request 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.

7.2.6.2.3 Transitions between switching states

This subclause provides the set of rules necessary to coordinate a transition between switching states.

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 bridge request over the long path or an 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 bridge request over the long path or an 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 bridge 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 bridge 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 #2 – SWITCH PREEMPTION:

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

- drop the span bridge and switch immediately,
- execute the ring bridge 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 bridge request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) for its adjacent span of greater priority than the span switch it is executing, it shall drop the span switch, signal No Request in K1 and Bridged in K2 in the direction of the span bridge request, and signal the ring request in K1 and Idle in K2 in the direction of the ring 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, signal No Request in K1 and Bridged in K2 in both directions.

Rule S-S #2d: If a span switching node that is bridged and switched receives a No Request 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 No Request, then the node shall source No Request in K1 and Idle in K2 in both directions.
- A span bridge 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 bridge 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 bridge request destined to another node, then the node shall enter full pass-through (as detailed in Rule S-P #1b).
- A span bridge request status destined to another node, then the node shall enter K-byte pass-through (as detailed in Rule S-P #1d).
- A span bridge request (due to a locally detected failure or externally initiated command) for the same span, the node shall signal the span bridge request in K1 and Idle in K2.

Rule S-S #2e – If a span switching node that is bridged receives 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 No Request, then the node shall source No Request in K1 and Idle in K2 in both directions.
- A span bridge 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 bridge 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 bridge request destined to another node, then the node shall enter full pass-through (as detailed in Rule S-P #1b).
- A span bridge request status destined to another node, then the node shall enter K-byte pass-through (as detailed in Rule S-P #1d).
- A span bridge request (due to a locally detected failure or externally initiated command) for the same span, the node shall signal the span bridge request in K1 and Idle in K2.

Rule S-S #2f – When an NE that is currently executing a ring switch receives a span or ring bridge request due to a locally detected failure, an externally initiated command, or a span or ring bridge request destined to) 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 bridge 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 bridge 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 bridge request.

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

Rule S-S #3a – When a failure condition affecting only one span clears at a node, the node shall enter Wait-to-Restore and remain in Wait-to-Restore for the appropriate timeout 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 – As soon as a node which was requested to bridge, but did not actually detect the failure, receives a Wait-to-Restore code (unidirectional failure case), it shall continue to send out Reverse Request on the short path, and it shall send out WTR on the long path.

Rule S-S #4 – SPAN SWITCH TIME-OUT: For a four-fibre ring, when it is not possible to execute a span bridge request (due to a locally detected failure, an externally initiated command, or a span bridge request destined to it) because no acknowledgment is received on the short path (timeout, whose duration is an equipment issue), or because the protection channels become unavailable, the equivalent ring switch shall be attempted.

Rule S-S #5 – A node receiving long-path ring bridge requests destined to itself from both of its neighbours shall drop its bridge and switch.

Rule S-S #6 – If a span is locked out, the LP-S bridge request shall be signalled over the short path. If the highest priority condition detected requires a ring switch for the same span (the locked-out span), the ring bridge request shall be signalled on the long path. Otherwise, LP-S bridge request status shall be signalled on the long path.

7.2.6.2.4 Transitions between switching and pass-through states

Rule S-P #1 – SWITCH PREEMPTION 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 No Request in K1 and in Idle in K2 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 the node shall enter 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 No Request in K1 and Idle in K2 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 K-byte pass-through.

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 enter 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 enter 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 K-byte pass-through.

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.

Rule S-P #2b – The transition of a node from K-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 ring bridge request is preempted by a span bridge request, (due to a locally detected failure, an externally initiated command, or a span bridge request destined to it), the node preempting the ring switch shall insert AU-AIS on all protection channels other than those on the requested span, unless they are used by another span switch.

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 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.

7.2.6.2.5 Transitions between pass-through states

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

The following transition rules apply.

Rule P-P #1 – Transition from K-byte pass-through to full pass-through: A node in K-byte pass-through that receives a long-path ring bridge request not destined to itself shall enter full pass-through.

Rule P-P #2 – Transition from full pass-through to K-byte pass-through: A node in full pass-through that receives a span bridge request status not destined to itself from both directions shall enter K-byte pass-through.

7.2.7 Examples

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

7.3 MS dedicated protection rings

This is for further study.

7.4 Linear VC trail protection

7.4.1 Network architecture

LO/HO VC trail protection is a path layer protection mechanism and may be used to protect a trail across an entire operator's network or multiple operators' networks. It is a dedicated end-to-end protection scheme which can be used in different network structures; meshed networks, rings, etc. Protection switching may be either single-ended or dual-ended.

Trail protection generically protects against failures in the server layer, and failures and degradations in the client layer.

The protection scheme can be either 1 + 1, where the dedicated protection trail is only used for protection purposes, or 1:1 where the dedicated protection trail can be used to support extra traffic. Dual-ended protection switching and 1:1 protection switching require an APS protocol to coordinate between the local and remote switch and bridge operations.

As VC trail 1:1 dedicated protection is a linear protection mechanism, the working and extra traffic trail termination functions overlap. In a network application, this implies that the working and extra traffic patterns must coincide. As VC trail protection is a dedicated trail protection mechanism, there is no fundamental limitation on the number of NEs within the network connection.

7.4.2 Network objectives

The following network objectives apply:

1) *Switch time* – The APS algorithm for LO/HO VC trail protection shall operate as fast as possible. A value of 50 ms has been proposed as a target time. Concerns have been expressed over this proposed target time when many VCs are involved. This is for further study. Protection switch completion time excludes the detection time necessary to initiate the protection switch, and the hold-off time.

2) *Transmission delay* – The transmission delay depends on the physical length of the trail and the processing functions within the trail. The maximum transmission delay of a dedicated VC protected trail scheme is for further study. Limitations on the transmission delay may be imposed if the target switch completion time for dual-ended operation is to be met.

3) *Hold-off times* – Hold-off times are useful for inter-working of protection schemes. The objective is that these times should be provisionable on an individual VC basis. The defect condition should be continuously monitored for the full duration of the hold-off time before switching occurs. The hold-off time should therefore be provisionable from 0 to 10 seconds in steps of the order of 100 ms.

4) *Extent of protection* – LO/HO VC trail protection shall restore all traffic which has been interrupted due to a failure of a link connection which has been designated as forming part of a VC trail protection scheme. The traffic terminating at a failed node may be disrupted but traffic passing through to other nodes can survive by switching to the protection trail.

5) *Switching types* – Both 1 + 1 and 1:1 trail protection should support single-ended switching, dual-ended switching, or both.

6) *APS protocol and algorithm* – Both the Lower Order and Higher Order VC trail protection APS protocols shall be identical for all network applications. The minimum requirement for the protocol is that it can support 1 + 1 dedicated protection. A 1:1 option to accommodate extra traffic is desirable and is for further study.

7) *Operation modes* – 1 + 1 single-ended switching should support revertive switching, non-revertive switching, or both. 1:1 revertive dual-ended switching with extra traffic is for further study. (It is noted that a principal advantage of a 1:1 architecture is its ability to carry extra traffic.) The routing of working traffic (i.e. uniform or diverse) should not be constrained by the SNC protection scheme. The network operator has a choice of uniform or diverse routing on a per-SNC basis.

8) *Manual control* – Externally initiated commands may be provided for manual control of protection switching by the operations systems or the craftpersons. Externally initiated commands are the same as (or a subset) of those used for linear multiplex section protection.

9) *Switch initiation criteria* – Switch initiation criteria for Signal Fail (SF) and/or Signal Degrade (SD) should be in harmony with definitions used in Recommendation G.783. Switch initiation criteria for VC trail protection should be identical to that for the corresponding SNC/N protection.

7.4.3 Application architecture

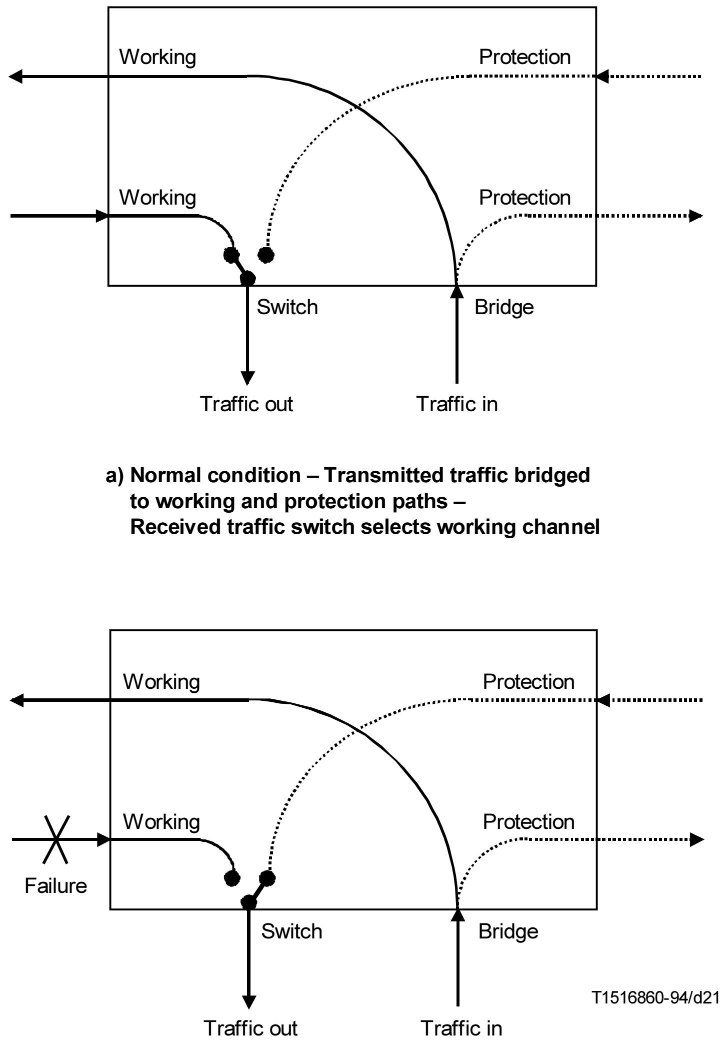
7.4.3.1 Routing

The following routings apply to the working channels under non-failure conditions. As a general principle, for each direction of transmission, the protection channels should follow a separate routing from the working channels.

As noted in the network objectives, the network operator has a choice of uniform or diverse routing on a per-trail basis. For the simplest case whereby working trails and protection trails are placed on separate routes, the difference in provisioning a node for uniform routing versus diverse routing is illustrated for 1 + 1 protection in Figures 7-9 and 7-10. For linear VC trail protection, the nodes illustrated contain the termination of the trails involved.

A node using 1 + 1 uniform routing under normal operating conditions is shown in Figure 7-9 a). A bridge is used to simultaneously transmit signals onto the working and protection trails. The receiver uses a switch to select the working trail under normal operating conditions. Note that the working trails are placed on the same facilities (i.e. the left side of the node). Figure 7-9 b) shows the node when there is a failure in the working trail. In this case, the receiver will detect the loss of signal and will switch to the protection trail.

A node using 1 + 1 diverse routing under normal operating conditions is shown in Figure 7-10 a). A bridge is used to simultaneously transmit signals onto the working and protection trails. The receiver uses a switch to select the working trail under normal operating conditions. Note that the working trails are placed on different facilities (i.e. one on the left side of the node, the other on the right). Figure 7-10 b) shows the node when there is a failure in the working trail. In this case, the receiver will detect the loss of signal and will switch to the protection trail.

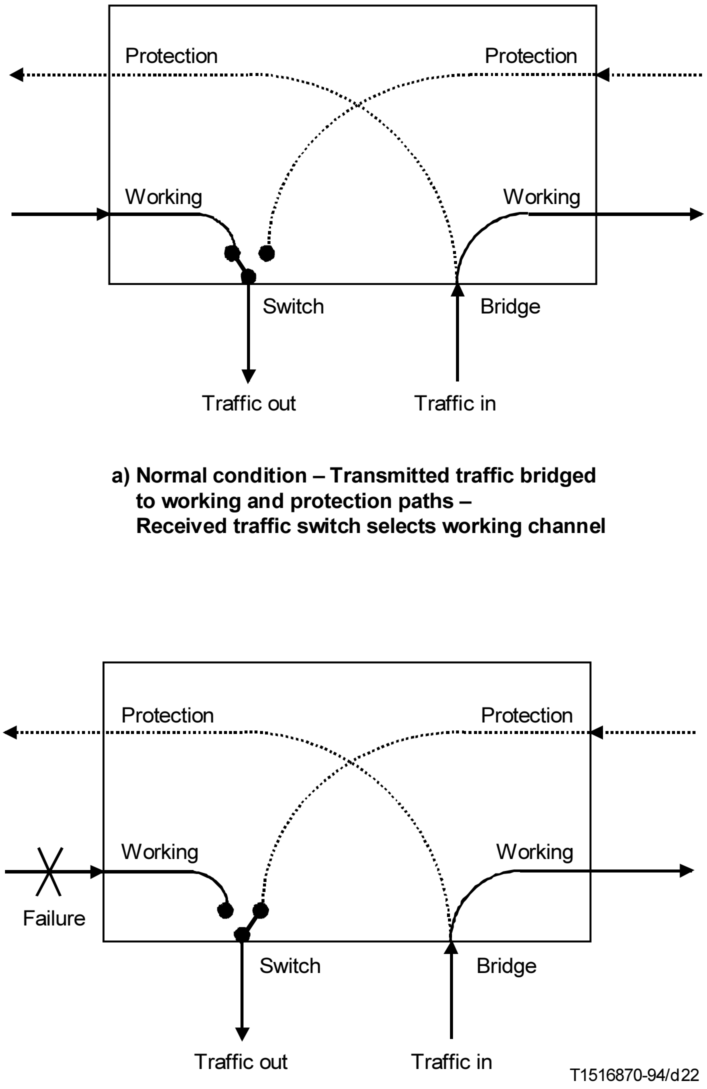


a) Normal condition – Transmitted traffic bridged to working and protection paths – Received traffic switch selects working channel

b) Failure in working channel of incoming traffic – Receiver switch selects protection path

FIGURE 7-9/G.841

Node using uniform routing for 1 + 1 trail or SNC protection



a) Normal condition – Transmitted traffic bridged to working and protection paths – Received traffic switch selects working channel

b) Failure in working channel of incoming traffic – Receiver switch selects protection path

FIGURE 7-10/G.841

Node using diverse routing for 1 + 1 trail or SNC protection

7.4.3.2 1 + 1 single-ended protection

Single-ended protection is illustrated in Figure 7-11 for a uniformly routed 1 + 1 architecture. It is identical to dual-ended protection, except that for unidirectional failures the unaffected direction of transmission is not switched. Consequently, an APS channel is not required to coordinate switching of the unaffected direction of transmission.

Figure 7-11 a) illustrates a 1 + 1 uniformly routed trail protection network with traffic transmitted between Nodes A and C. Traffic inserted at Node A is transmitted on different trails in two directions to Node C. Under normal operating conditions, the receiver at Node C selects the working traffic. Traffic inserted at Node C is also transmitted in two directions to Node A.

When there is a unidirectional failure on the working trail, as shown in either Figure 7-11 b) or Figure 7-11 c), the tail end switch selects the protection trail. If a single point failure cuts both directions of transmission, then both directions of transmission on the working path fail and both directions of transmission switch automatically to the protection trail.

Traffic can be restored when multiple failures affect traffic on only one of the trails (either working or protection). If both trails are affected by certain failures, then traffic cannot be restored. Traffic terminating at a failed node is disrupted, but traffic passing through to other nodes can survive by switching to the protection trail.

1 + 1 VC trail protection may also use diverse routing.

7.4.3.3 1 + 1 dual-ended protection

Figure 7-12 a) illustrates a 1 + 1 diversely routed trail protection network with traffic transmitted between Nodes A and C. Traffic inserted at Node A is transmitted on different trails in two directions to Node C. Under normal operating conditions, the receiver at Node C selects the working traffic. Traffic inserted at Node C is also transmitted in two directions to Node A.

When there is a unidirectional failure on the working trail, as shown in Figure 7-12 b), the tail end switch selects the protection trail. For dual-ended switching, an indication is sent via the APS protocol to force the unaffected direction of transmission to also switch to the protection trail. This maintains uniform routing (i.e. both directions of transmission using the same routes) even under unidirectional failures. If a single point failure cuts both directions of transmission, then both directions of transmission on the working path fail and both directions of transmission switch automatically to the protection trail.

Traffic can be restored when multiple failures affect traffic on only one of the trails (either working or protection). If both trails are affected by certain failures, then traffic cannot be restored. Traffic terminating at a failed node is disrupted, but traffic passing through to other nodes can survive by switching to the protection trail.

1 + 1 VC trail protection may also use diverse routing.

7.4.3.4 1:1 protection

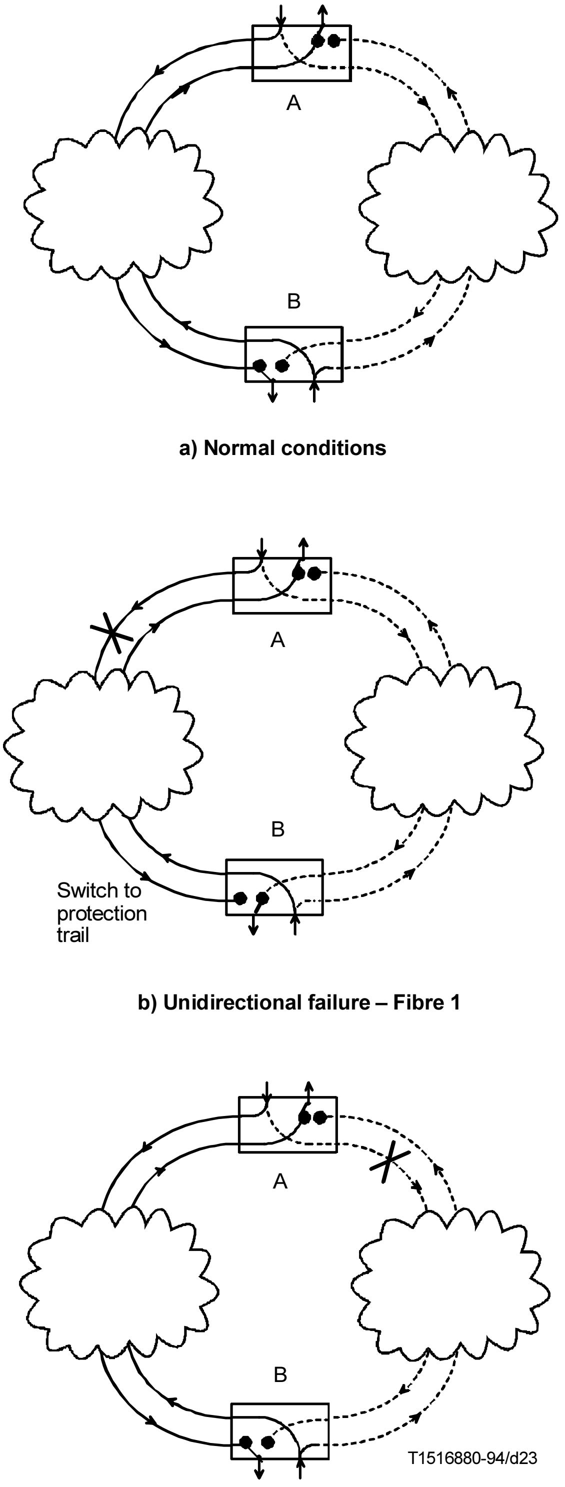
This protection scheme is for further study.

7.4.3.5 Traffic misconnection

This is for further study.

7.4.4 Switch initiation criteria

LO/HO VC trail protection switch requests are automatically initiated based on trail signal fail and trail signal degrade commands (such as AU-AIS and error performance) and APS commands.



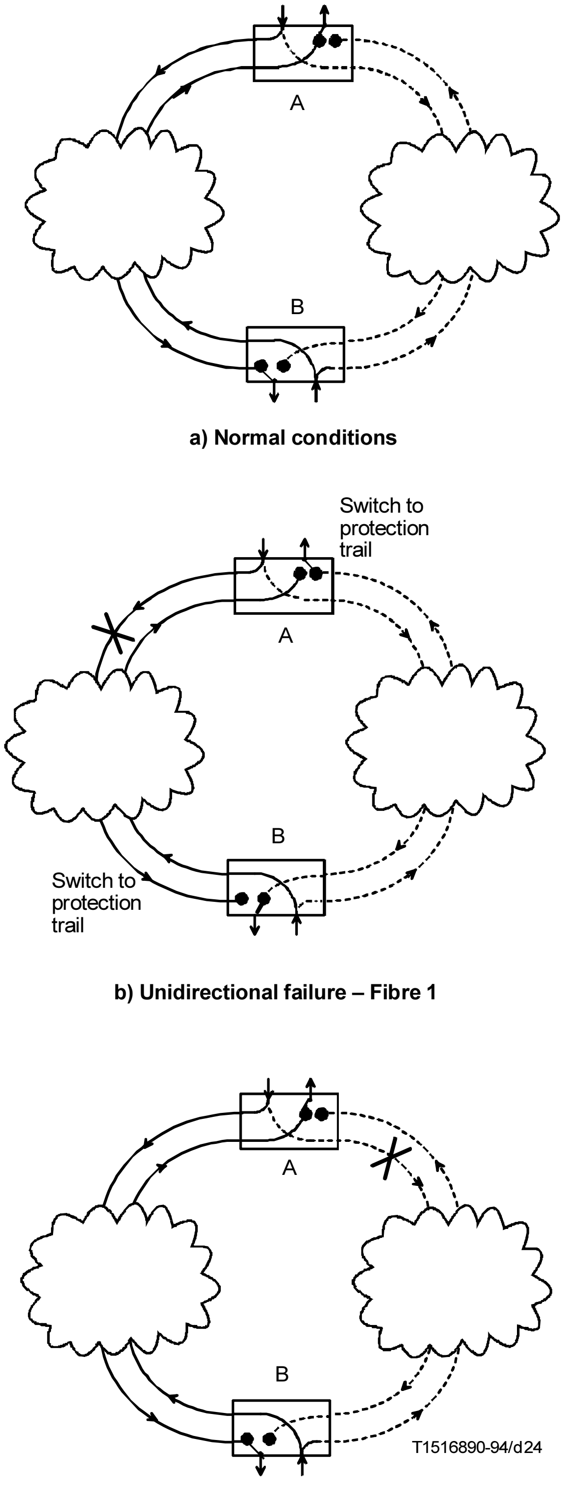
a) Normal conditions

b) Unidirectional failure – Fibre 1

c) Unidirectional failure – Fibre 2

FIGURE 7-11/G.841

Two-fibre uniformly routed 1 + 1 trail protection network with single-ended switching



a) Normal conditions

b) Unidirectional failure – Fibre 1

c) Unidirectional failure – Fibre 2

FIGURE 7-12/G.841

Two-fibre uniformly routed 1 + 1 trail protection network with dual-ended switching

7.4.4.1 1 + 1 single-ended protection

A request can be:

1) an automatically initiated command (SF or SD) associated with a VC trail;

2) a state (Wait-to-Restore, No Request) of the VC trail protection process; or

3) an externally initiated command (Clear, Lockout, Forced Switch, Manual Switch).

For the 1 + 1 architecture, all requests are local. The priority of local requests is given in Table 7-6.

NOTES

1 A forced switch to protection should not be overridden by a Signal Fail on the protection channel. Since single-ended switching is being performed and no APS protocol is supported over the protection channel, Signal Fail on the protection channel does not interfere with the ability to perform a forced switch to protection.

2 The working channel number need not be a part of the switch commands, since a 1 + 1 system has only one working and one protection channel.

TABLE 7-6/G.841

Priority of local requests

Local request (i.e. automatically initiated command, state, or externally initiated command)	Order of priority
Clear	Highest
Lockout of Protection	|
Forced Switch	|
Signal Fail	|
Signal Degrade	|
Manual Switch	|
Wait-to-Restore	|
No Request	Lowest

7.4.4.1.1 Externally initiated commands

Externally initiated commands are listed below in the descending order of priority. These commands are applicable for both revertive and non-revertive operation. However, depending on the operation mode, some commands may result in the same action taken. The functionality of each is described below.

7.4.4.1.1.1 clear: Clears all switch commands listed below.

7.4.4.1.1.2 Lockout of Protection (LP): Prevents the selector from switching to the protection VC trail, by issuing a Lockout of Protection request.

7.4.4.1.1.3 Forced Switch to Protection (FS-P): Switches the selector from the working VC trail to the protection VC trail (unless an equal or higher priority switch request is in effect).

7.4.4.1.1.4 Forced Switch to Working (FS-W): Switches the selector from the protection VC trail to the working VC trail (unless an equal or higher priority switch request is in effect).

NOTE – The FS-W command is unique only in 1 + 1 non-revertive systems, since the LP command would produce the same effect on a revertive system. Since Forced Switch has higher priority than Signal Fail or Signal Degrade commands on the working VC trail, this command will be carried out regardless of the condition of the working VC trail.

7.4.4.1.1.5 Manual Switch to Protection (MS-P): Switches the selector from the working VC trail to the protection VC trail (unless an equal or higher priority switch request is in effect).

7.4.4.1.1.6 Manual Switch to Working (MS-W): Switches the selector from the protection VC trail to the working VC trail (unless an equal or higher priority switch request is in effect).

NOTE – The MS-W command is unique only in 1 + 1 non-revertive systems, since the clear command would produce the same result on a revertive system. Since Manual Switch has lower priority than Signal Fail or Signal Degrade on a working VC trail, this command will be carried out only if the working VC trail is not in the Signal Fail or Signal Degrade condition.

7.4.4.1.2 Automatically initiated commands

The two automatically initiated commands are Signal Fail and Signal Degrade.

7.4.4.1.2.1 Higher order automatically initiated commands

For HO VCs, the Signal Fail automatically initiated command is defined as the presence of one or more of the following defect conditions detected in the higher order path termination function (described in Recommendation G.783):

- Higher order Path Server Signal Fail (HP-SSF) defect – HP-SSF arises from such server layer defects as AU Loss of Pointer (AU-LOP) or AU-AIS;
- Higher order Path Unequipped (HP-UNEQ) defect;
- Higher order Path Trace Identifier Mismatch (HP-TIM) defect (if this condition is enabled by the network provider to be used);
- Higher order Path Excessive error (HP-EXC) defect (if this condition is enabled by the network provider to be used).

  The HP-EXC and HP-TIM contributions to the SF condition are optional, and their definitions are for further study.

For HO VCs, the Signal Degrade automatically initiated command is defined as the presence of the following defect condition detected in the higher order path termination function (described in Recommendation G.783):

- Higher order Path Degraded (HP-DEG) defect.

7.4.4.1.2.2 Lower order automatically initiated commands

For LO VCs, the Signal Fail automatically initiated command is defined as the presence of one or more of the following defect conditions detected in the lower order path termination function (described in Recommendation G.783):

- Lower order Path Server Signal Fail (LP-SSF) defect – LP-SSF arises from such server layer defects as TU loss of pointer (TU-LOP) or TU-AIS;
- Lower order Path Unequipped (LP-UNEQ) defect;
- Lower order Path Trace Identifier Mismatch (LP-TIM) defect (if this condition is enabled by the network provider to be used);

- Lower order Path Excessive error (LP-EXC) defect (if this condition is enabled by the network provider to be used).

  The LP-EXC and LP-TIM contributions to the SF automatically initiated command are optional, and their definitions are for further study.

For LO VCs, the Signal Degrade automatically initiated command is defined as the presence of the following defect condition detected in the lower order path termination function (described in Recommendation G.783):

- Lower order Path Degraded (LP-DEG) defect.

7.4.4.2 1 + 1 dual-ended protection

For further study.

7.4.4.3 1:1 protection

For further study.

7.4.5 Protection switching protocol

7.4.5.1 1 + 1 single-ended protection

In this architecture, there is no APS channel required.

7.4.5.2 1 + 1 dual-ended protection

At the HO VC level, the APS channel can make use of bits 1-4 of byte K3 (formerly byte Z4). At the LO VC level, the APS channel can make use of bits 1-4 of byte K4 (formerly byte Z7). The specific protocol is for further study.

7.4.5.3 1:1 protection

This is for further study.

7.4.6 Protection algorithm operation

7.4.6.1 1 + 1 single-ended protection

7.4.6.1.1 Control of the bridge

In the 1 + 1 architecture, the working channel is permanently bridged to protection.

7.4.6.1.2 Control of the selector

In the 1 + 1 architecture in single-ended operation, the selector is controlled by the highest priority local condition, state, or externally initiated command. Therefore, each end operates independently of the other. If a condition of equal priority (e.g. SF, SD) exists on both channels, switching shall not be performed. (Note that this algorithm makes no distinction between the "severity" of a Signal Degrade, only that a Signal Degrade condition exists.)

For automatically initiated commands, the protection switch completion shall operate as fast as possible. A value of 50 ms has been proposed as a target time. Concerns have been expressed over this proposed target time when many trails are involved. This is for further study. Protection switch completion time excludes the detection time necessary to initiate the protection switch, and hold-off time.

7.4.6.1.2.1 Revertive mode

In the revertive mode of operation, the working channel shall be restored, i.e. the signal on the protection trail shall be switched back to the working trail when this working trail has recovered from the fault.

To prevent frequent operation of the selector due to an intermittent fault, a failed trail must become fault-free. After the failed trail meets this criterion, (and no other externally initiated commands are present) a fixed period of time shall elapse before it is used again as the working channel. This period, called Wait-To-Restore, should be on the order of 5-12 minutes, and should be capable of being set using one second steps. During this state, switching does not occur. An

SF or SD condition shall override the WTR. After the WTR period is completed, a No Request state is entered. Switching then occurs from the protection channel to the working channel.

NOTE – This revertive mode could be used to support certain services where the shortest physical route is maintained under non-failure conditions for a bidirectional connection.

7.4.6.1.2.2 Non-revertive mode

When the failed trail is no longer in an SD or SF condition, and no other externally initiated commands are present, a No Request state is entered. During this state, switching does not occur.

7.4.6.2 1 + 1 dual-ended protection

This is for further study.

7.4.6.3 1:1 protection

This is for further study.

8 SDH subnetwork connection protection

8.1 Network architecture

SNC/I protection, generically, protects against failures in the server layer. The protection process and the defect detection process are performed by two adjacent layers. The server layer performs the defect detection process, and forwards the status to the client layer by means of the Server Signal Fail (SSF) signal.

SNC/N protection, generically, protects against failures in the server layer, and failures and degradations in the client layer.

LO/HO SNC protection is another path layer protection. It is a dedicated protection scheme which can be used in different network structures; meshed networks, rings, etc.

This is dedicated 1 + 1 or 1:1 protection in which the working traffic and the protection traffic at the transmit end of a subnetwork connection are transmitted two separate ways. The 1:1 dedicated protection would be able to support extra traffic.

In the case of 1 + 1 dedicated protection, the transmit end is permanently bridged, where the traffic will be transmitted on both the working and protection subnetwork connections. At the receive end of the SNC, a protection switch is effected by selecting one of the signals based on purely local information. No APS protocol is required for this protection scheme if it is single-ended.

In the case of dual-ended protection switching, 1:1 protection switching or carriage of extra traffic in the protection trail, an APS protocol is required to coordinate between the local and remote switch and bridge operations. This may require a sub-layering technique, and is for further study.

8.2 Network objectives

The following network objectives apply:

1) *Switch time* – The algorithm for LO/HO SNC protection shall operate as fast as possible. A value of 50 ms has been proposed as a target time. Concerns have been expressed over this proposed target time when many subnetwork connections are involved. This is for further study. Protection switch completion time excludes the detection time necessary to initiate the protection switch, and the hold-off time.

2) *Transmission delay* – 1 + 1 single-ended switching does not require transmission of APS signalling, so signalling transmission delays are not present.

3) *Hold-off times* – Hold-off times are useful for inter-working of protection schemes. The objective is that these times should be provisionable on an individual VC basis. The defect condition should be continuously monitored for the full duration of the hold-off time before switching occurs. The hold-off time should therefore be provisionable from 0 to 10 seconds in steps of the order of 100 ms.

4) *Extent of protection* – LO/HO SNC protection shall restore all traffic (except extra traffic) which has been interrupted due to a failure of a link connection which has been designated as forming part of a SNC protection scheme.

5) *Switching types* – 1 + 1 SNC protection should support single-ended switching. Other architectures are for further study.

6) *APS protocol and algorithm* – The SNC protection process should operate in a similar manner at both the HO and LO layers.

7) *Operation modes* – 1 + 1 single-ended switching should support revertive switching, non-revertive switching, or both. 1:1 revertive dual-ended switching with extra traffic is for further study. (It is noted that a principal advantage of a 1:1 architecture is its ability to carry extra traffic.) The routing of working traffic (i.e. uniform or diverse) should not be constrained by the SNC protection scheme. The network operator has a choice of uniform or diverse routing on a per-SNC basis.

8) *Manual control* – Externally initiated commands may be provided for manual control of protection switching by the operations systems or the craftpersons. Externally initiated commands are the same as (or a subset of) those used for linear multiplex section protection.

9) *Switch initiation criteria* – Switch initiation criteria for Signal Fail (SF) and/or Signal Degrade (SD) based on either BER or block error performance should be in harmony with definitions used in Recommendation G.783. Switch initiation criteria for SNC/N protection should be identical to that for the corresponding VC trail protection.

8.3 Application architecture

8.3.1 Routing

The following routings apply to the working channels under non-failure conditions. As a general principle, for each direction of transmission, the protection channels should follow a separate routing from the working channels.

As noted in the network objectives, the network operator has a choice of uniform or diverse routing on a per-SNC basis. For the simplest case whereby working subnetwork connections and protection subnetwork connections are placed on separate routes, the difference in provisioning a node for uniform routing versus diverse routing for 1 + 1 protection is illustrated in Figures 7-9 and 7-10. For SNC protection (in contrast to linear VC trail protection), the nodes illustrated may not necessarily terminate the trails involved.

A node using 1 + 1 uniform routing under normal operating conditions is shown in Figure 7-9 a). A bridge is used to simultaneously transmit signals onto the working and protection SNCs. The receiver uses a switch to select the working SNC under normal operating conditions. Note that the working SNCs are placed on the same facilities (i.e. the left side of the node). Figure 7-9 b) shows the node when there is a failure in the working SNC. In this case, the receiver will detect the loss of signal and will switch to the protection SNC.

A node using diverse 1 + 1 routing under normal operating conditions is shown in Figure 7-10 a). A bridge is used to simultaneously transmit signals onto the working and protection routes. The receiver uses a switch to select the working SNC under normal operating conditions. Note that the working SNCs are placed on different facilities (i.e. one on the left side of the node, the other on the right). Figure 7-10 b) shows the node when there is a failure in the working SNC. In this case, the receiver will detect the loss of signal and will switch to the protection SNC.

8.3.2 1 + 1 single-ended protection

Figure 8-1 a) illustrates diversely routed SNC protection with traffic transmitted between nodes A and C. Traffic inserted at Node A is transmitted on different SNCs in separate directions to Node C (e.g. a working SNC and a protection SNC). Under normal operating conditions, the receiver at Node C selects the working SNC traffic. When there is a failure on the working SNC, as shown in Figure 8-1 b), the tail end switch selects the protection SNC. If there is a failure in the protection SNC, as shown in Figure 8-1 c), then the receiver will not need to switch and will continue to detect traffic from the working SNC.

Diversely routed SNCs are capable of surviving certain multiple failures, including cable cuts, if they result in the same SNC being disrupted, as shown in Figure 8-2 a). Connectivity will be broken if failures occur which affect both SNCs, as shown in Figure 8-2 b). Figure 8-2 c) gives an example of protection switching due to a nodal failure. Traffic terminating at the failed node is disrupted, but traffic passing through to other nodes can survive by switching to the protection SNC.

8.3.3 Other architectures

1:1 revertive dual-ended switching with extra traffic is for further study.

8.4 Switch initiation criteria

8.4.1 1 + 1 single-ended protection

A request can be:

1) an automatically initiated command (SF or SD) associated with a VC subnetwork connection;

2) a state (Wait-to-Restore, No Request) of the SNC protection process; or

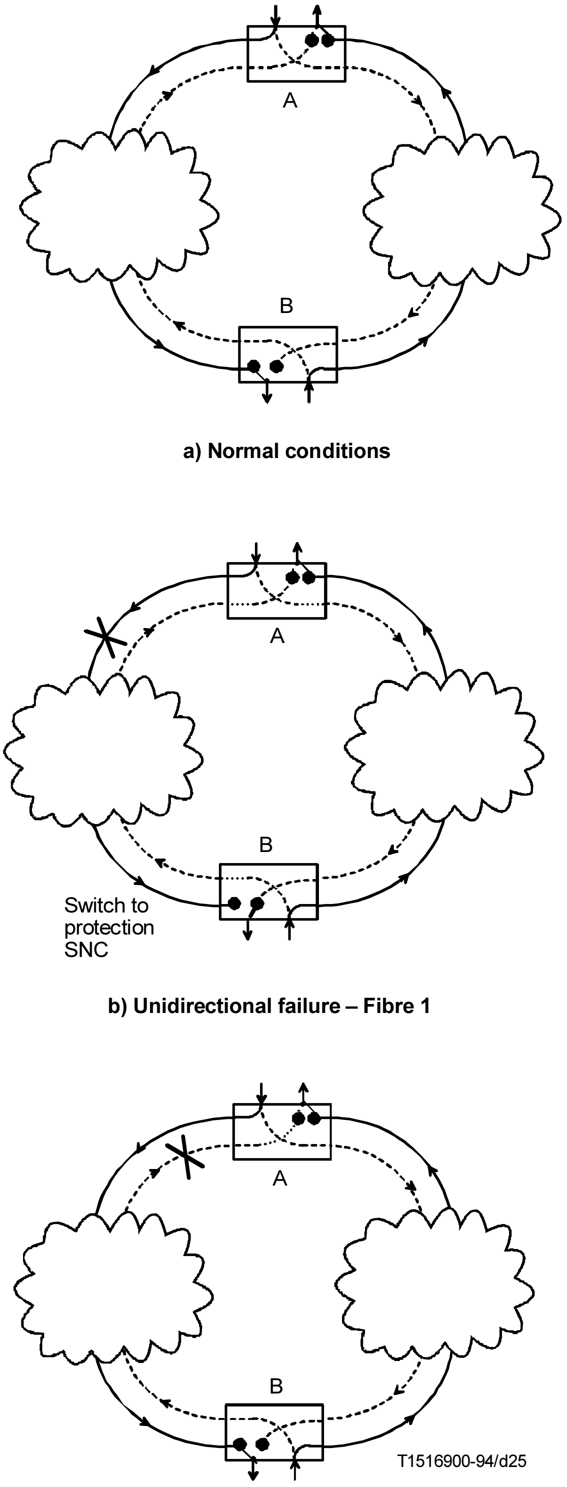
3) an externally initiated command (Clear, Lockout, Forced Switch, Manual Switch).

For the 1 + 1 architecture, all requests are local. The priority of local requests is given in Table 8-1.

NOTES

1 A forced switch to protection should not be overridden by a Signal Fail on the protection channel. Since single-ended switching is being performed and no APS protocol is supported over the protection channel, Signal Fail on the protection channel does not interfere with the ability to perform a forced switch to protection.

2 The working channel number need not be a part of the switch commands, since a 1 + 1 system has only one working and one protection channel.



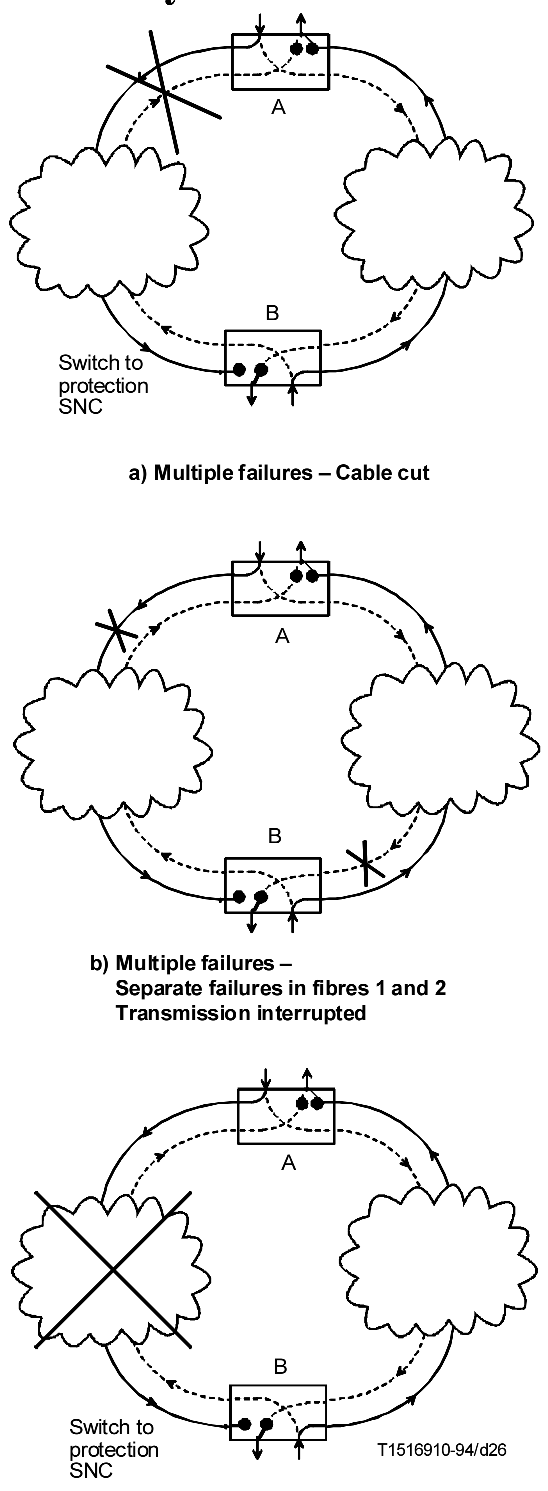
a) Normal conditions

b) Unidirectional failure – Fibre 1

c) Unidirectional failure – Fibre 2

FIGURE 8-1/G.841

Two-fibre diversely routed 1 + 1 SNC protection network with single failure



a) Multiple failures – Cable cut

b) Multiple failures –
Separate failures in fibres 1 and 2
Transmission interrupted

c) Node failure within SNC

FIGURE 8-2/G.841

Two-fibre diversely routed 1 + 1 SNC protection network with multiple failures

TABLE 8-1/G.841

Priority of local requests

Local request (i.e. automatically initiated command, state, or externally initiated command)	Order of priority
Clear	Highest
Lockout of Protection	|
Forced Switch	|
Signal Fail	|
Signal Degrade	|
Manual Switch	|
Wait-to-Restore	|
No Request	Lowest

8.4.1.1 Externally initiated commands

Externally initiated commands are listed below in the descending order of priority. These commands are applicable for both revertive and non-revertive operation. However, depending on the operation mode, some commands may result in the same action taken. The functionality of each is described below.

8.4.1.1.1 **clear**: Clears all switch commands listed below.

8.4.1.1.2 **Lockout of Protection (LP):** Prevents the selector from switching to the protection VC subnetwork connection, by issuing a Lockout of Protection request.

8.4.1.1.3 **Forced Switch to Protection (FS-P):** Switches the selector from the working VC subnetwork connection to the protection VC subnetwork connection (unless an equal or higher priority switch request is in effect).

8.4.1.1.4 **Forced Switch to Working (FS-W):** Switches the selector from the protection VC subnetwork connection to the working VC subnetwork connection (unless an equal or higher priority switch request is in effect).

NOTE – The FS-W command is unique only in 1 + 1 non-revertive systems, since the LP command would produce the same effect on a revertive system. Since Forced Switch has higher priority than Signal Fail or Signal Degrade commands on the working VC subnetwork connection, this command will be carried out regardless of the condition of the working VC subnetwork connection.

8.4.1.1.5 **Manual Switch to Protection (MS-P):** Switches the selector from the working VC subnetwork connection to the protection VC subnetwork connection (unless an equal or higher priority switch request is in effect).

8.4.1.1.6 **Manual Switch to Working (MS-W):** Switches the selector from the protection VC subnetwork connection to the working VC subnetwork connection (unless an equal or higher priority switch request is in effect).

NOTE – The MS-W command is unique only in 1 + 1 non-revertive systems, since the clear command would produce the same effect on a revertive system. Since Manual Switch has lower priority than Signal Fail or Signal Degrade on a working VC subnetwork connection, this command will be carried out only if the working VC subnetwork connection is not in the Signal Fail or Signal Degrade automatically initiated command.

8.4.1.2 Automatically initiated commands

The two automatically initiated commands are Signal Fail and Signal Degrade.

8.4.1.2.1 Higher order automatically initiated commands

For HO VCs, the Signal Fail automatically initiated command is defined as the presence of one or more of the following defect conditions detected in the higher order path overhead monitoring function (described in Recommendation G.783):

For SNC/N and SNC/I:

- Higher order Path Server Signal Fail (HP-SSF) defect. HP-SSF arises from such server layer defects as AU loss of pointer (AU-LOP) or AU-AIS;

For SNC/N only:

- Higher order Path Unequipped (HP-UNEQ) defect;
- Higher order Path trace Identifier Mismatch (HP-TIM) defect (if this condition is enabled by the network provider to be used);
- Higher order Path Excessive error (HP-EXC) defect (if this condition is enabled by the network provider to be used).

  The HP-EXC and HP-TIM contributions to the SF condition are optional, and their definitions are for further study.

For HO VCs, using SNC/N, the Signal Degrade automatically initiated command is defined as the presence of the following defect condition detected in the higher order path overhead monitoring function (described in Recommendation G.783):

- Higher order Path Degraded (HP-DEG) defect.

8.4.1.2.2 Lower order automatically initiated commands

For LO VCs, the Signal Fail automatically initiated command is defined as the presence of one or more of the following defect conditions detected in the lower order path overhead monitoring function (described in Recommendation G.783):

For SNC/N and SNC/I:

- Lower order Path Server Signal Fail (LP-SSF) defect. LP-SSF arises from such server layer defects as TU Loss of Pointer (TU-LOP) or TU-AIS.

For SNC/N only:

- Lower order Path Unequipped (LP-UNEQ) defect;
- Lower order Path Trace Identifier Mismatch (LP-TIM) defect (if this condition is enabled by the network provider to be used);
- Lower order Path Excessive error (LP-EXC) defect (if this condition is enabled by the network provider to be used).

  The LP-EXC and LP-TIM contributions to the SF automatically initiated command are optional, and their definitions are for further study.

For LO VCs using SNC/N, the Signal Degrade automatically initiated command is defined as the presence of the following defect condition detected in the lower order path overhead monitoring function (described in Recommendation G.783):

- Lower order Path Degraded (LP-DEG) defect.

8.4.2 Other architectures

For further study.

8.5 Protection switching protocol

8.5.1 1 + 1 single-ended protection

In this architecture, there is no APS channel required.

8.5.2 Other architectures

For further study.

8.6 Protection algorithm operation

8.6.1 1 + 1 single-ended protection algorithm

8.6.1.1 Control of the bridge

In the 1 + 1 architecture, the working channel is permanently bridged to protection.

8.6.1.2 Control of the selector

In the 1 + 1 architecture in single-ended operation, the selector is controlled by the highest priority local condition, state, or externally initiated command. Therefore, each end operates independently of the other. If a condition of equal priority (e.g. SF, SD) exists on both channels, switching shall not be performed. (Note that this algorithm makes no distinction between the "severity" of a Signal Degrade, only that a Signal Degrade condition exists.)

For automatically initiated commands, the protection switch completion shall operate as fast as possible. A value of 50 ms has been proposed as a target time. Concerns have been expressed over this proposed target time when many subnetwork connections are involved. This is for further study. Protection switch completion time excludes the detection time necessary to initiate the protection switch, and hold-off time.

8.6.1.2.1 Revertive mode

In the revertive mode of operation, the working channel shall be restored, i.e. the signal on the protection subnetwork connection shall be switched back to the working subnetwork connection when this working subnetwork connection has recovered from the fault.

To prevent frequent operation of the selector due to an intermittent fault, a failed subnetwork connection must become fault-free. After the failed subnetwork connection meets this criterion, (and no other externally initiated commands are present) a fixed period of time shall elapse before it is used again as the working channel. This period, called Wait-to-Restore, should be on the order of 5-12 minutes, and should be capable of being set using one second steps. During this state, switching does not occur. An SF or SD automatically initiated command shall override the WTR. After the WTR period is completed, a No Request state is entered. Switching then occurs from the protection channel to the working channel.

NOTE – This revertive mode could be used to support certain services where the shortest physical route is maintained under non-failure conditions for a bidirectional connection.

8.6.1.2.2 Non-revertive mode

When the failed SNC is no longer in an SD or SF condition, and no other externally initiated commands are present, a No Request state is entered. During this state, switching does not occur.

8.6.2 Other architectures

For further study.

Annex A

MS shared protection rings (transoceanic application)

(This annex forms an integral part of this Recommendation)

A.1 Application

Because of the unique character of transoceanic systems, i.e. very long transmission paths, the approach described for general purpose MS shared protection rings is insufficient. For some types of failures, a total adaptation of the general purpose MS shared protection ring would lead to restoration transmission paths that would cross the ocean three times. The inherent delays in such an approach will only result in degraded performance.

Therefore, additional text for implementing the "transoceanic application" option demonstrates 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 will only manifest themselves in long haul networks, where the distances between the nodes on the ring exceed 1500 km.

When a ring switch occurs on the transoceanic ring network, all AU-4 tributaries affected by the failure are bridged at their source nodes onto the protection channels that travel away from the failure. When the affected tributaries reach their final destination nodes, they are switched to their original drop points. This is illustrated in Figure A.1. This is accomplished by using the local node ring maps and the K-byte protocol. The differences in Figures 6-2 and A.1 illustrate the differences in the length of the protection channel.

For the non-transoceanic ring network, the extra traffic remains off the ring network until the failure is cleared. Since only the affected AU-4 tributaries are switched for the transoceanic ring network, the preempted extra traffic can be re-established on the protection channels not used to restore the normal working traffic. The signalling channel used to re-establish the extra traffic is the DCC.

A.2 Network objectives

For transoceanic applications of MS shared protection rings, some additional network objectives apply:

1) *Switch time* – The switch completion time shall be less than 300 milliseconds, independent of whether the ring is carrying extra traffic. This supersedes objective 1) of 7.2.2.

2) *Extent of protection* – Objective 4 b) of 7.2.2 is superseded by the following: b) The ring shall restore all traffic possible, even under conditions of multiple bridge requests of the same priority.

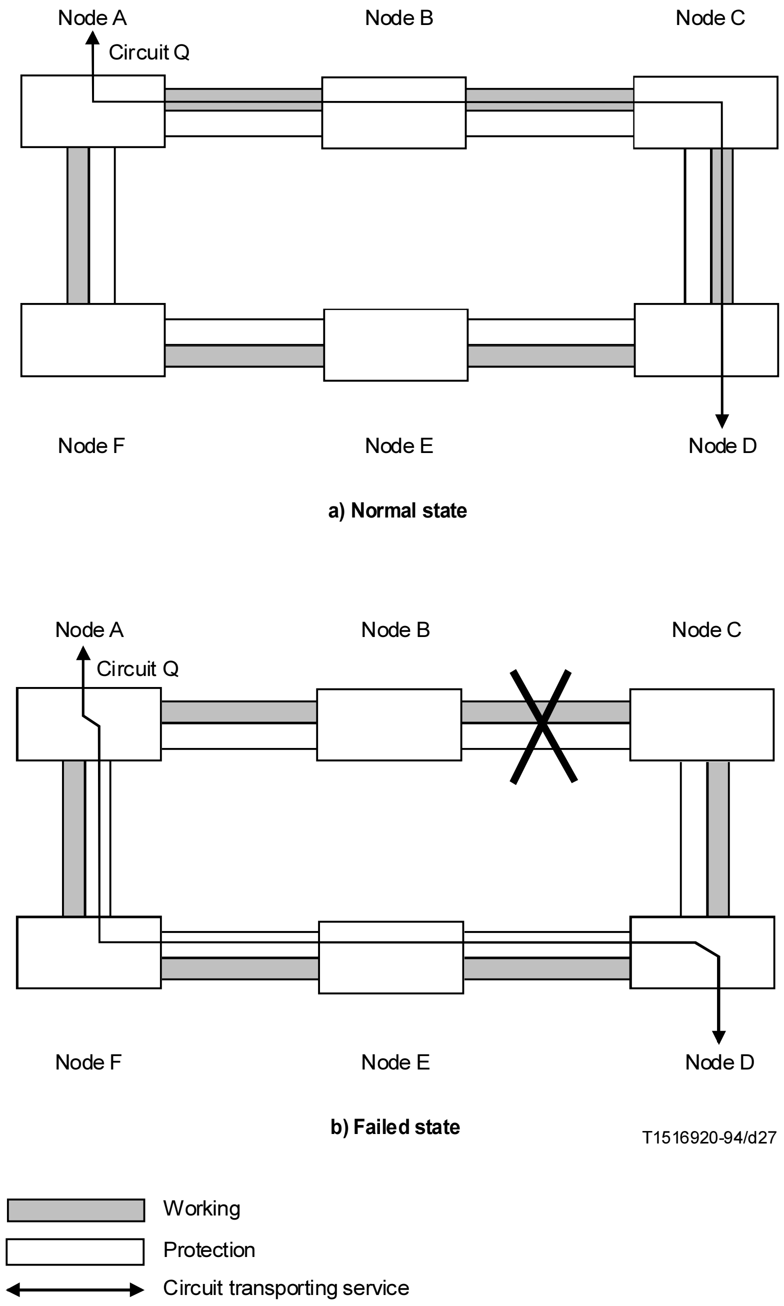
3) *APS protocol and algorithm*

   a) AUG squelching is not required. This supersedes objective 6 j) of 7.2.2.

   b) During a failure, preempted extra traffic can be re-established on the protection channels not used to restore the normal working traffic.

   c) For transoceanic applications, ring maps are used to switch traffic affected by a failure at intermediate nodes. A mechanism should be accommodated that auto-provisions the data required for these maps, and maintains its consistency. The mechanism proposed for use is the DCC.

   d) Objective 6 i) of 7.2.2 is superseded by the following: i) If a ring switch exists and a failure of equal priority occurs on another span requiring a ring switch, then, if the priority of the bridge request is Signal Fail (Ring) or higher, both ring switches shall be established resulting in the ring segmenting into two separate segments.



a) Normal state

b) Failed state

FIGURE A.1/G.841

Example of circuit routing in failure state for a ring switch (transoceanic application)

A.3 Application architecture

An MS shared protection ring in a transoceanic application uses SDH multiplex section layer indications to trigger the protection switching. Switching action is performed only on AU-4 tributaries affected by the failure. Multiplex section indicators include MS failure conditions, and signalling messages that are sent between nodes to affect a coordinated MS protection switch.

In the event of a failure, ring switches are established at any node whose traffic is affected by the failure. Unlike the general purpose approaches described earlier, no loopbacks are established. Loopbacks and switching only at the nodes adjacent to a failure are the cause of triple ocean crossing encountered by the traffic restoration path mentioned above. Therefore, in the transoceanic approach, all nodes are allowed to switch and use the existing protocol in conjunction with ring maps. As in the general purpose cases described in 7.2.1.1 and 7.2.1.2, the affected traffic is rerouted away from the failure over the protection channels.

The problem of misconnection is eliminated for the transoceanic ring application because there are no loopbacks at the switching nodes. It is the looping at switching nodes that sets up the potential for misconnections. As a consequence, the "squelching" described for general purpose MS shared protection rings is not necessary. Additionally, single and multiple failures resulting in ring switching are executed in the same manner, by simply bridging and switching and taking advantage of the ring map information just described.

A.4 Switching criteria

The criteria found in 7.2.4 applies, with the following additional interpretations:

A.4.1 forced switche working to protection-ring (FS-R): This command performs the ring switch from working channels to the protection channels 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 channels, unless the protection channels are satisfying a higher priority bridge request, or a signal failure (or a K-byte failure) exists on the long-path protection channels. For transoceanic applications, the FS-R is meant to prompt the same switching response as that for a cable cut on the span between the node at which the command is initiated and the adjacent node to which the command is destined. As in the behaviour for cable cuts, however, no loopbacks are established. Working traffic between any two nodes that had been using the affected span is now re-routed away from this span via the protection channels.

A.4.2 manual switch-ring (MS-R): For transoceanic applications, the note under the FS-R description also applies here.

A.4.3 exercise-ring (EXER-R): For transoceanic applications, no extra traffic is affected either.

A.4.4 exercise-span (EXER-S): For transoceanic applications, no extra traffic is affected either.

As described in 7.4.2, the SF bridge request is used to protect working traffic affected by a hard failure, while the SD bridge request is used to protect against a soft failure. 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. For transoceanic applications, this activity occurs at both the switching nodes and the intermediate nodes.

As described also in 7.4.2, the WTR bridge request is used to prevent frequent oscillation between the protection channels and the working channels. The intent is to minimize oscillations, since hits are incurred during switching. The WTR bridge request is issued after the working channels' BER meets the restoral threshold. The WTR is issued only after an SF or an SD condition and, thus, does not apply for externally initiated bridge requests. For ring switches in a transoceanic application, a WTR bridge request received bidirectionally by an intermediate node with bridged and switched traffic results in the following. The intermediate node initiates a local WTR whose time interval is one half that of the switching node WTR interval. For transoceanic applications, the WTR interval is set to the same value at all nodes.

A.5 Protection switch protocol

The protocol is the same as described in 7.2.5.

A.6 Protection algorithm operation

For transoceanic applications, the pass-through state at intermediate nodes may also involve switching activity when ring switches are required, as described below.

In transoceanic applications, intermediate nodes may engage in some switching activity. As described in 6.2, all nodes are allowed to switch if their added/dropped traffic is affected by a failure. This includes intermediate nodes. When a ring switch is required, any intermediate node shall execute bridges and switches if its added/dropped traffic is affected by the failure. The determination of affected traffic is made by examining the K1 bridge requests (which indicate the nodes adjacent to the failure or failures) and the stored ring maps (which indicate the relative position of the failure and the added/dropped traffic destined toward that failure). Only those AU-4 tributaries affected by the failure are bridged and switched, using the same rules as described in this Recommendation. Specific details of the bridging and switching at intermediate nodes are given in the figures of the examples shown in Appendix I.

The following rules modify or extend those found in 7.2.6 in order to satisfy the needs of the transoceanic application:

Rule Basic #3 – K2 BITS 6-8 UPDATE: Given that “All bridge and switch actions shall be reflected by updating byte K2 bits 6-8, unless an MS-RDI condition exists”, for transoceanic applications, this only occurs at switching nodes. The rest of this rule applies as stated in 7.2.6.2.

Rule Basic #4 – For transoceanic applications, the following supersedes Rule Basic #4: Bridge requests (due to a locally detected failute, an externally initiated command, or received K-bytes) shall preempt bridge requests in the prioritized order given in Table 7-1. Bridge requests shall preempt bridge request status signalling regardless of the priority of each. Bridge request status signalling shall never preempt a bridge request.

Rule I-S #1b – Since transoceanic applications do not require squelching, the squelching activities described in this rule are not taken.

Rule S-S #1a – Since transoceanic applications do not require squelching, the squelching activities described in this rule are not taken. For transoceanic applications only, the following supersedes Rule S-S #1a:

1) Coexistence of FS-R with SF-R does not apply to transoceanic applications.

2) When a ring switching node receives the new ring bridge request with an “Idle” status code, it shall either:

   a) maintain the Bridge and Switch (and drop the extra traffic, which is re-established if applicable), and change the status code to “Idle” for both sides if the node had been sendin ‘Bridged and Switched’; or

   b) change the status code to “Bridged and Switched” for both sides, if the node had been sending “Idle”.

3) When the node which executes 2) receives the ring bridge request with a “Bridged and Switched” status, it changes the status code to “Bridged and Switched” for the both sides if the node had been sending «idle».

Rule S-S #1b – Since transoceanic applications do not require squelching, the squelching activities described in this rule are not taken. For transoceanic applications only, the following supersedes Rule S-S #1b:

1) Coexistence of FS-R with SF-R does not apply to transoceanic applications.

2) When a ring switching node receives the new ring bridge request with an "Idle" status code, it shall either:

   a) maintain the Bridge and Switch (and drop the extra traffic, which is re-established if applicable), and change the status code to "Idle" for the both sides, if the node had been sending "Bridged and Switched; or

   b) change the status code to "Bridged and Switched" for both sides, if the node had been sending "Idle".

3) When the node which executes 2) receives the ring bridge request with a "Bridged" status, code. it shall either:

   a) change the status code to "Bridged" for the long path side, if the node had been sending "Idle"; or

   b) change the status code to "Bridged and switched" for both sides, if the node had been sending "Bridged".

4) When the node which executes 3) receives the ring bridge request with a "Bridged and Switched" status code, it changes the status code to "Bridged and Switched" for the both sides, if the node had been sending "Bridged".

Rule S #4a – For the FS-R with FS-R coexisting switches, and the SF-R and SF-R coexisting switches, the ring does not split into multiple subrings. For the transoceanic application of MS shared protection rings, the ring switching used for transoceanic systems does not require looping traffic at switching nodes. Consequently, the ring is segmented, but not into smaller rings. The segmentation is into separate linear add/drop chains separated by cable failures and/or the number of forced switches (ring) existing on the ring. Coexistence of FS-R with SF-R does not apply to transoceanic applications.

Rule S-P #2c – This rule is not required for transoceanic applications.

Rule S #1d – For transoceanic applications, the following supersedes Rule S #1d: Whenever a node detects an incoming failure on the working and on the protection channels, it shall always source over the short path a short path-ring bridge request, even in the case of multiple failures, as long as the ring bridge request is not preeempted by a higher priority bridge request which is located on the same span. [See Figure 7-8 b).] This rule takes precedence over Rule S #1c. Note that whenever a node receives in one direction a ring bridge request on the short path, (indicating that the signal it is sending has failed) and detects on the other side an incoming failure on the working and on the protection channels, it shall the detected failure over both the short and the long paths (see Figure 7-8 c)].

Rule S-S #2d – For transoceanic applications, the following supersedes Rule S-S #2d: If a bridge request (due to a locally) detected failure, an externally initiated command, or received K-bytes) over a different span preempts an SF-R bridge request, the switching node sourcing the SF-R bridge request shall continue signalling its bridge request, shall drop its bridge and switch, and shall insert AU-AIS over failed tributaries.

Rule S-P #1e – For transoceanic applications, the following supersedes Rule S-P #1e: When a node that is currently executing a ring switch receives a ring bridge request for a non-adjacent span of greater priority than the ring switch it is executing , it shall either:

1) maintain ring bridges and switches on the tributaries affected by the first failure, if the lon-path ring bridge request is still signalling that failure; or

2) drop ring bridges and switches on the tributaries affected by the first failure, if the long-path ring request is not still signalling that failure. It then enters full pass-through.

Rule S-P #1f – For transoceanic applications, the following supersedes Rule S-P #1f: When a node that is currently executing a ring-switch has as its highest priority input long path ring bridge request not destined to itself from both direction, it shall either:

1) maintain ring bridges and switches on the tributaries affected by the first failure, if the long-path ring bridge requests are still signalling that failure; or

2) drop ring bridges and switches on the tributaries affected by the first failure, if the lon-path ring bridge requests are not still signalling that failure. It then enters full pass-through.

Rule S-P #1g – For transoceanic applications, this rule does not apply.

Rule S-P #2a – For transoceanic applications, the following supersedes Rule S-P #2a: The transition of a node from full pass-through to switching shall be triggered by:

1) an equal or higher priority externally initiated commad;

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

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

4) the detection of an SF-R condition (even if lower priority); or

5) the receipt of an SF-R bridge request destined to that NE.

Rule S-P #3 – For transoceanic applications, the following supersedes Rule S-P #3: If a node that was in the pass-through state due to a SF-R or FS-R bridge request is now sourcing a SF-R or FS-R request (due to Rule S-P #2a), the node shall drop extra traffic and maintain the first failure's ring bridge and switch.

Appendix I

Examples of protection switching in an MS shared protection ring

(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.

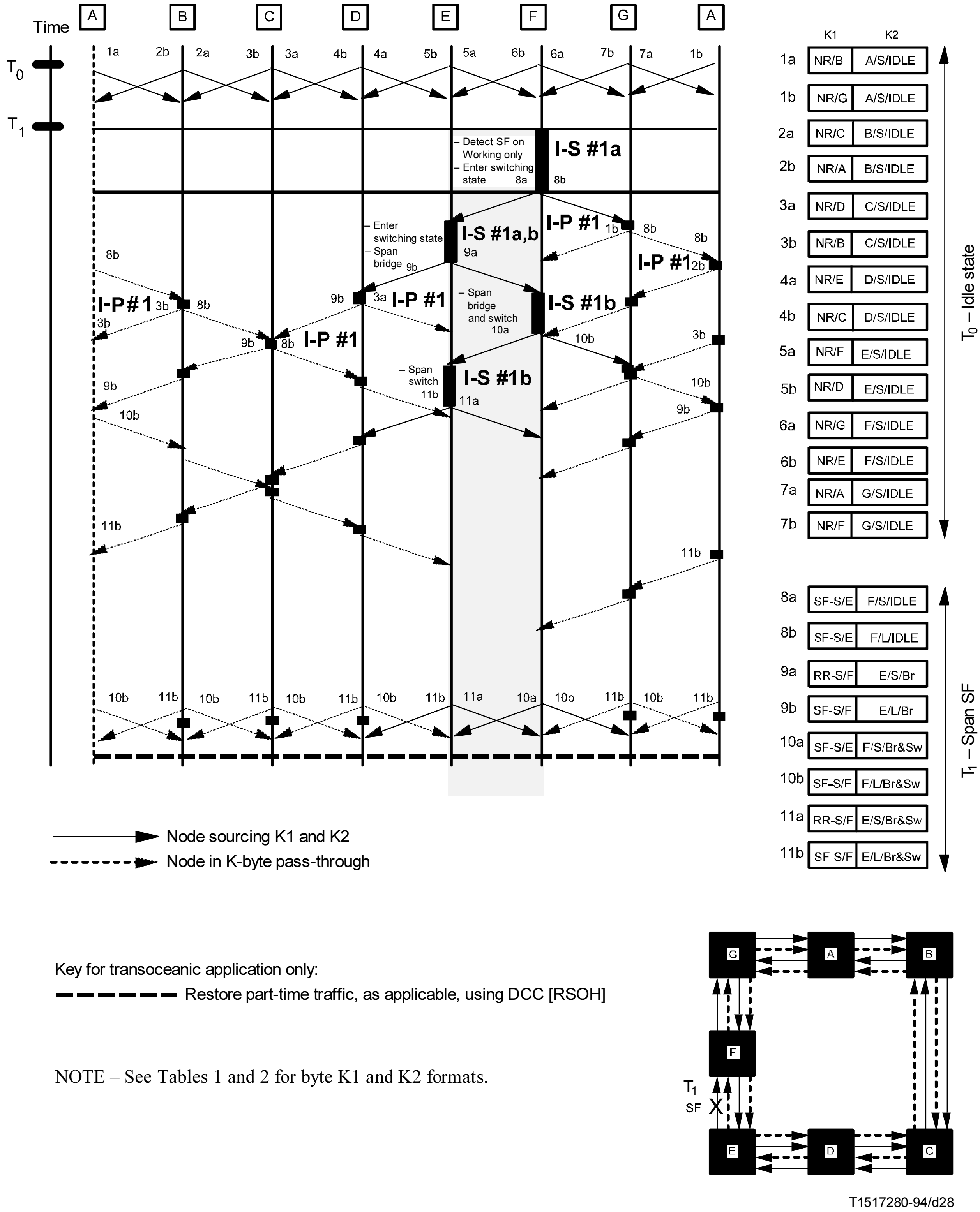
I.1 Unidirectional signal fail (span) in a four-fibre ring

See Figure I.1.

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 K-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 Reverse Request 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 K-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 transoceanic applications, the switching activities that would take place at the intermediate nodes. On all AU-4 protection channels not being used to protect working channels, extra traffic is restored using the DCC.

At time T_2, the span SF condition clears, and Node F enters the Wait-to-Restore 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 Reverse Request 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 No Request codes (Rule I-S #2). Node E, upon reception of the No Request 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.



	K1	K2
1a	NR/B	A/S/IDLE
1b	NR/G	A/S/IDLE
2a	NR/C	B/S/IDLE
2b	NR/A	B/S/IDLE
3a	NR/D	C/S/IDLE
3b	NR/B	C/S/IDLE
4a	NR/E	D/S/IDLE
4b	NR/C	D/S/IDLE
5a	NR/F	E/S/IDLE
5b	NR/D	E/S/IDLE
6a	NR/G	F/S/IDLE
6b	NR/E	F/S/IDLE
7a	NR/A	G/S/IDLE
7b	NR/F	G/S/IDLE
8a	SF-S/E	F/S/IDLE
8b	SF-S/E	F/L/IDLE
9a	RR-S/F	E/S/Br
9b	SF-S/F	E/L/Br
10a	SF-S/E	F/S/Br&Sw
10b	SF-S/E	F/L/Br&Sw
11a	RR-S/F	E/S/Br&Sw
11b	SF-S/F	E/L/Br&Sw

NOTE – See Tables 1 and 2 for byte K1 and K2 formats.

FIGURE I.1/G.841

Four-fibre MS shared protection ring-unidirectional failure (span) on working from E to F

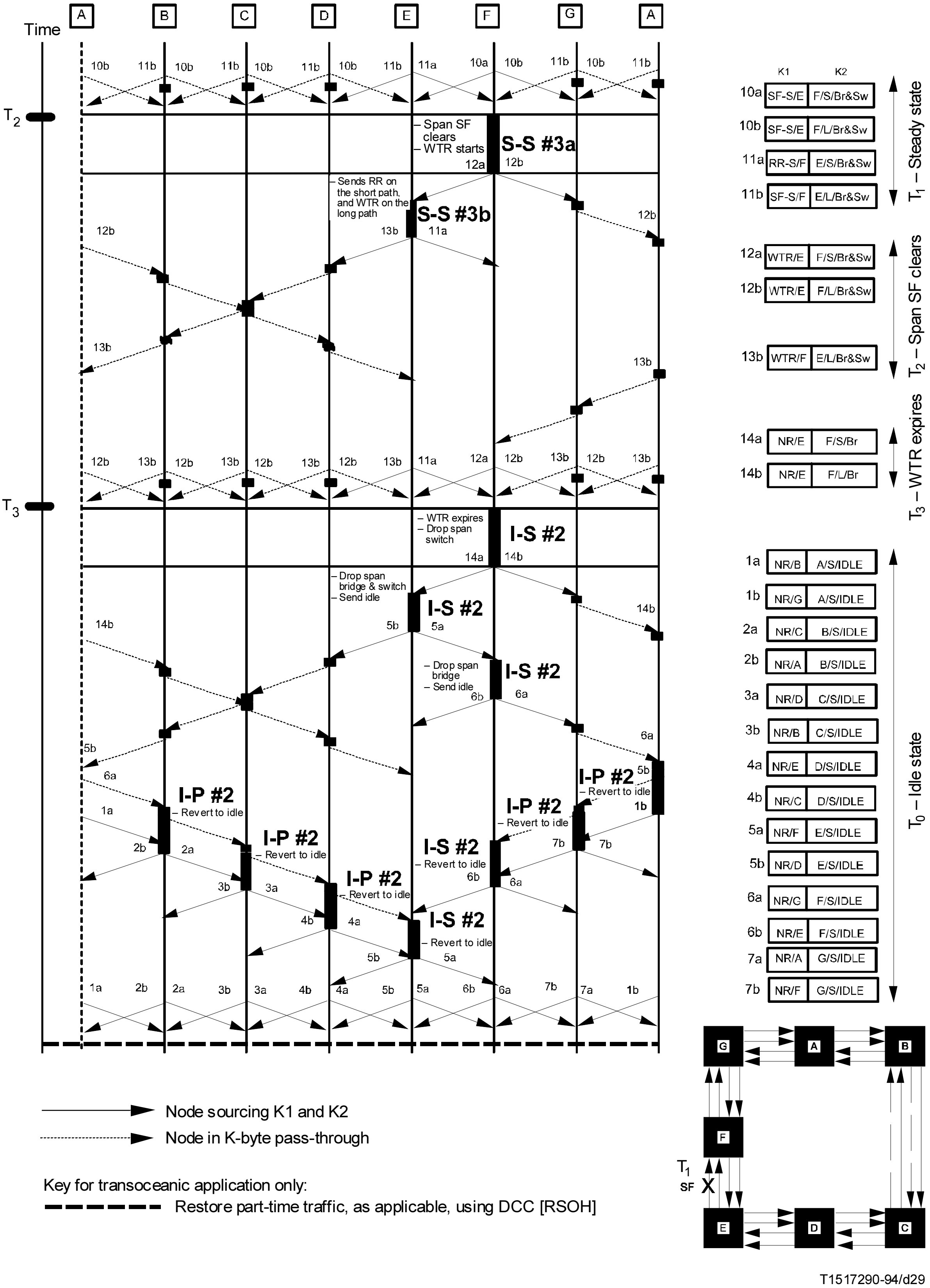


FIGURE I.1/G.841 (*end*)

Four-fibre MS shared protection ring-unidirectional failure (span) on working from E to F

I.2 Unidirectional signal fail (ring)

See Figure I.2.

This example covers the case of a unidirectional SF condition in a two-fibre ring, and 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 Reverse Request 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 byte K2 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 K-byte signalling (Rule I-S #1b). Signalling reaches steady state.

For transoceanic applications, the switching activities that would take place at the intermediate nodes. On all AU-4 protection channels not being used to protect working channels, extra traffic is restored using the DCC.

At time T_2, the ring SF condition clears, and Node F enters the Wait-to-Restore 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 Reverse Request 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 No Request codes (Rule I-S #2). Node E, upon reception of the No Request 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.

This example covers the case of a bidirectional SF condition in a two-fibre ring, and 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 byte K2 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 byte K2 bits 6-8 (Rule I-S #1b). Signalling reaches steady state.

For transoceanic applications, the switching activities that would take place at the intermediate nodes. On all AU-4 protection channels not being used to protect working channels, extra traffic is restored using the DCC.

At time T_2 when the SF-R condition clears, the K-byte values that nodes E and F receive indicate to both E and F that they are Head Ends of a unidirectional SF condition on the span, which preempts 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 No Request 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.

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 Reverse Request 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 byte K2 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 K-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 transoceanic applications, the switching activities that would take place at the intermediate nodes. On all AU-4 protection channels not being used to protect working channels, extra traffic is restored using the DCC.

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

I.5 Node failure

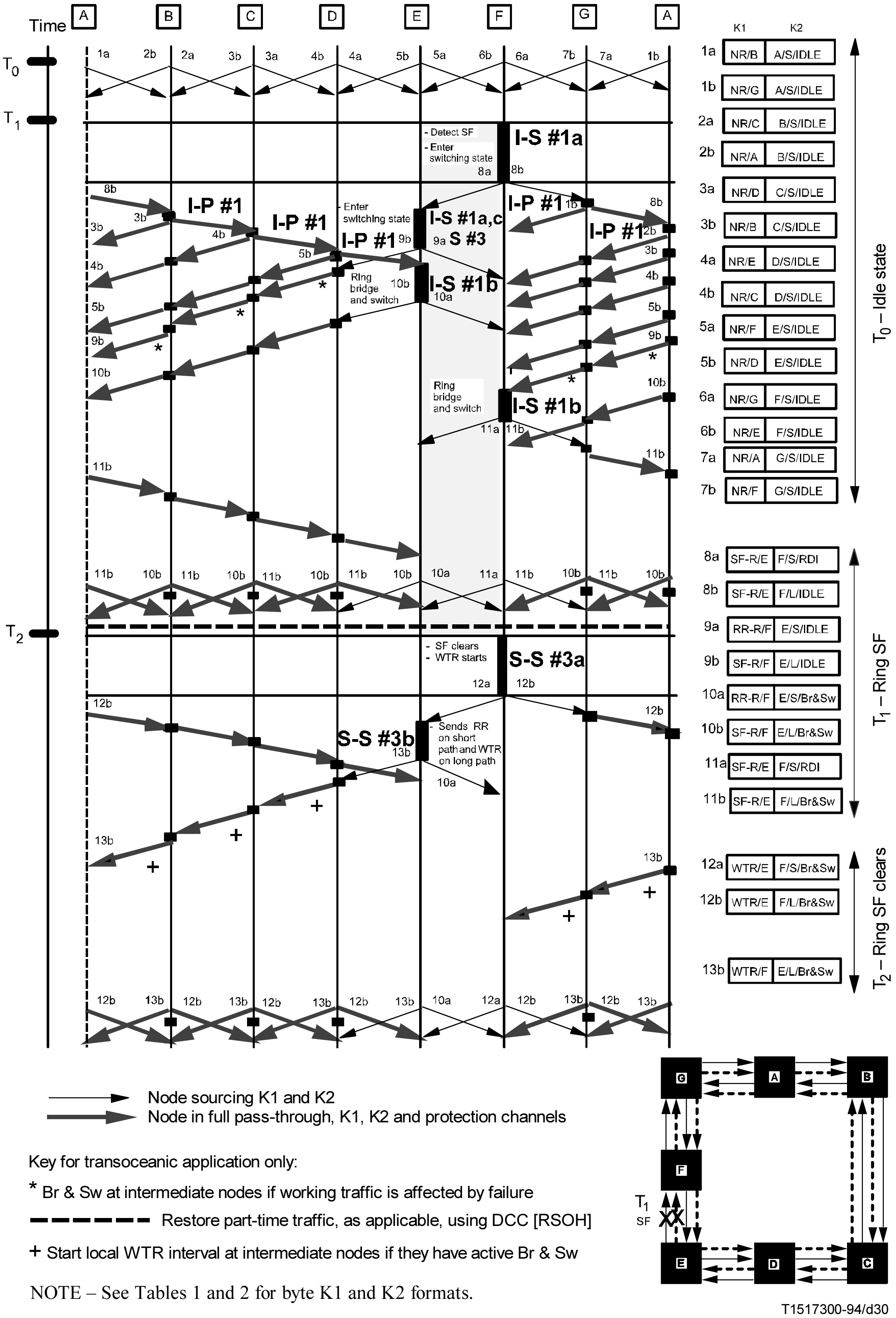
See Figure I.5.

This example covers the case of a node failure in both two-and four-fibre rings. Node failure here means that all transmission, 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 byte K2 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 byte K2 bits 6-8 (Rule I-S #1b). Signalling reaches steady state.

For transoceanic applications, the switching activities would take place at the intermediate nodes. On all AU-4 protection channels not being used to protect working channels, extra traffic is restored using the DCC.

At time T_2, the failed node has recovered physically but has not fully-recovered its provisioning information, preventing the recovering node from proper K-byte signalling. Until the recovering node is capable of proper K-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.



	K1	K2
1a	NR/B	A/S/IDLE
1b	NR/G	A/S/IDLE
2a	NR/C	B/S/IDLE
2b	NR/A	B/S/IDLE
3a	NR/D	C/S/IDLE
3b	NR/B	C/S/IDLE
4a	NR/E	D/S/IDLE
4b	NR/C	D/S/IDLE
5a	NR/F	E/S/IDLE
5b	NR/D	E/S/IDLE
6a	NR/G	F/S/IDLE
6b	NR/E	F/S/IDLE
7a	NR/A	G/S/IDLE
7b	NR/F	G/S/IDLE
8a	SF-R/E	F/S/RDI
8b	SF-R/E	F/L/IDLE
9a	RR-R/F	E/S/IDLE
9b	SF-R/F	E/L/IDLE
10a	RR-R/F	E/S/Br&Sw
10b	SF-R/F	E/L/Br&Sw
11a	SF-R/E	F/S/RDI
11b	SF-R/E	F/L/Br&Sw
12a	WTR/E	F/S/Br&Sw
12b	WTR/E	F/L/Br&Sw
13b	WTR/F	E/L/Br&Sw

T_0 – Idle state (1a–7b)

T_1 – Ring SF (8a–11b)

T_2 – Ring SF clears (12a–13b)

→ Node sourcing K1 and K2

➡ Node in full pass-through, K1, K2 and protection channels

Key for transoceanic application only:

* Br & Sw at intermediate nodes if working traffic is affected by failure

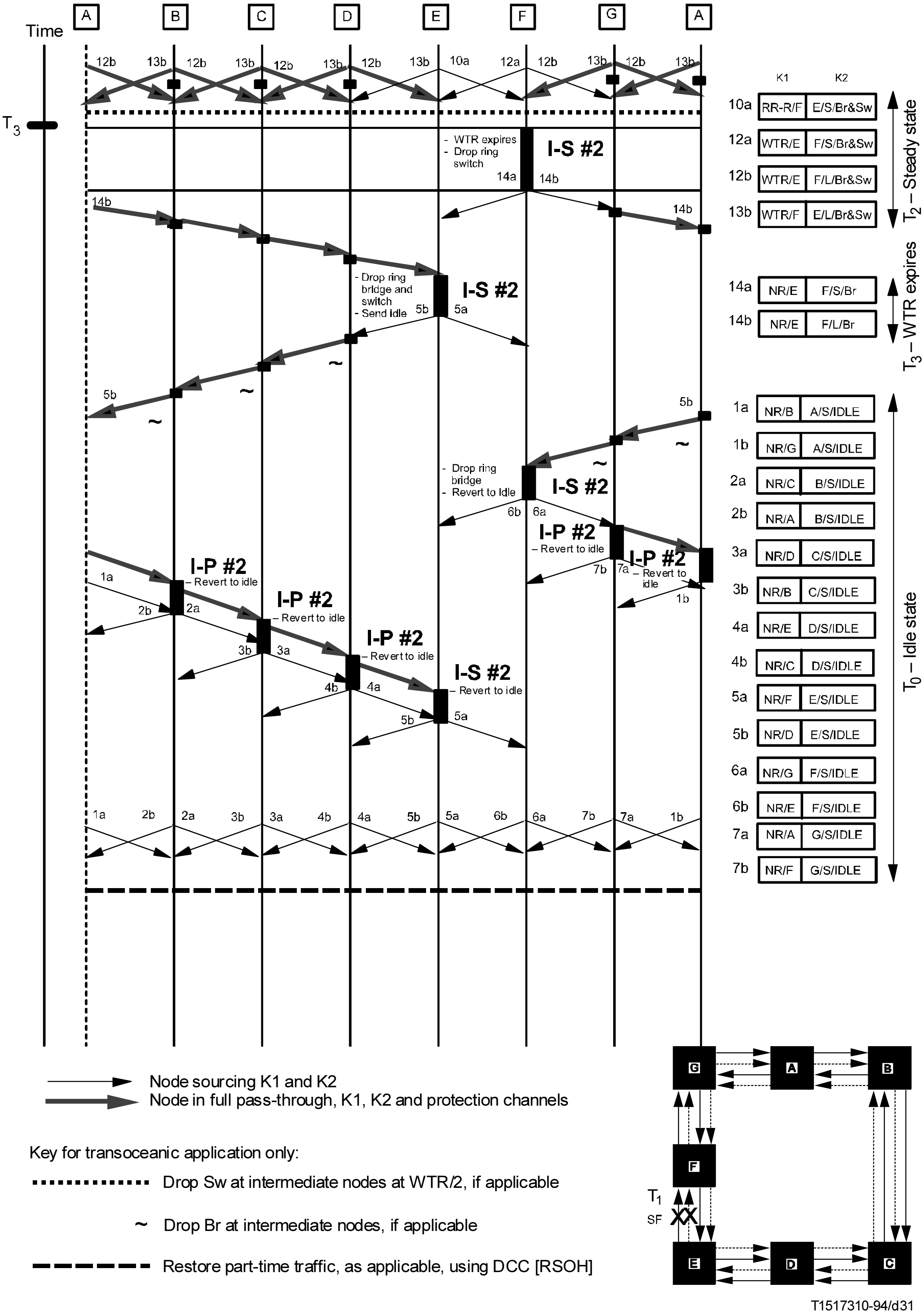
– – – – – – Restore part-time traffic, as applicable, using DCC [RSOH]

+ Start local WTR interval at intermediate nodes if they have active Br & Sw

NOTE – See Tables 1 and 2 for byte K1 and K2 formats.

FIGURE I.2/G.841

Two- or four-fibre MS shared protection ring – Unidirectional SF (ring)

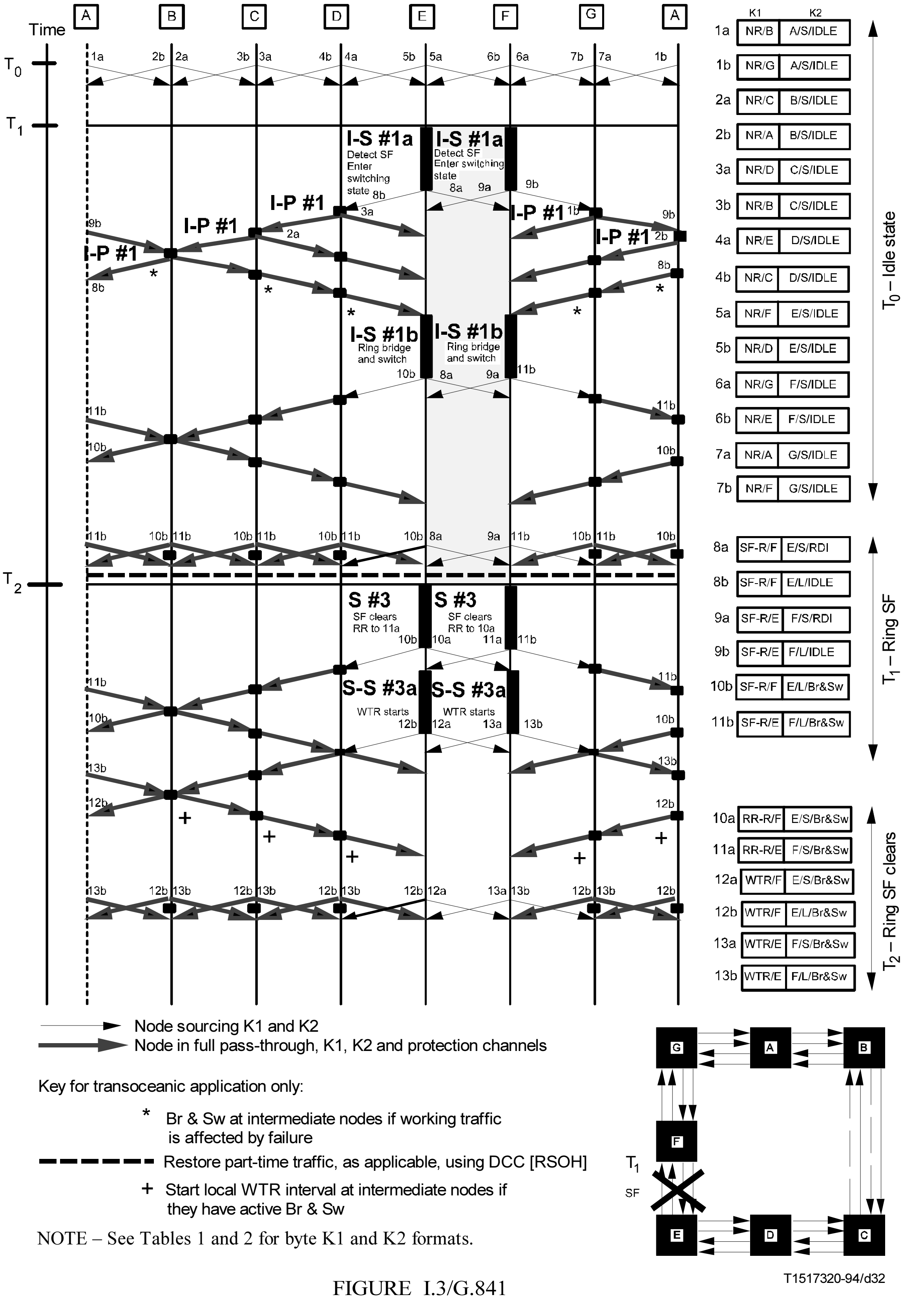


Time
T3
A
B
C
D
E
F
G
A
12b
13b
10a
12a
14a
14b
- WTR expires
- Drop ring switch
I-S #2
- Drop ring bridge and switch
- Send idle
5b
5a
~
- Drop ring bridge
- Revert to idle
6b
6a
I-P #2
– Revert to idle
7b
7a
1a
1b
2a
2b
3a
3b
4a
4b
T2 – Steady state
T3 – WTR expires
T0 – Idle state
T1
SF
G
A
B
F
E
D
C
Node sourcing K1 and K2
Node in full pass-through, K1, K2 and protection channels
Key for transoceanic application only:
Drop Sw at intermediate nodes at WTR/2, if applicable
~ Drop Br at intermediate nodes, if applicable
Restore part-time traffic, as applicable, using DCC [RSOH]
T1517310-94/d31

	K1	K2
10a	RR-R/F	E/S/Br&Sw
12a	WTR/E	F/S/Br&Sw
12b	WTR/E	F/L/Br&Sw
13b	WTR/F	E/L/Br&Sw
14a	NR/E	F/S/Br
14b	NR/E	F/L/Br
1a	NR/B	A/S/IDLE
1b	NR/G	A/S/IDLE
2a	NR/C	B/S/IDLE
2b	NR/A	B/S/IDLE
3a	NR/D	C/S/IDLE
3b	NR/B	C/S/IDLE
4a	NR/E	D/S/IDLE
4b	NR/C	D/S/IDLE
5a	NR/F	E/S/IDLE
5b	NR/D	E/S/IDLE
6a	NR/G	F/S/IDLE
6b	NR/E	F/S/IDLE
7a	NR/A	G/S/IDLE
7b	NR/F	G/S/IDLE

FIGURE I.2/G.841 (*end*)

Two- or four-fibre MS shared protection ring – Unidirectional SF (ring)

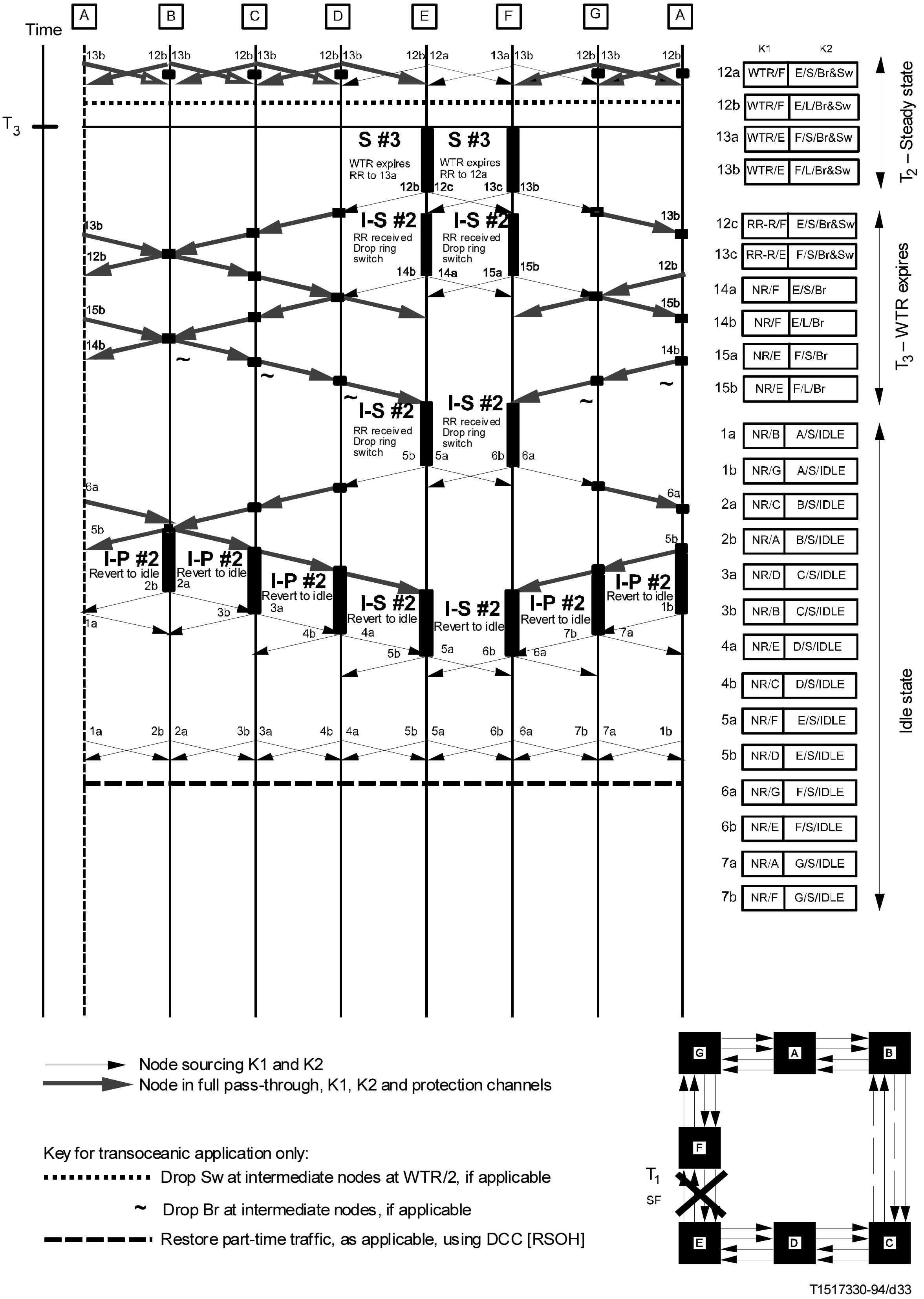


	K1	K2
1a	NR/B	A/S/IDLE
1b	NR/G	A/S/IDLE
2a	NR/C	B/S/IDLE
2b	NR/A	B/S/IDLE
3a	NR/D	C/S/IDLE
3b	NR/B	C/S/IDLE
4a	NR/E	D/S/IDLE
4b	NR/C	D/S/IDLE
5a	NR/F	E/S/IDLE
5b	NR/D	E/S/IDLE
6a	NR/G	F/S/IDLE
6b	NR/E	F/S/IDLE
7a	NR/A	G/S/IDLE
7b	NR/F	G/S/IDLE
8a	SF-R/F	E/S/RDI
8b	SF-R/F	E/L/IDLE
9a	SF-R/E	F/S/RDI
9b	SF-R/E	F/L/IDLE
10b	SF-R/F	E/L/Br&Sw
11b	SF-R/E	F/L/Br&Sw
10a	RR-R/F	E/S/Br&Sw
11a	RR-R/E	F/S/Br&Sw
12a	WTR/F	E/S/Br&Sw
12b	WTR/F	E/L/Br&Sw
13a	WTR/E	F/S/Br&Sw
13b	WTR/E	F/L/Br&Sw

NOTE – See Tables 1 and 2 for byte K1 and K2 formats.

FIGURE I.3/G.841

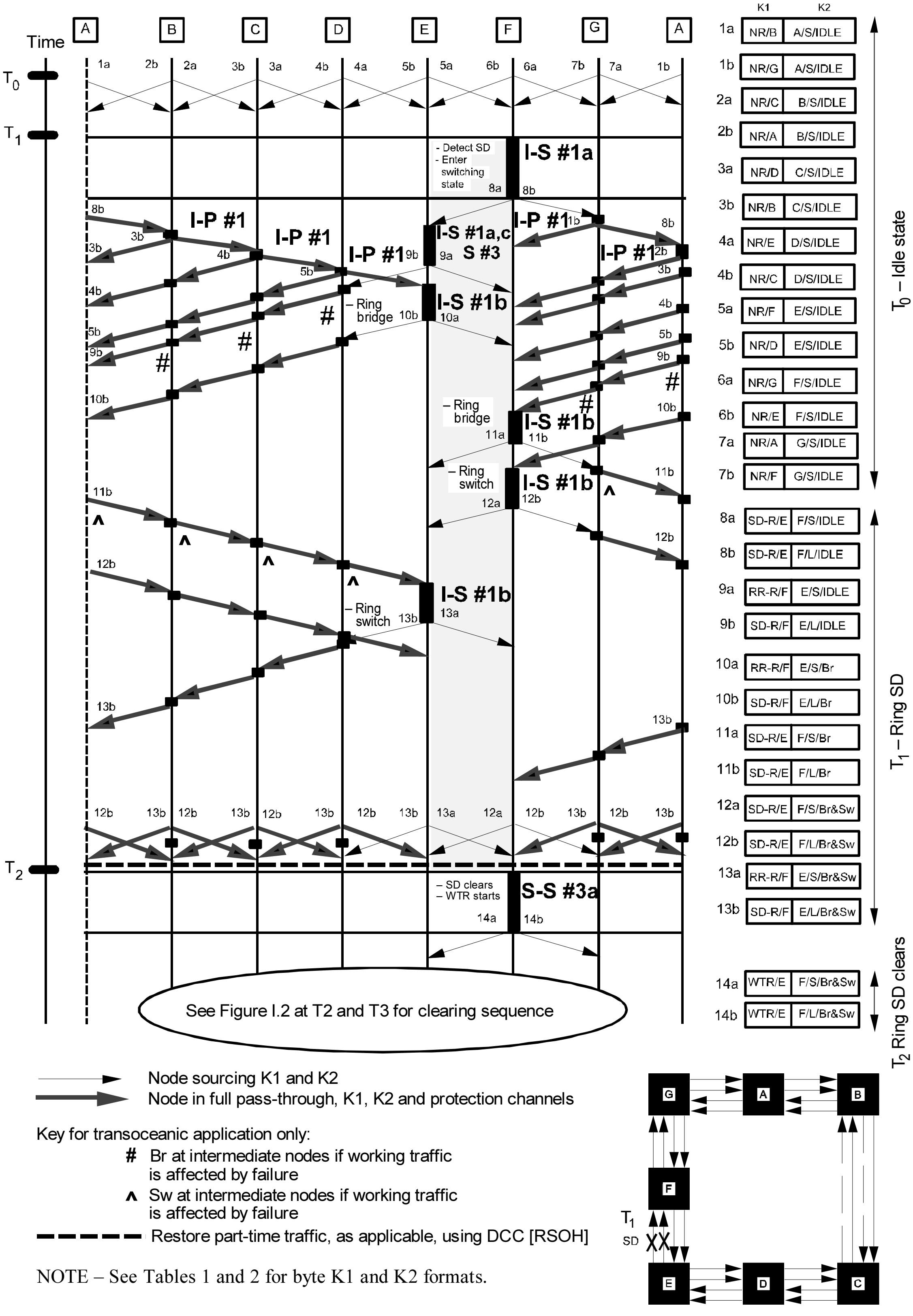
Two- or four-fibre MS shared protection ring – Bidirectional SF (ring)


Time
A
B
C
D
E
F
G
A
T$_3$
S #3
WTR expires
RR to 13a
S #3
WTR expires
RR to 12a
I-S #2
RR received
Drop ring
switch
I-P #2
Revert to idle
I-S #2
Revert to idle
T$_2$ – Steady state
T$_3$ – WTR expires
Idle state
Node sourcing K1 and K2
Node in full pass-through, K1, K2 and protection channels
Key for transoceanic application only:
Drop Sw at intermediate nodes at WTR/2, if applicable
~ Drop Br at intermediate nodes, if applicable
Restore part-time traffic, as applicable, using DCC [RSOH]
G
A
B
F
T$_1$
SF
E
D
C
T1517330-94/d33

	K1	K2
12a	WTR/F	E/S/Br&Sw
12b	WTR/F	E/L/Br&Sw
13a	WTR/E	F/S/Br&Sw
13b	WTR/E	F/L/Br&Sw
12c	RR-R/F	E/S/Br&Sw
13c	RR-R/E	F/S/Br&Sw
14a	NR/F	E/S/Br
14b	NR/F	E/L/Br
15a	NR/E	F/S/Br
15b	NR/E	F/L/Br
1a	NR/B	A/S/IDLE
1b	NR/G	A/S/IDLE
2a	NR/C	B/S/IDLE
2b	NR/A	B/S/IDLE
3a	NR/D	C/S/IDLE
3b	NR/B	C/S/IDLE
4a	NR/E	D/S/IDLE
4b	NR/C	D/S/IDLE
5a	NR/F	E/S/IDLE
5b	NR/D	E/S/IDLE
6a	NR/G	F/S/IDLE
6b	NR/E	F/S/IDLE
7a	NR/A	G/S/IDLE
7b	NR/F	G/S/IDLE

FIGURE I.3/G.841 (*end*)

Two- or four-fibre MS shared protection ring – Bidirectional SF (ring)



	K1	K2
1a	NR/B	A/S/IDLE
1b	NR/G	A/S/IDLE
2a	NR/C	B/S/IDLE
2b	NR/A	B/S/IDLE
3a	NR/D	C/S/IDLE
3b	NR/B	C/S/IDLE
4a	NR/E	D/S/IDLE
4b	NR/C	D/S/IDLE
5a	NR/F	E/S/IDLE
5b	NR/D	E/S/IDLE
6a	NR/G	F/S/IDLE
6b	NR/E	F/S/IDLE
7a	NR/A	G/S/IDLE
7b	NR/F	G/S/IDLE
8a	SD-R/E	F/S/IDLE
8b	SD-R/E	F/L/IDLE
9a	RR-R/F	E/S/IDLE
9b	SD-R/F	E/L/IDLE
10a	RR-R/F	E/S/Br
10b	SD-R/F	E/L/Br
11a	SD-R/E	F/S/Br
11b	SD-R/E	F/L/Br
12a	SD-R/E	F/S/Br&Sw
12b	SD-R/E	F/L/Br&Sw
13a	RR-R/F	E/S/Br&Sw
13b	SD-R/F	E/L/Br&Sw
14a	WTR/E	F/S/Br&Sw
14b	WTR/E	F/L/Br&Sw

→ Node sourcing K1 and K2

➞ Node in full pass-through, K1, K2 and protection channels

Key for transoceanic application only:

Br at intermediate nodes if working traffic is affected by failure

^ Sw at intermediate nodes if working traffic is affected by failure

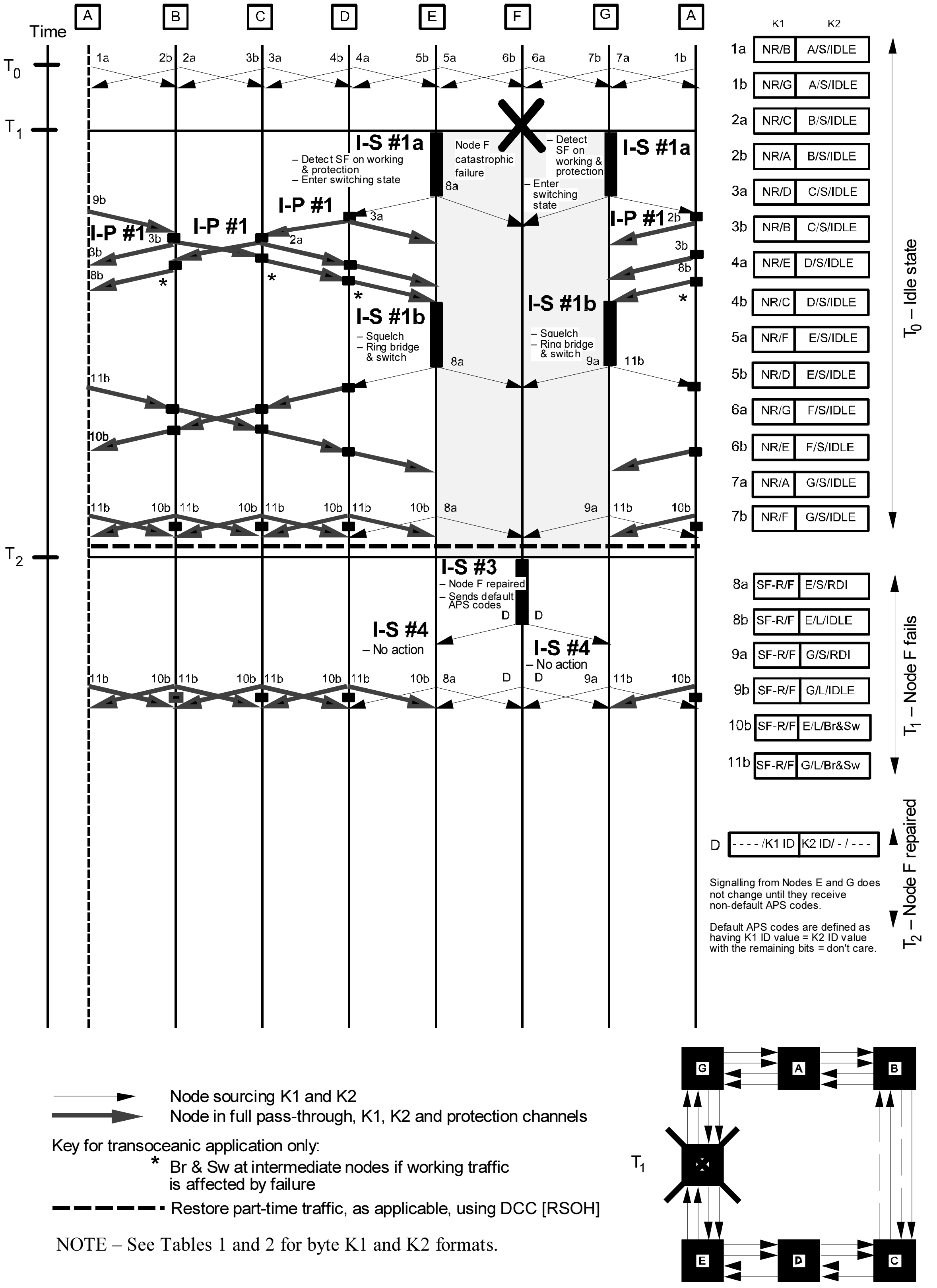
– – – – – Restore part-time traffic, as applicable, using DCC [RSOH]

NOTE – See Tables 1 and 2 for byte K1 and K2 formats.

T1517340-94/d34

FIGURE I.4/G.841

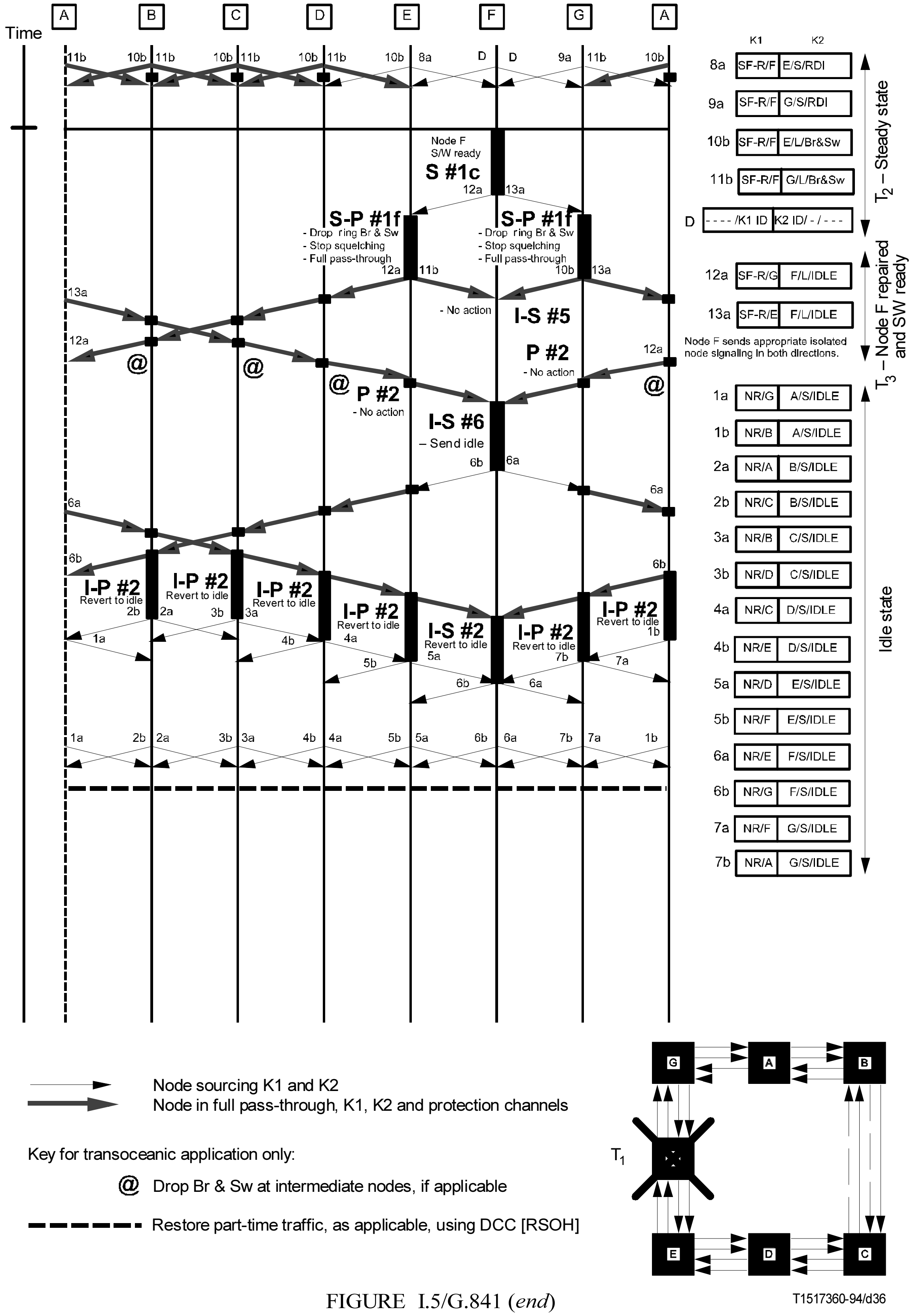
Two- or four-fibre MS shared protection ring – Unidirectional SD (ring)



NOTE – See Tables 1 and 2 for byte K1 and K2 formats.

FIGURE I.5/G.841

**Four-fibre MS shared protection ring –
Node failure**



	K1	K2
8a	SF-R/F	E/S/RDI
9a	SF-R/F	G/S/RDI
10b	SF-R/F	E/L/Br&Sw
11b	SF-R/F	G/L/Br&Sw
D	- - - - /K1 ID	K2 ID/ - / - - -
12a	SF-R/G	F/L/IDLE
13a	SF-R/E	F/L/IDLE
1a	NR/G	A/S/IDLE
1b	NR/B	A/S/IDLE
2a	NR/A	B/S/IDLE
2b	NR/C	B/S/IDLE
3a	NR/B	C/S/IDLE
3b	NR/D	C/S/IDLE
4a	NR/C	D/S/IDLE
4b	NR/E	D/S/IDLE
5a	NR/D	E/S/IDLE
5b	NR/F	E/S/IDLE
6a	NR/E	F/S/IDLE
6b	NR/G	F/S/IDLE
7a	NR/F	G/S/IDLE
7b	NR/A	G/S/IDLE

FIGURE I.5/G.841 (*end*)

**Four-fibre MS shared protection ring –
Node failure**

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 preempted 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 preempting a unidirectional SD-S on non-adjacent spans

See Figure I.6.

This example covers the case of a unidirectional signal fail-ring condition on a four-fibre ring preempting a unidirectional signal degrade-span 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:

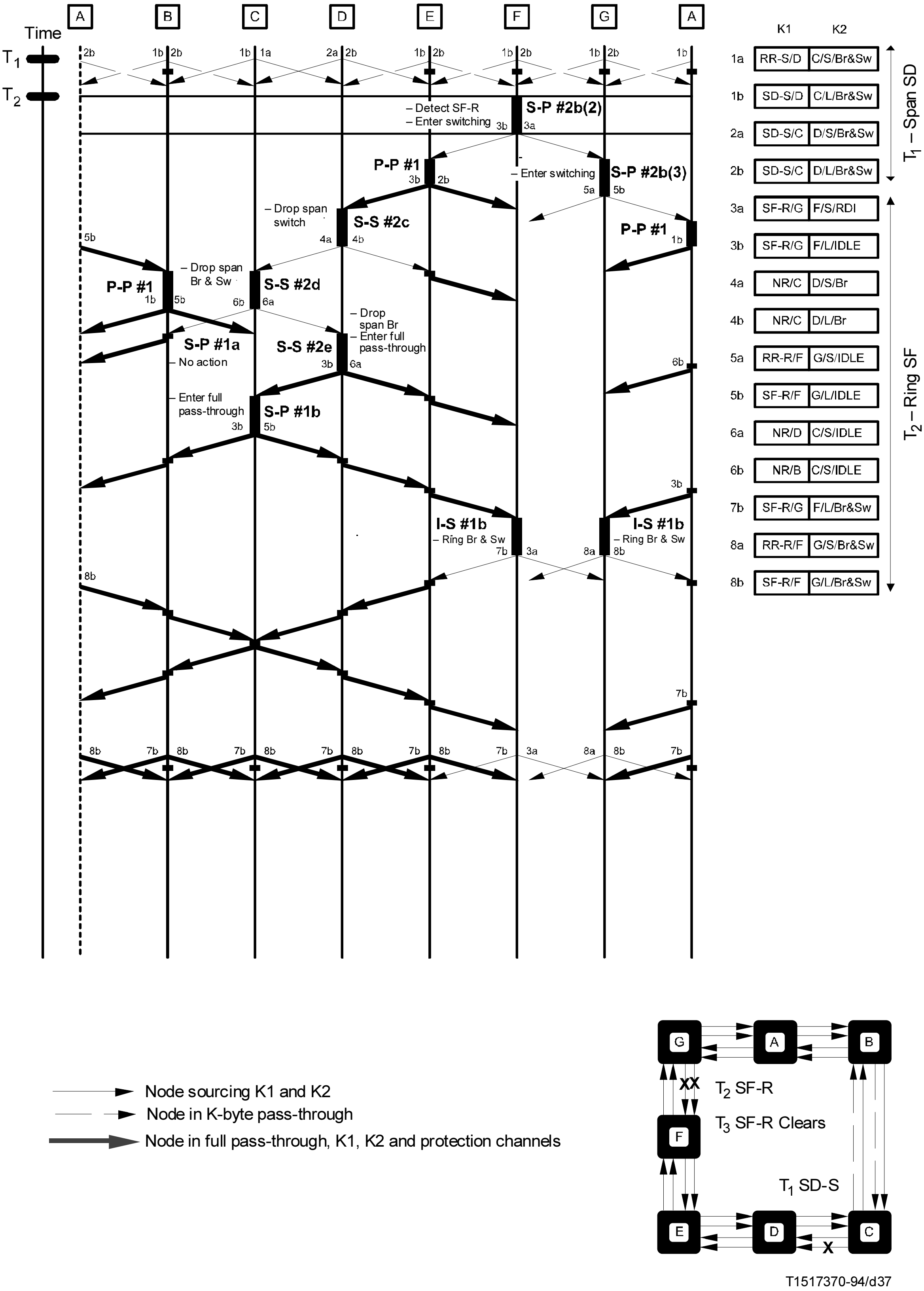
1) the switching nodes become Nodes C and D, not Nodes E and F; and

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 Reverse Request back on the short path, and SF-R on the long path (Rule S #3). Intermediate Nodes A, B, and E change from K-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 byte K2 bits 6-8, and sources No Request in both directions (Rule S-S #2c). Node C, upon seeing a No Request and dropped switch from Node D, drops its bridge and switch, updates byte K2 bits 6-8-, and acts on its highest priority input (Rule SS #2d, first point) to source No Request. Node C eventually sees a ring bridge request destined to Node F, but this does not change Node C's signalling (Rule S-P #la). 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 #lb) 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 byte K2 bits 6-8. Signalling reaches steady state.

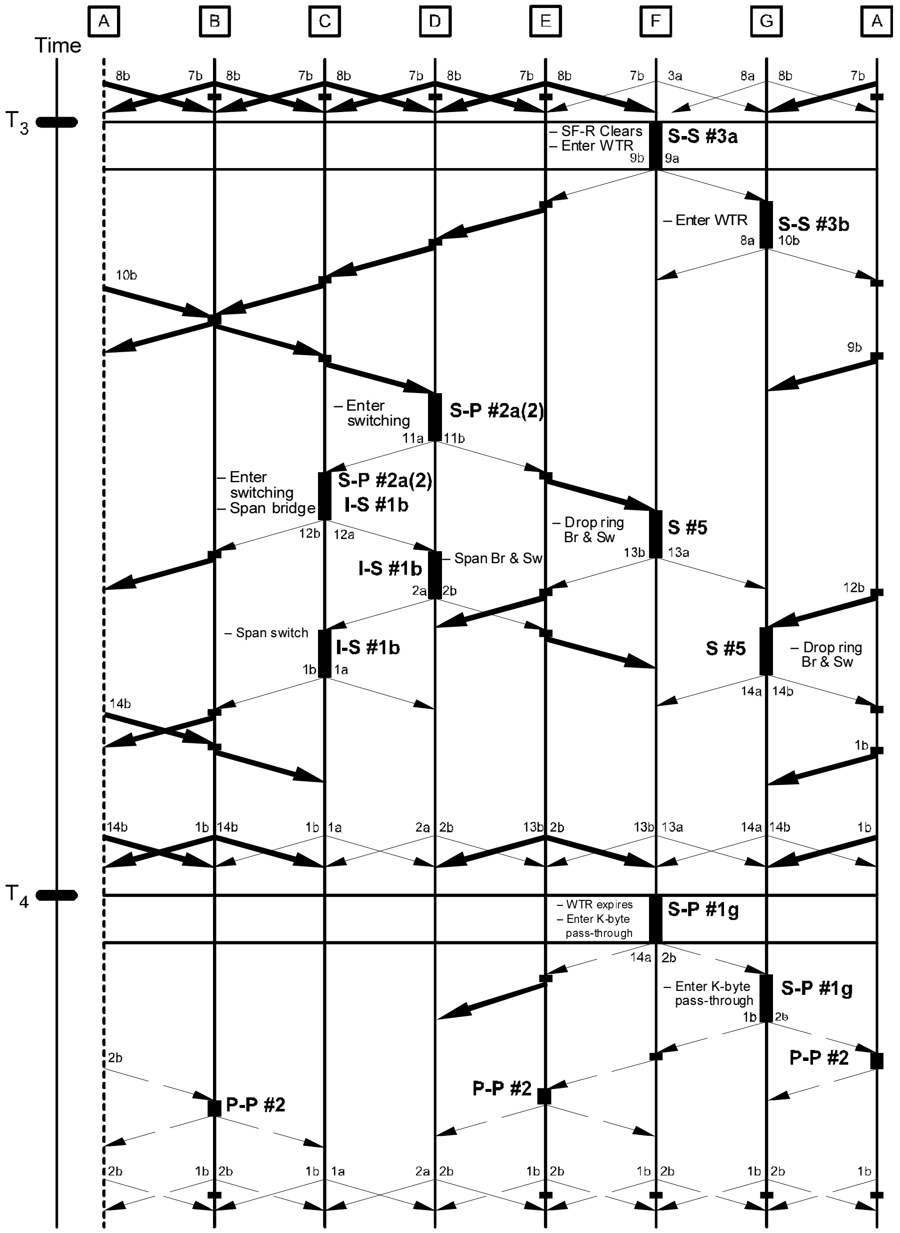
At time T_3, the SF condition on the working and protection channels from Node E to Node F clears. Node F enters Wait-to-Restore (Rule S-S #3a). Node G, upon seeing the WTR bridge request from Node F, also enters Wait-to-Restore (Rule S-S #3b). Node D, upon seeing two WTR bridge requests which are lower 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 byte K2 bits 6-8 (Rule I-S #lb). 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, and signals its highest priority (WTR) input (Rule S #5). Similarly, when Node G loses its long-path ring bridge request, it drops its bridge and switch and signals its highest priority input (Rule S #5). Node D, upon seeing a Bridged code on the short path from Node C, executes a span bridge and switch, and updates byte K2 bits 6-8 (Rule I-S #lb). Node C, upon seeing a Bridged and Switched code from Node D, completes the process by executing a span switch and updating byte K2 bits 6-8 (Rule I-S #lb).



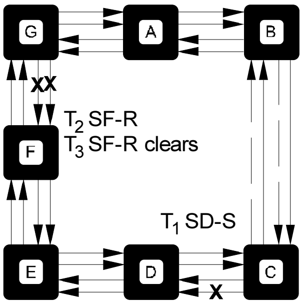
	K1	K2
1a	RR-S/D	C/S/Br&Sw
1b	SD-S/D	C/L/Br&Sw
2a	SD-S/C	D/S/Br&Sw
2b	SD-S/C	D/L/Br&Sw
3a	SF-R/G	F/S/RDI
3b	SF-R/G	F/L/IDLE
4a	NR/C	D/S/Br
4b	NR/C	D/L/Br
5a	RR-R/F	G/S/IDLE
5b	SF-R/F	G/L/IDLE
6a	NR/D	C/S/IDLE
6b	NR/B	C/S/IDLE
7b	SF-R/G	F/L/Br&Sw
8a	RR-R/F	G/S/Br&Sw
8b	SF-R/F	G/L/Br&Sw

FIGURE I.6/G.841

Four-fibre MS shared protection ring – Unidirectional SF-R preempting a unidirectional SD-S on non-adjacent spans



	K1	K2	
1a	RR-S/D	C/S/Br&Sw	T1 – Span SD
1b	SD-S/D	C/L/Br&Sw	
2a	SD-S/C	D/S/Br&Sw	
2b	SD-S/C	D/L/Br&Sw	
3a	SF-R/G	F/S/RDI	T2 – Ring SF
3b	SF-R/G	F/L/IDLE	
4a	NR/C	D/S/Br	
4b	NR/C	D/L/Br	
5a	RR-R/F	G/S/IDLE	
5b	SF-R/F	G/L/IDLE	
6a	NR/D	C/S/IDLE	
6b	NR/D	C/L/IDLE	
7b	SF-R/G	F/L/Br&Sw	
8a	RR-R/F	G/S/Br&Sw	
8b	SF-R/F	G/L/Br&Sw	
9a	WTR/G	F/S/Br&Sw	T3 – Ring SF clears
9b	WTR/G	F/L/Br&Sw	
10b	WTR/F	G/L/Br&Sw	
11a	SD-S/C	D/S/IDLE	
11b	SD-S/C	D/L/IDLE	
12a	SD-S/D	C/S/Br	
12b	SD-S/D	C/L/Br	
13a	WTR/G	F/S/IDLE	
13b	WTR/G	F/L/IDLE	
14a	RR-R/F	G/S/IDLE	
14b	WTR/F	G/L/IDLE	



Node sourcing K1 and K2

Node in K-byte pass-through

Node in full pass-through, K1, K2 and protection channels

T1517380-94/d38

FIGURE I.6/G.841 (*end*)

Four-fibre MS shared protection ring – Unidirectional SF-R preempting a unidirectional SD-S on non-adjacent spans

At time T_4, the WTR at Node F expires. Node F's highest priority input is now a span bridge request status destined for Node C, so Node F enters K-byte pass-through (Rule S-P #1g). Node G, upon seeing a span bridge request status not destined to itself from both directions, also enters K-byte pass-through. Intermediate Nodes A, E, and B, then move from full pass-through to K-byte pass-through. Signalling reaches the same steady state as found at time T_1.

At time T_5 (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 T_2 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 preempting a unidirectional SF-R on adjacent spans

See Figure I.7.

This example covers the case of a unidirectional signal fail-span condition on a four-fibre ring preempting a unidirectional signal fail-ring 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 (Rule 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 byte K2 bits 6-8, and sources SF-R in byte K1 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 #l b, third point, and Rule S #3). Node E, upon seeing the Bridged code from Node D, executes a span bridge and switch, and updates byte K2 bits 6-8 (Rule I-S #lb, third point). Node D, upon seeing the Bridged code from Node E, executes a switch, and updates byte K2 bits 6-8 accordingly (Rule I-S #lb, 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 Wait-to-Restore, 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 No Request in byte K1, and Bridged in byte K2 (Rule S-S #2c). Node D, upon seeing the No Request 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 byte K2 bits 6-8 (Rule I-S #lb). Node C, upon seeing a long path ring bridge request from Node D, also executes a ring bridge and switch, and updates byte K2 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 a 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.

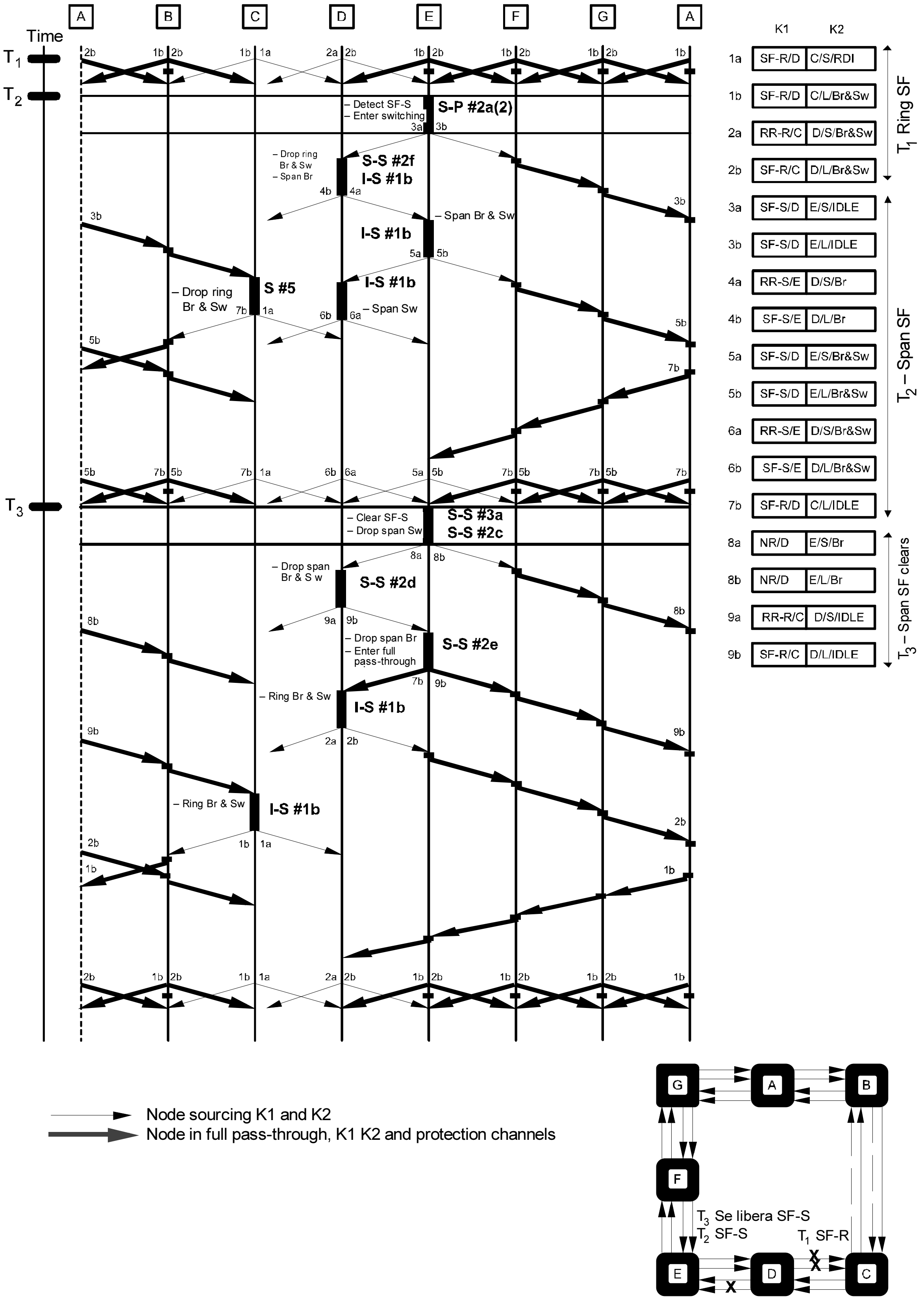


FIGURE I.7/G.841

Four-fibre MS shared protection ring – Unidirectional SF-S preempting a unidirectional SF-R on adjacent spans

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

See Figure I.8.

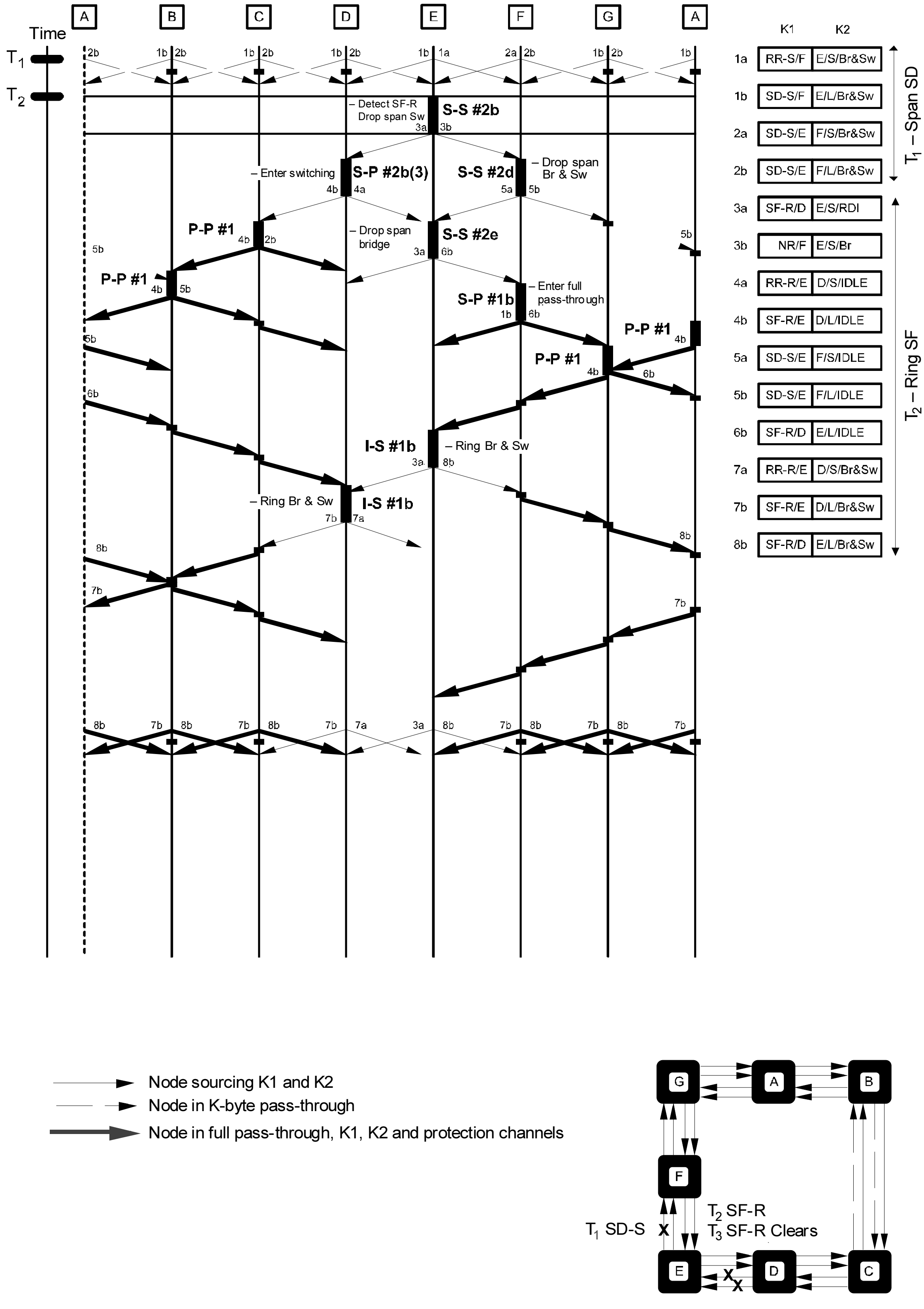
This example covers the case of a unidirectional signal fail-ring condition an a four-fibre ring preempting a unidirectional signal degrade-span condition that had previously existed on an adjacent span.

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 a 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 Signal Fail ring bridge request (in byte K1) and MS RDI (in byte K2) towards Node D, and sources No Request (in byte K1) and Bridged (in byte K2) towards Node F (Rule S-S #2b). Node D becomes a switching node (Rule S-P #2b, point 3). Node D sources Reverse Request on the short path, and a Signal Fail ring bridge request on the long path (Rule S #3). This long-path ring bridge request changes Nodes C, B, and A from K-byte pass-through to full pass-through (Rule P-P #1). Node F, upon seeing a No Request and dropped switch from Node E, drops its bridge and switch, updates byte K2 bits 6-8, and acts on its highest priority input (Rule S-S #2d, last point) to source a Signal Degrade span bridge request towards Node E. Node E, upon seeing a dropped switch at Node F, drops its bridge, updates byte K2 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 #lb) to enter full pass-through. This permits a long path ring bridge request to reach Node G, and Node G changes from K-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 #lb. second point) and update byte K2 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 Wait-to-Restore period, and signals so (Rule S-S #3a). Node D, upon seeing the WTR bridge request from Node E, also starts its Wait-to-Restore 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 #lb, third point). Node F, upon seeing the Bridged code from Node F, executes a span bridge and switch, and updates byte K2 bits 6-8 (Rule I-S #lb, third point). Node E, upon seeing the Bridged and Switched code from Node F, completes the process by executing a span switch and updating byte K2 bits 6-8 (Rule I-S #lb, 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 K-byte pass-through (Rule S-P #lg). 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 K-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.

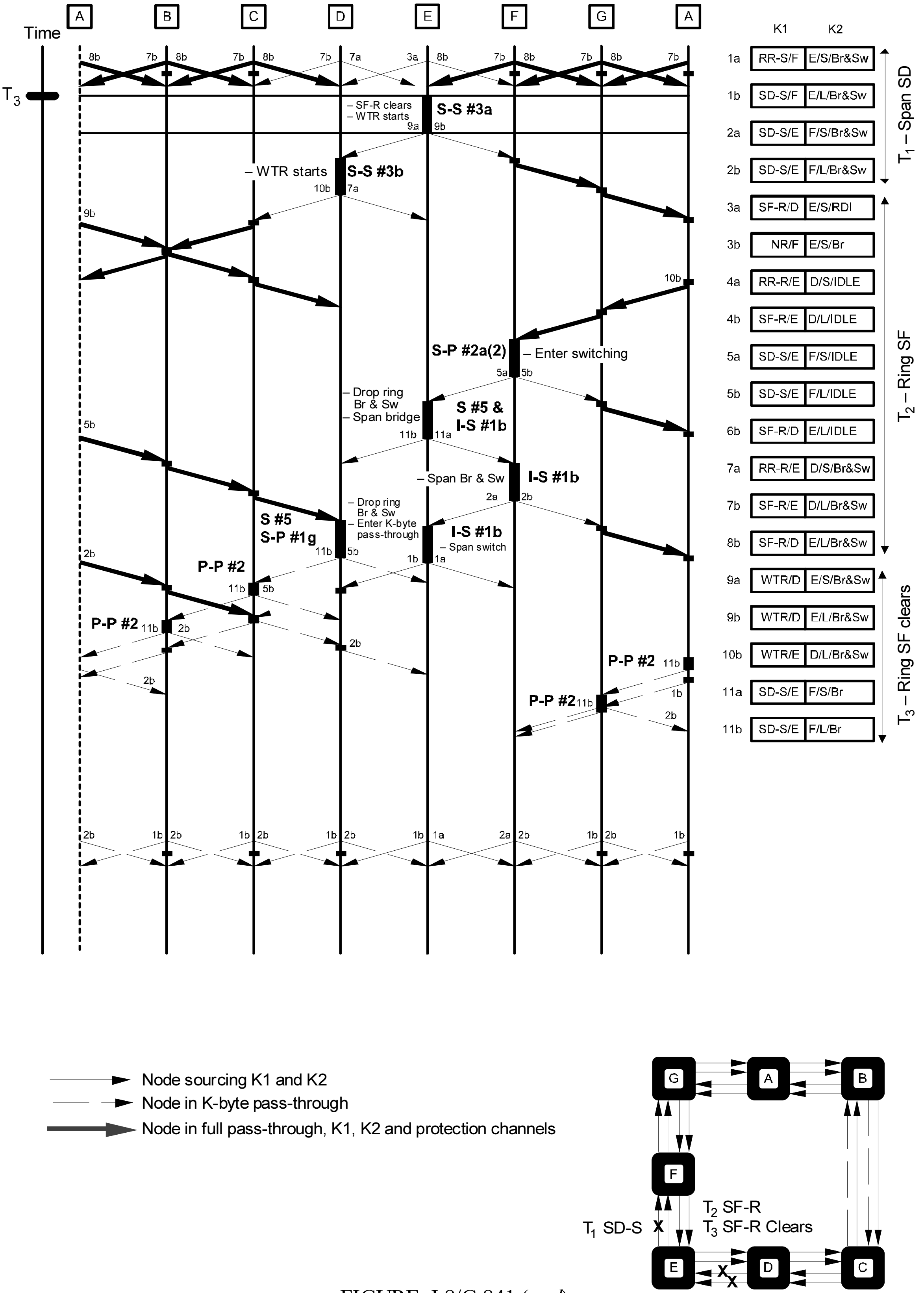


	K1	K2
1a	RR-S/F	E/S/Br&Sw
1b	SD-S/F	E/L/Br&Sw
2a	SD-S/E	F/S/Br&Sw
2b	SD-S/E	F/L/Br&Sw
3a	SF-R/D	E/S/RDI
3b	NR/F	E/S/Br
4a	RR-R/E	D/S/IDLE
4b	SF-R/E	D/L/IDLE
5a	SD-S/E	F/S/IDLE
5b	SD-S/E	F/L/IDLE
6b	SF-R/D	E/L/IDLE
7a	RR-R/E	D/S/Br&Sw
7b	SF-R/E	D/L/Br&Sw
8b	SF-R/D	E/L/Br&Sw

T1517400-94/d40

FIGURE I.8/G.841

Four-fibre MS shared protection ring – Unidirectional SF-R preempting a unidirectional SD-S on adjacent spans



	K1	K2
1a	RR-S/F	E/S/Br&Sw
1b	SD-S/F	E/L/Br&Sw
2a	SD-S/E	F/S/Br&Sw
2b	SD-S/E	F/L/Br&Sw
3a	SF-R/D	E/S/RDI
3b	NR/F	E/S/Br
4a	RR-R/E	D/S/IDLE
4b	SF-R/E	D/L/IDLE
5a	SD-S/E	F/S/IDLE
5b	SD-S/E	F/L/IDLE
6b	SF-R/D	E/L/IDLE
7a	RR-R/E	D/S/Br&Sw
7b	SF-R/E	D/L/Br&Sw
8b	SF-R/D	E/L/Br&Sw
9a	WTR/D	E/S/Br&Sw
9b	WTR/D	E/L/Br&Sw
10b	WTR/E	D/L/Br&Sw
11a	SD-S/E	F/S/Br
11b	SD-S/E	F/L/Br

T1517410-94/d41

FIGURE I.8/G.841 (*end*)

Four-fibre MS shared protection ring – Unidirectional SF-R preempting a unidirectional SD-S on adjacent spans

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

See Figure I.9.

This example covers the case of a unidirectional signal fail-ring condition on a four-fibre ring coexisting with another unidirectional signal fail-ring 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.

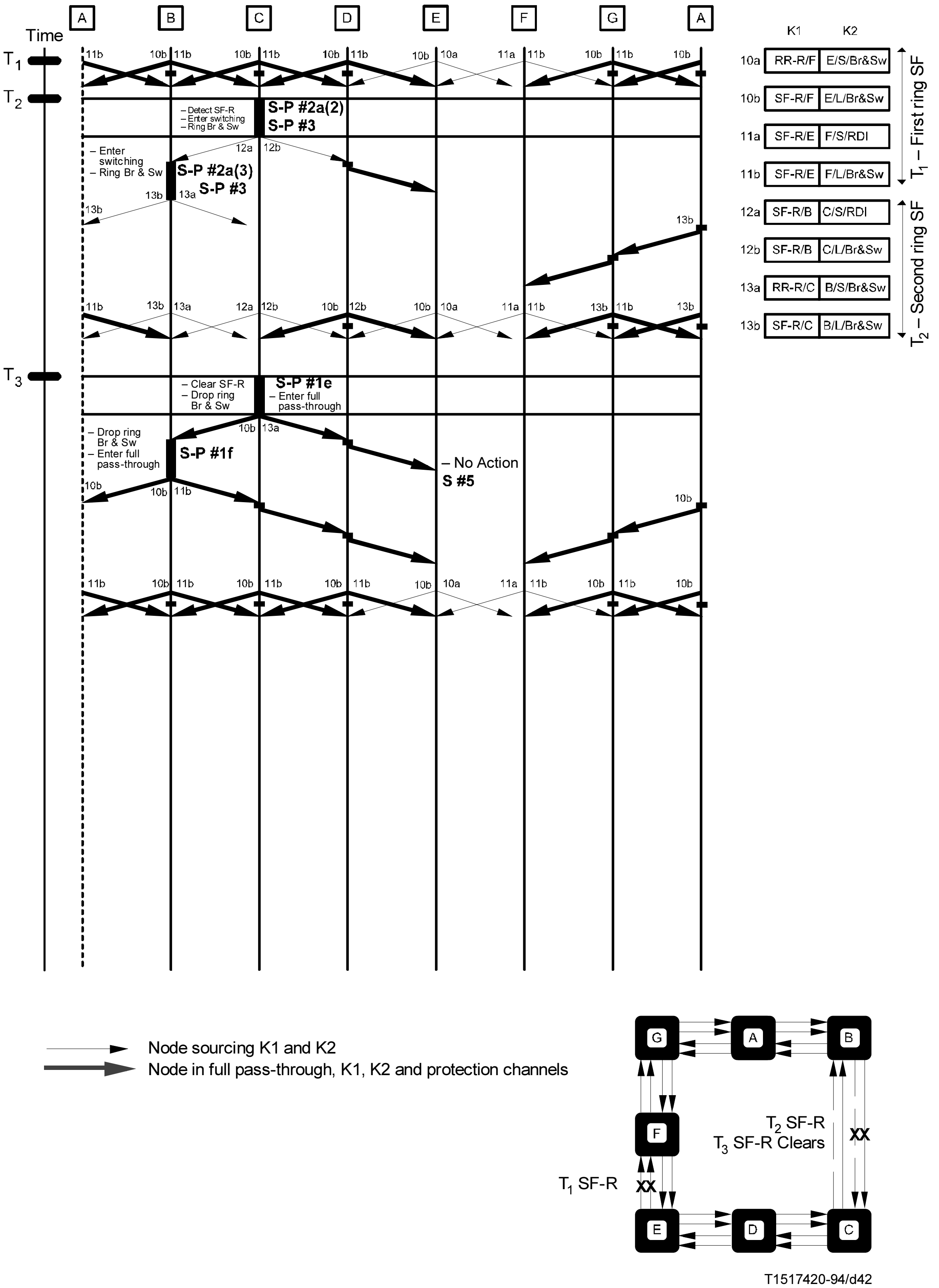
At time T_2, Node C detects an SF condition on its working and protection channels. Node C becomes a switching node (Rule S-P #2a, point 2), squelches traffic if necessary, executes a ring bridge and switch, and sources ring bridge requests in both directions (S-P #3). Node B, upon seeing the bridge 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 transoceanic 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 Annex A). 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 Annex A). 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 byte K2 bits 6-8 to the Idle code (Rule S-S #1a, point 2, in Annex A). Node C (B), upon seeing the ring bridge request and an Idle code from Node E (F), updates byte K2 bits 6-8 to Bridged and Switched (Rule S-S #la, point 2, in Annex A). Node E (F), upon seeing the ring bridge request and the Bridged and Switched code from Node C (B), updates byte K2 bits 6-8 to Bridged and Switched (Rule S-S #la, point 3, in Annex A). 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 Reverse Request 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, Note). 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 transoceanic 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 Annex A). This permits the short-path ring Reverse Request 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, Note). 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 #lf, point 1, in Annex A). Signalling reaches the same steady state as described for Figure I.9.

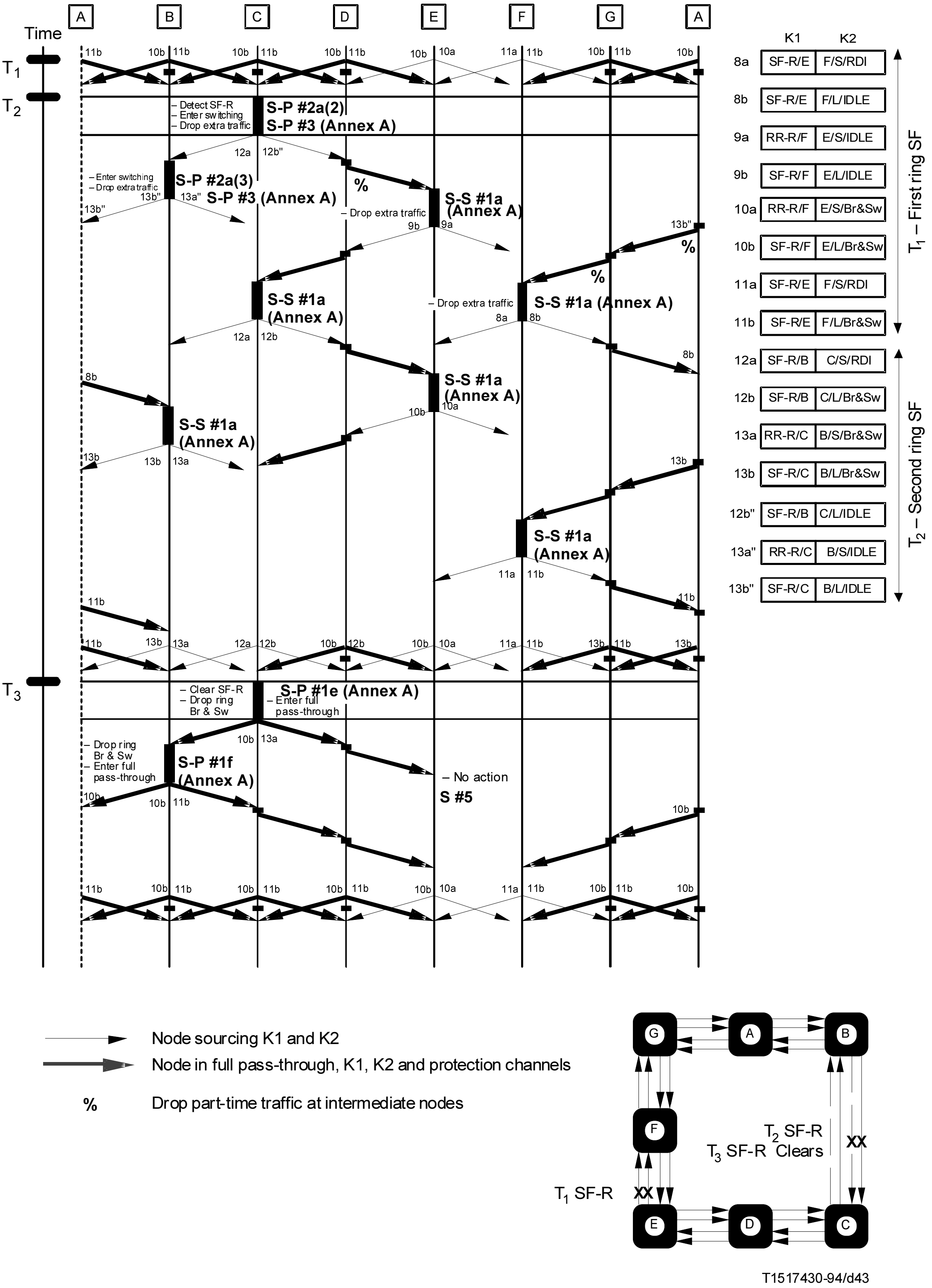
At time T_4 (not shown), the SF condition on the working and protection channels from Node E to Node F clears. The signalling proceeds in a manner as shown in Figure I.2 (at time T_3 in the figure).



	K1	K2
10a	RR-R/F	E/S/Br&Sw
10b	SF-R/F	E/L/Br&Sw
11a	SF-R/E	F/S/RDI
11b	SF-R/E	F/L/Br&Sw
12a	SF-R/B	C/S/RDI
12b	SF-R/B	C/L/Br&Sw
13a	RR-R/C	B/S/Br&Sw
13b	SF-R/C	B/L/Br&Sw

FIGURE I.9/G.841

Four-fibre MS shared protection ring – Unidirectional SF-R plus unidirectional SF-R on non-adjacent spans



	K1	K2
8a	SF-R/E	F/S/RDI
8b	SF-R/E	F/L/IDLE
9a	RR-R/F	E/S/IDLE
9b	SF-R/F	E/L/IDLE
10a	RR-R/F	E/S/Br&Sw
10b	SF-R/F	E/L/Br&Sw
11a	SF-R/E	F/S/RDI
11b	SF-R/E	F/L/Br&Sw
12a	SF-R/B	C/S/RDI
12b	SF-R/B	C/L/Br&Sw
13a	RR-R/C	B/S/Br&Sw
13b	SF-R/C	B/L/Br&Sw
12b"	SF-R/B	C/L/IDLE
13a"	RR-R/C	B/S/IDLE
13b"	SF-R/C	B/L/IDLE

FIGURE I.10/G.841

Four-fibre MS shared protection ring – Unidirectional SF-R plus unidirectional SF-R on non-adjacent spans (transoceanic application)