INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.841

(10/98)

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

Digital transmission systems – Digital networks – SDH network characteristics

Types and characteristics of SDH network protection architectures

ITU-T Recommendation G.841

(Previously CCITT Recommendation)

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
INTERNATIONAL ANALOGUE CARRIER SYSTEM	
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TESTING EQUIPMENTS	
TRANSMISSION MEDIA CHARACTERISTICS	G.600–G.699
DIGITAL TRANSMISSION SYSTEMS	
TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
General aspects	G.800–G.809
Design objectives for digital networks	G.810–G.819
Quality and availability targets	G.820–G.829
Network capabilities and functions	G.830–G.839
SDH network characteristics	**G.840–G.849**
Telecommunications management network	G.850–G.859
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999

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

ITU-T RECOMMENDATION G.841

TYPES AND CHARACTERISTICS OF SDH NETWORK PROTECTION ARCHITECTURES

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.

Source

ITU-T Recommendation G.841 was revised by ITU-T Study Group 15 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 13th of October 1998.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the 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.

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

NOTE

In this Recommendation the term *recognized operating agency (ROA)* includes any individual, company, corporation or governmental organization that operates a public correspondence service. The terms *Administration, ROA* and *public correspondence* are defined in the *Constitution of the ITU (Geneva, 1992)*.

INTELLECTUAL PROPERTY RIGHTS

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

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

CONTENTS

Page

Page

Page

Recommendation G.841

TYPES AND CHARACTERISTICS OF SDH NETWORK PROTECTION ARCHITECTURES

(revised in 1998)

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 scenarios 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 (1996), *Network node interface for the Synchronous Digital Hierarchy (SDH).*

– CCITT Recommendation G.774 (1992), *Synchronous Digital Hierarchy (SDH) management information model for the network element view*.

– ITU-T Recommendation G.783 (1997), *Characteristics of Synchronous Digital Hierarchy (SDH) equipment functional blocks.*

– ITU-T Recommendation G.784 (1994), *Synchronous Digital Hierarchy (SDH) management.*

– ITU-T Recommendation G.803 (1997), *Architectures of transport networks based on the Synchronous Digital Hierarchy (SDH).*

3 Terms and definitions

This Recommendation defines the following terms:

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: Normal or extra traffic inserted into working, protection, or non-pre-emptible unprotected channels on the ring at a ring node.

3.4 Administrative Unit (AU): See Recommendation G.707.

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 APS request: That set of signals into an APS controller that determines its behaviour. An APS request can be either an externally initiated command or an automatically initiated command.

3.7 AU-AIS: See Recommendation G.783.

3.8 AU pointer: See Recommendation G.707.

3.9 automatically initiated command: An APS request that is initiated by any one of the following: 1) multiplex section performance criteria; 2) local equipment performance criteria; or 3) received bridge requests.

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

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

3.12 bidirectional protection switching: A protection switching architecture in which, for a unidirectional failure (i.e. a failure affecting only one direction of transmission), both directions (of the "trail", "subnetwork connection", etc.) including the affected direction and the unaffected direction, are switched to protection.

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

3.14 Bit Interleaved Parity N (BIP-N): See Recommendation G.707.

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

3.16 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 normal traffic signals onto the protection channels.

3.17 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.

3.18 container: See Recommendation G.707.

3.19 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.

3.20 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).

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

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

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

3.24 diverse routing of go & return: Bidirectional transport entity/signal (i.e. go and return) is set up on/routed over different physical facilities. Such routing may apply to individual trails, subnetwork connections, or signals. This is illustrated in Figure 3-2.

3.25 diverse routing of [trail/SNC] protection pair: Diverse routing of a working trail/SNC and its associated protection trail/SNC – where the working trail/SNC (in both directions of transmission) takes one (physical) route, and the protection trail/SNC (in both directions of transmission) takes another.

3.26 drop traffic: Normal or extra traffic extracted from working, protection, or non-pre-emptible unprotected channels on the ring at a ring node.

3.27 externally initiated command: An APS request that is initiated by either an OS or a craftsperson.

3.28 extra traffic: Traffic that is carried over the protection channels when that capacity is not used for the protection of normal traffic. Extra traffic is not protected. Whenever the protection channels are required to protect the normal traffic, the extra traffic is pre-empted.

3.29 full pass-through: The action of transmitting the same K1, K2, and protection channels that are being received. Full pass-through may be either unidirectional or bidirectional as specified in the text. When a node enters unidirectional full pass-through, it shall continue sourcing the previously sourced K-bytes in the opposite direction, with the exception that K2 bits 6-8 shall reflect the appropriate status code.

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

3.31 higher order virtual container: See Recommendation G.707.

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

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

3.34 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.

3.35 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.

3.36 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.

3.37 Loss Of Frame (LOF): See Recommendation G.783.

3.38 Loss Of Signal (LOS): See Recommendation G.783 for SDH systems, and G.775 for PDH systems.

3.39 lower order virtual container: See Recommendation G.707.

3.40 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.

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

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

3.43 Multiplex Section (MS): See Recommendation G.803.

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

3.45 Multiplex Section Remote Defect Indication (MS-RDI): Formerly known as multiplex section far end remote failure. See Recommendation G.707.

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

3.47 network node interface (NNI): See Recommendation G.707.

3.48 non-pre-emptible unprotected channel: A channel in a MS shared protection ring provisioned bidirectionally to provide transport without MS shared protection ring automatic protection switching. Non-pre-emptible unprotected channels are provisioned from (corresponding) working and protection channel pairs.

3.49 non-pre-emptible unprotected traffic: Unprotected traffic carried on protection locked-out channel which may not be pre-empted (e.g. by protection switches).

3.50 normal traffic: Traffic that is normally carried in the working channels/sections, except in the event of a protection switch, in which case it is restored on the protection channels/sections. Normal traffic is protected.

3.51 null signal: The null signal is indicated on the protection channels if they are not used to carry normal or extra traffic. The null signal can be any kind of signal that conforms to the signal structure of the specific layer and is ignored (not selected) at the tail-end of the protection.

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

3.53 path: See Recommendation G.803.

3.54 path overhead: See Recommendation G.707.

3.55 protection channels: The channels allocated to transport the normal traffic during a switch event. Protection channels may be used to carry extra traffic in the absence of a switch event. When there is a switch event, normal traffic on the affected working channels is bridged onto on the protection channels.

3.56 regenerator section: See Recommendation G.803.

3.57 remote error indication: Formerly far-end block error. See Recommendation G.707.

3.58 restoral threshold: For automatically initiated commands, a hysteresis method is used when switching normal traffic 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.

3.59 restoration: See Recommendation G.803.

3.60 **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.

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

3.62 **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.

3.63 **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.

3.64 **section overhead**: See Recommendation G.707.

3.65 **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).

3.66 **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.

3.67 **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.

3.68 **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.

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

3.70 **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 normal traffic is carried over the protection channels on the same span as the failure.

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

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

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

3.74 **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.

3.75 **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.

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

3.77 **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.

3.78 **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.

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

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

3.81 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.

3.82 Time Slot Interchange (TSI): For purposes of this Recommendation, TSI is the capability of changing the time slot position of through-connected traffic (i.e. traffic that is not added or dropped from the node).

3.83 trail: See Recommendation G.803.

3.84 trail protection: Normal traffic is carried over/selected from a protection trail instead of a working trail if the working trail fails, or if its performance falls below a required level.

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

3.86 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.

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

3.88 unidirectional protection switching: A protection switching architecture in which, for a unidirectional failure (i.e. a failure affecting only one direction of transmission), only the affected direction (of the "trail", "subnetwork connection", etc.) is switched to protection.

3.89 unidirectional ring: In a unidirectional ring (path switched or multiplex section switched), normal routing of the normal 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.

3.90 uniform routing of go & return: Bidirectional transport entity/signal (i.e. go and return) is set up on/routed over the same physical facilities. Such routing may apply to individual trails, subnetwork connections, or signals. This is illustrated in Figure 3-2.

3.91 virtual container (VC): See Recommendation G.707.

3.92 working channels: The channels over which normal traffic is transported when there are no switch events.

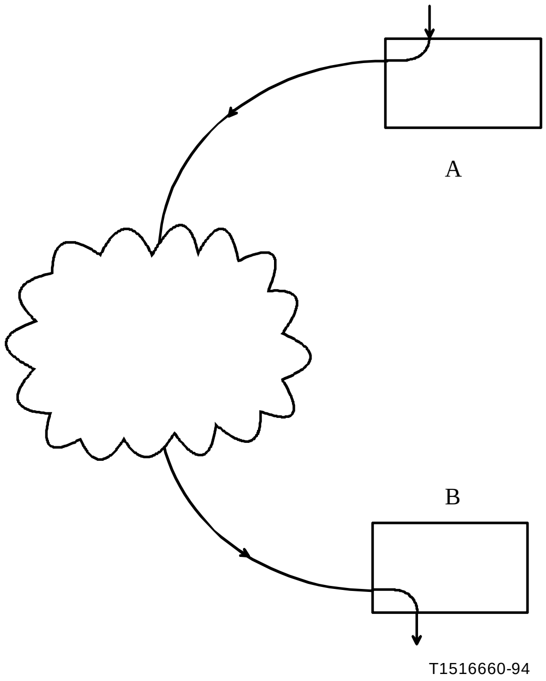
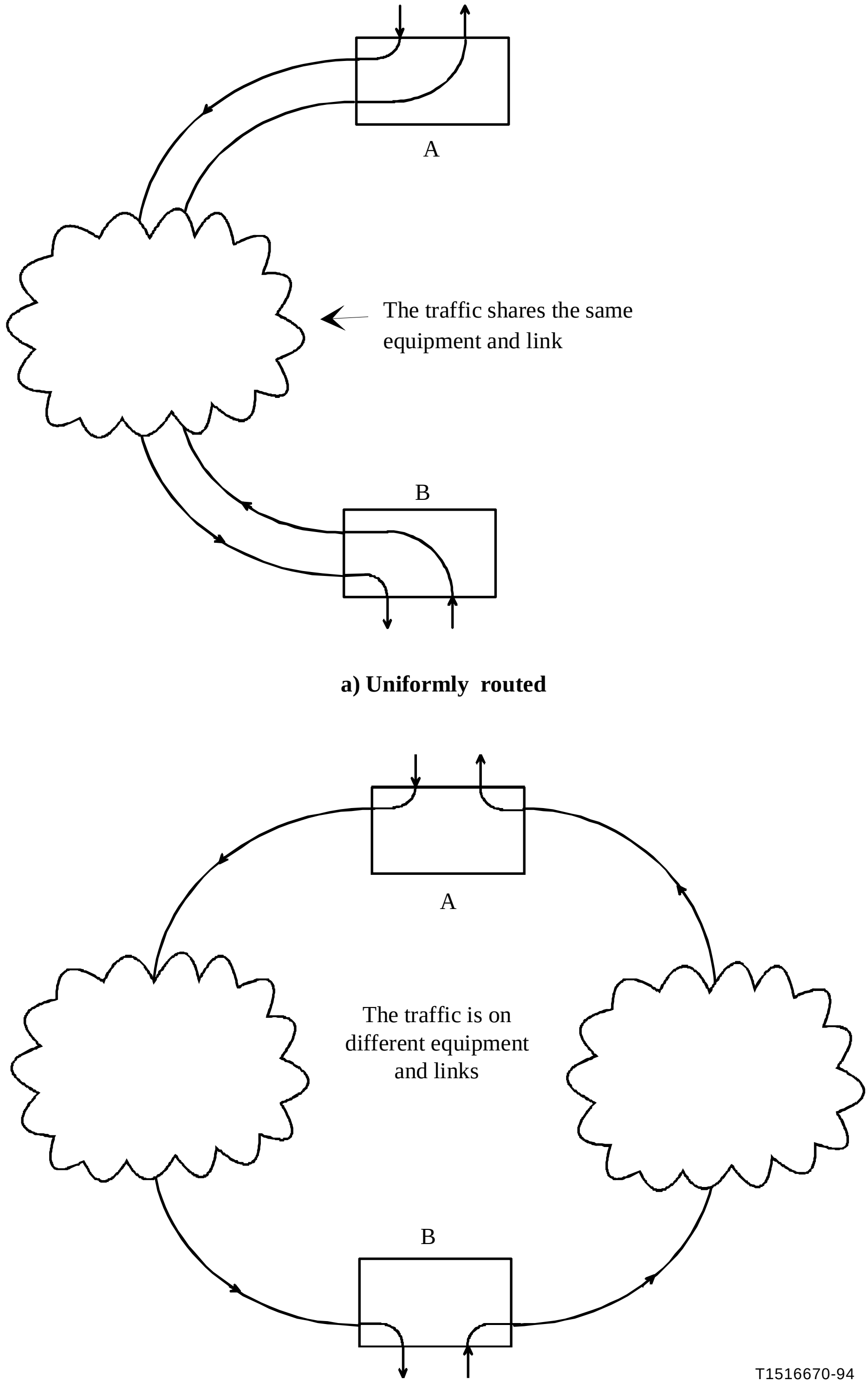


Figure 3-1/G.841 – Unidirectional connection


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

a) Uniformly routed

b) Diversely routed

Figure 3-2/G.841 – Uniformly routed and diversely routed bidirectional connection

4 Abbreviations

This Recommendation uses the following abbreviations:

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
BLSR	Bidirectional Line Switched Rings
Br	Bridge(d)
CP	Connection Point
DCC	Data Communications Channel
DCN	Data Communications Network
ET	Extra Traffic
EXER-R	Exerciser - Ring
EXER-S	Exerciser - Span
FS-P	Forced Switch to Protection
FS-R	Forced Switched Normal Traffic to Protection - Ring
FS-S	Forced Switched Normal Traffic to Protection - Span
FS-W	Forced Switch Normal Traffic to Working
HO	Higher Order
HO VC	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
LO VC	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 Normal Traffic to Protection - Ring
MS-S	Manual Switch Normal Traffic to Protection - Span
MS-W	Manual Switch Normal Traffic to Working
NE	Network Element
NNI	Network Node Interface
NR	No Request
NUT	Non-pre-emptible unprotected traffic
OAM&P	Operations, Administration, Maintenance & 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

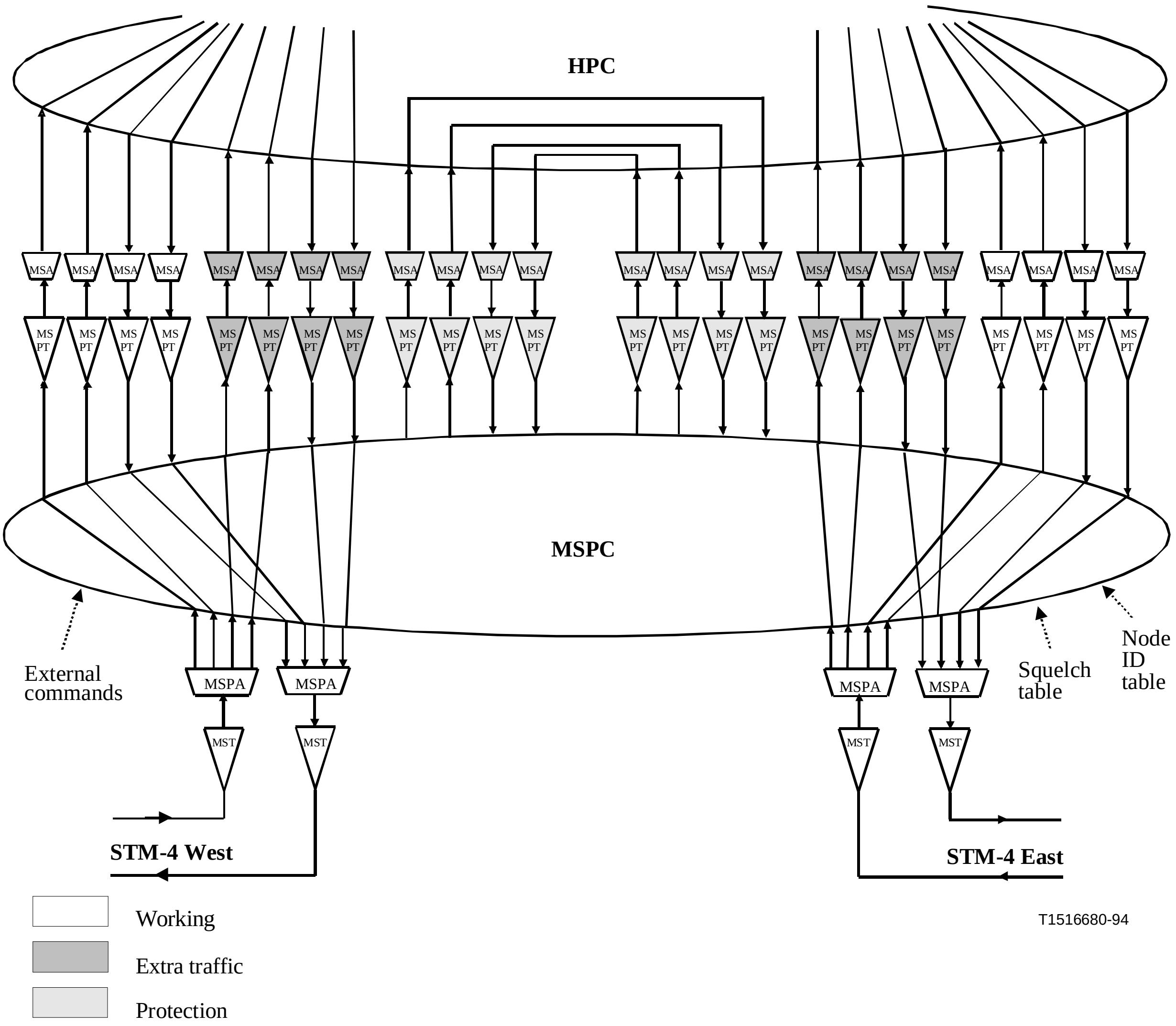
5 Protection classifications

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 an 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 connections. 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.

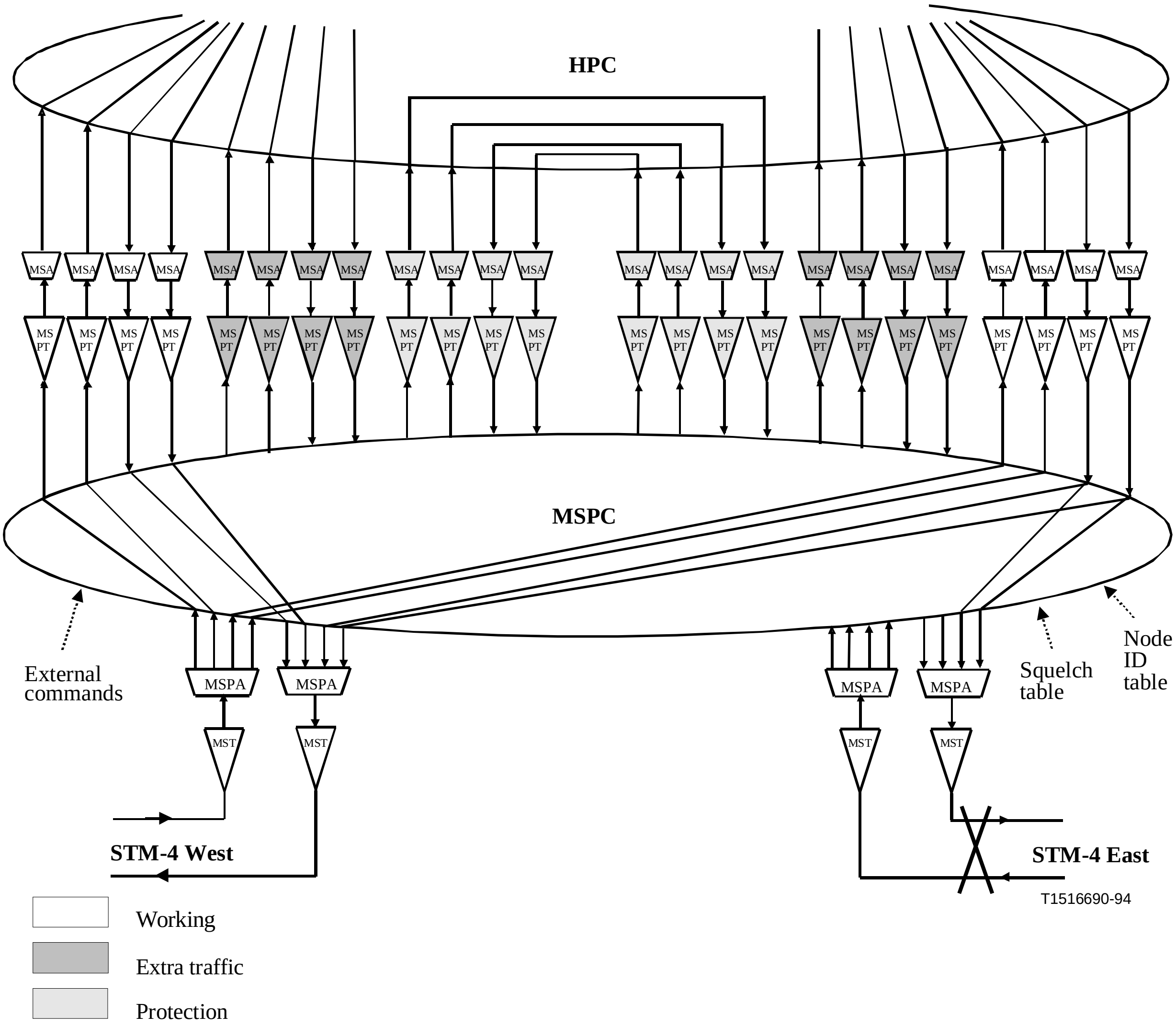
Figure 5-4 shows the generic functional model for 1 + 1 VC trail protection. Figure 5-5 shows the generic functional model for 1:1 revertive VC trail protection and Figure 5-6 shows the generic functional model for 1:1 non-revertive VC trail protection.

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).



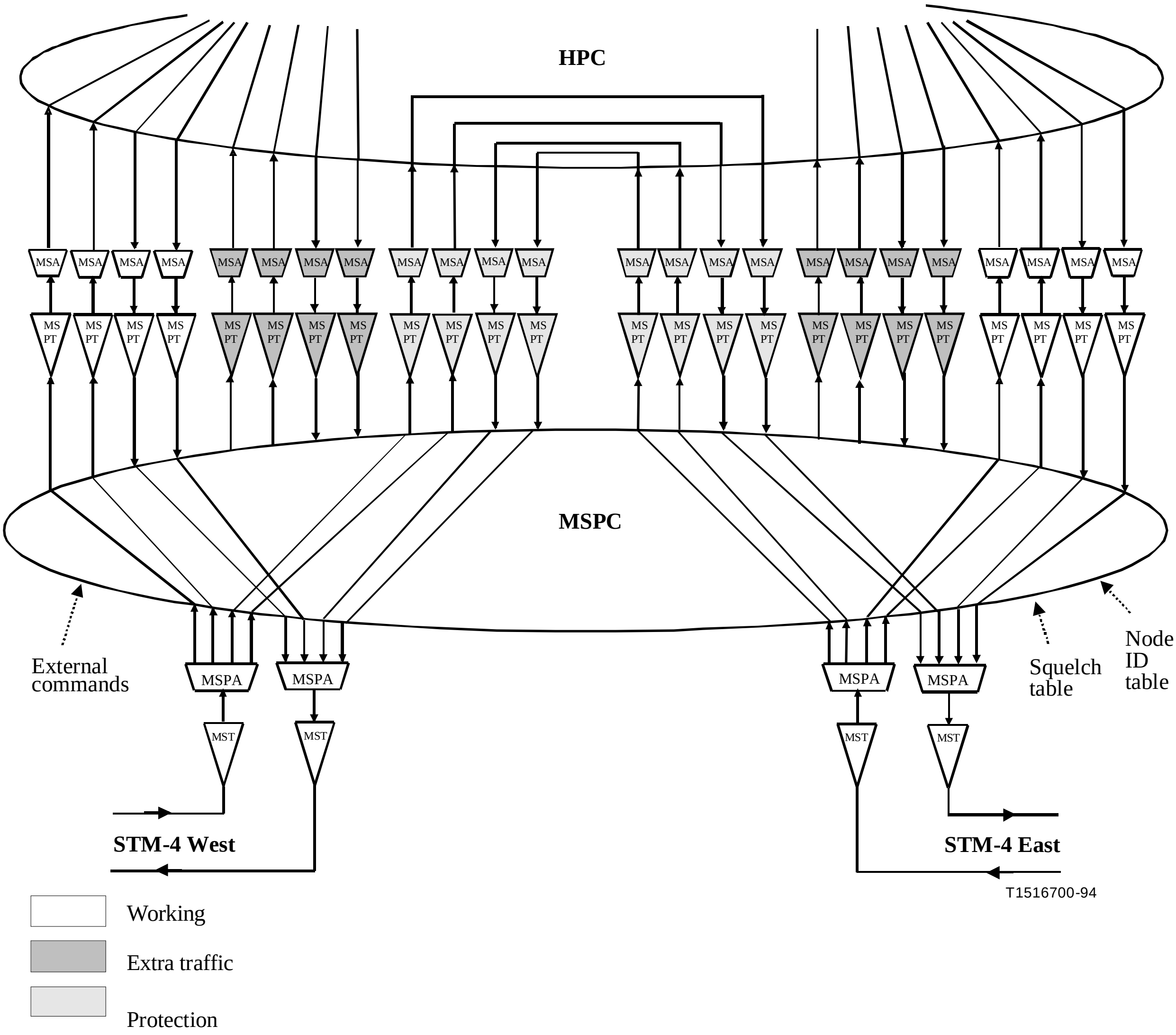
HPC	Higher order Path Connection
MSA	Multiplex Section Adaptation
MSPA	Multiplex Section Protection Adaptation
MSPC	Multiplex Section Protection Connection
MSPT	Multiplex Section Protection Termination
MST	Multiplex Section Termination

Figure 5-1/G.841 – Functional model for a two-fibre protection ring – Normal state with extra traffic



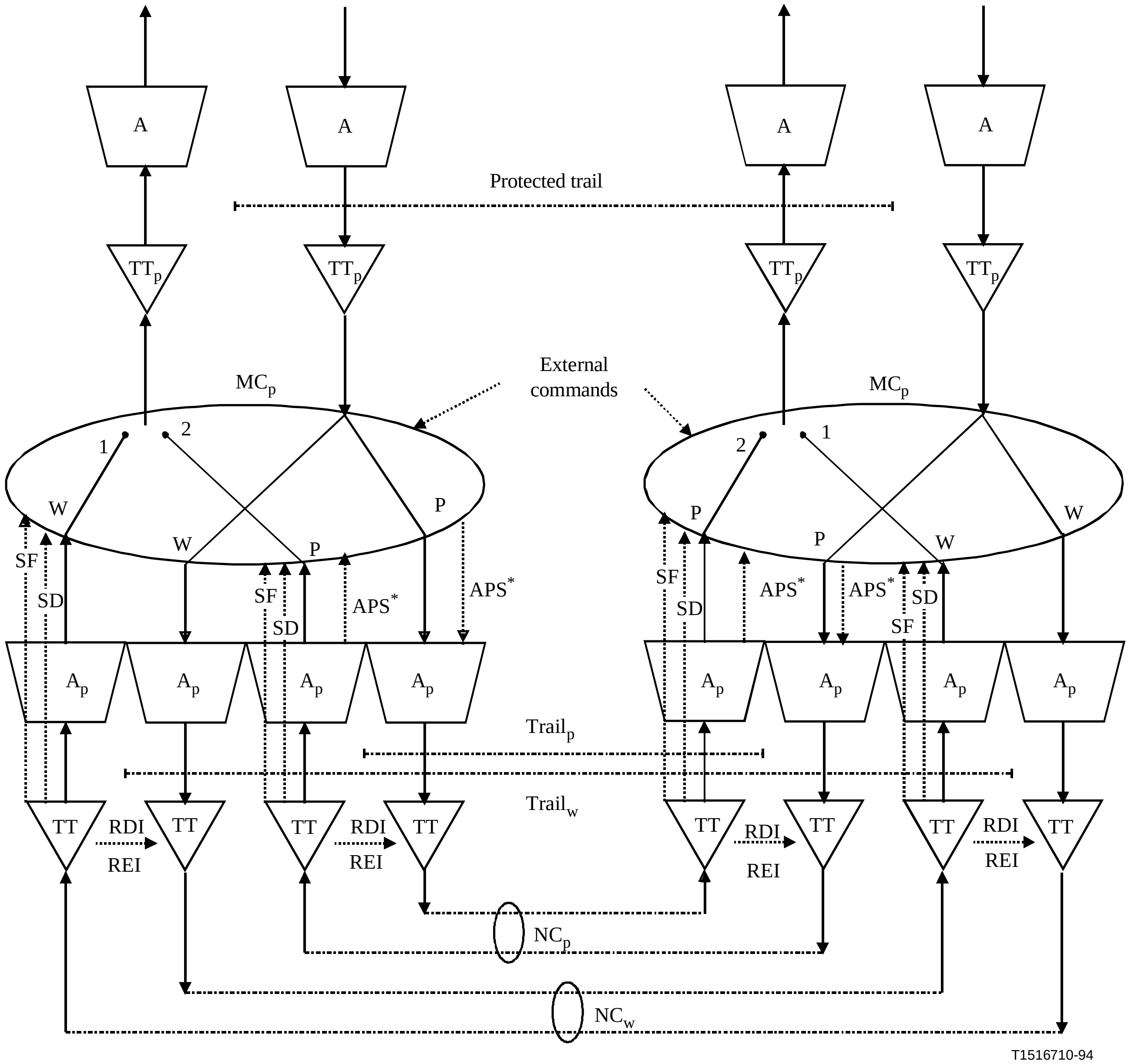
HPC	Higher order Path Connection
MSA	Multiplex Section Adaptation
MSPA	Multiplex Section Protection Adaptation
MSPC	Multiplex Section Protection Connection
MSPT	Multiplex Section Protection Termination
MST	Multiplex Section Termination

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

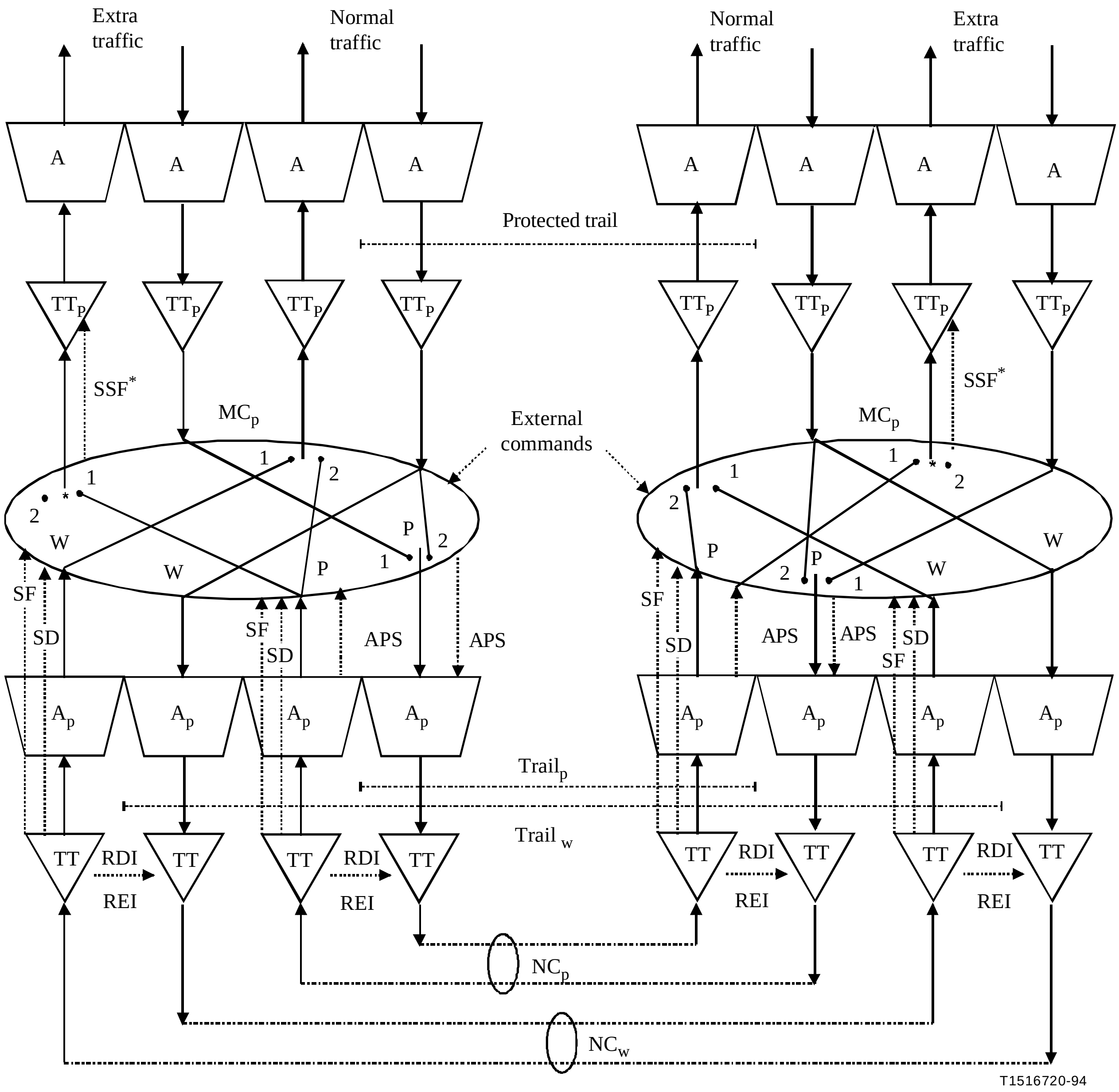


* Required for dual-ended switching.
Not required for single-ended switching.

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

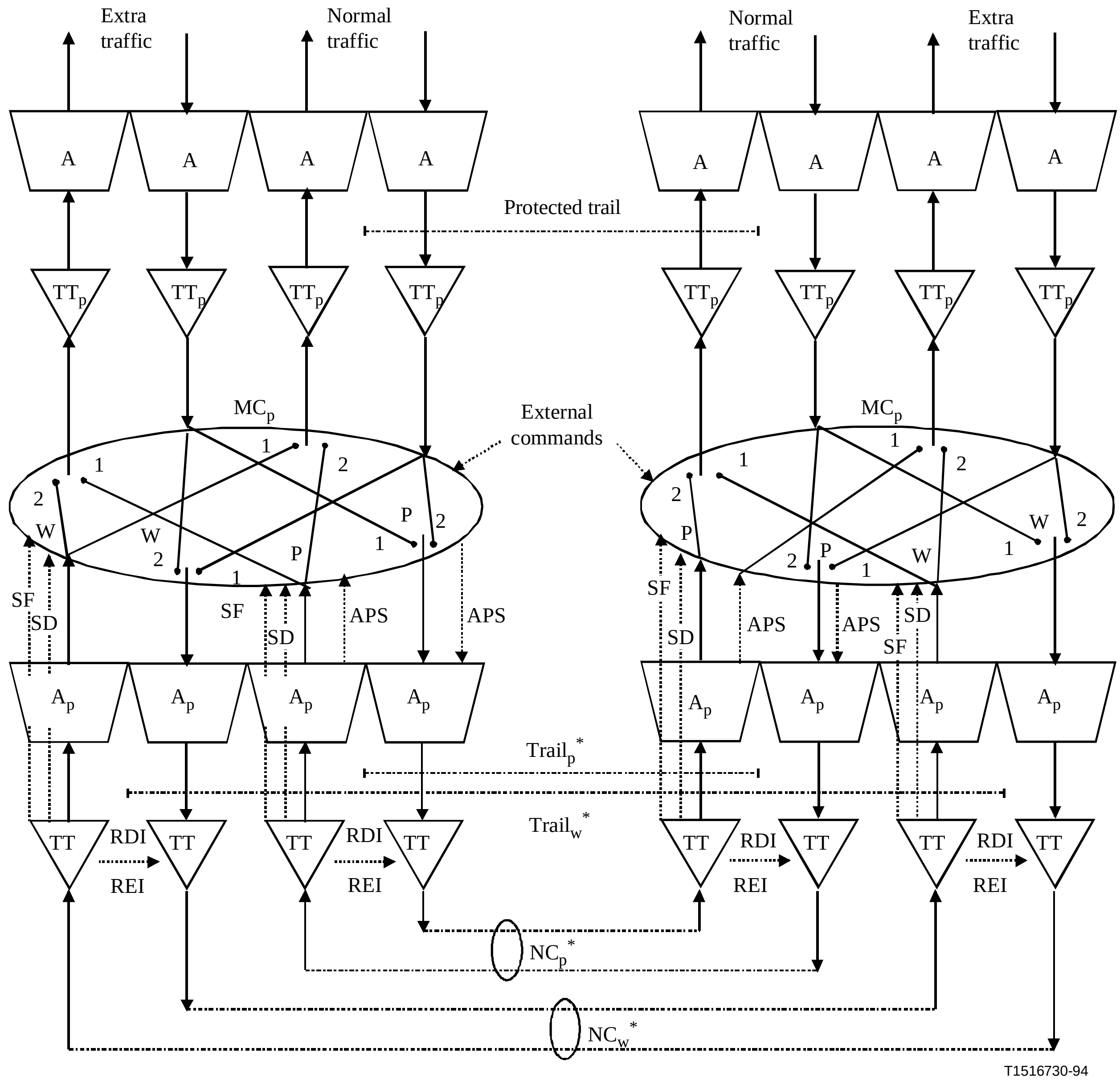


* SSF active on open connection [Failure state (2)]. This is for further study.

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

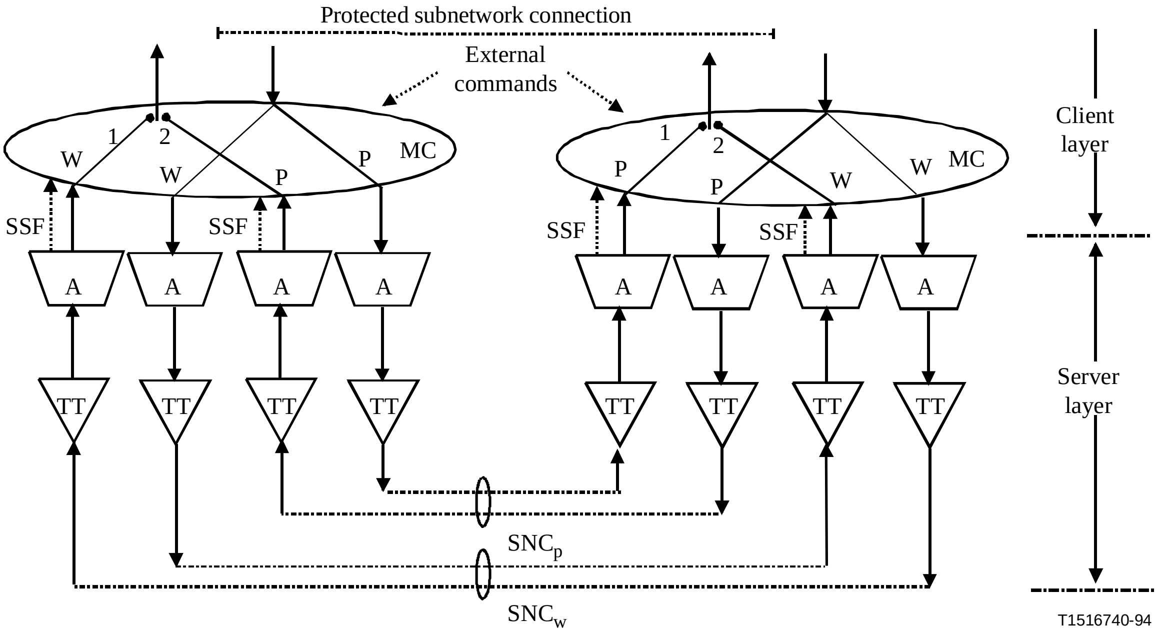


* On failure state (2), Trail_p becomes Trail_w, Trail_w becomes Trail_p, NC_p becomes NC_w, and NC_w becomes NC_p.

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

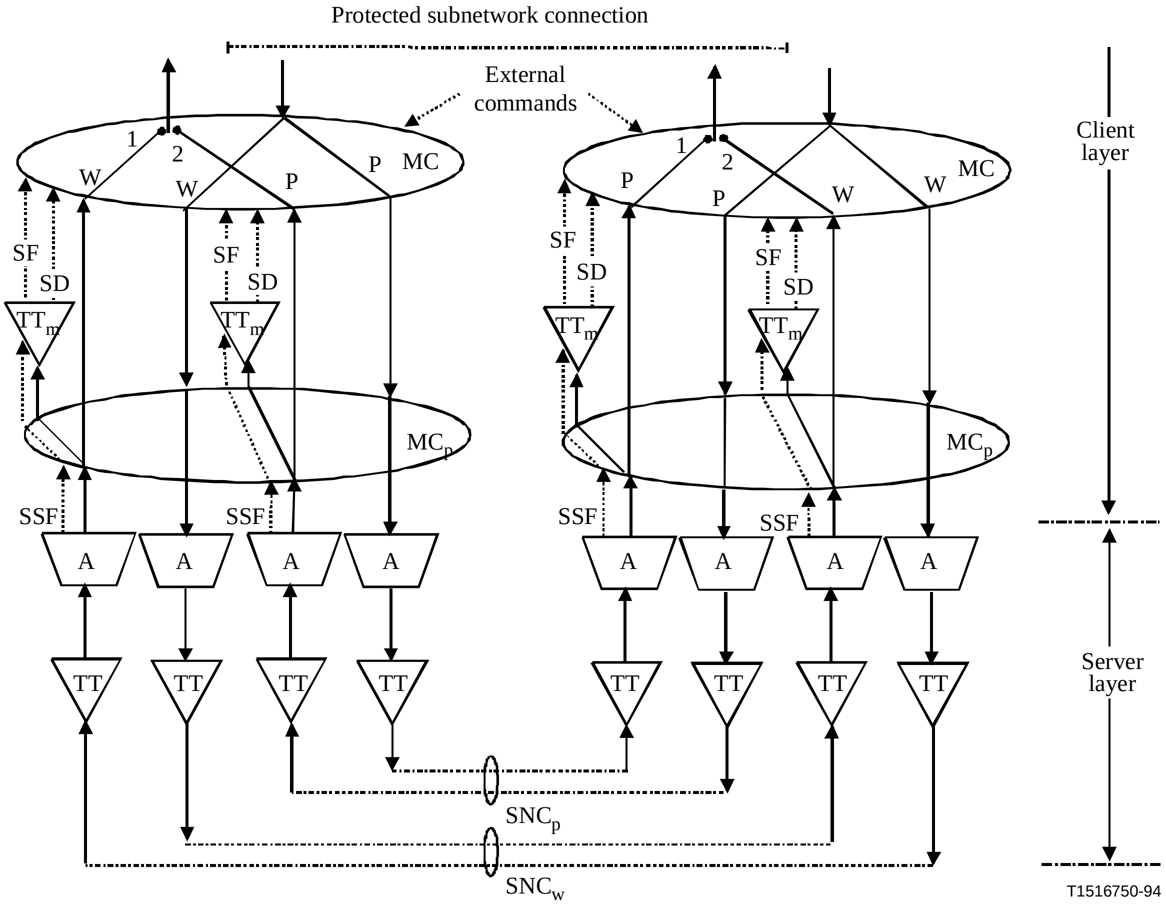
Figure 5-6/G.841 – Functional model for generic 1:1 linear trail protection – Non-revertive operation



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 the normal traffic signals to be protected while the protection channels are reserved for protection of this service. Protection channels may be used to carry extra traffic when not being used for protection of normal traffic. Normal traffic signals are 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 normal traffic signals, they can be used to carry extra traffic signals. In the event of a protection switch, the normal traffic on the working channels will access the protection channels causing any extra traffic to be removed from the protection channels.

During a ring switch, normal traffic transmitted toward the failed span is 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 normal traffic from the protection channels are switched back onto the working channels. In the other direction, the normal traffic is 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.

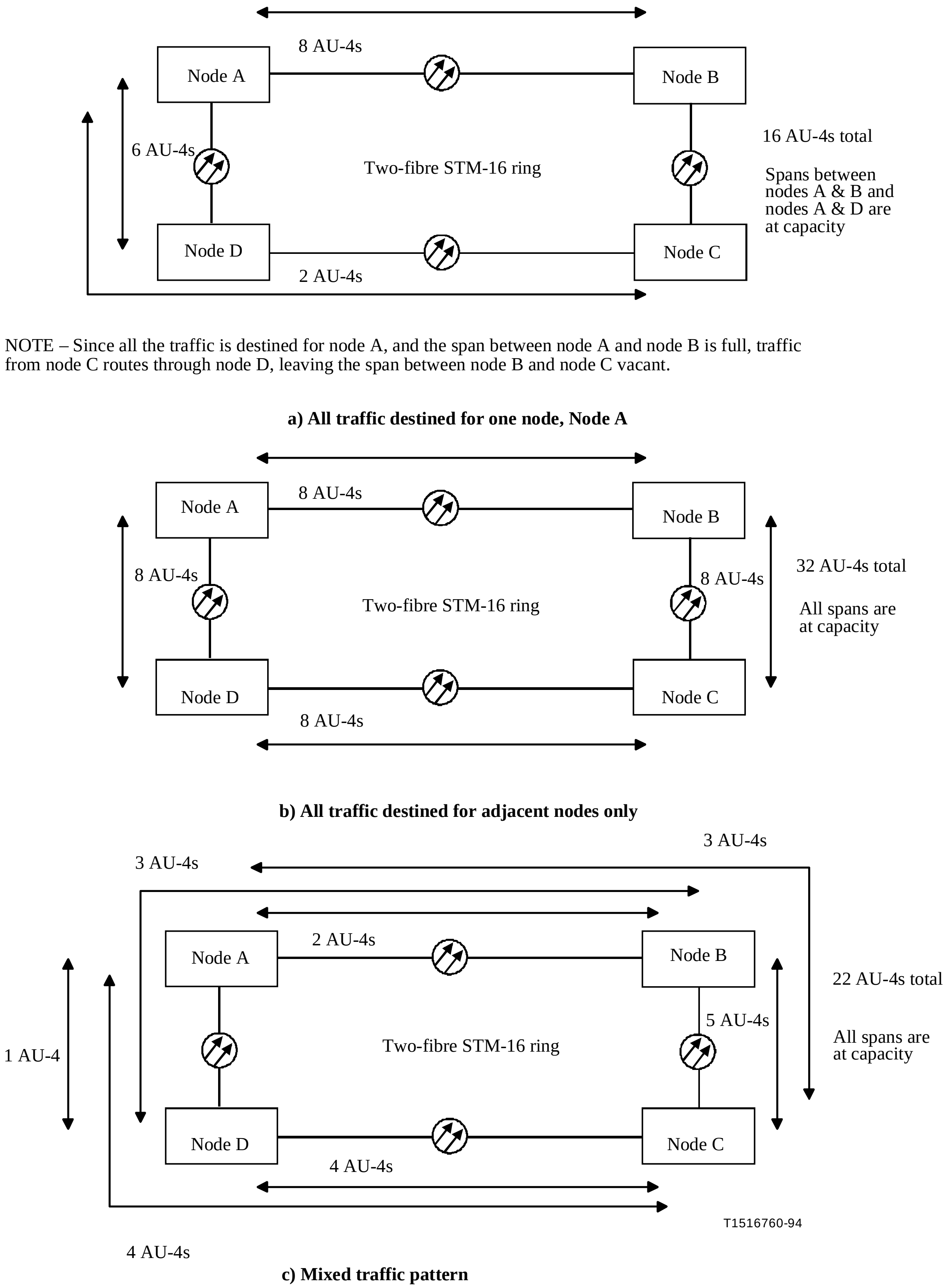
MS SPRING protocols allow the available bandwidth to be partitioned into three types of channels: working channel to carry normal traffic, protection channel which may be used to carry extra traffic, and NUT channel to carry non-pre-emptible unprotected traffic. Normal traffic is protected against failure events via the MS SPRING APS protocol, while extra traffic is unprotected traffic carried on the protection channels. Any failure event that may require the protection channels for protection purposes shall pre-empt the extra traffic.

Non-pre-emptible unprotected traffic is unprotected traffic that is carried on channels with the MS SPRING APS protection switching mechanism disabled for certain HO VC channels (i.e. working channels and their corresponding protection channels). Traffic carried on these channels is unprotected and non-pre-emptible. Thus, NUT carried on non-pre-emptible unprotected channels afford a higher level of survivability as compared to extra traffic, but lower level of survivability as compared to normal traffic.

Examples of how NUT channels can be used are given in Figures 6-3 and 6-4:

– Figure 6-3 shows a logical ring in which SNCP is used as a protection mechanism partially embedded in an MS SPRING using NUT. This arrangement avoids unnecessary layering of protection mechanisms and is more bandwidth efficient than the same application without NUT.

– Figure 6-4 shows a similar application, this time with the NUT channels supporting HO VC connectivity among ATM switches. Under the assumption that the ATM traffic is protected by other means or does not need to be protected, this application of NUT has the same advantages as the previous example.



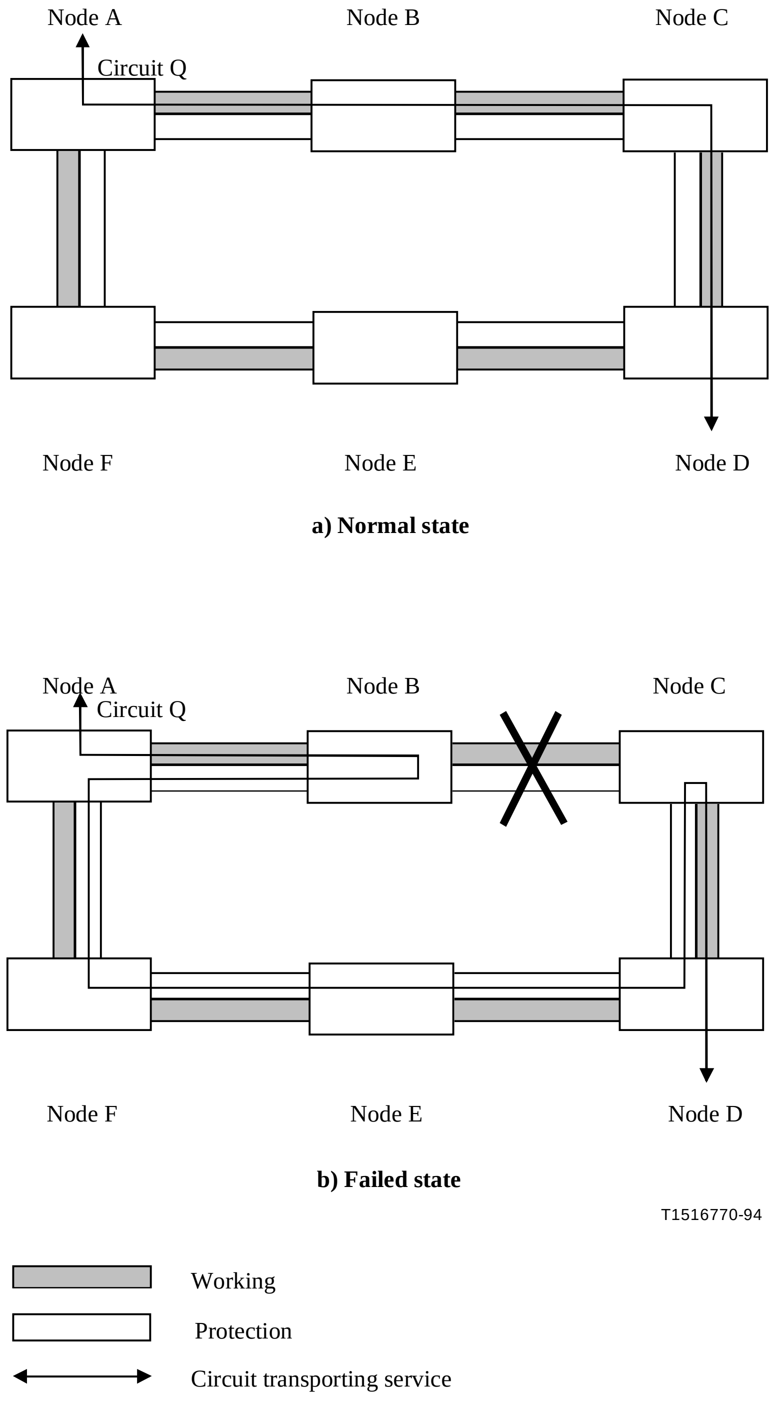
NOTE – Since all the traffic is destined for node A, and the span between node A and node B is full, traffic from node C routes through node D, leaving the span between node B and node C vacant.

a) All traffic destined for one node, Node A

b) All traffic destined for adjacent nodes only

c) Mixed traffic pattern

Figure 6-1/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

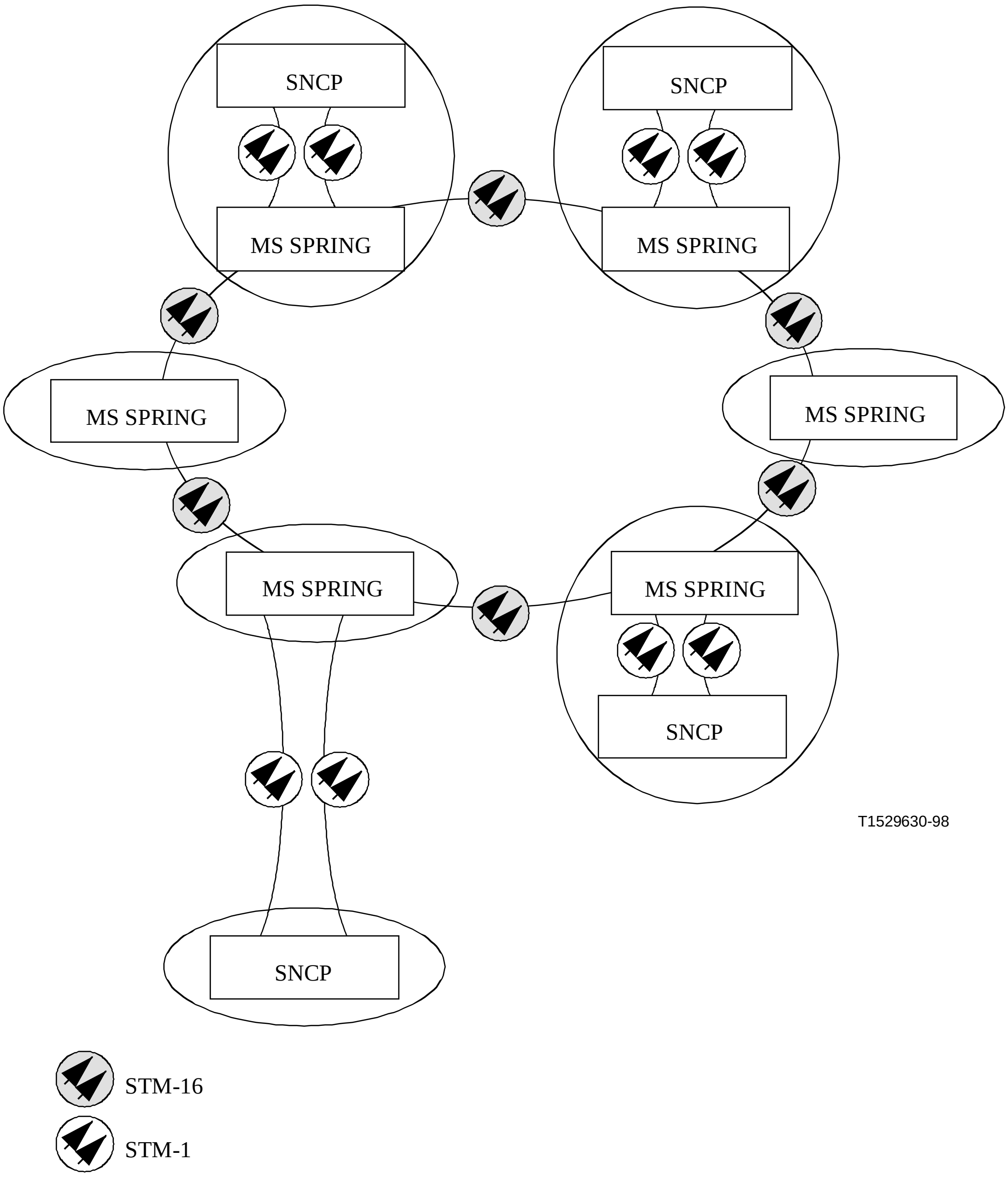


Figure 6-3/G.841 – Logical ring in which SNCP is used as a protection mechanism partially embedded in an MS shared protection ring

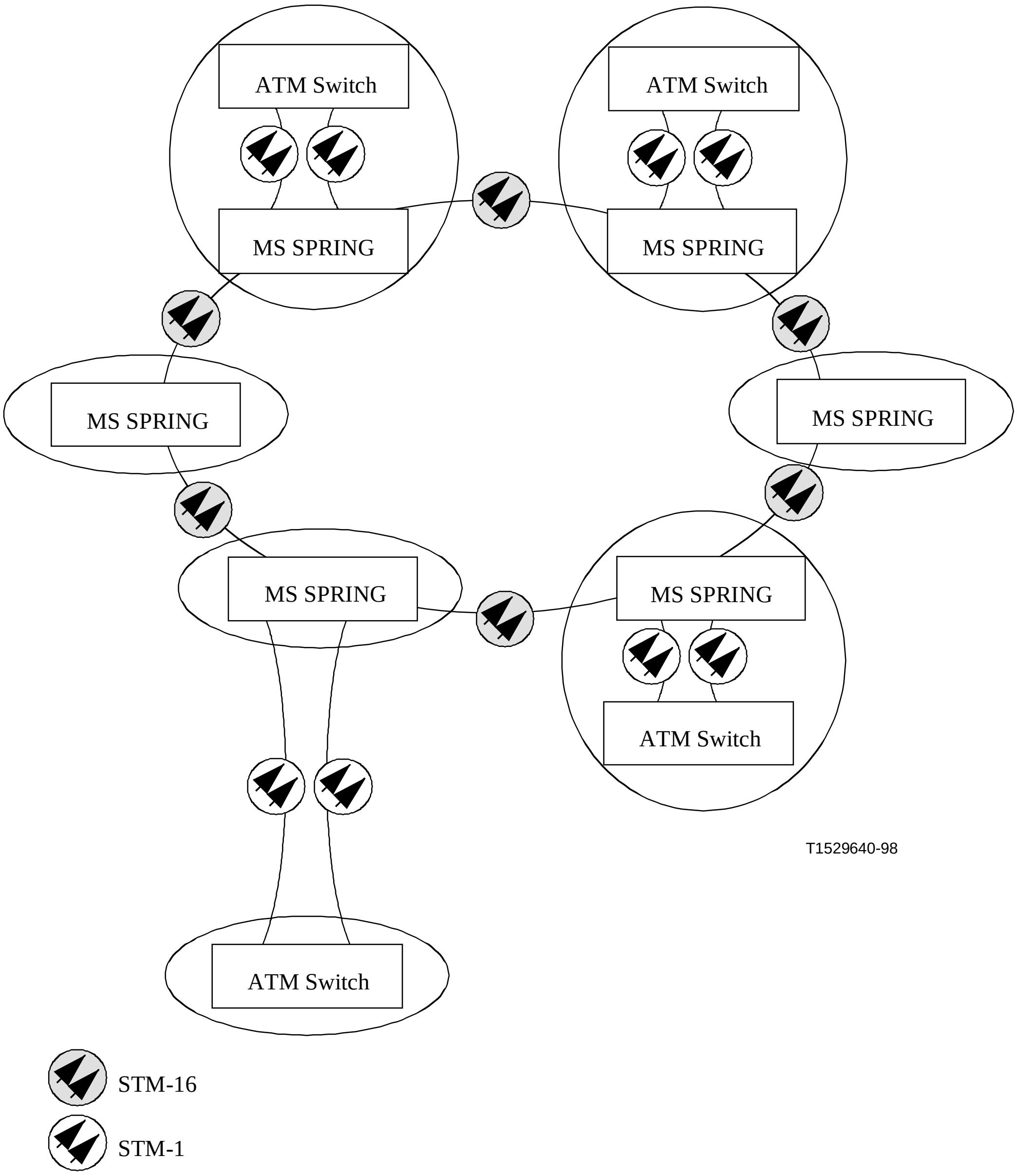


Figure 6-4/G.841 – NUT Channels supporting HO VC connectivity among ATM switches

6.2 MS shared protection rings (transoceanic application)

This application, including its additional requirements and operating characteristics, are 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 normal traffic to be protected while the other is reserved for protection of this normal 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.

6.4 Unidirectional and bidirectional protection switching

Possible advantages of unidirectional protection switching include:

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

2) Unidirectional protection switching can be faster than bidirectional protection switching because it does not require a protocol.

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

Possible advantages of bidirectional protection switching when uniform routing is used include:

1) With bidirectional protection switching 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 bidirectional protection 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) Bidirectional protection switching is easier to manage because both directions of transmission use the same equipments along the full length of the trail.

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

5) Bidirectional protection switching also has the ability to carry extra traffic on the protection 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 switching can operate in a unidirectional or bidirectional manner. Bidirectional protection 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 paths segments are available) between two Connection Points (CPs) or between a CP and a Termination Connection Point (TCP), or the full end-to-end path between two TCPs. It switches on server failures (using inherent monitoring) or it switches using client layer information (using non-intrusive monitoring).

SNC protection is a linear protection scheme which can be applied on an individual basis to VC-n signals. It need not be used on all VCs within a multiplex section. It need not be used on all LO VCs within a HO VC.

The individual HO VCs [LO VCs] transported within the network may either be all unprotected, all 1 + 1 HO VC [LO VC] SNC/I protected, all 1 + 1 HO VC[LO VC] SNC/N protected, all HO VC [LO VC] trail protected (see 6.5), or a mixture of unprotected, 1 + 1 HO VC [LO VC] SNC/I protected, 1 + 1 HO VC [LO VC] SNC/N protected and HO VC [LO VC] trail protected.

HO VCs [LO VCs] which are unprotected at their own HO [LO] path layer may be protected indirectly at their server layer; e.g. a HO VC signal in a MS Spring protected ring is protected against faults in the ring by means of MS Spring protection.

On the other hand, client signals transported within an unprotected HO VC (e.g. LO VCs, ATM VPs) may be protected by means of their client layer protection schemes (e.g. LO VC SNC protection, ATM VP SNC protection).

The decision to protect a signal and the actual protection type used are outside the scope of this Recommendation: this is determined by the network architecture and the quality of service needs.

SNC protection operates in a unidirectional protection switching manner. The ability to perform bidirectional protection switching and the carriage of extra traffic is for further study.

6.7 Linear multiplex section protection switching

Linear multiplex section protection switching 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 the normal traffic from a number (N) of working multiplex sections. It cannot protect against node failures. It can operate in a unidirectional or bidirectional manner, and it can carry extra traffic on the protection multiplex section in bidirectional operation.

7 SDH trail protection

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

7.1 Linear multiplex section protection

This subclause describes the MSP protocol compatible with 1:n operation. Annex B describes the MSP protocol optimized for 1 + 1 non-revertive operation.

7.1.1 MSP protocol

The MSP functions, at the ends of a multiplex section, make requests for and give acknowledgements of switch action by using the APS bytes (K1 and K2 bytes in the MSOH of the protection section). The bit assignments for these bytes and the bit-oriented protocol are defined as follows.

7.1.1.1 K1 byte

The K1 byte indicates a request of a traffic signal for switch action.

Bits 1-4 indicate the type of request, as listed in Table 7-1. A request can be:

1) a condition (SF and SD) associated with a section. A condition has high or low priority. The priority is set for each corresponding section;

2) a state (wait-to-restore, do not revert, no request, reverse request) of the MSP function; or

3) an external request (lockout of protection, forced or manual switch, and exercise).

Bits 5-8 indicate the number of the traffic signal or section for which the request is issued, as shown in Table 7-2.

Table 7-1/G.841 – Types of request

Bits	**Condition, state or external request**	**Order (Note 1)**
1 2 3 4		
1 1 1 1	Lockout of protection (Note 2)	Highest
1 1 1 0	Forced switch	↑
1 1 0 1	Signal fail high priority	.
1 1 0 0	Signal fail low priority	.
1 0 1 1	Signal degrade high priority	.
1 0 1 0	Signal degrade low priority	.
1 0 0 1	Unused (Note 3)	.
1 0 0 0	Manual switch	.
0 1 1 1	Unused (Note 3)	.
0 1 1 0	Wait-to restore	.
0 1 0 1	Unused (Note 3)	.
0 1 0 0	Exercise	.
0 0 1 1	Unused (Note 3)	.
0 0 1 0	Reverse request	.
0 0 0 1	Do not revert	↓
0 0 0 0	No request	Lowest

NOTE 1 – An SF condition on the protection section is higher priority than any of the requests that would cause a normal traffic signal to be selected from the protection section.

NOTE 2 – Only the null signal (0) is allowed with a Lockout of Protection request.

NOTE 3 – Some network operators may use these codes for network specific purposes. The receiver shall be capable of ignoring these codes.

NOTE 4 – Requests are selected from the table depending on the protection switching arrangements; i.e. in any particular case, only a subset of the requests may be required.

Table 7-2/G.841 – K1 traffic signal number

Signal number	Requesting switch action
0	Null signal (no normal or extra traffic signal). Conditions and associated priority (fixed high) apply to the protection section.
1-14	Normal traffic signal (1-14) Conditions and associated priority (high or low) apply to the corresponding working sections. For 1 + 1 only traffic signal 1 is applicable, with fixed high priority. 1 + 1 systems may treat (incorrect) low priority request received over the K-bytes as equivalent to the corresponding high priority request.
15	Extra traffic signal Conditions are not applicable. Exists only when provisioned in a 1:n architecture.

7.1.1.2 K1 byte generation rules

Local SF and SD conditions, wait-to-restore or do-not-revert state and the external request are evaluated by a priority logic, based on the descending order of request priorities in Table 7-1. If local conditions (SF or SD) of the same level are detected on different sections at the same time, the condition with the lowest section number takes priority. Of these evaluated requests, the one of the highest priority replaces the current local request, only if it is of higher priority.

Locally detected SF and SD conditions and externally initiated requests for normal traffic signals that have "lockout of normal traffic signal from protection" control command (see 7.1.1.2.2) applied to them are not evaluated during K1 byte generation.

7.1.1.2.1 In bidirectional operation

The priorities of the local request and the remote request on the received K1 byte are compared according to the descending order of priorities in Table 7-1. Note that a received reverse request or a remote request for a normal traffic signal that has a "lockout of normal traffic signal from protection" applied to it are not considered in the comparison.

The sent K1 shall indicate:

a) a reverse request if the remote bridge request is for a traffic signal that is not locked out and;

   i) the remote request is of higher priority, or if

   ii) the requests are of the same level (and are higher priority than a no request) and the sent K1 byte already indicates reverse request, or if

   iii) the requests are of the same level (and are higher priority than a no request) and the sent K1 byte does not indicate reverse request and the remote request indicates a lower traffic signal number;

b) the local request in all other cases.

7.1.1.2.2 In unidirectional operation

The sent K1 byte shall always indicate the local request. Therefore, reverse request is never indicated.

7.1.1.3 Revertive/non-revertive modes

In revertive mode of operation, when the protection is no longer requested, i.e. the failed working section is no longer in SD or SF condition (and assuming no other requesting sections), a local wait-to-restore state shall be activated. Since this state becomes the highest in priority, it is indicated on the sent K1 byte, and maintains the normal traffic signal from the previously failed working section on the protection section. This state shall normally time out and become a no request null signal (0) [or no request extra traffic signal (15), if applicable]. The wait-to-restore timer deactivates earlier if the sent K1 byte no longer indicates wait-to-restore, i.e. when any request of higher priority pre-empts this state.

In non-revertive mode of operation, applicable only to 1 + 1 architecture, when the failed working section is no longer in SD or SF condition, the selection of the normal traffic signal from protection is maintained by activating a do-not-revert state rather than a no-request state.

Both wait-to-restore and do-not-revert requests in the sent K1 byte are normally acknowledged by a reverse request in the received K1 byte. However, no request is acknowledged by another No Request received.

7.1.1.4 K2 byte

Bits 1-5 indicate the status of the bridge in the MSP switch (see Figure 7-1). Bits 6-8 are used for MS-AIS and MS-RDI indication (see Recommendation G.707).

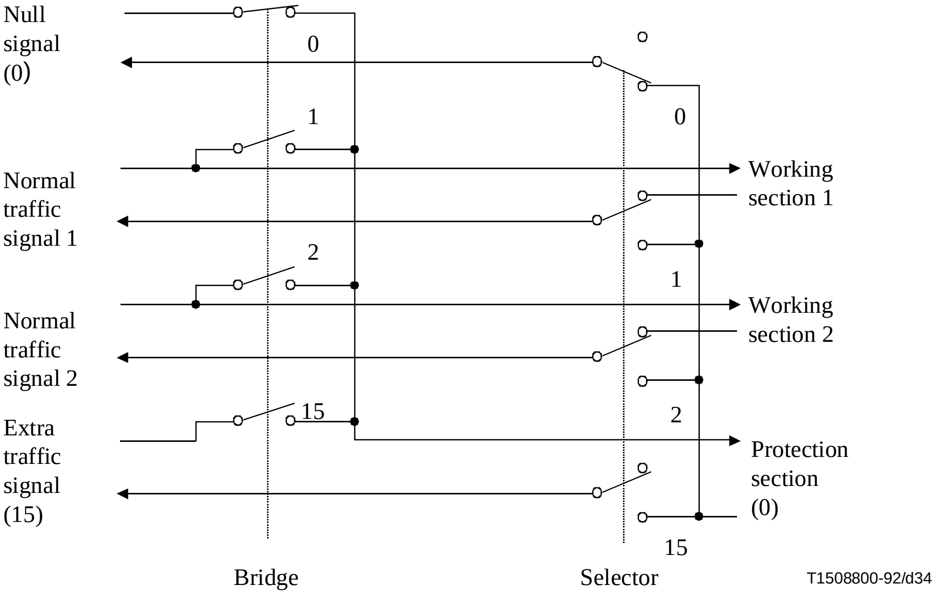


Figure 7-1/G.841 – MSP switch – 1:n architecture (shown in released position)

NOTE – In some regional applications, when MS-RDI is not being generated, bits 6-8 are used to indicate the switching mode (i.e. unidirectional, using code 100, and bidirectional, using code 101). Such applications are outside the scope of this Recommendation.

Bits 1-4 indicate a signal number, as shown in Table 7-3. Bit 5 indicates the type of the MSP architecture: set 1 indicates 1:n architecture and set 0 indicates 1 + 1 architecture.

Table 7-3/G.841 – K2 traffic signal number

Traffic signal number	Indication
0	Null traffic signal
1-14	Normal traffic signal (1-14) For 1 + 1, only normal traffic signal 1 is applicable.
15	Extra traffic signal Exists only when provisioned in a 1:n architecture.

7.1.1.5 K2 byte generation rules

The sent K2 byte shall indicate in bits 1 to 4, for all architectures and operation modes, null signal (0) if the received K1 byte indicates null signal and the extra traffic is not bridged. For all other cases the number of the signal which is bridged shall be indicated by the sent K2 byte.

The sent K2 byte shall indicate in bit 5:

a) 0 if 1 + 1 architecture;

b) 1 if 1:n architecture.

7.1.1.6 Control of the bridge

7.1.1.6.1 1 + 1 uni/bidirectional architecture

In 1 + 1 architecture, the working channel 1 is permanently bridged to the working and protection section and thus no bridge control is needed.

7.1.1.6.2 1:n unidirectional architecture

In 1:n unidirectional architecture, the signal number indicated on the received K1 byte is bridged to the protection section. If extra traffic is supported and if the received K1 byte indicates 0 or 15 and the received K1 byte indicates no Lockout of protection request, the extra traffic signal is bridged to the protection section.

If, at the bridge end, the protection section is in SF condition, the bridge is frozen (current bridge maintained).

7.1.1.6.3 1:n bidirectional architecture

In an 1:n bidirectional architecture, the control of the bridge is done by comparing the signal numbers of the received and sent K1 bytes:

a) If the signal number in the received and sent K1 byte indicate the same working traffic signal, the corresponding working traffic signal is bridged to the protection section.

b) If extra traffic is supported and if the signal number in the received K1 byte indicates 0 or 15, and the sent K1 byte also indicates 0 or 15 (all 4 combinations are allowed), and neither the received nor the transmitted K1 byte indicate a Lockout of protection request, the extra traffic signal is bridged to the protection section.

c) If neither a) nor b) are fulfilled or the protection section is in SF condition, the bridge is released (null signal bridged)

7.1.1.7 Control of the selector

7.1.1.7.1 1 + 1 unidirectional architecture

In 1 + 1 architecture in unidirectional operation, the selector is controlled by the highest priority local request. If the protection section is in SF condition, the selector is released.

7.1.1.7.2 1 + 1 bidirectional architecture

In 1 + 1 architecture in bidirectional operation, the selector is controlled by comparing the signal numbers indicated on received K2 and sent K1 bytes. If there is a match, then the indicated signal is selected from the protection section. If there is a mismatch, the selector is released. Note that a match on 0000 also releases the selector. If the mismatch persists for 50 ms, a mismatch is indicated at reference point MSP_MP. If the protection section is in SF condition, the selector is released and the mismatch indication is disabled.

7.1.1.7.3 1:n uni/bidirectional architecture

In a 1:n architecture, the control of the selector is done by comparing the signal numbers of the received K2 byte and the sent K1 byte:

a) If the signal number in the received K2 byte and the sent K1 byte indicate the same working traffic signal, the corresponding working traffic signal is selected from the protection section.

b) If the signal number in the received K2 byte indicates 15 and the sent K1 byte indicates 0 or 15, the extra traffic signal is selected from the protection section.

c) If neither a) nor b) are fulfilled, the selector is released (no signal selected). If this condition is present for 50 ms, a K1/K2 mismatch is reported at the reference point MSP_MP.

d) If the protection section is in SF condition, the selector is released (no signal selected) and an active K1/K2 mismatch indication is cleared.

NOTE – In the G.783 definition of the 1:n protocol, the extra traffic was removed from the protection section in case of SD for the protection section. In case of interworking between equipment where the 1:n protocol with extra traffic is designed according to the G.783 definition and between equipment where the protocol is designed according to the new definition of this Recommendation, the equipment with the G.783 definition will report a K1/K2 mismatch failure in case of SD for the protection section. Such a failure shall be ignored by the management.

7.1.1.8 Transmission and acceptance of APS bytes

Byte K1 and bits 1 to 5 of byte K2 shall be transmitted on the protection section. Although they may also be transmitted identically on working sections, receivers should not assume so, and should have the capability to ignore this information on the working sections.

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

The following conditions are reported as APS defect conditions at the MSP_MP and result in the release of the selector in addition to the condition defined in 7.1.1.7.

– A mismatch of bit 5 of the sent and received K2 for 50 ms (optional);

– In bidirectional operation, an inappropriate code that persists for 50 ms in the received K1 bits 1-4. Appropriate codes are a higher priority request than the local request, an identical request to the local request, or a reverse request for any local request except no request. Any other value that persists for 50 ms is considered an inappropriate code;

– In bidirectional operation, an inappropriate or invalid traffic signal number that persists for 50 ms in the received K1 bits 5-8.

7.1.2 MSP commands

The MSP function receives MSP control parameters and switch requests from the synchronous equipment management function at the MSP_MP reference point. A switch command issues an appropriate external request at the MSP function. Only one switch request can be issued at the MSP_MP. A control command sets or modifies MSP parameters or requests the MSP status.

Any external switch command not acknowledged by the far end within 2.5 s should be reported as failed, and the command and K-byte request should be withdrawn. If an external switch command was acknowledged initially but is overruled later on, the external command is dropped consequently.

NOTE – This behaviour was not fully defined in previous versions of Recommendation G.841 and G.783.

7.1.2.1 Switch commands

A switch command issued at the MSP APS controller interface initiates one external bridge request for evaluation as described in 7.1.1.1.1. Switch commands are listed below in the descending order of priority and the functionality of each is described.

1) *Clear* – This command clears all the externally initiated switch commands listed below and WTR at the node to which the command was addressed.

   NOTE – In the G.783 definition of the linear MSP, the clear command did not clear WTR. Equipment which was designed according to the G.783 definition will not clear WTR if a clear command is sent to this equipment. However, it is possible to achieve a similar behavior by a carefully selected sequence of external commands (e.g. manual switch followed by clear).

2) *Lockout of protection* – Denies all normal traffic signals (and the extra traffic signal, if applicable) access to the protection section by issuing a "Lockout of Protection" request unless equal protection switch command is in effect.

3) *Forced switch #* – For normal traffic signal #s, switches normal traffic signal # to the protection section, unless an equal or higher priority switch command is in effect or SF condition exists on the protection section, by issuing a forced switch request for that traffic signal.

   For 1 + 1 systems or 1:n systems without extra traffic, forced switch null traffic signal transfers the normal traffic signal from protection section to the working section, unless an equal or higher priority request is in effect. Since forced switch has higher priority than SF or SD on a working section, this command will be carried out regardless of the condition of the working section(s). "Forced Switch Null Traffic signal" has higher priority than "Forced Switch – Normal Traffic signal #" when both commands are detected at the same time.

   For 1:n systems with extra traffic, forced switch extra traffic signal will transfer the normal traffic signal from the protection section to the working section and restore the extra traffic signal on the protection section, unless an equal or higher priority request is in effect.

4) *Manual switch #* – Switches normal traffic signal # to the protection section, unless a failure condition exists on other sections (including the protection section) or an equal or higher priority switch command is in effect, by issuing a manual switch request for that normal traffic signal.

   For 1 + 1 systems or 1:n systems without extra traffic, manual switch null signal transfers the working section back from protection to the working section, unless an equal or higher priority request is in effect. Since manual switch has lower priority than SF or SD on a working section, this command will be carried out only if the working section is not in SF or

SD condition. "Manual Switch Null Signal" has higher priority than "Manual Switch – Normal Traffic Signal 1" when both commands are detected at the same time.

5) *Exercise #* – Issues an exercise request for that signal and checks responses on APS bytes, unless the protection section is in use. The switch is not actually completed, i.e. the selector is released by an exercise request on either the sent or the received and acknowledged K1 byte. The exercise functionality may not exist in all MSP functions.

Note that a functionality and a suitable command for freezing the current status of the MSP function is for further study.

7.1.2.2 Control commands

Control commands set and modify MSP protocol operation. The control commands that are currently defined apply only to 1:n (unidirectional or bidirectional) switching.

Clear Lockout of Normal Traffic Signal from Protection – Clears the Lockout of Normal Traffic Signal from Protection command for the normal traffic signal (or normal traffic signals) specified.

Lockout of Normal Traffic Signal from Protection – Prevents the specified normal traffic signal (or normal traffic signals) from switching to the protection section.

These commands are not to be confused with the Lockout of protection request, which prevents all normal or extra traffic signals from using the protection section. The request to lock out an individual normal traffic signal from protection or to clear the lockout of a normal traffic signal from protection shall be received at reference point MSP_MP. Lockout of Normal Traffic signal from Protection can be activated or cleared for each normal traffic signal independently, and any number of normal traffic signals can be locked out at the same time. The locked-out status of a normal traffic signal is not directly reflected in the K-bytes.

The operation of lockout of a normal traffic signal from protection depends on the mode of operation at the MS protection sublayer at which it is applied. If the operation is bidirectional, then the lockout also operates bidirectionally. If a section has a lockout of normal traffic signal from protection command applied, then local bridge requests are not issued for the locked-out normal traffic signal (i.e. local conditions for the associated working section and external requests for the normal traffic signal are not considered in the K1 byte generation process), and remote bridge requests for the signal are not acknowledged (i.e. remote requests for the signal are not considered in the K1 byte generation process and the requested bridge is not performed). Note that for bidirectional operation, the lockout of normal traffic signal from protection command must be applied at both ends for proper operation.

If the operation is unidirectional, the lockout also operates unidirectionally. If a normal traffic signal has a lockout of normal traffic signal from protection command applied, then local bridge requests are not issued for the locked out normal traffic signal. However, remote bridge requests for that normal traffic signal are acknowledged by performing the bridge and signalling that bridge in the K2 byte.

7.1.3 MSP conditions

The following MSP conditions can trigger protection switching:

SF is defined as the presence of the TSFprot condition generated by the MS Trail Termination function defined in Recommendation G.783.

NOTE – The SF condition is extended for the protection section. See 7.1.1.8.

Signal Degrade is defined as the presence of the TSD condition generated by the MS Trail Termination function defined in Recommendation G.783.

7.1.4 Switch operation

7.1.4.1 1:n bidirectional switching without extra traffic

Table 7-4 illustrates protection switching action between two multiplexer sites, denoted by A and C, of a 1:n bidirectional protection switching system without extra traffic.

When the protection section is not in use, null signal is indicated on both sent K1 and K2 bytes. Generation of the null signal is equipment dependent. The null signal could be, for example, unequipped, AIS, or an arbitrary normal traffic signal bridged to the protection section at the head-end. The tail-end must not assume or require any specific signal on the protection section. For example, in the example in Table 7-4, site C may bridge normal traffic signal 3 as the null signal, while site A may bridge normal traffic signal 4 as the null signal.

When a fail condition is detected or a switch command is received at the tail end of a multiplex section, the protection logic compares the priority of this new condition with the request priority of the traffic signal on the protection section. The comparison includes the priority of any bridge order; i.e. of a request on received K1 byte. If the new request is of higher priority, then the K1 byte is loaded with the request and the number of the traffic signal requesting use of the protection section. In the example, SD is detected at C on working section 2, and this condition is sent on byte K1 as a bridge order at A.

At the head-end, when this new incoming K1 byte has been verified (after being received identically for three successive frames) and evaluated (by the priority logic), the requested normal traffic signal is bridged onto the protection section, outgoing byte K2[1-4] is sent to confirm the requested bridge, and outgoing byte K1 is set with a reverse request to order a bridge at the tail-end for that normal traffic signal, initiating a bidirectional switch. Note that a reverse request is returned for exerciser and all other requests of higher priority. This clearly identifies which end originated the switch request. If the head-end had also originated an identical request (not yet confirmed by a reverse request) for the same signal, then both ends would continue transmitting the identical K1 byte and perform the requested switch action.

Also, at the head-end, the indicated traffic signal is bridged to protection. When the signal is bridged, byte K2 is set to indicate the number of the traffic signal on protection.

At the tail-end, when the traffic signal on received byte K2 matches the number of the traffic signal requesting the switch, that traffic signal is selected from protection. This completes the switch of a traffic signal to protection for one direction. The tail-end also performs the bridge as ordered by byte K1 and indicates the bridged signal on byte K2.

The head-end completes the bidirectional switch by selecting the signal from protection when it receives a matching K2 byte.

If the switch is not completed because the requested/bridged signals did not match within 50 ms, the selectors would remain released and the failure of the protocol would be indicated. This may occur when one end is provisioned as unidirectional and the other as bidirectional. A mismatch may also occur when a locked-out traffic signal at one end is not locked out at the other. Note that a mismatch may also occur when a 1 + 1 architecture connects to a 1:1 architecture (which is not in a provisioned for 1 + 1 state), due to a mismatch of bit 5 on K2 bytes. This may be used to provision the 1:1 architecture to operate as 1 + 1.

The example further illustrates a priority switch, when an SF condition on working section 1 pre-empts the normal traffic signal 2 switch. Note that selectors are temporarily released before selecting normal traffic signal 1 from protection due to temporary signal number mismatch on sent K1 and received K2 bytes. Further in the example, switching normal traffic signal 2 back to protection after failed section 1 is repaired is illustrated.

When the switch is no longer required, e.g. the failed working section has recovered from failure and wait-to-restore has expired, the tail-end indicates No Request for null signal on byte K1 (0000 0000). This releases the selector due to section number mismatch.

The head end then releases the bridge and replies with the same indication on byte K1 and null signal indication on byte K2. The selector at the head-end is also released due to mismatch.

Receiving null signal on K1 byte causes the tail-end to release the bridge. Since the K2 bytes now indicate null signal which matches the null signal on the K1 bytes, the selectors remain released without any mismatch indicated, and restoration is completed.

Table 7-4/G.841 – 1:n bidirectional protection switching without extra traffic example

Failure condition or controller state	**APS bytes**				**Action**	
	C → A		**A → C**			
	Byte K1	**Byte K2**	**Byte K1**	**Byte K2**	**At C**	**At A**
No failures (protection section not in use)	0000 0000	0000 1000	0000 0000	0000 1000	Null signal is bridged to protection. Selector is released.	Null signal is bridged to protection. Selector is released.
Working section 2 degraded in direction A → C	1010 0010	0000 1000	0000 0000	0000 1000	Failure detected. Request normal traffic signal 2 bridge – SD.	
	1010 0010	0000 1000	0010 0010	0010 1000		Bridge normal traffic signal 2. Reverse request normal traffic signal 2 bridge.
	1010 0010	0010 1000	0010 0010	0010 1000	Switch normal traffic signal 2 from protection section. Bridge normal traffic signal 2 to protection.	
	1010 0010	0010 1000	0010 0010	0010 1000		Switch normal traffic signal 2 from protection. Bidirectional switch completed.
Working section 1 failed in direction C → A	1010 0010	0010 1000	1100 0001	0000 1000		Failure detected. Request normal traffic signal 1 bridge – SF. Release normal traffic signal 2 switch.

Table 7-4/G.841 – 1:n bidirectional protection switching without extra traffic example *(continued)*

Failure condition or controller state	APS bytes				Action	
	C → A		A → C			
	Byte K1	Byte K2	Byte K1	Byte K2	At C	At A
(This pre-empts the normal traffic signal 2 switch)	0010 0001	0001 1000	1100 0001	0010 1000	Bridge normal traffic signal 1 to protection. Reverse request normal traffic signal 1 bridge. Release normal traffic signal 2 switch.	
	0010 0001	0001 1000	1100 0001	0001 1000		Switch normal traffic signal 1. Bridge normal traffic signal 1.
	0010 0001	0001 1000	1100 0001	0001 1000	Switch normal traffic signal 1. Bidirectional switch completed.	
Working section 1 Repaired (Working section 2 still degraded)	0010 0001	0001 1000	0110 0001	0001 1000		Wait to restore.
	1010 0010	0001 1000	0110 0001	0001 1000	Request normal traffic signal 2 bridge. Release normal traffic signal 1 switch.	
	1010 0010	0001 1000	0010 0010	0010 1000		Bridge normal traffic signal 2. Reverse request normal traffic signal 2 bridge. Release normal traffic signal 1 switch.
	1010 0010	0010 1000	0010 0010	0010 1000	Bridge normal traffic signal 2. Switch normal traffic signal 2.	
	1010 0010	0010 1000	0010 0010	0010 1000		Switch normal traffic signal 2. Bidirectional switch completed.
Working section 2 repaired	0110 0010	0010 1000	0010 0010	0010 1000	Wait to restore normal traffic signal 2.	

Table 7-4/G.841 – 1:n bidirectional protection switching without extra traffic example *(concluded)*

Failure condition or controller state	APS bytes				Action	
	C → A		A → C			
	Byte K1	Byte K2	Byte K1	Byte K2	At C	At A
Wait to restore expired (no failures)	0000 0000	0010 1000	0010 0010	0010 1000	Drop normal traffic signal 2 bridge order. Release normal traffic signal 2 switch.	
	0000 0000	0010 1000	0000 0000	0000 1000		Drop normal traffic signal 2 bridge. Drop normal traffic signal 2 bridge request. Release normal traffic signal 2 switch.
	0000 0000	0000 1000	0000 0000	0000 1000	Drop normal traffic signal 2 bridge. Null signal is bridged to protection.	Null signal is bridged to protection.

7.1.4.2 1:1 bidirectional switching with extra traffic

Table 7-5 illustrates protection switching action between two multiplexer sites, denoted by A and C, of a 1:n bidirectional protection switching system with extra traffic.

When the protection section is not in use, the extra traffic signal is transferred via the protection section.

When a signal fail or signal degrade condition is detected or a switch command is received at the tail end of a multiplex section, the protection logic compares the priority of this new condition with the request priority of the signal (if any) on the protection. The comparison includes the priority of any bridge order; i.e. of a request on received K1 byte. If the new request is of higher priority, then the K1 byte is loaded with the request and the number of the signal requesting use of the protection section. In the example, SD is detected at C on working section 2, and this condition is sent on byte K1 as a bridge order at A.

At the head-end, when this new K1 byte has been verified and evaluated (by the priority logic), byte K1 is set with a reverse request as a confirmation of the signal to use the protection and order a bridge at the tail-end for that signal. This initiates a bidirectional switch. Note that a reverse request is returned for exerciser and all other requests of higher priority. This clearly identifies which end originated the switch request. If the head-end had also originated an identical request (not yet confirmed by a reverse request) for the same channel, then both ends would continue transmitting the identical K1 byte and perform the requested switch action.

Also, at the head-end, the indicated signal is bridged to protection. When the signal is bridged, byte K2 is set to indicate the number of the signal on protection.

At the tail-end, when the signal number on received byte K2 matches the number of the signal requesting the switch, that signal is selected from protection. This completes the switch to protection for one direction. The tail-end also performs the bridge as ordered by byte K1 and indicates the bridged signal on byte K2.

The head-end completes the bidirectional switch by selecting the signal from protection when it receives a matching K2 byte.

If the switch is not completed because the requested/bridged signal did not match within 50 ms, the selectors would remain released and the failure of the protocol would be indicated. This may occur when one end is provisioned as unidirectional and the other as bidirectional. A mismatch may also occur when a locked-out signal at one end is not locked out at the other. Note that a mismatch may also occur when a 1 + 1 architecture connects to a 1:1 architecture (which is not in a provisioned for 1 + 1 state), due to a mismatch of bit 5 on K2 bytes. This may be used to provision the 1:1 architecture to operate as 1 + 1.

The example further illustrates a priority switch, when an SF condition on working section 1 pre-empts the WS 2 switch. Note that selectors are temporarily released before selecting WS 1, due to temporary signal number mismatch on sent K1 and received K2 bytes. Further in the example, switching back WS 2 after failed section 1 is repaired is illustrated.

When the switch is no longer required, e.g. the failed working section has recovered from failure and wait-to-restore has expired, the tail end indicates No Request for extra traffic signal on byte K1 (null signal if extra traffic is not provided). This releases the selector and bridge due to signal number mismatch. The head-end then releases the selector, bridges the extra traffic signal and replies with the same indication on byte K1 and extra traffic signal indication on byte K2. The tail-end now selects and bridges the extra traffic signal and replies with extra traffic signal indication on byte K2. The head end selects the extra traffic in response, which completes the bidirectional switch to the extra traffic signal.

Table 7-5/G.841 – 1:n bidirectional protection switching with extra traffic example

Failure condition or controller state	APS bytes				Action	
	C → A		A → C			
	Byte K1	Byte K2	Byte K1	Byte K2	At C	At A
No failures (extra traffic on protection section)	0000 1111	1111 1000	0000 1111	1111 1000	Extra traffic signal is bridged and selected.	Extra traffic signal is bridged and selected.
Working section 2 degraded in direction A → C	1010 0010	0000 1000	0000 1111	1111 1000	Failure detected. Order WS 2 bridge – SD. Release bridge. Release selector.	
	1010 0010	0000 1000	0010 0010	0010 1000		Release selector. Reverse order WS 2 bridge. Bridge WS 2.
	1010 0010	0010 1000	0010 0010	0010 1000	Select WS 2. Bridge WS 2.	
	1010 0010	0010 1000	0010 0010	0010 1000		Select WS 2. Bidirectional switch completed.

Table 7-5/G.841 – 1:n bidirectional protection switching with extra traffic example *(concluded)*

Failure condition or controller state	APS bytes				Action	
	C → A		A → C			
	Byte K1	Byte K2	Byte K1	Byte K2	At C	At A
Working section 1 failed in direction C → A	1010 0010	0010 1000	1100 0001	0000 1000		Failure detected Order WS 1 bridge – SF. Release selector. Release bridge.
(This pre-empts the WS 2 switch)	0010 0001	0001 1000	1100 0001	0000 1000	Release WS 2 selector. Reverse order WS 1 bridge. Bridge WS 1.	
	0010 0001	0001 1000	1100 0001	0001 1000		Select WS 1. Bridge WS 1.
	0010 0001	0001 1000	1100 0001	0001 1000	Select WS 1. Bidirectional switch completed.	
Working section 1 repaired	0010 0001	0001 1000	0110 0001	0001 1000		Wait to restore.
(Working section 2 still degraded)	1010 0010	0000 1000	0110 0001	0001 1000	Order WS 2 bridge. Release selector. Release bridge.	
	1010 0010	0000 1000	0010 0010	0010 1000		Reverse order WS 2 bridge. Bridge WS 2. Release selector.
	1010 0010	0010 1000	0010 0010	0010 1000	Bridge WS 2. Select WS 2.	
	1010 0010	0010 1000	0010 0010	0010 1000		Select WS 2. Bidirectional switch completed.
Working section 2 repaired	0110 0010	0010 1000	0010 0010	0010 1000	Wait to restore WS 2.	
Wait to restore expired (no failures, extra traffic selected)	0000 1111	0000 1000	0010 0010	0010 1000	Order extra traffic bridge – NR. Release selector. Release bridge.	
	0000 1111	0000 1000	0000 1111	1111 1000		Order extra traffic bridge – NR. Bridge extra traffic. Release selector.
	0000 1111	1111 1000	0000 1111	1111 1000	Bridge extra traffic. Select extra traffic.	
	0000 1111	1111 1000	0000 1111	1111 1000		Select extra traffic. Bidirectional switch completed.

7.1.4.3 1:n unidirectional switching

All actions are as described in 7.1.4.1 except that the unidirectional switch is completed when the tail-end selects from protection the section for which it issued a request. This difference in operation is obtained by not considering remote requests in the priority logic and therefore not issuing reverse requests.

7.1.4.4 1 + 1 unidirectional switching

For 1 + 1 unidirectional switching, the signal selection is based on the local conditions and requests. Therefore each end operates independently of the other end, and bytes K1 and K2 are not needed to coordinate switch action. However, byte K1 is still used to inform the other end of the local action, and bit 5 of byte K2 is set to zero.

7.1.4.5 1 + 1 bidirectional switching

The operation of 1 + 1 bidirectional switching can be optimized for a network in which 1:n protection switching is widely used and which is therefore based on compatibility with a 1:n arrangement; alternatively it can be optimized for a network in which predominantly 1 + 1 bidirectional switching is used. This leads to two possible switching operations described below and in Annex B.

7.1.4.5.1 1 + 1 bidirectional switching compatible with 1:n bidirectional switching

Bytes K1 and K2 are exchanged as described in 7.1.4.1 to complete a switch. Since the bridge is permanent, i.e. the normal traffic signal is always bridged to the protection section, normal traffic signal 1 is indicated on byte K2, unless received K1 indicates null signal (0). Switching is completed when both ends select the signal from protection, and may take less time because K2 indication does not depend on a bridging action.

For revertive switching, the restoration takes place as described in 7.1.4.1. For non-revertive switching, Table 7-6 illustrates the operation of a 1 + 1 bidirectional protection switching system.

For non-revertive operation, assuming the normal traffic signal is on protection, when the working section is repaired, or a switch command is released, the tail-end maintains the selection and indicates do not revert for the normal traffic signal. The head-end also maintains the selection and continues indicating reverse request. The do not revert is removed when pre-empted by a failure condition or an external request.

Table 7-6/G.841 – Example of 1 + 1 bidirectional switching compatible with 1:n bidirectional switching

Failure condition or controller state	APS bytes				Action	
	C → A		A → C			
	Byte K1	Byte K2	Byte K1	Byte K2	At C	At A
No failures (assume protection section not in use)	0000 0000	0000 0000	0000 0000	0000 0000	Selector is released.	Selector is released.
Working section 1 failed in direction A → C	1101 0001	0000 0000	0000 0000	0000 0000	Failure detected. Request normal traffic signal 1 bridge – SF.	
	1101 0001	0000 0000	0010 0001	0001 0000		Indicate normal traffic signal 1 bridged. Reverse request normal traffic signal 1 bridge.
	1101 0001	0001 0000	0010 0001	0001 0000	Indicate normal traffic signal 1 bridged. Select normal traffic signal from protection section.	
	1101 0001	0001 0000	0010 0001	0001 0000		Select normal traffic signal from protection section. Bidirectional switch completed.
Working section 1 repaired. Maintain switch (non-revertive)	0001 0001	0001 0000	0010 0001	0001 0000	Send Do not revert.	
Protection section degraded in direction A → C	1011 0000	0001 0000	0010 0001	0001 0000	Failure detected. Request null signal bridge – SD. Select normal traffic signal from working section.	
	1011 0000	0001 0000	0010 0000	0000 0000		Reverse request null signal bridge. Drop normal traffic signal bridge indication. Select normal traffic signal from working section.
	1011 0000	0000 0000	0010 0000	0000 0000	Drop normal traffic signal bridge indication.	
Protection section repaired	0000 0000	0000 0000	0010 0000	0000 0000	Send no request.	
	0000 0000	0000 0000	0000 0000	0000 0000		Send no request.

7.2 MS shared protection rings

7.2.1 Two- and four-fibre MS shared protection rings

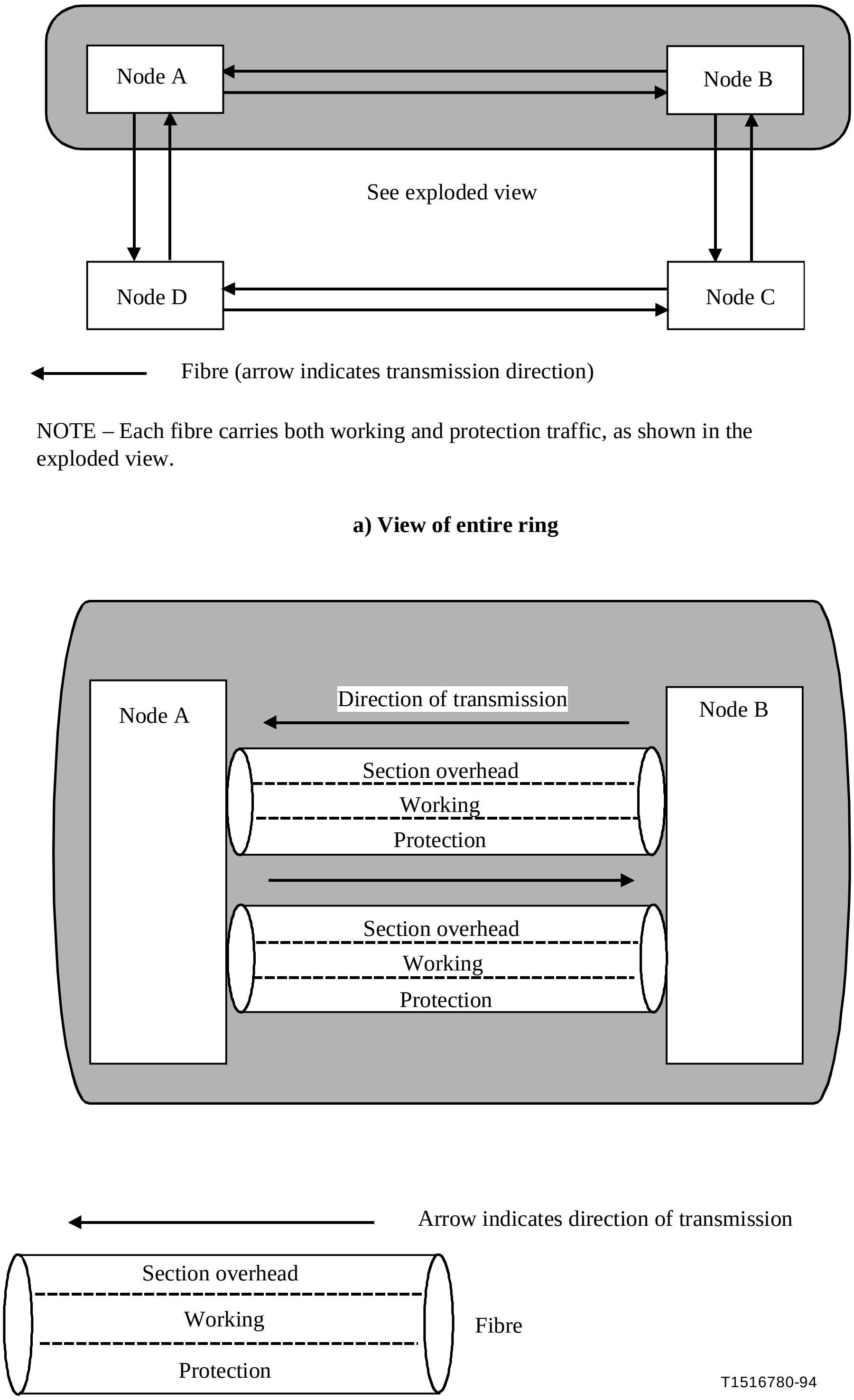
All MS shared protection rings support ring switching. In addition, four-fibre MS shared protection rings support span switching.

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 normal traffic carried on working channels in one fibre are protected by the protection channels travelling in the opposite direction around the ring (See Figure 7-2.). This permits the bidirectional transport of normal 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 normal traffic is switched from the working channels to the protection channels in the opposite direction.

If Non-pre-emptible Unprotected Traffic (NUT) is supported, selected channels on the working bandwidth and their corresponding protection channels may be provisioned as non-pre-emptible unprotected channels. The remaining working channels are still protected by the corresponding protection channels. The non-pre-emptible unprotected channels will have no BLSR APS protection.



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 7-2/G.841 – Two-fibre MS shared protection ring

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 7-3, 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 normal 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.

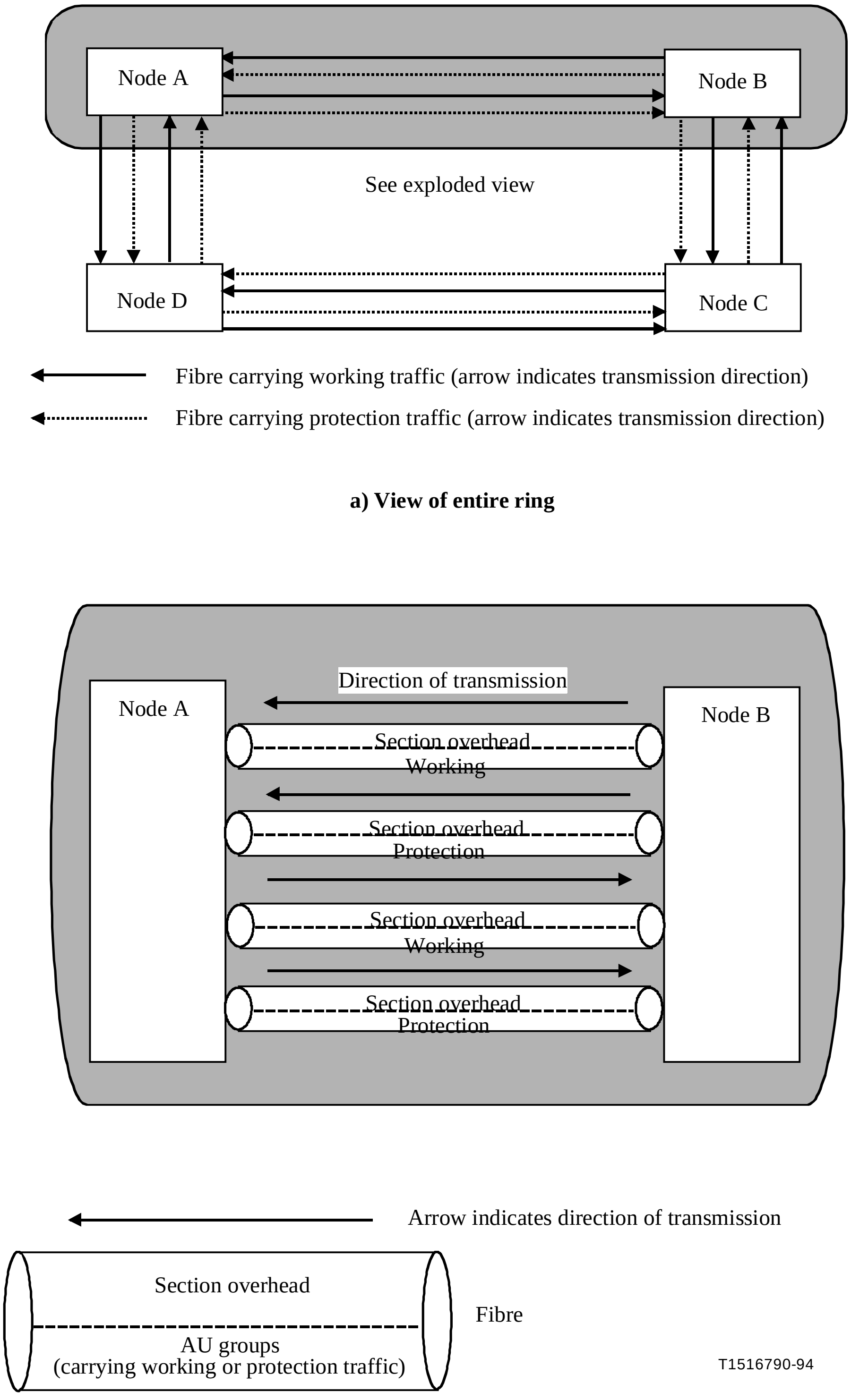
If NUT is supported, then on each span, selected channels on the working bandwidth and their corresponding protection channels may be provisioned as non-pre-emptible unprotected channels. The remaining working channels are still protected, for both span and ring switching, by their corresponding protection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

- ring switching is disabled on that channel everywhere on the ring (as in the two-fibre case);
- span switching is disabled for that channel on the provisioned span.

Hence, the NUT channel has no MS SPRING APS protection on the provisioned span; on other spans, the same channel (if not provisioned as NUT) has only span switching available to it. Note that if these channels are provisioned as working channels on other spans, they will have lower survivability than other working channels since ring switching is unavailable to them.

Support of non-pre-emptible unprotected channel provisioning requires that a NUT table be present at each node on the MS SPRING. Figure 7-4 gives a conceptual representation and example of a NUT table. This table contains information to identify the channels that have been provisioned for NUT, and identifies which type of switching (i.e. span or ring switch) is prohibited by the NUT. Since provision of a working channel for non-pre-emptible unprotected automatically ensures that the corresponding protection channel is also provisioned for non-pre-emptible unprotected, only the working channel ID need to be stored in the table. The corresponding table for two-fibre operation only needs a column for ring switching.

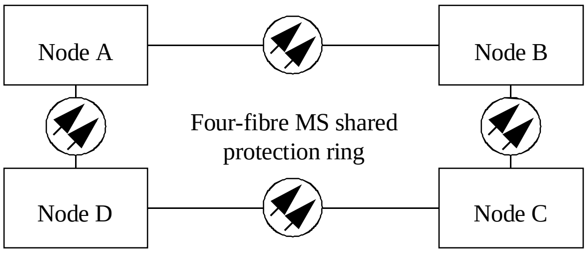
Four-fibre MS shared protection rings may have the capability of operating similar to a linear ADM chain when not fully connected as a continuous ring (i.e. they can lock out ring switches and use span switches only to protect existing traffic). This configuration may exist because an isolated ring segment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


Node A
Node B
See exploded view
Node D
Node C
Fibre carrying working traffic (arrow indicates transmission direction)
Fibre carrying protection traffic (arrow indicates transmission direction)
Direction of transmission
Node A
Node B
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

a) View of entire ring

b) Exploded view of the shaded portion of the ring

Figure 7-3/G.841 – Four-fibre MS shared protection ring



- All spans have NUT for AU-4 #1
- The span between B and C has NUT on AU-4 #2

Node A

AU-4 #	Ring switch	Span switch	
		East	West
1	–	–	–
2	–		
3			
4			
5			
· · ·			

Node B

AU-4 #	Ring switch	Span switch	
		East	West
1	–	–	–
2	–	–	
3			
4			
5			
· · ·			

Node C

AU-4 #	Ring switch	Span switch	
		East	West
1	–	–	–
2	–		–
3			
4			
5			
· · ·			

Node D

AU-4 #	Ring switch	Span switch	
		East	West
1	–	–	–
2	–		
3			
4			
5			
· · ·			

T1529650-98

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

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

Figure 7-4/G.841 – Conceptual representation and example of a NUT table

7.2.2 Network objectives

The following network objectives apply:

1) *Switch time* – In a ring with no extra traffic, all nodes in the idle state (no detected failures, no active automatic or external commands, and receiving only Idle K-bytes), and with less than 1200 km of fibre, the switch (ring and span) completion time for a failure on a single span shall be less than 50 ms. On rings under all other conditions, the switch completion time can exceed 50 ms (the specific interval is under study) to allow time to remove extra traffic, or to negotiate and accommodate coexisting APS requests.

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* – Bidirectional protection 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* – Time-slot interchange will allow better utilization of bandwidth of the ring. If Time-Slot Interchange (TSI) is allowed, the traffic having a time-slot 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 time-slot interchange through the failed location will be restored.

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, the normal traffic carried on 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 ms).

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

A node on the ring may insert normal or extra traffic into channels in either direction, drop normal or extra traffic from channels from either direction, or pass channels directly through to allow other nodes to be connected. Because MS shared protection rings can support extra traffic, this capability may apply not only to the working channel, but also, as an option, to the protection channels. 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 Figure 7-5 and an example of a squelch table is provided in Figure 7-6.

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

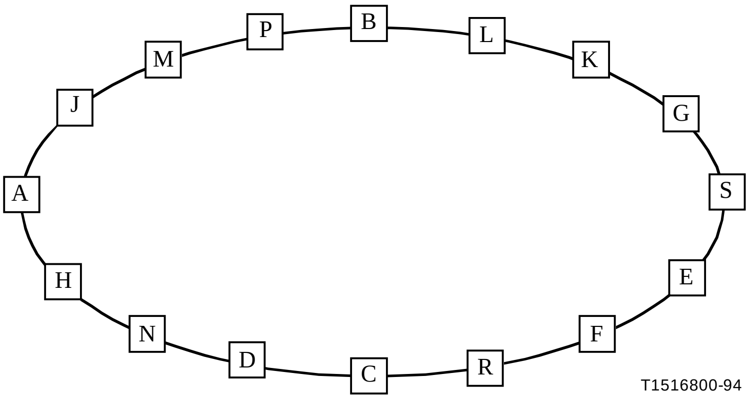
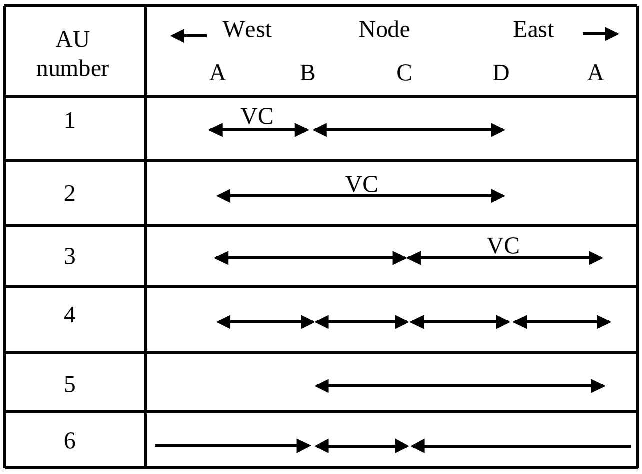


Figure 7-5/G.841 – Conceptual representation of a ring topology map



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		C	B	

Node B

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

Node C

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

Node D

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

T1516810-94

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 7-6/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.707. This point is for further study. The exception is extra traffic that may be added, dropped, or passed through similar to normal traffic.

A switch shall be initiated by one of the criteria specified in 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 status (or bridge request), it can initiate its own bridge requests more quickly. In the case of span bridge requests on four-fibre rings, signalling on the long path informs other nodes on the ring that a span switch exists elsewhere on the ring. This mechanism denies lower priority ring switches.

The destination node is the node that is adjacent to the source node across the failed span. When a node that is not the destination 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 7-7. In a two-fibre ring, B will bridge the normal traffic from 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 normal traffic from protection channels received from B by way of A back onto the working channels toward D. This action is referred to as the switch.

If the ring switch in this example is on a four-fibre ring, B will bridge the normal traffic from 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 normal traffic from 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, normal 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 pre-empts the long-path protection channels.

Ring and span switches can be pre-empted by bridge requests of higher priority as determined by Table 7-8. 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.

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

As soon as a request of higher priority than the No Request priority is received by the node, and only if that request is a ring request other than EXER-R, or requires the usage of the protection channels carrying the extra traffic, extra traffic is pre-empted.

If a ring switch exists and a failure of equal priority occurs on another span requiring a ring switch (including the combination of SF-R and FS-R), 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 pre-empt a bridge request unless they have a higher priority bridge request. In order to accommodate this ring state knowledge, signalling over the long path during a bridge request, in addition to the short path, shall be used. For example, although span bridges can be established with only short-path signalling, a Bridged indication is sent on the long path in order to inform other nodes of the state of the ring. In addition, OAM&P messages transported over the DCC can be used to determine the details regarding the condition of the ring.

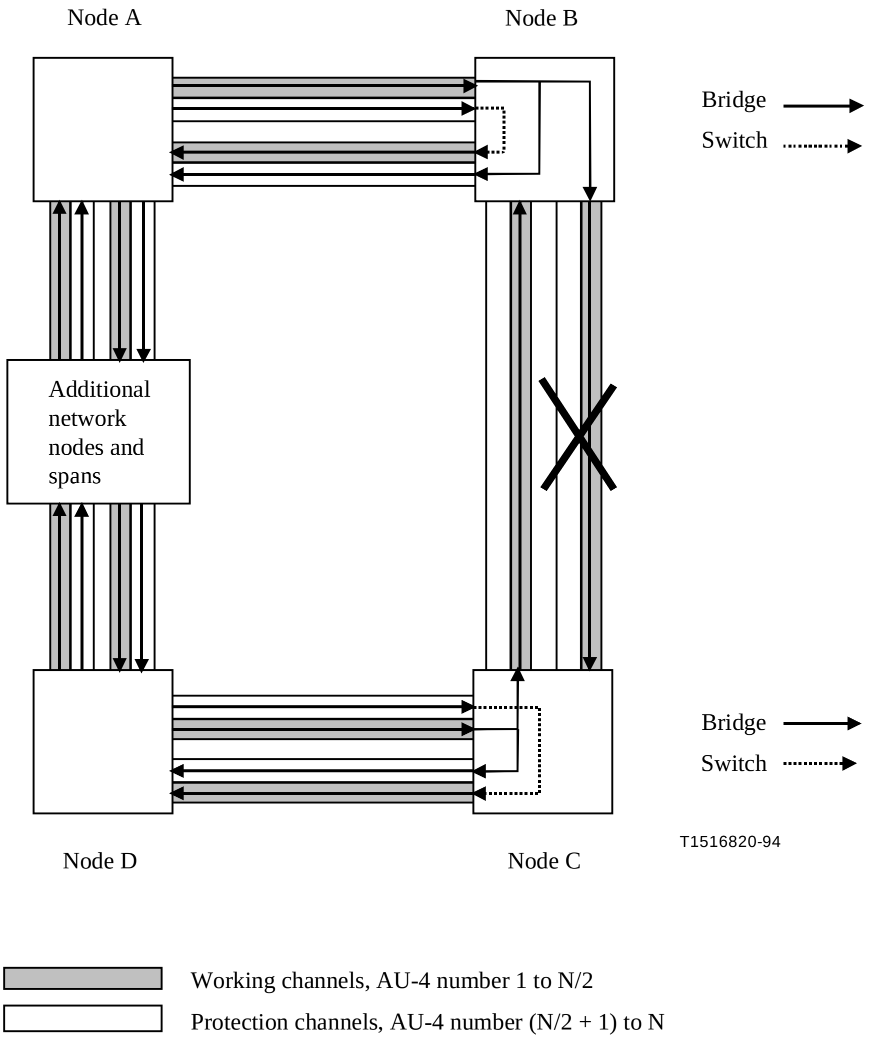
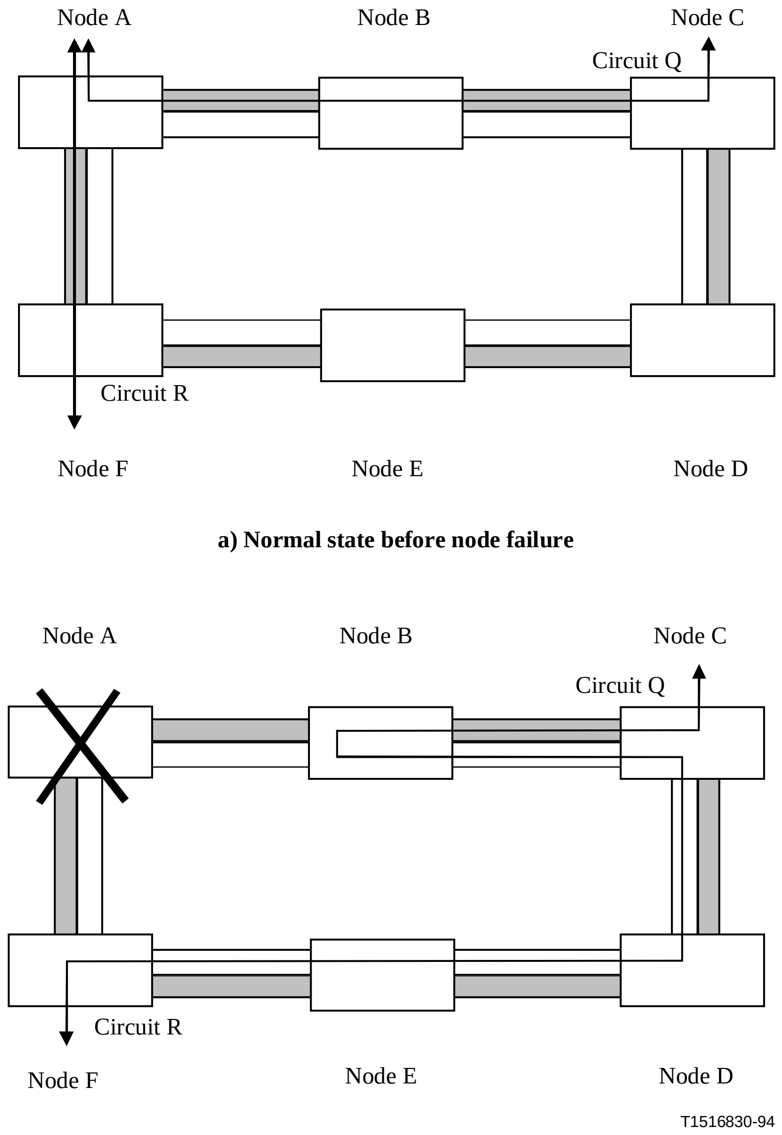

Node A
Node B
Bridge
Switch
Additional network nodes and spans
Bridge
Switch
T1516820-94
Node D
Node C
Working channels, AU-4 number 1 to N/2
Protection channels, AU-4 number (N/2 + 1) to N

Figure 7-7/G.841 – Bridge and switch in a two-fibre MS shared protection ring



a) Normal state before node failure

b) Misconnection after node failure

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

▨ Working

□ Protection

↔ Circuit transporting service

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

Figure 7-8/G.841 – Example of misconnection

7.2.3.1 Extra traffic

During fault-free conditions, it is possible to use the protection channels to carry additional traffic. This additional traffic, which is referred to as extra traffic, has lower priority than the normal traffic on the working channels and has no means for protection. The extra traffic is set up by provisioning the add and drop nodes for the traffic. Intermediate nodes along the ring are provisioned so that the protection channel AU-3/4s carrying extra traffic are passed through the node (Protection channels that are not carrying extra traffic are terminated at the intermediate nodes). Nodes that are inserting, dropping, or passing through extra traffic indicate its presence on those spans by inserting the extra traffic code in byte K2. Note that non-pre-emptible unprotected traffic is not considered extra traffic, and as such, shall not set the ET code.

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

7.2.3.2 Squelching to avoid misconnected traffic

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 normal 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, normal traffic 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. Referring to Figure 7-8, a cut in both the spans between nodes A and F and between nodes A and B (isolating node A) causes circuits Q and R to attempt to access time slot #1P on the protection channels.

A potential misconnection is determined by identifying the nodes that will act as the switching nodes for a bridge request, and by examining the traffic that will be affected by the switch. The switching nodes can be determined from the node addresses in the 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. Specifically, the traffic that is sourced or dropped at the node(s) isolated from the ring by the failure shall be squelched. For rings operating at an AU-4 level, this squelching occurs at the switching nodes. AU level squelching occurs for the normal or extra traffic into or out of the protection channels (i.e. normal traffic into or out of working channels is never squelched). 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) a ring map that contains information regarding the order in which the nodes appear on the ring;
2) a cross-connect map that contains the AU-4 time-slot assignments for traffic that is both terminated at that node and passed-through that node;
3) a squelch table that contains, for each of these 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, the map requirements are under study.

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

– a simple directed connection sourced in one node and terminated in another node;
– a multiply dropped circuit (such as the drop and continue used in ring interworking [see Recommendation G.842]);
– a multiply sourced circuit (such as the reverse direction of the drop and continue direction of a ring interworking circuit).

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

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

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

A node that pre-empts extra traffic should squelch the extra traffic channels that are pre-empted in the following manner:

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

7.2.3.3 LO VC access

Some nodes on the ring, referred to as LO VC access nodes, may be capable of inserting, dropping, or cross-connecting LO VCs from the AUs. When multiple nodes on the ring add LO VCs or crossconnect LO VCs between AUs, the payload for a given AU may have multiple source nodes or be dropped among multiple nodes. Such AUs are referred to in this Recommendation as LO VC-accessed AUs. LO VC access is for further study.

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, received bridge requests, and received bridge request status information. 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

Externally initiated commands are initiated at an NE by either the OS or the craftsperson. The externally initiated command 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.

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.

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

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

lockout of protection - all spans: This command prevents protection switching on the entire ring. If any normal traffic is using the protection facility on any span, this command causes normal traffic to switch back to the working 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.

Lockout of Protection - Span (LP-S): This command prevents the usage of the span for any protection activity and prevents using ring switches anywhere in the ring. If any ring switches exist in the ring, this command causes the switches to drop. If there is a span switch for this span, it is dropped. Thus, all ring switching is prevented (and pre-empted), and span switching is prevented only on the locked-out span.

Forced Switch to protection - Ring (FS-R): This command performs the ring switch of normal traffic from working 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.

Forced Switch to protection - Span (FS-S): This command switches the normal 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.

Manual Switch to protection - Ring (MS-R): This command performs the ring switch of the normal traffic 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).

Manual Switch to protection - Span (MS-S): This command switches the normal 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).

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

Exercise - Span (EXER-S): This command exercises span protection of the requested channel without completing the actual bridge and switch. The command is issued and the responses are checked, but no normal traffic 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 normal traffic affected by defects, while the SD bridge request is used to protect against signal degradations due to bit errors. The bridge requests are transmitted on both the short and long paths. Each intermediate node verifies the destination node ID of the long-path bridge request and relays the bridge request. The destination node receives the bridge request, performs the activity according to the priority level, and sends the bridged indication.

The WTR bridge request is used to prevent frequent oscillation between the protection 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 commands.

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

Signal Fail - Span (SF-S): An SF is defined as the presence of the TSFprot condition generated by the MS Trail Termination function 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.

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. For a four-fibre ring, a SF-R results from the combination of LOW-S and a detected or received working line failure on the same span or the following combination of detected or received conditions on the working and protection lines:

– working line failed and protection line failed on the same span;

– working line failed and protection line degraded on the same span;

– working line degraded and protection line failed on the same span.

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 (as defined previously for span switching). 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.

Signal Degrade - Span (SD-S): Signal Degrade is defined as the presence of the TSD condition generated by the MS Trail Termination function 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 normal traffic to the protection channels in the same span where the failure is located.

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, a SD-R results from the combination of LOW-S and a detected or received working line degrade on the same span or the combination of detected or received signal degrade conditions on the working and protection lines on the same span.

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.

Reverse Request - Span (RR-S): This command is transmitted to the tail-end NE as an acknowledgment for receiving the short-path span bridge request. It is transmitted on the short path only.

Reverse Request - Ring (RR-R): This command is transmitted to the tail-end NE on the short path as an acknowledgment for receiving the short-path ring bridge request.

Wait-To-Restore (WTR): This command is issued when working 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 pre-empted 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.

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

7.2.5.1 Byte K1

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

Table 7-7/G.841 – Byte K1 functions

Bridge Request code (Bits 1-4)		Destination Node Identification (Bits 5-8)
Bits		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).
1 2 3 4		
1 1 1 1	Lockout of Protection (Span) LP-S or Signal Fail (Protection)	
1 1 1 0	Forced Switch (Span) FS-S	
1 1 0 1	Forced Switch (Ring) FS-R	
1 1 0 0	Signal Fail (Span) SF-S	
1 0 1 1	Signal Fail (Ring) SF-R	
1 0 1 0	Signal Degrade (Protection) SD-P	
1 0 0 1	Signal Degrade (Span) SD-S	
1 0 0 0	Signal Degrade (Ring) SD-R	
0 1 1 1	Manual Switch (Span) MS-S	
0 1 1 0	Manual Switch (Ring) MS-R	
0 1 0 1	Wait-To-Restore WTR	
0 1 0 0	Exerciser (Span) EXER-S	
0 0 1 1	Exerciser (Ring) EXER-R	
0 0 1 0	Reverse Request (Span) RR-S	
0 0 0 1	Reverse Request (Ring) RR-R	
0 0 0 0	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 7-8.

Table 7-8/G.841 – Byte K2 functions

Source node identification (Bits 1-4)	Long/Short (Bit 5)		Status (Bits 6-8)	
Source node ID is set to the node's own ID.	Bit		Bit	
	5		6 7 8	
	0	Short path code (S)	1 1 1	MS-AIS
	1	Long path code (L)	1 1 0	MS-RDI
			1 0 1	Reserved for future use
			1 0 0	Reserved for future use
			0 1 1	Extra Traffic on protection channels
			0 1 0	Bridged and Switched (Br&Sw)
			0 0 1	Bridged (Br)
			0 0 0	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. Subclause 7.2.6.1 covers the three classes of ring node APS states, and the steady-state behavior of the node in these states. Subclause 7.2.6.2 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 7-9 illustrates the conceptual operation of an MS shared protection ring APS controller.

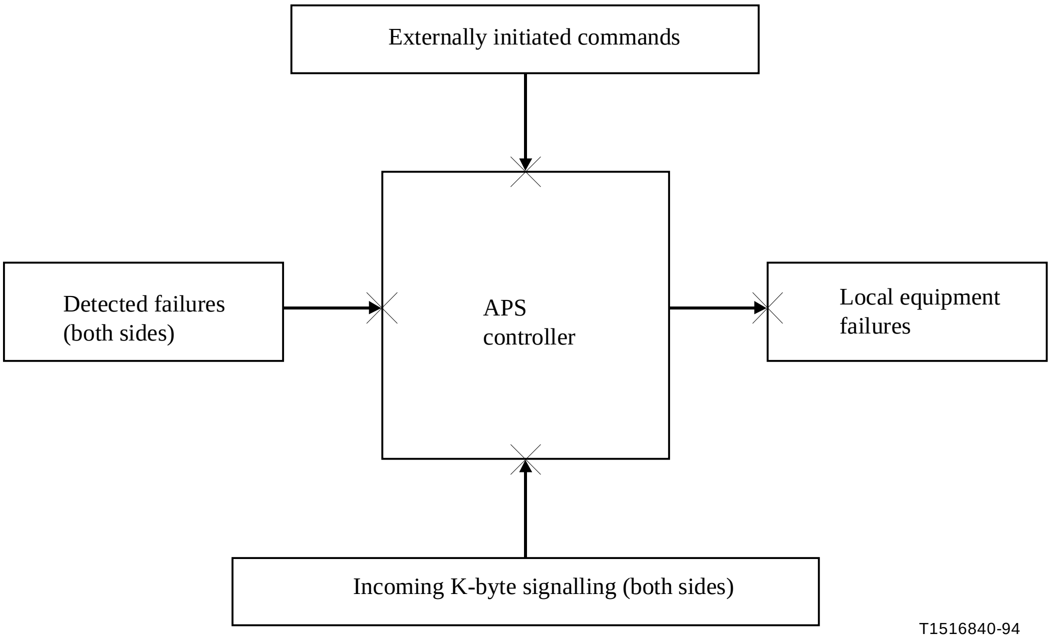

Externally initiated commands
Detected failures (both sides)
APS controller
Local equipment failures
Incoming K-byte signalling (both sides)
T1516840-94

Figure 7-9/G.841 – Conceptual 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.

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

The relationship among bridge request codes, bridge request status information, and K-byte indications is shown in Table 7-9.

Table 7-9/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 sourcing or receiving any APS requests or bridge request status and it is receiving Idle or ET codes from both directions.

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

Rule I #1a: Any node in the idle state not inserting, dropping, or passing through extra traffic shall source the K-bytes in both directions as given in Table 7-10.

Table 7-10/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)

Rule I #1b: Any node in the idle state inserting, dropping, or passing through extra traffic shall source the K-bytes shown in Table 7-10 with the exception that byte K2 bits 6-8 transmitted over any span that contains extra traffic shall have the value 011 (Extra Traffic 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

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

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

Rule S #1a: Any node in the switching state shall source K-bytes as shown in Table 7-11:

Table 7-11/G.841 – Byte K1 and K2 values sourced by a node in the switching state

K1 [1-4]	=	Bridge Request (Status) 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 (or bridge request status) on the long path. Both the bridge request and the bridge request status have the same priority (or one of them is a Reverse Request), and protect the same span. Exceptions to this can occur when there are more than one switch requests active at a node. The exceptions are as follows:

- The isolated node cases described in Rules S #1c and S #1d.
- The case of a span bridge request on each side of the node, the node shall source a bridge request on each short path, where the status bits indicate the state of the bridge and switch for the corresponding span.
- The case of a ring bridge request pre-empting a span bridge request on an adjacent span as described in Rule S-S #2b.
- Cases where SF-P and SD-P coexist with a ring switch on the same span. Table 7-12 defines the signalling for these cases.

Table 7-12/G.841 – SD-P and SF-P coexisting with ring switches on the same span

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

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, the long-path bridge request shall be signalled rather than the short-path reverse requests. This rule takes precedence over Rule S #1b in case of multiple bridge requests at the same node [see Figure 7-10 a)].

Rule S #1d: Whenever a node detects a condition requiring a ring switch or an externally initiated command for a ring switch applied at that node, it shall always source over the short path a short-path ring bridge request as long as the ring bridge request is not pre-empted by a higher priority bridge request [See Figure 7-10 b)]. This rule takes precedence over Rule S #1c. Note that whenever a node receives in one direction a short-path ring bridge request on one side and detects one of the above-mentioned conditions on the other side, it shall signal the bridge request associated with that condition [see Figure 7-10 c)].

Rule S #1e: A node in the switching state shall insert the ET code in K2 bits 6-8 on spans that are carrying extra traffic.

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:

– SD-P with any span switch;

– LP-S or SF-P with any span switch for other spans;

– SF-P or SD-P with any ring switch on the same span;

– LP-S with SD-P;

– LP-S with LP-S;

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

Rule S #4b: When multiple equal priority bridge requests over different spans of SD-R, MS-R, or EXER-R exist at the same time, no bridge or switch shall be executed and existing switches and bridges shall be dropped. (Note that in case of multiple SD-R failures, all failures will be reported or alarmed. However, this behaviour can be considered as expected by the user.) The nodes shall signal the ring bridge request in byte K1, and byte K2 bits 6-8 shall be set to Idle.

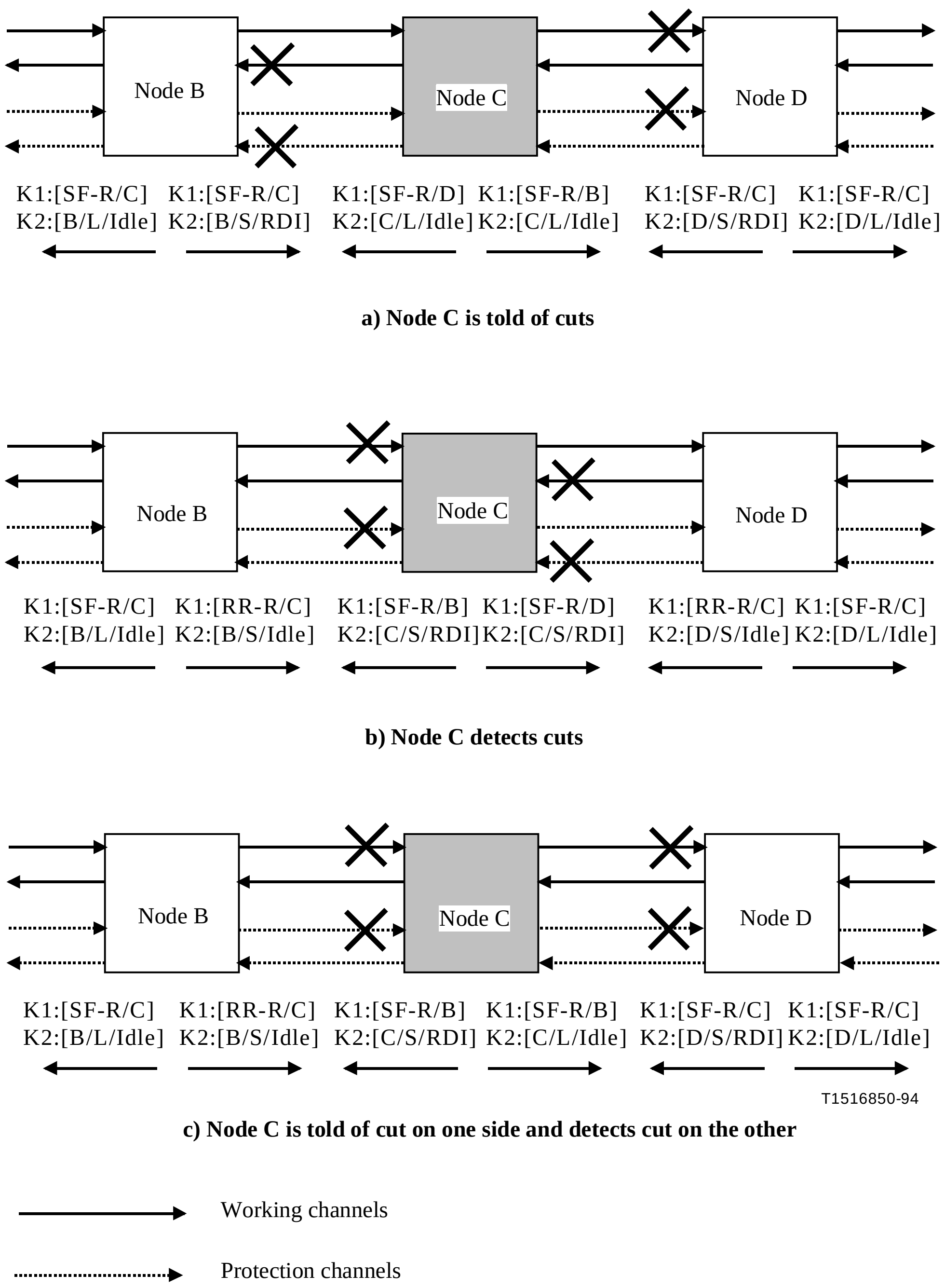
Rule S #5 – LOSS OF RING BRIDGE REQUEST: If a node executing a ring bridge and switch no longer receives a valid ring bridge request on the long path, it shall drop its ring bridge and switch, and shall signal and act based on its highest priority input.

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

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

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

Rule S #9 – A node in a ring switching state that receives the external command LOW-R for the affected span shall drop its bridge and switch and shall signal No Request, SF-P, or SD-P. Upon the reception of No Request in combination with either Idle or ET code or bridge request status from the span away from the LOW-R span, the node shall re-insert extra traffic that was pre-empted on that span.


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]

a) Node C is told of cuts

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]

b) Node C detects cuts

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

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

Working channels
Protection channels

Figure 7-10/G.841 – Isolated node signalling (signalling states prior to nodes B and D establishing a ring bridge and switch)

7.2.6.1.3 Pass-through state

A node is in the pass-through state when its highest priority APS request is a bridge request or bridge request status not destined to or sourced by itself. The pass-through can be either unidirectional or bidirectional, depending on its nature. There are three types of pass-through: unidirectional full pass-through, bidirectional full pass-through, and 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. A node in the K-byte pass-through state shall source the ET code in bits 6-8 on spans that are carrying extra traffic. A K-byte pass-through node receiving the Extra Traffic code shall source Idle in the opposite direction if no extra traffic exists on the opposite span. A node in unidirectional full pass-through shall continue sourcing the previously sourced K-bytes in the opposite direction, with the exception that K2 bits 6-8 shall reflect the appropriate status code.

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

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

7.2.6.2 Ring node APS state transition rules

Subclause 7.2.6.1 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 command, or locally detected multiplex section or equipment performance criteria.

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, or the span is carrying extra traffic. 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. MS-RDI and MS-AIS terminate at multiplex section terminating elements as specified in Recommendation G.783. A node shall signal the ET code on any span that is carrying extra traffic.

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

7.2.6.2.1 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 span bridge request status or the EXER-R bridge request, the intermediate nodes on the long path shall go into K-byte pass-through. Actions taken at an intermediate node upon receiving a valid ring bridge request other than EXER-R are:

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

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

Rule I-P #2 – TRANSITION FROM THE PASS-THROUGH STATE TO THE IDLE STATE: A node shall revert from any pass-through state to the idle state when it detects No Request codes in K1 bits 1-4 and Idle or ET codes in K2 bits 6-8, from both directions. Both directions revert simultaneously from the pass-through state to the idle state. Extra traffic that was pre-empted shall be re-inserted and the ET code sourced as defined in Rule I #1b.

7.2.6.2.2 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-S, EXER-R, 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-S, EXER-R, 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.
- Extra traffic shall be dropped immediately on all spans for a ring switch, or on the span whose protection channels are required for a span switch.
- no bridge or switch shall be executed while the ET code is received on the span whose protection channels are required by that bridge and switch.

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

Rule I-S #2 – TRANSITION FROM THE SWITCHING STATE TO THE IDLE STATE: A node shall revert from the switching state to the idle state when it detects NR codes in byte K1 bits 1-4 and Idle or ET 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: When a WTR time expires or an externally initiated command is cleared at a node, and the node receives a Reverse Request from the short span, the node shall drop its switch, and signal the No Request code in byte K1 bits 1-4, and the Bridged code in byte K2 bits 6-8. (Note that this step may be executed in transitions from the switching state to the pass-through state.)
- Step 2: Upon reception of the 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. Extra traffic that was pre-empted shall be re-inserted and the ET code sourced as defined in Rule I #1b. An LP S code due to a signal fail - protection, that was pre-empted, shall be re-inserted.
- Step 4: Once the head-end detects incoming Idle or ET codes from both directions, it shall revert to the idle state. Extra traffic that was pre-empted shall be re-inserted and the ET code shall be sourced as defined in Rule I #1b. A LP-S code due to a signal fail - protection that was pre-empted shall be re-inserted.
- Note that there are cases in which no bridge or switch is to be executed due to other conditions on the ring. In these cases, the NE that initiated the request (i.e. tail-end) shall signal the 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 can not properly signal APS bytes, and therefore cannot properly execute protection switching.

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

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

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

Rule I-S #7 – When a node receives a 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 first provides a set of requirements and objectives with which each ring node shall comply to be able to perform a switch without creating misconnections, and then provides the set of rules necessary to coordinate a transition between switching states.

7.2.6.2.3.1 Ring map and squelch table information

Each node on a ring shall maintain a ring map describing the ring connectivity, and a local squelch table indicating the source and destination of all added, dropped, and pass-through AU-3/4s.

7.2.6.2.3.2 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 squelch table, it shall identify which AU-3/4s are added and dropped at these nodes and shall squelch them bidirectionally.

7.2.6.2.3.3 Transition rules

The following transition rules apply:

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

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

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

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

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

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

Rule S-S #1f: When a NE that is currently executing an EXER-S request receives a higher priority span APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) for the same span, with the exception of LP-S and SD-P, it shall remove any extra traffic from the short path. It shall then signal the new span bridge request with the Idle code in K2 bits 6-8 on the short path, and the new span bridge request on the long path. If there is extra traffic on the long path, the ET code shall be signalled in K2 bits 6-8. The node shall then execute the new span APS request as detailed in Rule I-S #1.

Rule S-S #2 – SWITCH PRE-EMPTION:

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

- drop the span bridge and switch immediately;
- execute the ring APS request (as detailed in Rule I-S #1).

Rule S-S #2b: When a node that is currently executing a span switch receives a ring APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) destined to it for its adjacent span of greater priority than the span switch it is executing, it shall drop the span switch, signal No Request in K1 and Bridged in K2 in the direction of the span APS request, and signal the ring request in K1 and Idle in K2 in the direction of the ring APS request.

Rule S-S #2c: When a node that is currently executing a span switch receives a long-path ring bridge request for a non-adjacent span of greater priority than the span switch it is executing, it shall drop the span switch and signal 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 APS request (due to a locally detected failure, an externally initiated command, or a span bridge request destined to it) for an adjacent span, then the node shall signal in accordance with that request;
- a ring APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) for an adjacent span, then the node shall execute the ring bridge request;
- a long-path ring APS request destined to another node, then the node shall signal in accordance with either Rule S-P #1a or S-P #1b, depending upon whether or not the Bridged indication is being received;
- a span bridge request status destined to another node, then the node shall signal in accordance with either Rule S-P #1c or S-P #1d, depending upon whether or not the Bridged indication is being received;
- a span APS request (due to a locally detected failure or externally initiated command) for the same span, the node shall signal the span bridge request in K1 and Idle in K2.

Rule S-S #2e: If a span switching node that is bridged receives a No Request and an indication that the switch has been dropped for that span, the node shall drop its bridge, and, if the node’s highest priority input is:

- a span bridge request status destined to the node itself, or No Request, then the node shall source No Request in K1 and Idle in K2 in both directions;
- a span APS request (due to a locally detected failure, an externally initiated command, or a span bridge request destined to it) for an adjacent span, then the node shall signal in accordance with that request;
- a ring APS request (due to a locally detected failure, an externally initiated command, or a ring bridge request destined to it) for an adjacent span then the node shall execute that request;

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

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

– a span APS request (due to a locally detected failure or externally initiated command) for the same span, the node shall signal the span bridge request in K1 and Idle in K2.

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

– drop the ring bridge and switch immediately;

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

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

– drop the ring bridge and switch immediately;

– execute the span APS request.

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

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

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

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

2) another failure is detected; or

3) an externally initiated command becomes active.

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

Rule S-S #3b: When a node that is executing a switch in response to an incoming SD-S, SD-R, SF-S, or SF-R bridge request (not due to a locally detected failure) receives a Wait-To-Restore code (unidirectional failure case), it shall send out Reverse Request on the short path and 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 an SD-S or SF-S bridge request because no acknowledgment is received on the short path (time-out, whose duration is an equipment issue), or because the protection channels become unavailable, including degradation or failure of the protection line or LOW-S, the appropriate ring switch shall be attempted.

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

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

7.2.6.2.4 Transitions between switching and pass-through states

Rule S-P #1 – SWITCH PRE-EMPTION RULES (Switching State to Pass-Through State):

Rule S-P #1a: If a span switching node that is not bridged or switched is receiving a Bridged code for that span, and its highest priority input is a long-path ring bridge request destined to another node, then the node shall signal No Request in K1 and 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:

- for NEs without extra traffic, the node shall enter bidirectional full pass-through;
- for NEs with extra traffic, the node shall drop extra traffic bidirectionally, and shall enter unidirectional full pass-through, in the direction of the bridge request only. Upon receiving the crossing K-bytes, the node shall enter bidirectional full pass-through.

Rule S-P #1c: If a span switching node that is not bridged or switched is receiving a Bridged code for that span, and its highest priority input is a span bridge request status destined to another node, then the node shall signal 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. It shall then reinsert any extra traffic that had been pre-empted.

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

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

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

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

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

1) an equal, higher priority, or allowed coexisting externally initiated command;
2) the detection of an equal, higher priority, or allowed coexisting failure;
3) the receipt of an equal, higher priority, or allowed coexisting bridge request destined to that NE;
4) the detection of an APS byte sourced by that NE.

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

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

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

2) execute the ring bridge and switch.

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

7.2.6.2.5 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:

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

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

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

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. Bidirectional 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 normal and extra traffic trail termination functions overlap. In a network application this implies that the normal 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 bidirectional protection switching operation is to be met.

3) *Hold-off times* – Hold-off times are useful for interworking of protection schemes. The objective is that these times should be provisionable on an individual VC basis. A hold-off timer is started when a defect condition is declared and runs for a non-resettable period which is provisionable from 0 to 10 s in steps of 100 ms. When the timer expires, protection switching is initiated if a defect condition is still present at this point. Note that a defect condition does not have to be present for the entire duration of the hold-off period; only the state at the expiry of the hold-off timer is relevant. Furthermore, the defect that triggers the hold-off timer does not need to be of the same type as the one at the expiry of the hold-off period.

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 unidirectional protection switching, bidirectional protection 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 unidirectional protection switching should support revertive switching, non-revertive switching, or both. 1:1 revertive bidirectional protection 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).

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

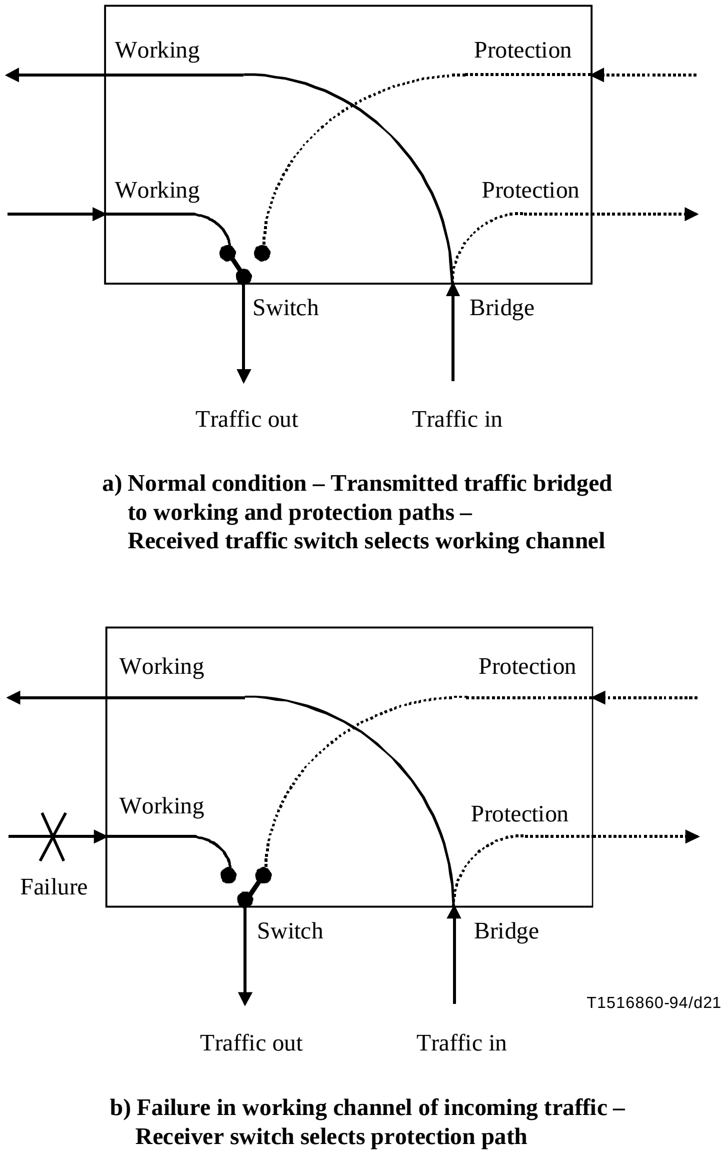
9) *Switch initiation criteria* – Switch initiation criteria for Signal Fail (SF) and/or Signal Degrade (SD) should be in harmony with definitions used in Recommendation G.783. Switch initiation criteria for VC trail protection should be identical to that for the corresponding SNC/N protection.

7.4.3 Application architecture

7.4.3.1 Routing

As a general principle, for each direction of transmission, the protection channels should follow a separate routing from the working channels.

A node under normal operating conditions is shown in Figure 7-11 a). A bridge is used to simultaneously transmit normal traffic signals onto the working and protection trails. The receiver uses a switch to select the signal from the working trail under normal operating conditions. Figure 7-11 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 7-11/G.841 – Node using 1 + 1 trail or SNC protection

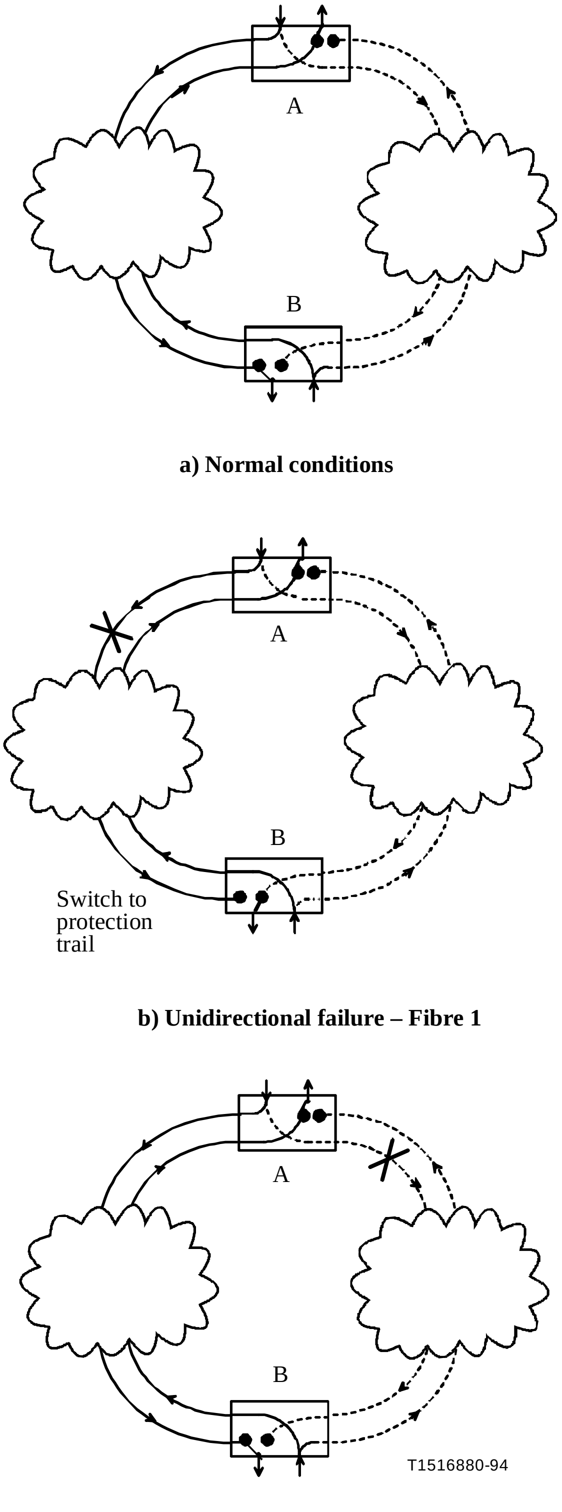
7.4.3.2 1 + 1 unidirectional protection switching

Unidirectional protection switching is illustrated in Figure 7-12 for a 1 + 1 architecture. It is identical to bidirectional protection switching, 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 7-12 a) illustrates a 1 + 1 trail protection network with traffic transmitted between nodes A and B. Traffic inserted at node A is transmitted on different trails in two directions to node B. Under normal operating conditions in revertive modes of operation, the receiver at node B selects the traffic from the working trail. Traffic inserted at node B 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 signal from the protection trail. If a single point failure cuts both directions of transmission, then both directions of transmission on the working trail 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.



a) Normal conditions

b) Unidirectional failure – Fibre 1

c) Unidirectional failure – Fibre 2

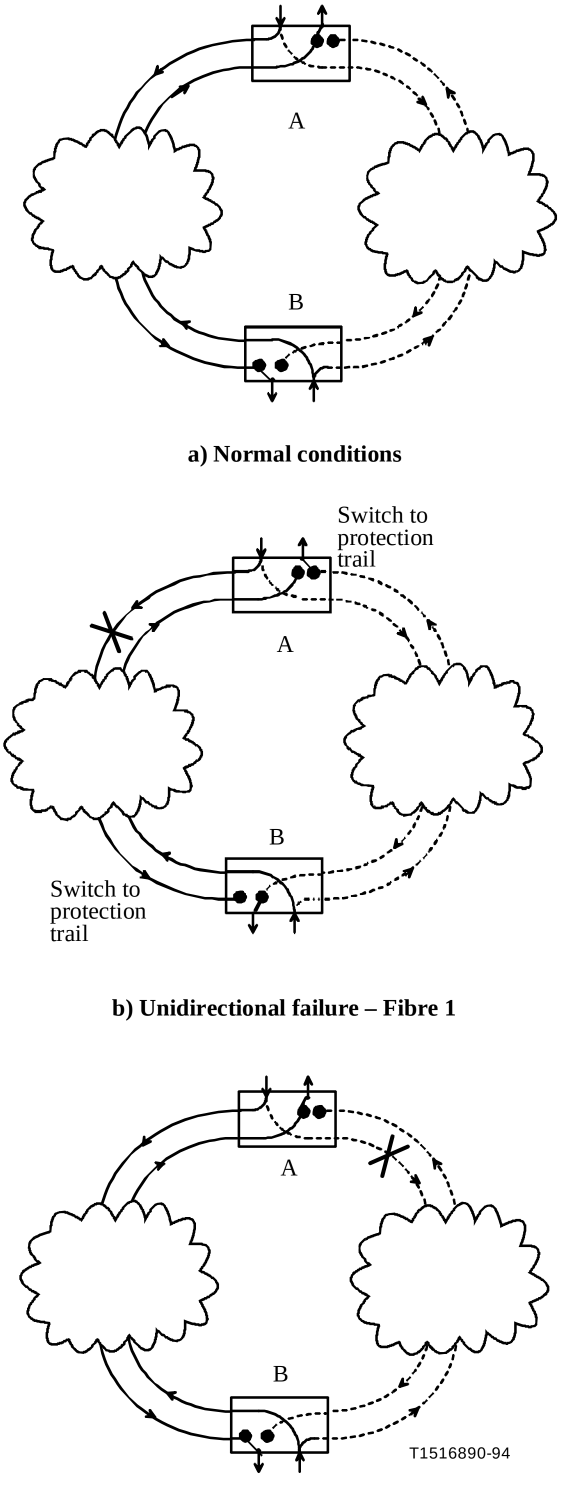
Figure 7-12/G.841 – Two-fibre 1 + 1 trail/SNC protection network with unidirectional protection switching

7.4.3.3 1 + 1 bidirectional protection switching

Figure 7-13 a) illustrates a 1 + 1 trail protection network with traffic transmitted between nodes A and B. Traffic inserted at node A is transmitted on different trails in two directions to node B. Under normal operating conditions in revertive mode of operation, the receiver at node B selects the traffic from the working trail. Traffic inserted at node B is also transmitted in two directions to node A.

When there is a unidirectional failure on the working trail, as shown in Figure 7-13 b), the tail-end switch selects the signal from the protection trail. For bidirectional protection switching, an indication is sent via the APS protocol to force the unaffected direction of transmission to also switch to the protection trail. If a single point failure cuts both directions of transmission, then both directions of transmission on the working trail 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.



a) Normal conditions

b) Unidirectional failure – Fibre 1

c) Unidirectional failure – Fibre 2

Figure 7-13/G.841 – Two-fibre 1 + 1 trail/SNC protection network with bidirectional protection switching

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.

7.4.4.1 1 + 1 unidirectional protection switching

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 7-13.

Table 7-13/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

NOTE 1 – A forced switch to protection should not be overridden by a Signal Fail on the protection channel. Since unidirectional protection 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.

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

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.

clear: This command clears all the externally initiated switch commands listed below and WTR at the node to which the command was addressed.

NOTE – In the definition of the VC trail protection in the 1995 version of Recommendation G.841, the clear command did not clear WTR. Equipment which was designed according to that 1995 definition will not clear WTR if a clear command is sent to this equipment. However, it is possible to achieve a similar behaviour by a carefully selected sequence of external commands (e.g. manual switch followed by clear).

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

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

Forced Switch to Working (FS-W): Switches the selector for normal traffic 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.

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

Manual Switch to Working (MS-W): Switches the selector for normal traffic 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 the TSFprot condition generated by the higher order Trail Termination function defined in Recommendation G.783.

For HO VCs, the Signal Degrade automatically initiated command is defined as the presence of the TSD condition generated by the lower order Trail Termination function defined in Recommendation G.783.

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 the TSFprot condition generated by the lower order Trail Termination function defined in Recommendation G.783.

For LO VCs, the Signal Degrade automatically initiated command is defined as the presence of the TSD condition generated by the lower order Trail Termination function defined in Recommendation G.783.

7.4.4.2 1 + 1 bidirectional protection switching

For further study.

7.4.4.3 1:1 protection switching

For further study.

7.4.5 Protection switching protocol

7.4.5.1 1 + 1 unidirectional protection switching

In this architecture, there is no APS channel required.

7.4.5.2 1 + 1 bidirectional protection switching

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.

The APS acceptance process is for further study.

7.4.5.3 1:1 protection switching

This is for further study.

7.4.6 Protection algorithm operation

7.4.6.1 1 + 1 unidirectional protection switching

7.4.6.1.1 Control of the bridge

In the 1 + 1 architecture, normal traffic is permanently bridged to the working and protection channels.

7.4.6.1.2 Control of the selector

In the 1 + 1 architecture in unidirectional protection switching 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 normal traffic signal shall be restored, i.e. the normal traffic 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 working trail must become fault-free. After the failed working trail meets this criterion (and no other externally initiated commands are present), a fixed period of time shall elapse before it is used again to carry the normal traffic signal. This period, called Wait-To-Restore, should be on the order of 5-12 minutes, and should be capable of being set using 1-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 of the normal traffic signal 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 bidirectional protection switching

This is for further study.

7.4.6.3 1:1 protection switching

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 against 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 traffic at the transmit end of a subnetwork connection is transmitted two separate ways over working and protection paths. 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 switching scheme if it is unidirectional.

In the case of bidirectional 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 unidirectional protection 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 interworking of protection schemes. The objective is that these times should be provisionable on an individual VC basis. A hold-off timer is started when a defect condition is declared and runs for a non-resettable period which is provisionable from 0 to 10 s in steps of 100 ms. When the timer expires, protection

switching is initiated if a defect condition is still present at this point. Note that a defect condition does not have to be present for the entire duration of the hold-off period, only the state at the expiry of the hold-off timer is relevant. Furthermore, the defect that triggers the hold-off timer does not need to be of the same type as the one at the expiry of the hold-off period.

4) *Extent of protection* – LO/HO SNC protection shall restore all LO/HO SNC protected 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 unidirectional protection 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 unidirectional protection switching should support revertive switching, non-revertive switching, or both. 1:1 bidirectional protection 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).

8) *Manual control* – Externally initiated commands may be provided for manual control of protection switching by the operations systems or craft. 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

As a general principle, for each direction of transmission, the protection channels should follow a separate routing from the working channels.

A node under normal operating conditions is shown in Figure 7-11 a). A bridge is used to simultaneously transmit signals onto the working and protection SNCs. The receiver uses a switch to select the signal from the working SNC under normal operating conditions in revertive mode of operation. Figure 7-11 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 automatically to the protection SNC.

8.3.2 1 + 1 unidirectional protection switching

Figure 7-12 a) illustrates SNC protection with traffic transmitted between nodes A and B. Traffic inserted at Node A is transmitted on different SNCs in separate directions to Node B (e.g. a working SNC and a protection SNC). Under normal operating conditions in revertive mode of operation, the receiver at node B selects the traffic signal on the working SNC. When there is a failure on the working SNC, as shown in Figure 7-12 b), the tail-end switch selects the protection SNC. If there is a failure in the protection SNC, as shown in Figure 7-12 c), then the receiver will not need to switch and will continue to detect traffic from the working SNC.

8.3.3 Other architectures

1:1 revertive bidirectional protection switching with extra traffic is for further study.

8.4 Switch initiation criteria

8.4.1 1 + 1 unidirectional protection switching

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.

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
NOTE 1 – A forced switch to protection should not be overridden by a Signal Fail on the protection channel. Since unidirectional protection 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. NOTE 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.	

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.

clear: This command clears all of the externally initiated switch commands listed below and WTR at the node to which the command was addressed.

NOTE – In the definition of the SNC protection in the 1995 version of Recommendation G.841, the clear command did not clear WTR. Equipment which was designed according to that 1995 definition will not clear WTR if a clear command is sent to this equipment. However, it is possible to achieve a similarly behaviour by a carefully selected sequence of external commands (e.g. manual switch followed by clear).

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

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).

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.

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).

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:

- For SNC/I, the SSF condition generated by the Server to the higher order Path Adaptation function (e.g. MS/Sn adaptation defined in Recommendation G.783);
- For SNC/N, the TSFprot condition generated by the higher order Path Termination function defined in Recommendation G.783.

For HO VCs, using SNC/N, the Signal Degrade automatically initiated command is defined as the presence of the TSD condition generated by the higher order Path Termination function defined in Recommendation G.783.

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:

- for SNC/I, the SSF condition generated by the Server to the lower order Path Adaptation function (e.g. Sn/Sm adaptation defined in Recommendation G.783);
- for SNC/N, the TSFprot condition generated by the lower order Path Termination function defined in Recommendation G.783.

For LO VCs using SNC/N, the Signal Degrade automatically initiated command is defined as the presence of the TSD condition generated by the lower order Path Termination function defined in Recommendation G.783.

8.4.2 Other architectures

For further study.

8.5 Protection switching protocol

8.5.1 1 + 1 unidirectional protection switching

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 unidirectional protection switching algorithm

8.6.1.1 Control of the bridge

In the 1 + 1 architecture, the normal traffic signal is permanently bridged to working and protection.

8.6.1.2 Control of the selector

In the 1 + 1 architecture in unidirectional protection switching 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 normal traffic signal 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 working subnetwork connection meets this criterion, (and no other externally initiated commands are present) a fixed period of time shall elapse before the normal traffic signal is restored to that subnetwork connection. This period, called Wait-To-Restore, should be on the order of 5-12 minutes, and should be capable of being set using 1-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)

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. While this annex was developed to meet the needs of the transoceanic application, the protocol modifications in this annex can be used to meet the needs of other high delay spans within an MS shared protection ring, such as those being transmitted over satellite systems.

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 pre-empted extra traffic can be re-established on the protection channels not used to restore the normal 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 ms, 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, pre-empted extra traffic can be re-established on the protection channels not used to restore the normal 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.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.

forced switch to protection - ring (FS-R): This command performs the ring switch of normal traffic signals 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. Normal traffic between any two nodes that had been using the affected span is now rerouted away from this span via the protection channels.

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

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

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 normal 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 failure, an externally initiated command, or received K-bytes) shall pre-empt bridge requests in the prioritized order given in Table 7-1. Bridge requests shall pre-empt bridge request status signalling regardless of the priority of each. Bridge request status signalling shall never pre-empt 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 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 and Switched' status code, it changes the status code to 'Bridged and Switched' for 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 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 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 pre-empted by a higher priority bridge request which is located on the same span [See Figure 7-10 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 7-10 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 pre-empts 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 the 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 long-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 bridge 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 requests not destined to itself from both directions, 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 long-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 command;

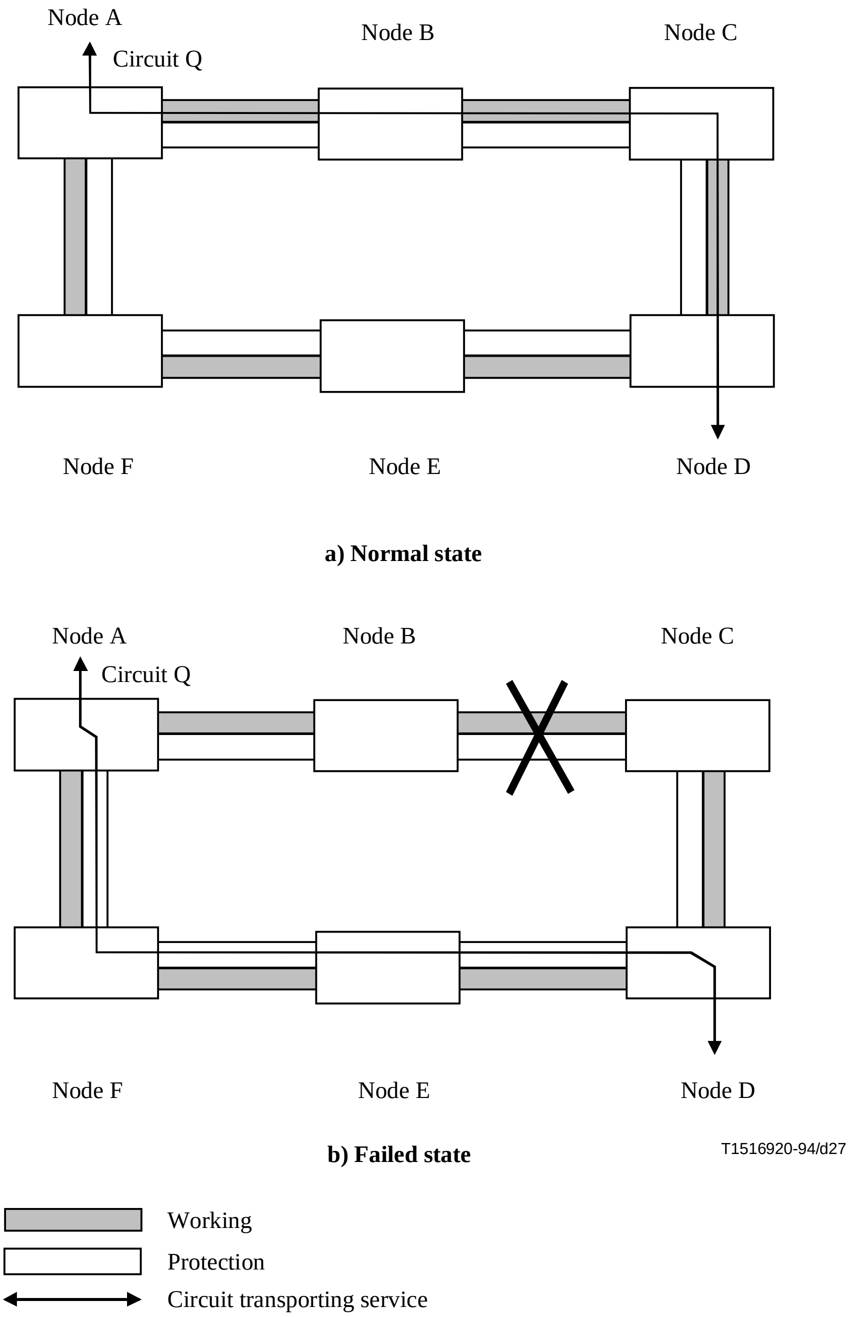
2) the detection of an equal or higher priority failure;

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.



a) Normal state

b) Failed state

Figure A.1/G.841 – Example of circuit routing in failure state for a ring switch (transoceanic application)

ANNEX B

Multiplex section protection (MSP) 1 + 1 optimized protocol, commands and operation

B.1 1 + 1 bidirectional switching optimized for a network using predominantly 1 + 1 bidirectional switching

This algorithm uses working sections 1 and 2 in order to realize high-speed 1 + 1 non-revertive protection switching. In other words, revertive action is prevented by switching between working sections.

Bytes K1 and K2 (b1-b5) are exchanged to complete a switch. Since the bridge is permanent (see Figure B.1), the traffic is always bridged to working section 1 and working section 2. Byte K2 indicates the number of the section which carries traffic when no switch is active. This will be referred to as the primary section. The other working section, referred to as the secondary section, provides protection for the primary section. Exchange of K1/K2 to control this protection occurs over the secondary section. The section number on byte K2 will be changed after a switch has cleared. Clearing of a switch is completed when both the receive end switches select the other working section as primary and receive no request.

In 1 + 1 bidirectional optimized switching, both sections 1 and 2 are equal to working sections. K1/K2 bytes are received on the secondary section. K1/K2 bytes need not always be received on the primary section, but in general, K1/K2 must be sent on both sections to provide for successful clearing operations and to allow recovery of the primary channel mismatch condition (See B.1.5).

In 1 + 1 bidirectional operation optimized for a network using predominately 1 + 1 bidirectional switching, the selector is on the primary section in the absence of a switch request. All switch requests are for a switch from the primary section to the secondary section. Once a switch request clears normally, traffic is maintained on the section to which it was switched by making that section the primary section.

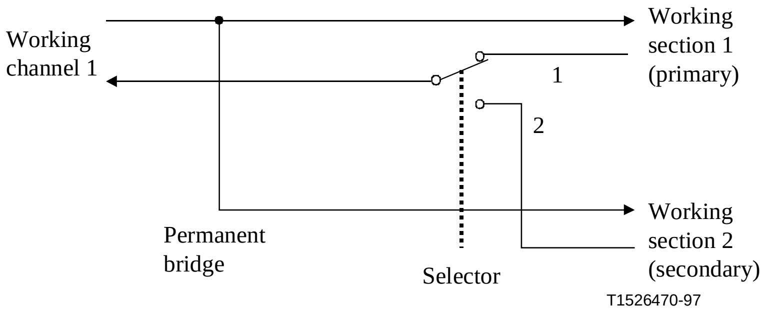


Figure B.1/G.841 – MSP Switch – 1 + 1 bidirectional switching, optimized (shown in released position with working section 1 as primary)

B.1.1 Lockout

In 1 + 1 bidirectional optimized switching, Lockout is considered as a local request which is not signalled across the K-bytes. The effect of lockout is to freeze the selector position and transmitted K-bytes until the lockout request is cleared. When a lockout request is cleared, the selector and transmitted K-bytes will be set by applying any changed section conditions and incoming K-bytes to the previous state.

B.1.2 Secondary section failure

The secondary section is considered failed whenever it is an SF or SD condition. As an option, the secondary section may also be considered failed whenever MS-RDI is being received for the secondary section.

No switch request will be issued or acknowledged when the secondary section has failed. When the secondary section has failed, the near end will always indicate no request on the K1 byte and the selector will choose service from the primary section. In addition, if the secondary section fails while a switch request is active and not locked, the switch request will be abandoned: That is, the selector will be returned to the primary section and no request will be sent on the K1 byte.

B.1.3 K1/K2 byte coding

The K1 byte indicates a request for switch action.

Bits 1-4 indicate the type of request, as listed in Table B.1. A request can be:

1) a condition (SF or SD) associated with the primary condition. Conditions are not indicated for the secondary section.

2) a state (wait-to-restore, no request, reverse request) of the MSP function. Wait-to-restore and reverse request always indicate the primary section. No request always indicates the null signal.

3) an external request (forced switch) to switch from the primary to the secondary line.

Table B.1/G.841 – Types of request

Bits	Condition, state or external request	Order
1 2 3 4		
1 1 1 1	Unused (Note 1)	–
1 1 1 0	Forced switch	Highest
1 1 0 1	Unused (Note 1)	↑
1 1 0 0	Signal fail	.
1 0 1 1	Unused (Note 1)	.
1 0 1 0	Signal degrade	.
1 0 0 1	Unused (Note 1)	.
1 0 0 0	Unused (Note 1)	.
0 1 1 1	Unused (Note 1)	.
0 1 1 0	Wait-to restore	.
0 1 0 1	Unused (Note 1)	.
0 1 0 0	Unused (Note 1)	.
0 0 1 1	Unused (Note 1)	.
0 0 1 0	Reverse request	.
		.
0 0 0 1	Unused (Note 1)	↓
0 0 0 0	No request	Lowest

NOTE 1 – When receiving an unused code, the equipment shall behave as though it is still receiving the most recently received used code.

NOTE 2 – In the case of Signal Degrade (SD) on both working sections, no protection switching should take place. Depending on the order in time of the individual SD, the selectors may be switched to section 1 or section 2. In any case, no switching should take place.

Bits 5-8 indicate the number of the section to be protected by the switch. This will be the null signal for no request, and the primary section for all other requests.

Table B.2/G.841 – K1 channel number

Channel number	Requesting switch action
0	No working section (no request only)
1	Working section 1 Indicates a request to switch away from section number 1.
2	Working section 2 Indicates a request to switch away from section number 2.

B.1.4 K2 byte coding

For 1 + 1 bidirectional switching optimized for a network using predominantly 1 + 1 bidirectional switching, the sent K2 byte shall indicate the selector position in bits 1-4:

a) Channel number 1 (0001) if section 1 is working;

b) Channel number 2 (0010) if section 2 is working.

Table B.3/G.841 – K2 channel number

Channel number	Indication
1	Section 1 is primary
2	Section 2 is primary

B.1.5 Primary section mismatch

In the event that the near end and far end disagree about which section is primary (i.e. one end is indicating section 1 in byte K2 and the other is indicating section 2), the side that believed section 2 was primary shall change so that section 1 is primary and set its state according to local line conditions and the incoming K-bytes.

B.2 Switch commands

Forced Switch

Transfers service to the secondary section, unless a local Lockout is in effect, an equal or higher priority request is in effect, or the secondary section has failed. Since forced switch has higher priority than SF or SD, Forced Switch will be indicated as the reason for the switch to the secondary section even if the primary section is in an SF or SD condition.

Forced Switch Clear

If no lockout is in effect and a forced switch is active, the switch will be cleared by changing the primary line indication to the currently active line and changing the request to no request. If no Forced switch is active, the Forced Switch Clear command is invalid.

B.3 Switch operation

Table B.4 illustrates the operation of a 1 + 1 bidirectional protection switching system for signal failure on the primary section when section 1 is primary. Table B.5 illustrates the operation of a 1 + 1 bidirectional optimized protection switching system for a Forced Switch from the primary to the secondary section when section 2 is primary. Note that for a Forced switch command, the wait to restore state is not necessary for clearing.

Table B.4/G.841 – Example of 1 + 1 bidirectional switching optimized for a network using predominantly 1 + 1 bidirectional switching – SF on working section 1

Failure condition or controller state	**APS bytes**				**Action**	
	C → A		**A → C**			
	Byte K1	**Byte K2**	**Byte K1**	**Byte K2**	**At C**	**At A**
No fault condition traffic on channel 1	0000 0000	0001 0000	0000 0000	0001 0000		
Signal fail on section 1 at side C	1100 0001	0001 0000	0000 0000	0001 0000	Detect local request. Update K1.	
	1100 0001	0001 0000	0010 0001	0001 0000		Detect remote request. Switch to channel 2. Issue Reverse Request.
	1100 0001	0001 0000	0010 0001	0001 0000	Detect reverse request. Switch to channel 2.	
Signal fail on section 1 at side C cleared and persistence check	0110 0001	0001 0000	0010 0001	0001 0000	Issue Wait-to-Restore Request.	
Wait to restore expires	0000 0000	0010 0000	0010 0001	0001 0000	Send no request. Update K1, K2.	
No fault condition. Traffic on section 2	0000 0000	0010 0000	0000 0000	0010 0000		Send no request. Update K1, K2.

Table B.5/G.841 – Example of 1 + 1 bidirectional switching optimized for a network using predominantly 1 + 1 bidirectional switching – Forced Switch from Working Section 2

Failure condition or controller state	APS bytes				Action	
	C → A		A → C			
	Byte K1	Byte K2	Byte K1	Byte K2	At C	At A
No fault condition traffic on channel 2	0000 0000	0010 0000	0000 0000	0010 0000		
Forced Switch from section 2 at side C	1110 0010	0010 0000	0000 0000	0010 0000	Detect local request. Update K1.	
	1110 0010	0010 0000	0010 0010	0010 0000		Detect remote request. Switch to channel 2. Issue Reverse Request.
	1110 0010	0010 0000	0010 0010	0010 0000	Detect reverse request. Switch to channel 2.	
Clear Forced Switch at side C	0000 0000	0001 0000	0010 0010	0010 0000	Send no request. Update K1, K2.	
No Switch active. Traffic on section 1.	0000 0000	0001 0000	0000 0000	0001 0000		Send no request. Update K1, K2.

APPENDIX I

Examples of protection switching in an MS shared protection ring

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.

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 nodes 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 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 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.

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

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

See Figure I.6.

This example covers the case of a unidirectional signal fail - ring condition on a four-fibre ring pre-empting 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 S-S #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 #1a). Node D, upon seeing a dropped switch at node C, drops its bridge and acts on its highest priority input (Rule S-S #2e) to enter full pass-through. Node C, upon seeing the dropped bridge from node D, acts on its highest priority input (Rule S-P #1b) to enter full pass-through. With all the intermediate nodes in full pass-through, nodes F and G finally receive long-path ring bridge requests. Nodes F and G each execute a bridge and switch (Rule I-S #1b, second point) and update 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 #1b). Node F loses its long path ring bridge request due to the span bridge request status from Node D. Node F drops its bridge and switch (Rule S #5), terminates its WTR signalling, and enters K-byte pass-through (Rule S #8). Similarly, when Node G loses its long-path ring bridge request, it drops its bridge and switch (Rule S #5), terminates its WTR signalling, and enters bidirectional K-byte pass-through. Node D, upon seeing a Bridged code on the short path from node C, executes a span bridge and switch, and updates byte K2 bits 6-8 (Rule I-S #1b). Node C, upon seeing a Bridged and Switched code from node D, completes the process by executing a span switch and updating byte K2 bits 6-8 (Rule I-S #1b). 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_4 (not shown), the span SD condition on the working channels from node C to node D clears. The signalling proceeds in a manner as shown at time T2 in Figure I.1, except that:

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

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

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

See Figure I.7.

This example covers the case of a unidirectional signal fail - span condition on a four-fibre ring pre-empting 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 (Rules S #1, G #1). Node C, upon seeing this span bridge request status, drops its ring bridge and switch because it is no longer receiving a long-path ring bridge request (Rule S #5). Node C updates its 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 #1b, third point, and Rule S #3). Node E, upon seeing the Bridged code from node D, executes a span bridge and switch, and updates byte K2 bits 6-8 (Rule I-S #1b, 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 #1b, third point). Signalling reaches steady state.

At time T_3, the SF condition on the working channels from node D to node E clears. Node E would enter 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 #1b). 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.

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

See Figure I.8.

This example covers the case of a unidirectional signal fail - ring condition on a four-fibre ring pre-empting 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 #1b) 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 #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 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 #1b, 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 #1b, third point). Node E, upon seeing the Bridged and Switched codes from node F, completes the process by executing a span switch and updating byte K2 bits 6-8 (Rule I-S #1b, third point). Meanwhile, node D, upon seeing the span bridge request from node F, loses its long-path ring bridge request from node E. Node D therefore drops its ring bridge and switch (Rule S #5), and acts on the span bridge request status destined to node E by entering K-byte pass-through (Rule S-P #1g). Intermediate full pass-through nodes A, B, C and G eventually receive a span bridge request status not destined to them from both directions, so they move into 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.

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 #1a, 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 #1a, 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). 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). Node B sees ring bridge requests that are not destined to it, due to the first SF-R between nodes E and F. Node B maintains ring bridges and switches on the tributaries affected by the first failure, and enters full pass-through [Rule S-P #1f, point 1), in 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).

I.10 Node failure on a ring with extra traffic capability (see Figure I.11)

Figure I.11 covers the case of extra traffic squelching on a ring after a node failure on either a two- or four-fiber ring. 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. Extra traffic is supported on the protection channels around the ring. At time T_1, both nodes E and G detect an SF condition on their working and protection channels. Nodes E and G drop extra traffic bidirectionally, become switching nodes (Rule I-S #1a, S #7), and source bridge requests on the long and short paths. All intermediate nodes will drop extra traffic bidirectionally, and enter into unidirectional full pass-through (Rule I-P #1). Non-LO VC access nodes enter bidirectional full pass-through upon receiving crossing K-bytes. Node E, upon reception of the bridge request from G on the long path, squelches all potentially misconnected traffic, executes a ring bridge and switch, and updates byte K2 bits 6-8 (Rule I-S #1b). Node G, upon reception of the bridge request from E on the long path squelches all potentially misconnected traffic, executes a ring bridge and switch, and updates byte K2 bits 6-8 (Rule I-S #1b). Signalling reaches steady state.

At time T_2, the failed node has recovered and the recovery sequence proceeds as per normal node recovery. Extra traffic is unsquelched when the node receives No Request and Idle or ET code from both directions.

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

See Figure I.11.

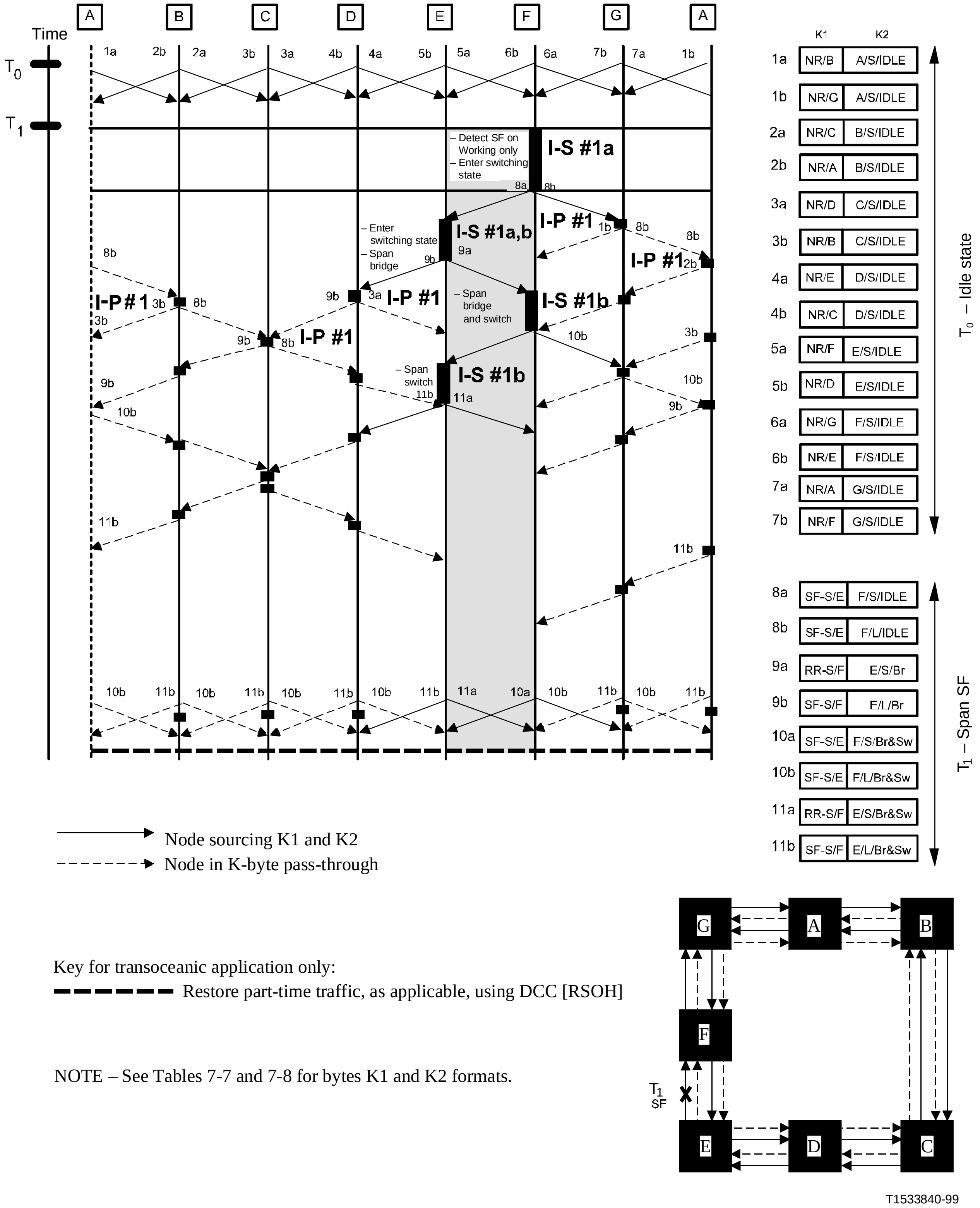
This example covers the case of a unidirectional signal fail - span condition on a four-fibre ring pre-empting a unidirectional signal fail - ring condition that had previously existed on an adjacent span.

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

At time T_2, node E detects a SF condition on its working channel from node D. Node E becomes a switching node (Rule S-P #2a) and sources a span bridge request towards node D and a span bridge request status towards node F destined for node D (Rules S #1, G #1). Node D, upon seeing the higher priority span bridge request from node E, drops its ring bridge and switch, and signals based on its highest allowed coexisting APS requests (Rules G #1c, S-S #2h). Node D's highest priority input allowed to coexist is SF-S request from node E, and SF-P detected from node C (Rule S-S #2 h). It executes a span bridge towards node E (Rule S-S #2f), and signals accordingly (Rules I-S #1b, S #3). Node D also signals SF-P and RDI towards node C, since SF-P and SF-S are allowed to coexist (Rules S #4 a, S-S #2 h). Node C, upon losing the ring bridge request and seeing SF-P destined for it on the short path, becomes a span switching node, and responds to the span request accordingly (Rules S-P #2 b, S #1b). Node E, upon seeing the Bridged code from Node D, executes a span bridge and switch, and updates byte K2 bits 6-8 (Rule I-S #1b). Node D, upon seeing the Bridged code from node E, executes a switch, and updates byte K2 bits 6-8 accordingly (Rule I-S #1b). Intermediate nodes enter K-byte pass through when crossing K-bytes are detected (Rule P-P #2). Signalling reaches steady state.

At time T_3, the SF condition on the working channels from node D to node E clears. Node E enters Wait-to-Restore and signals accordingly (Rule S-S #3a). Node D, upon seeing the WTR code from node E, drops its span bridge and switch, and acts on all its inputs, which is a detected SF-R and a lower priority WTR request from node E. Node D signals a ring bridge request toward node C on both the long and short path (Rule S-S #2d). Node E, upon seeing a ring bridge request destined to another node, enters bidirectional full pass-through (Rule S-P #1e). Node C, upon losing the span bridge request and seeing a long-path ring bridge request from node D, executes a ring bridge and switch, and updates byte K2 bits 6-8 (Rules S #6, I-S #1b). Node D, upon seeing a long-path ring bridge request from node C, also executes a ring bridge and switch, and updates 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 C to node D 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.



	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

——→ Node sourcing K1 and K2

- - - -→ Node in K-byte pass-through

Key for transoceanic application only:

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

NOTE – See Tables 7-7 and 7-8 for bytes K1 and K2 formats.

Figure I.1/G.841 – Four-fibre MS shared protection ring – Unidirectional failure (span) on working from E to F

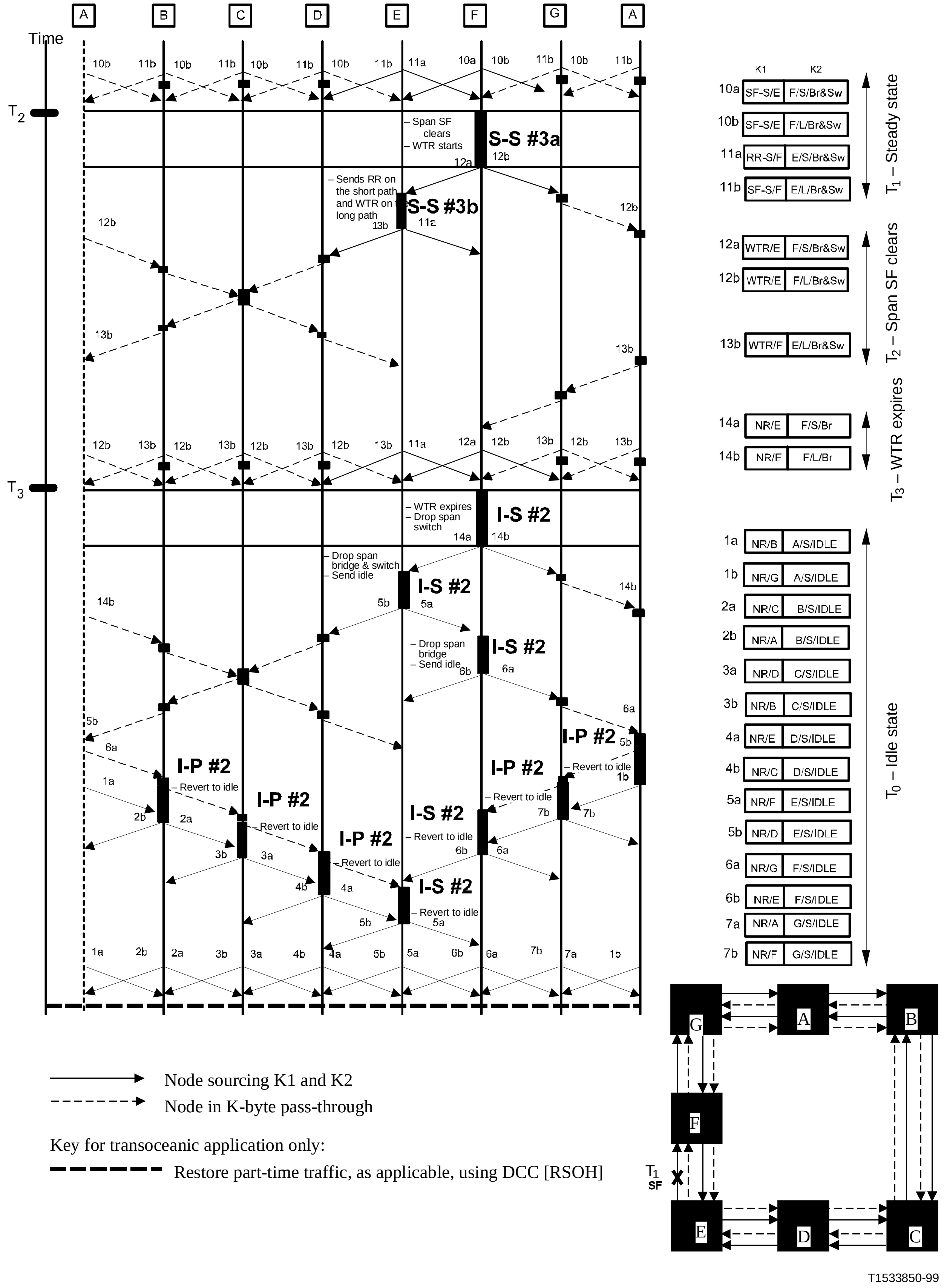
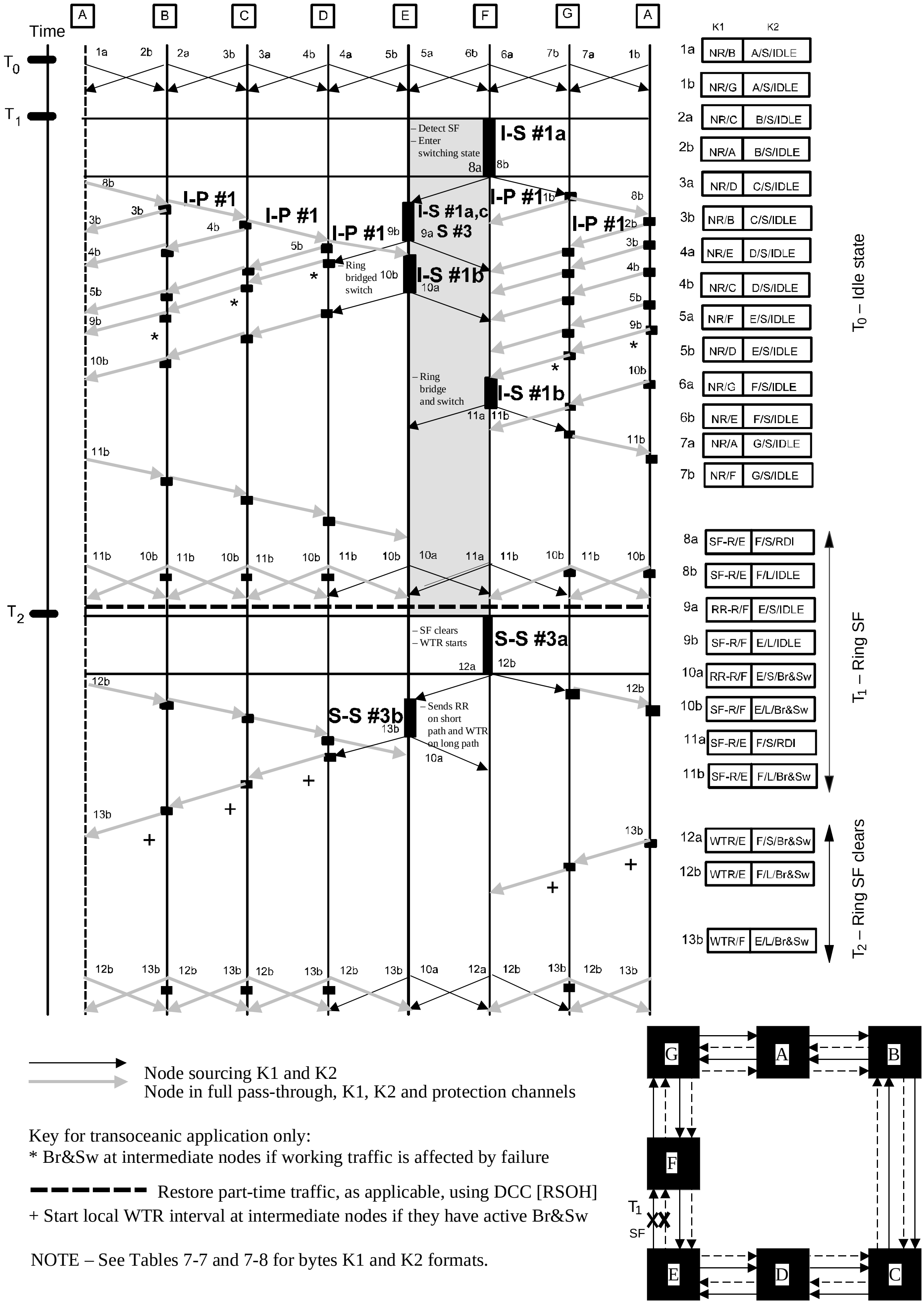


Figure I.1/G.841 – Four-fibre MS shared protection ring – Unidirectional failure (span) on working from E to F *(concluded)*



	K1	K2	
1a	NR/B	A/S/IDLE	T0 – Idle state
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	T1 – Ring SF
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	T2 – Ring SF clears
12b	WTR/E	F/L/Br&Sw	
13b	WTR/F	E/L/Br&Sw	

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 7-7 and 7-8 for bytes K1 and K2 formats.

Figure I.2/G.841 – Two- or four-fibre MS shared protection ring – Unidirectional SF (ring)

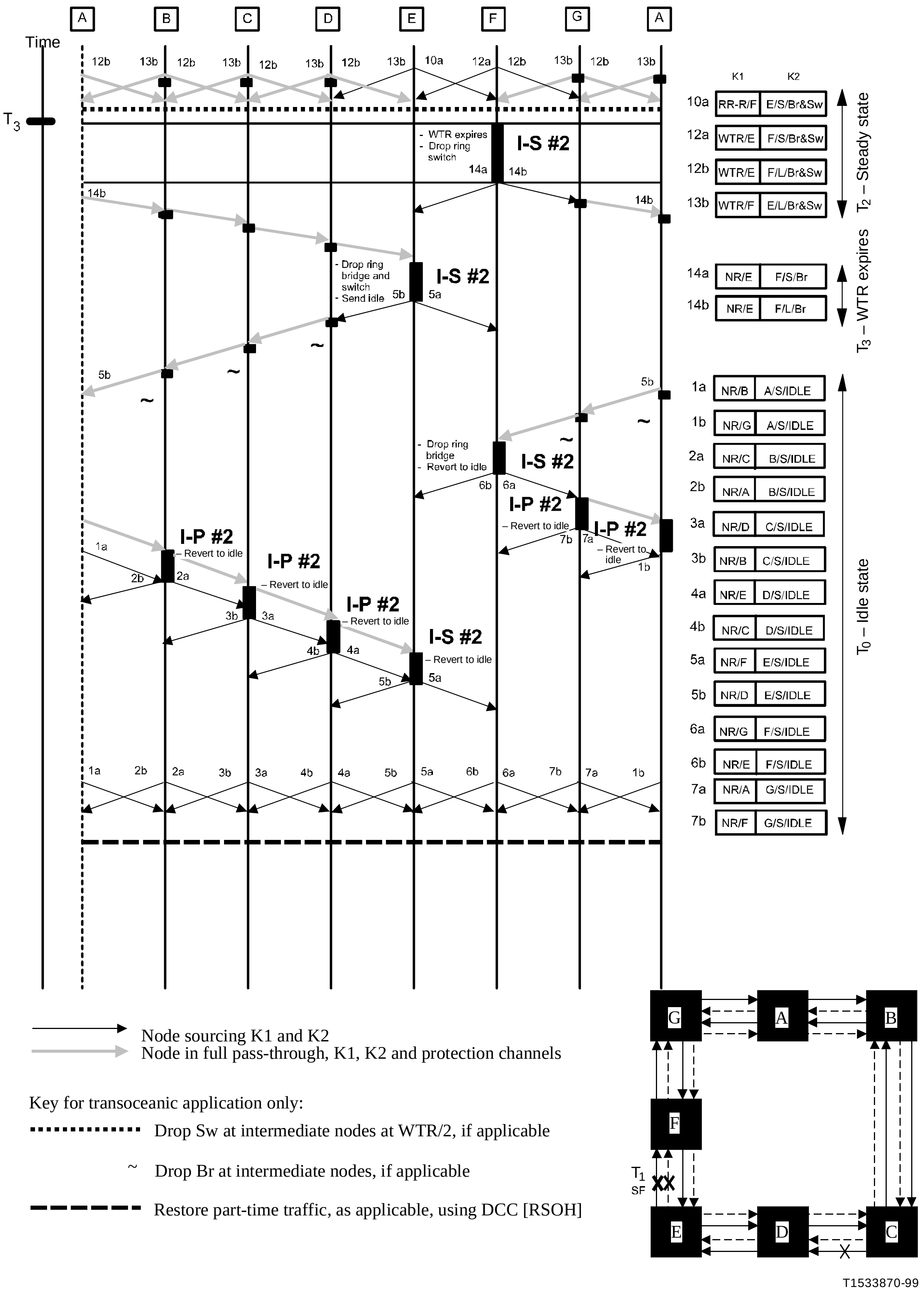
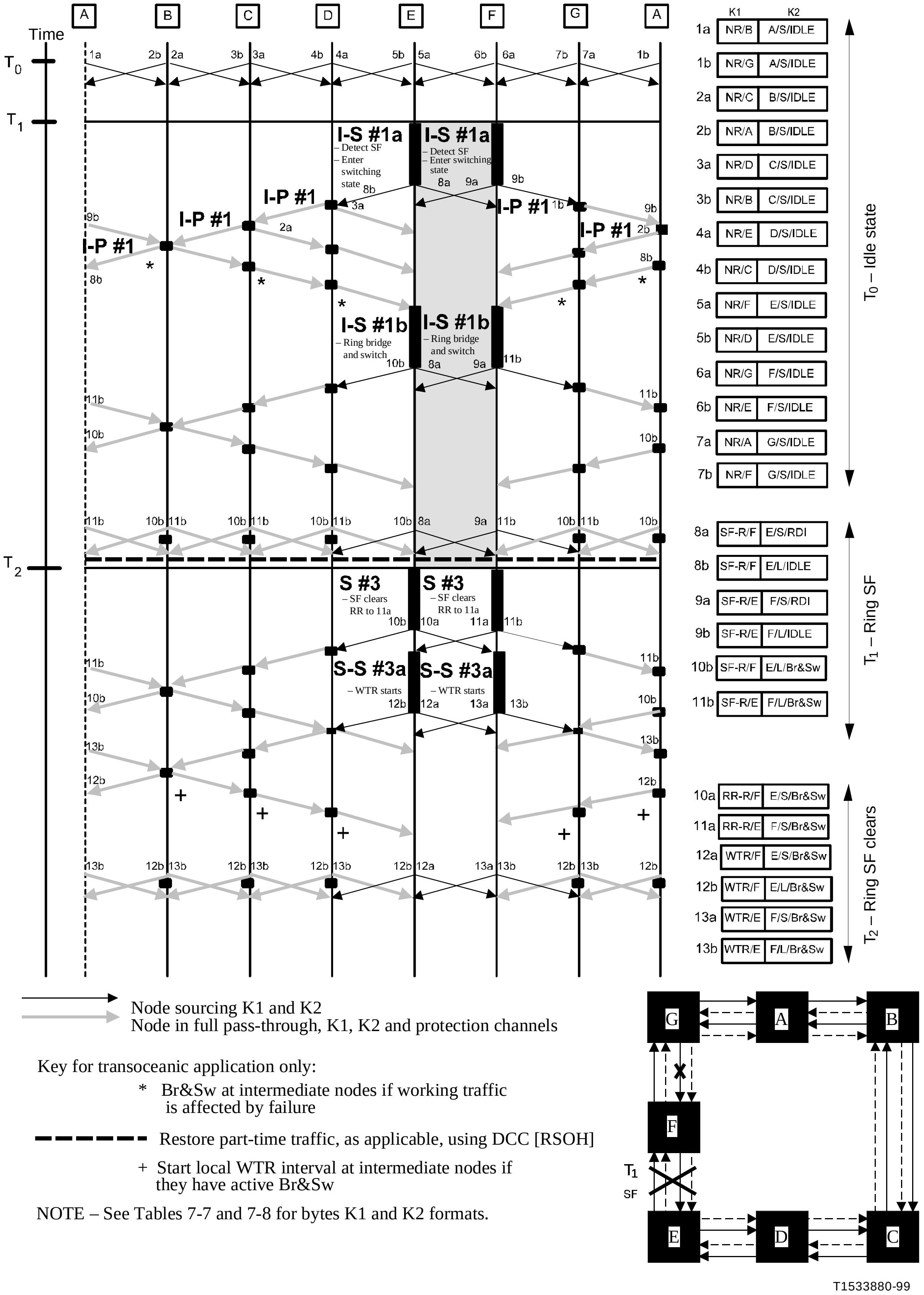


Figure I.2/G.841 – Two- or four-fibre MS shared protection ring – Unidirectional SF (ring) *(concluded)*



	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

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

Key for transoceanic application only:

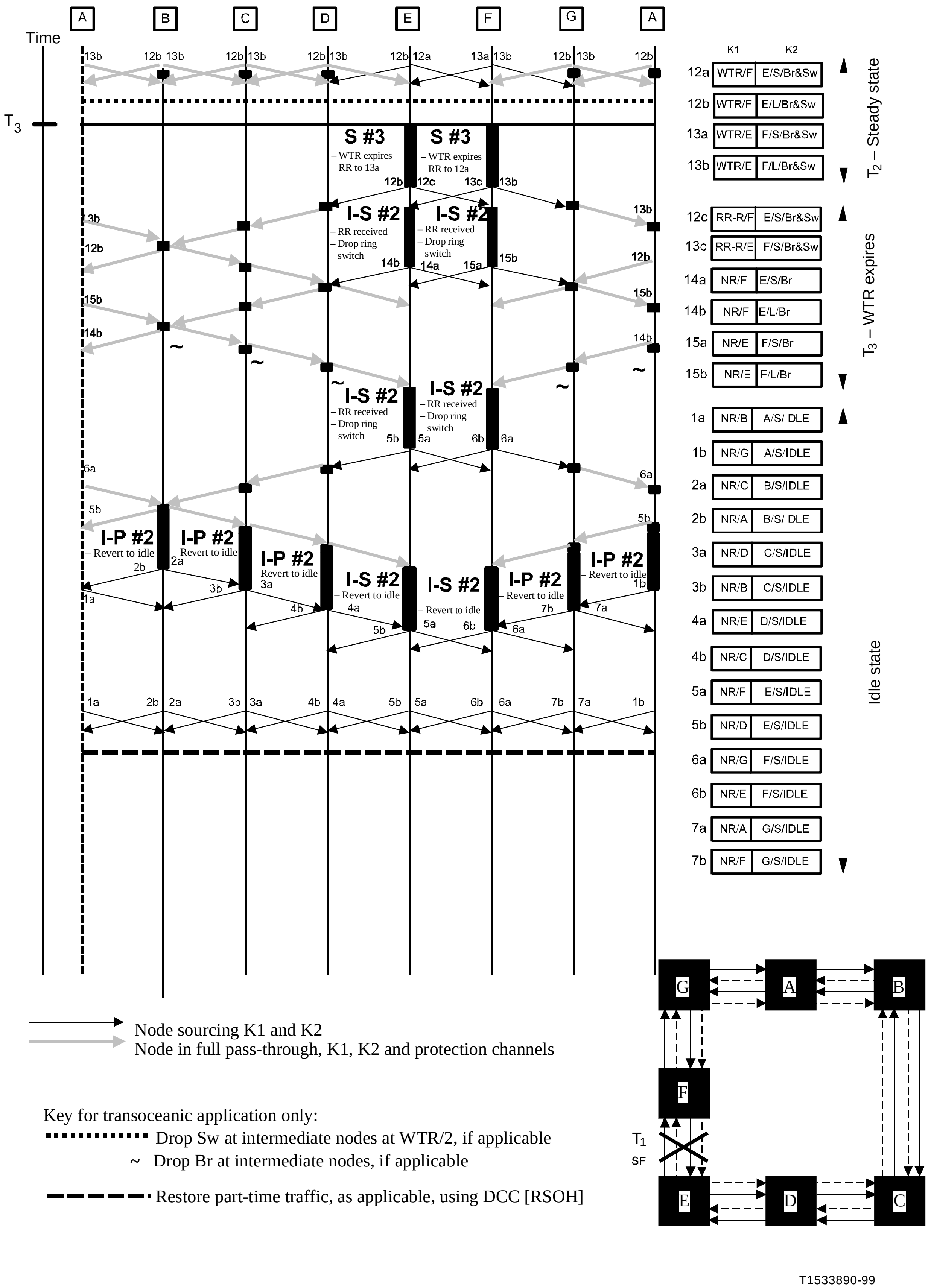
* Br&Sw at intermediate nodes if working traffic is affected by failure

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 7-7 and 7-8 for bytes K1 and K2 formats.

Figure I.3/G.841 – Two- or four-fibre MS shared protection ring – Bidirectional SF (ring)



	K1	K2	
12a	WTR/F	E/S/Br&Sw	T_2 – Steady state
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	T_3 – WTR expires
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	Idle state
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	

Node sourcing K1 and K2

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

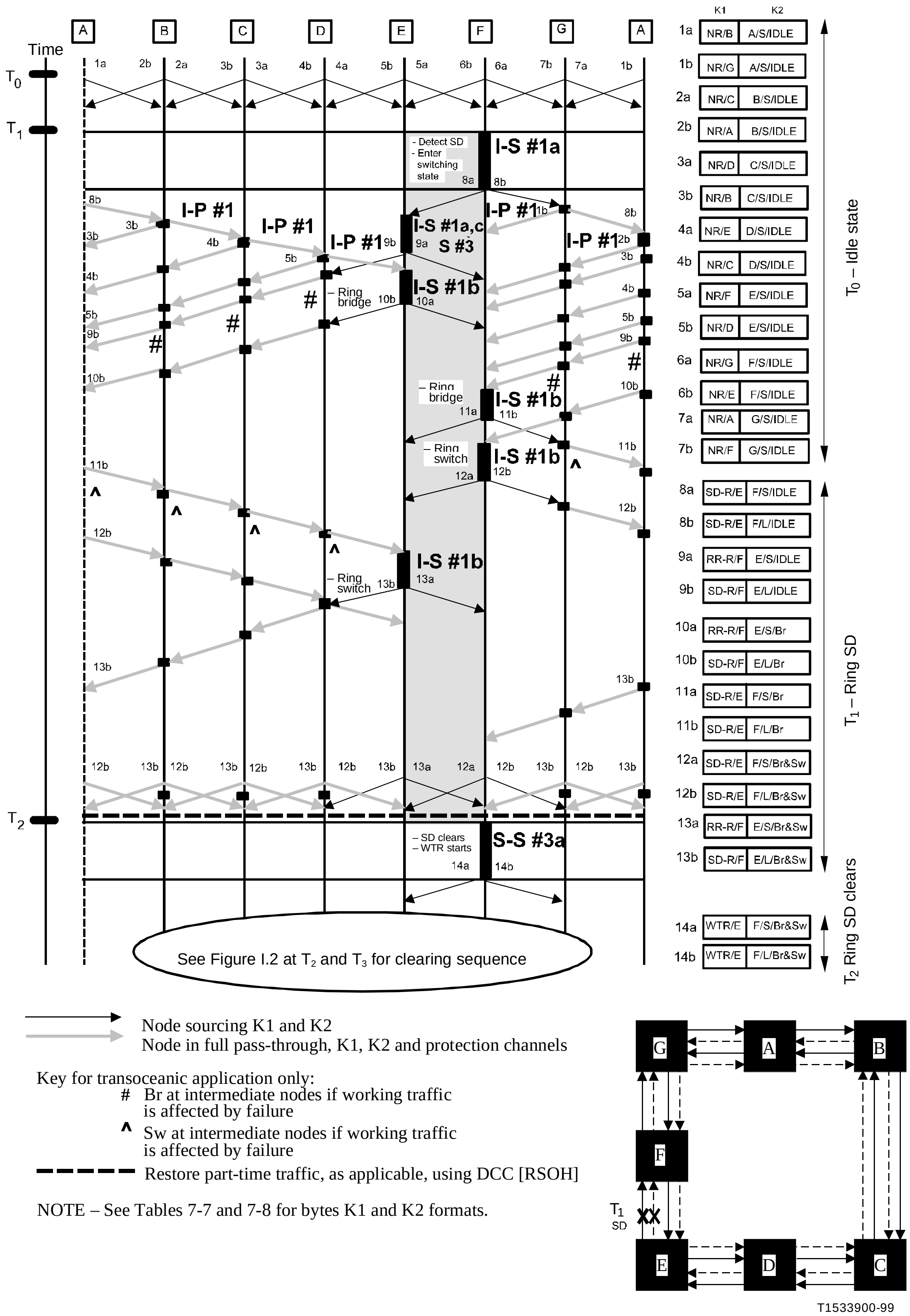
Key for transoceanic application only:

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]

Figure I.3/G.841 – Two- or four-fibre MS shared protection ring – Bidirectional SF (ring) ***(concluded)***



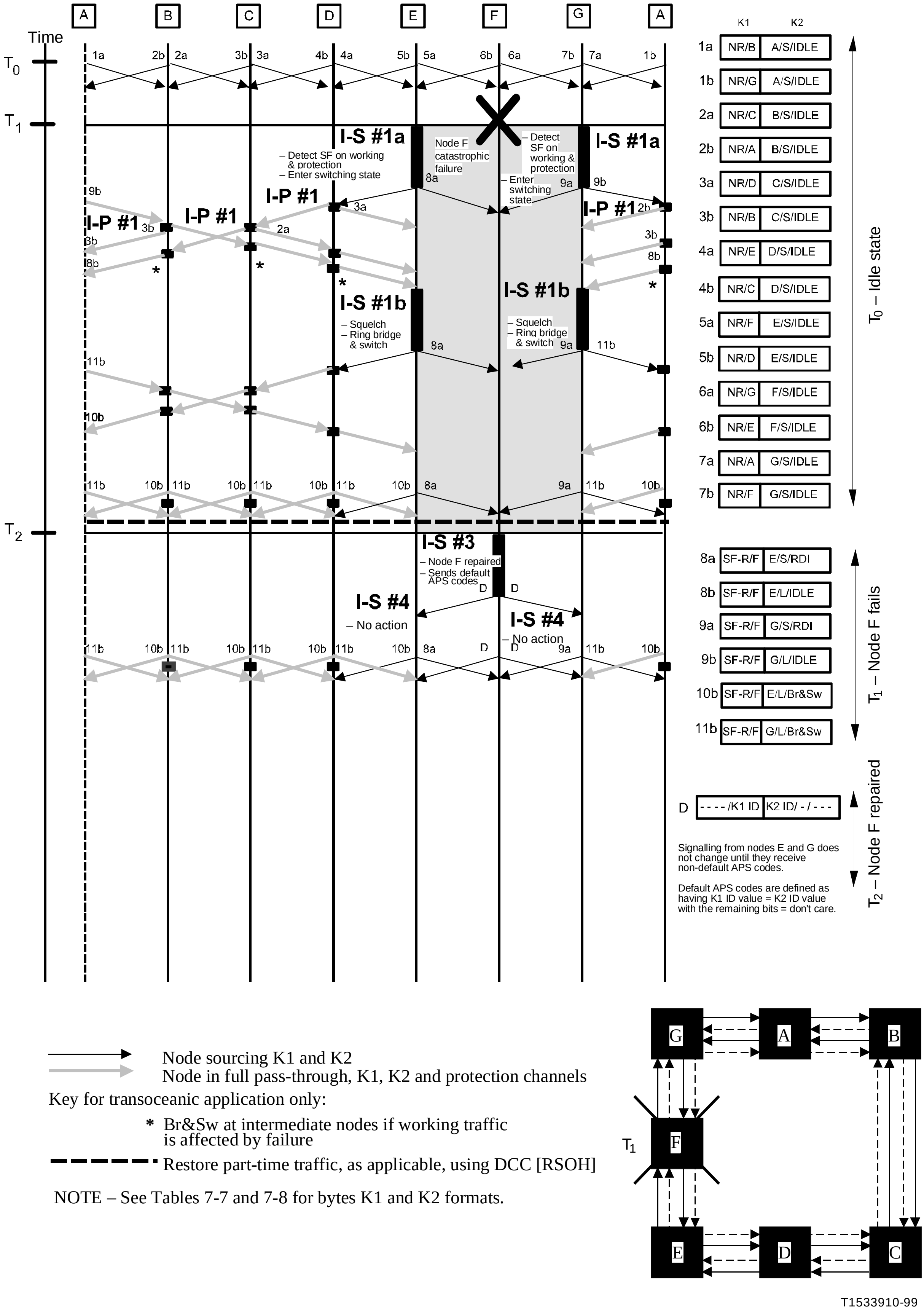
	K1	K2
1a	NR/B	A/S/IDLE
1b	NR/G	A/S/IDLE
2a	NR/C	B/S/IDLE
2b	NR/A	B/S/IDLE
3a	NR/D	C/S/IDLE
3b	NR/B	C/S/IDLE
4a	NR/E	D/S/IDLE
4b	NR/C	D/S/IDLE
5a	NR/F	E/S/IDLE
5b	NR/D	E/S/IDLE
6a	NR/G	F/S/IDLE
6b	NR/E	F/S/IDLE
7a	NR/A	G/S/IDLE
7b	NR/F	G/S/IDLE
8a	SD-R/E	F/S/IDLE
8b	SD-R/E	F/L/IDLE
9a	RR-R/F	E/S/IDLE
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 7-7 and 7-8 for bytes K1 and K2 formats.

Figure I.4/G.841 – Two- or four-fibre MS shared protection ring – Unidirectional SD (ring)



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]

NOTE – See Tables 7-7 and 7-8 for bytes K1 and K2 formats.

Figure I.5/G.841 – Four-fibre MS shared protection ring – Node failure

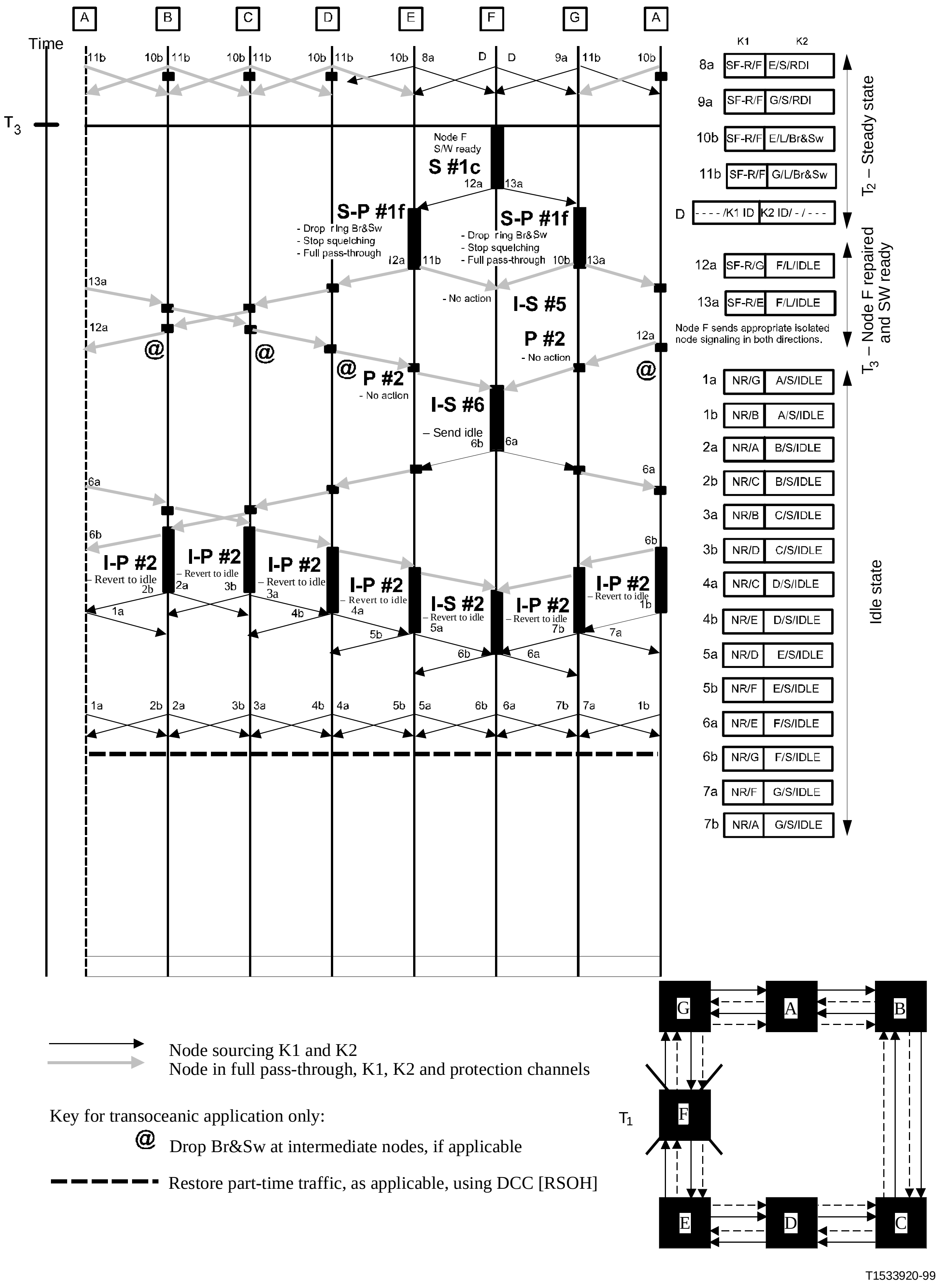
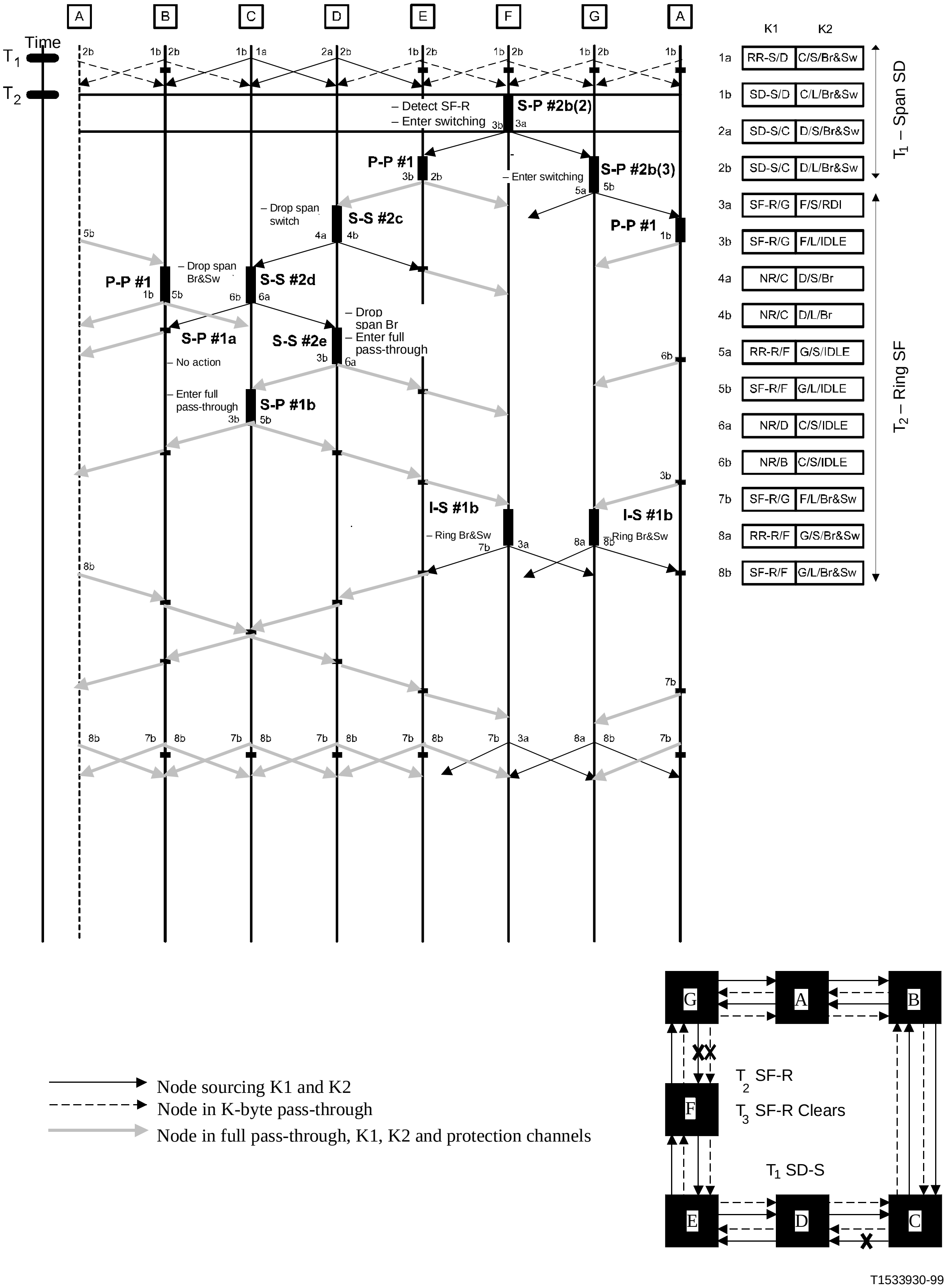


Figure I.5/G.841 – Four-fibre MS shared protection ring – Node failure *(concluded)*



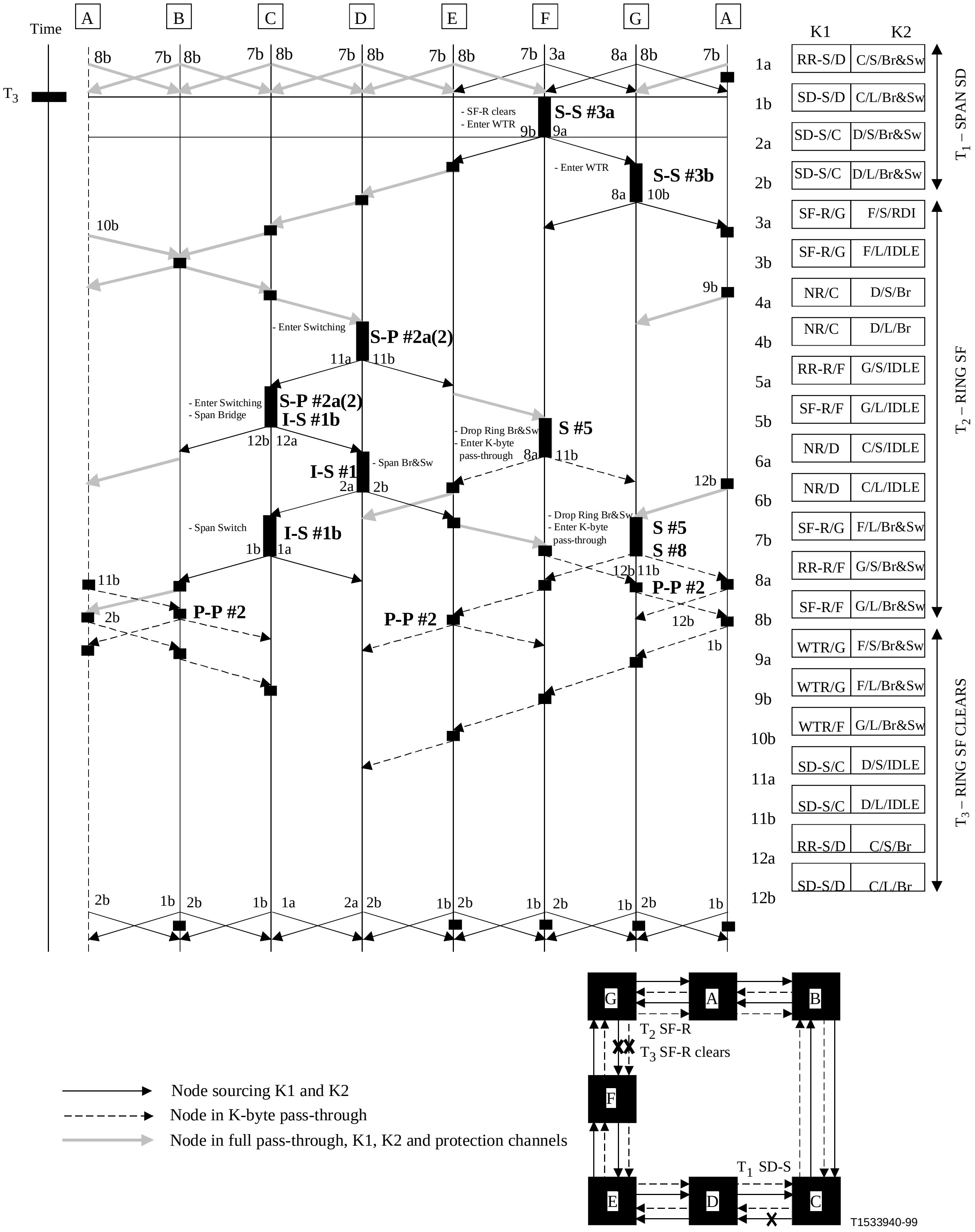
	K1	K2
1a	RR-S/D	C/S/Br&Sw
1b	SD-S/D	C/L/Br&Sw
2a	SD-S/C	D/S/Br&Sw
2b	SD-S/C	D/L/Br&Sw
3a	SF-R/G	F/S/RDI
3b	SF-R/G	F/L/IDLE
4a	NR/C	D/S/Br
4b	NR/C	D/L/Br
5a	RR-R/F	G/S/IDLE
5b	SF-R/F	G/L/IDLE
6a	NR/D	C/S/IDLE
6b	NR/B	C/S/IDLE
7b	SF-R/G	F/L/Br&Sw
8a	RR-R/F	G/S/Br&Sw
8b	SF-R/F	G/L/Br&Sw

Node sourcing K1 and K2

Node in K-byte pass-through

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

Figure I.6/G.841 – Four-fibre MS shared protection ring – Unidirectional SF-R pre-empting a unidirectional SD-S on non-adjacent spans



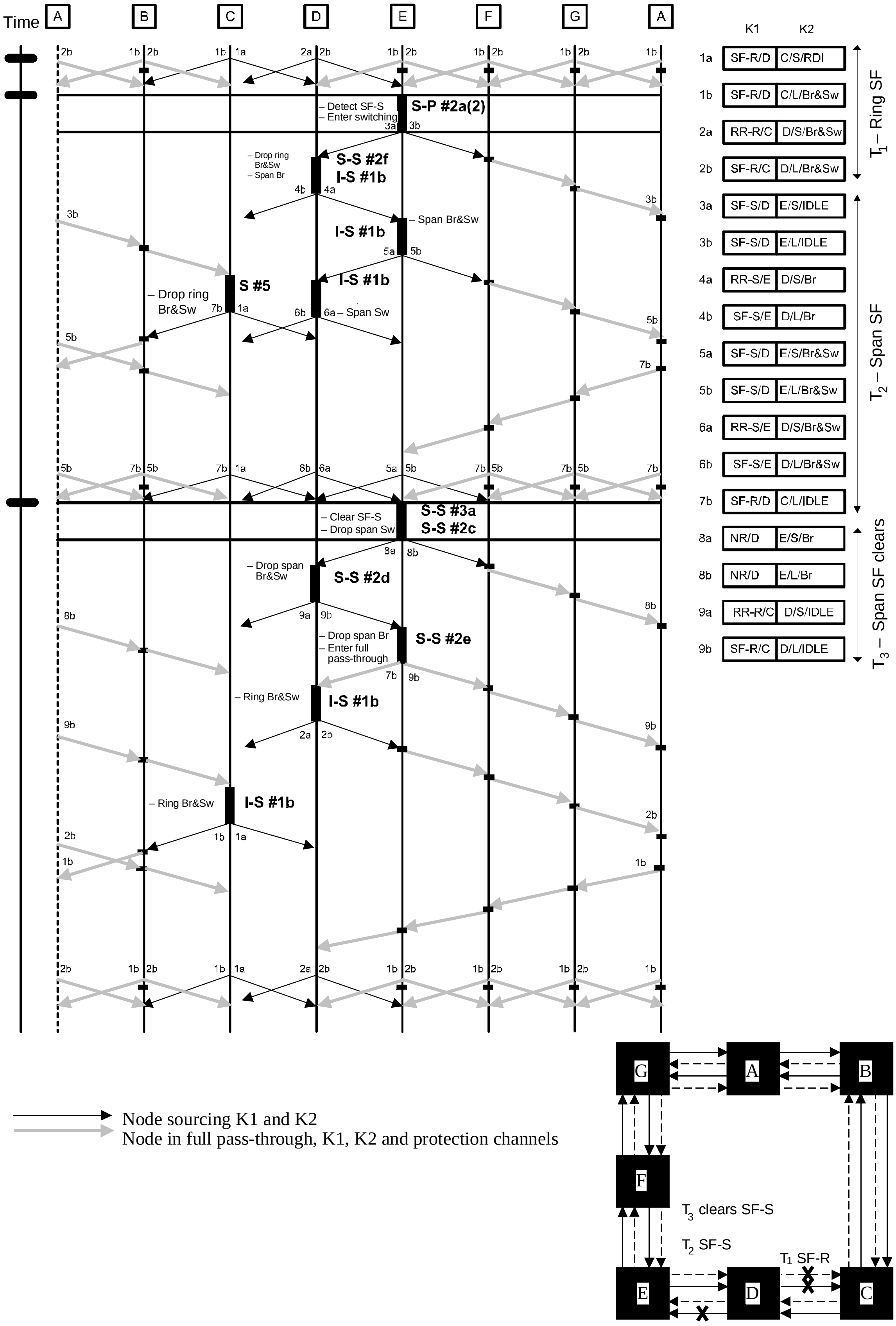
	K1	K2	
1a	RR-S/D	C/S/Br&Sw	T_1 – SPAN SD
1b	SD-S/D	C/L/Br&Sw	
2a	SD-S/C	D/S/Br&Sw	
2b	SD-S/C	D/L/Br&Sw	
3a	SF-R/G	F/S/RDI	T_2 – RING SF
3b	SF-R/G	F/L/IDLE	
4a	NR/C	D/S/Br	
4b	NR/C	D/L/Br	
5a	RR-R/F	G/S/IDLE	
5b	SF-R/F	G/L/IDLE	
6a	NR/D	C/S/IDLE	
6b	NR/D	C/L/IDLE	
7b	SF-R/G	F/L/Br&Sw	
8a	RR-R/F	G/S/Br&Sw	
8b	SF-R/F	G/L/Br&Sw	
9a	WTR/G	F/S/Br&Sw	T_3 – 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	RR-S/D	C/S/Br	
12b	SD-S/D	C/L/Br	

Node sourcing K1 and K2

Node in K-byte pass-through

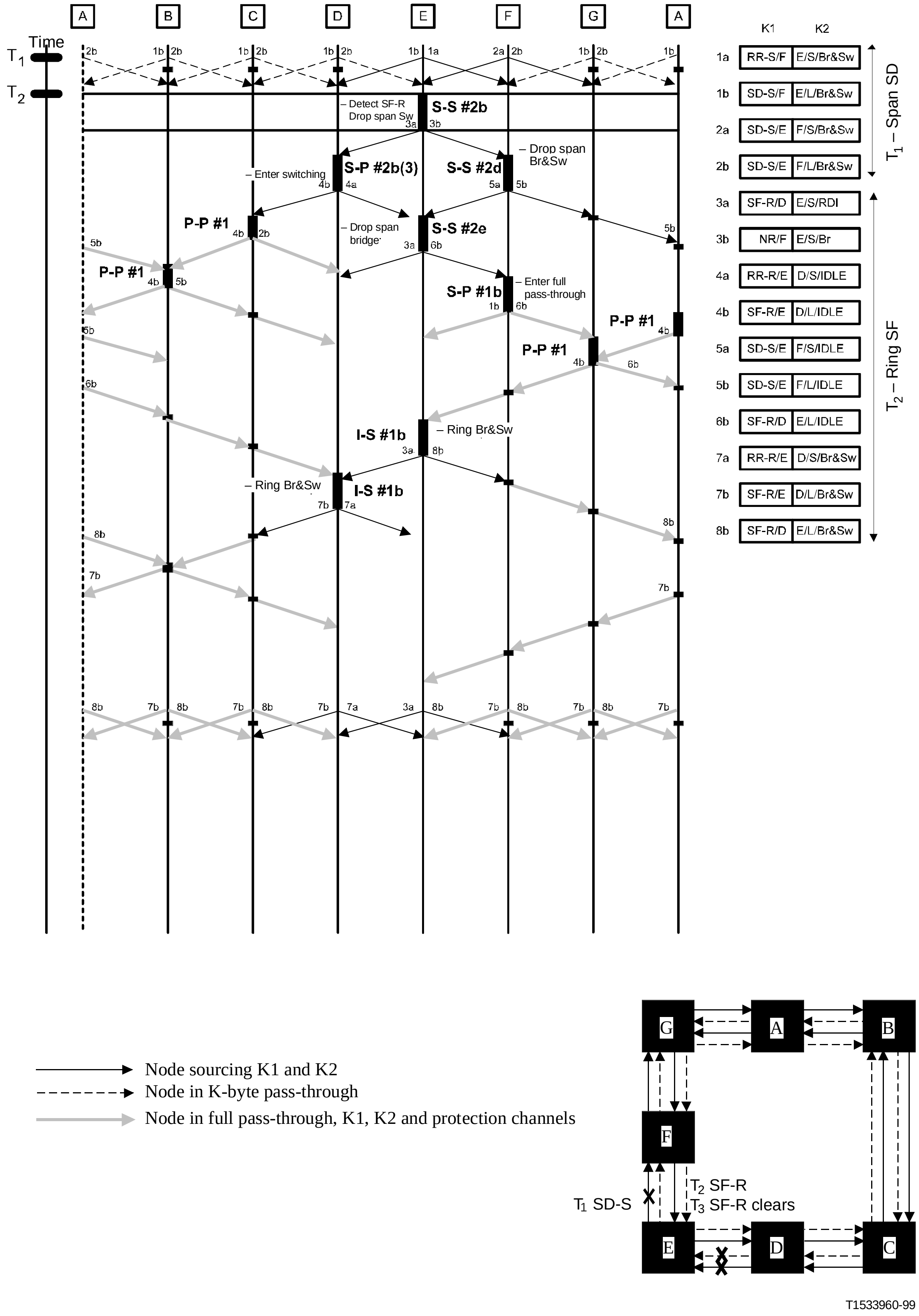
Node in full pass-through, K1, K2 and protection channels

Figure I.6/G.841 – Four-fibre MS shared protection ring – Unidirectional SF-R pre-empting a unidirectional SD-S on non-adjacent spans *(concluded)*



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

Figure I.7/G.841 – Four-fibre MS shared protection ring – Unidirectional SF-S pre-empting a unidirectional SF-R on adjacent spans



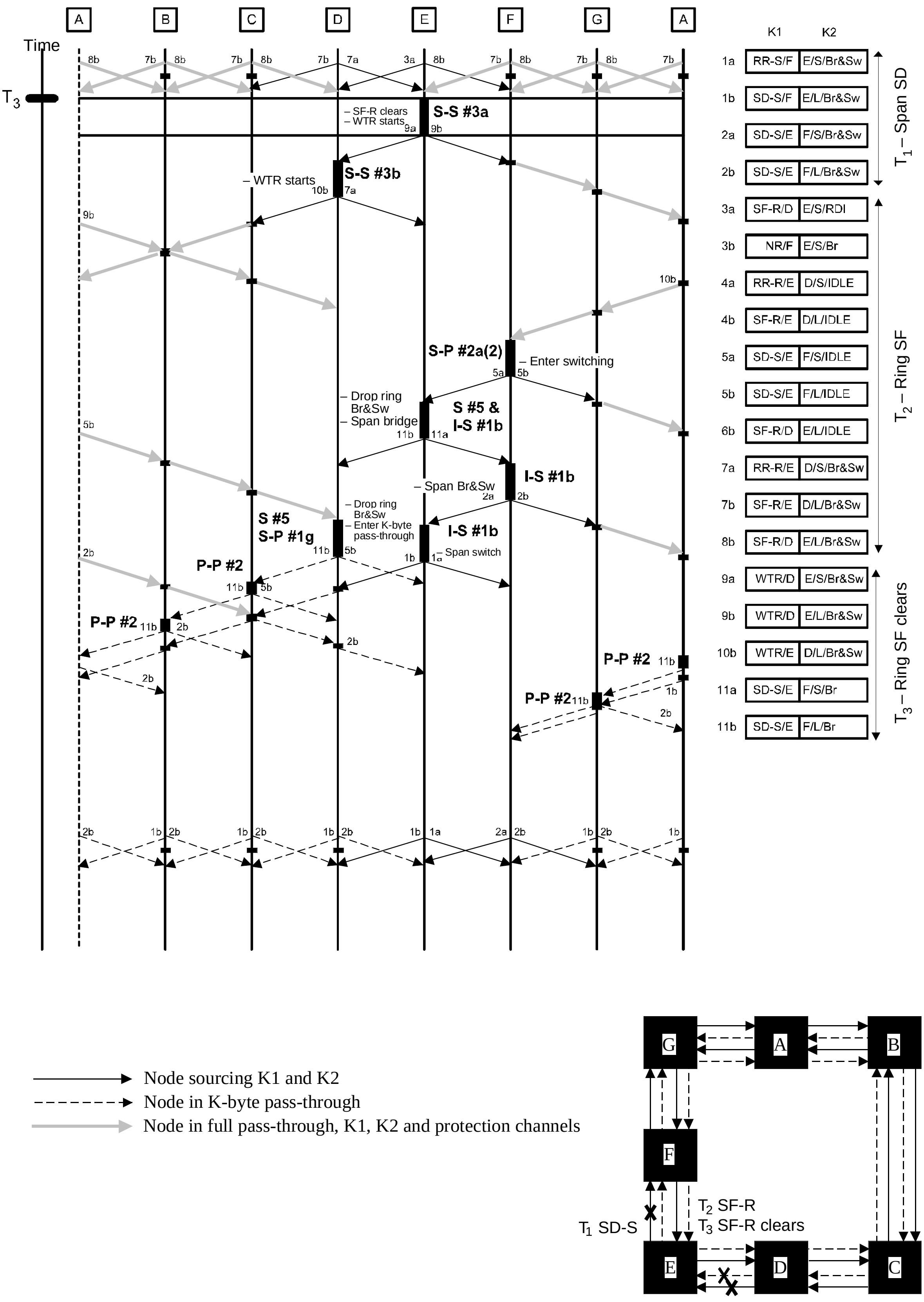
	K1	K2	
1a	RR-S/F	E/S/Br&Sw	T_1 – Span SD
1b	SD-S/F	E/L/Br&Sw	
2a	SD-S/E	F/S/Br&Sw	
2b	SD-S/E	F/L/Br&Sw	
3a	SF-R/D	E/S/RDI	T_2 – Ring SF
3b	NR/F	E/S/Br	
4a	RR-R/E	D/S/IDLE	
4b	SF-R/E	D/L/IDLE	
5a	SD-S/E	F/S/IDLE	
5b	SD-S/E	F/L/IDLE	
6b	SF-R/D	E/L/IDLE	
7a	RR-R/E	D/S/Br&Sw	
7b	SF-R/E	D/L/Br&Sw	
8b	SF-R/D	E/L/Br&Sw	

→ Node sourcing K1 and K2

⇢ Node in K-byte pass-through

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

Figure I.8/G.841 – Four-fibre MS shared protection ring – Unidirectional SF-R pre-empting a unidirectional SD-S on non-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

Figure I.8/G.841 – Four-fibre MS shared protection ring – Unidirectional SF-R pre-empting a unidirectional SD-S on non-adjacent spans *(concluded)*

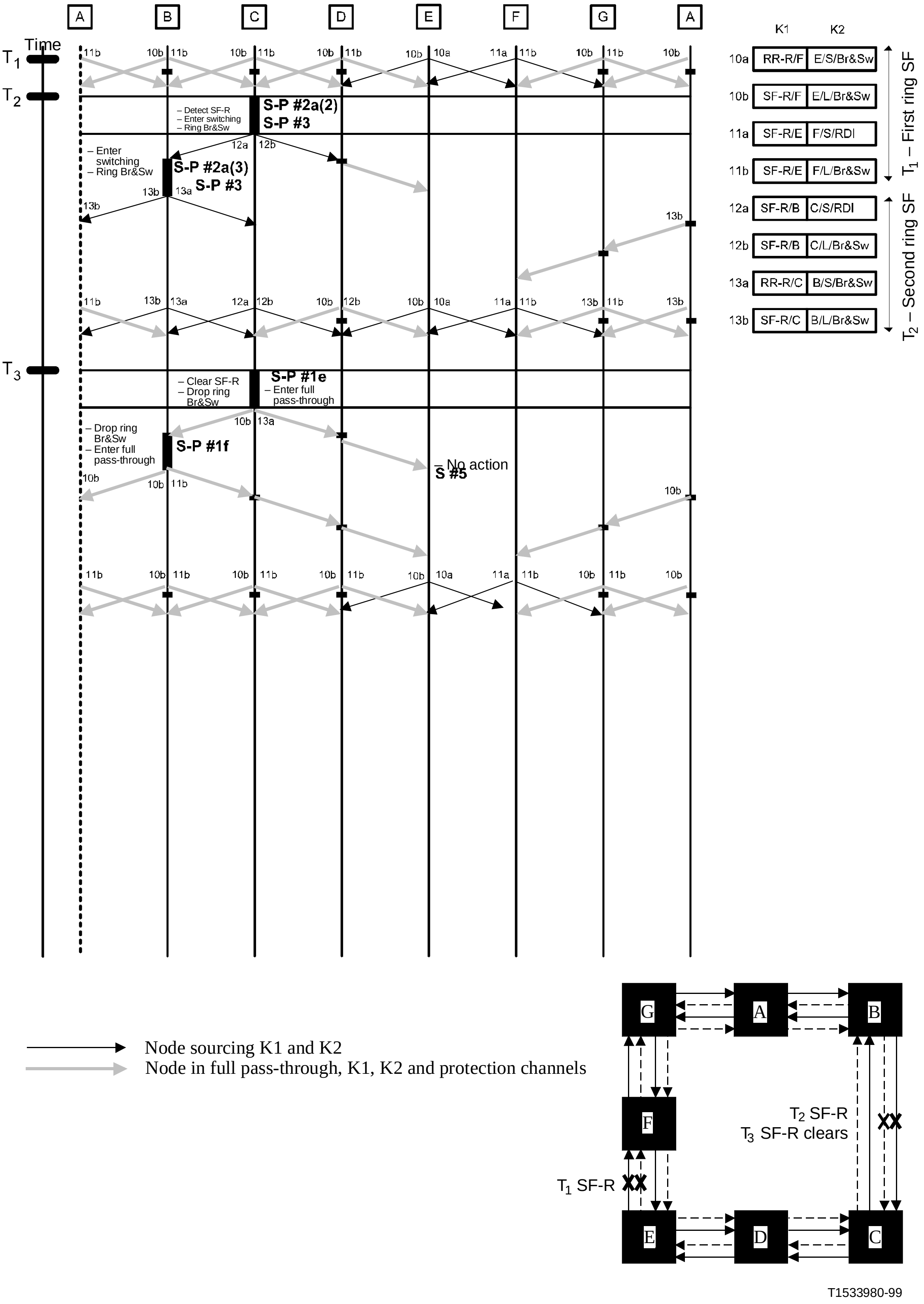
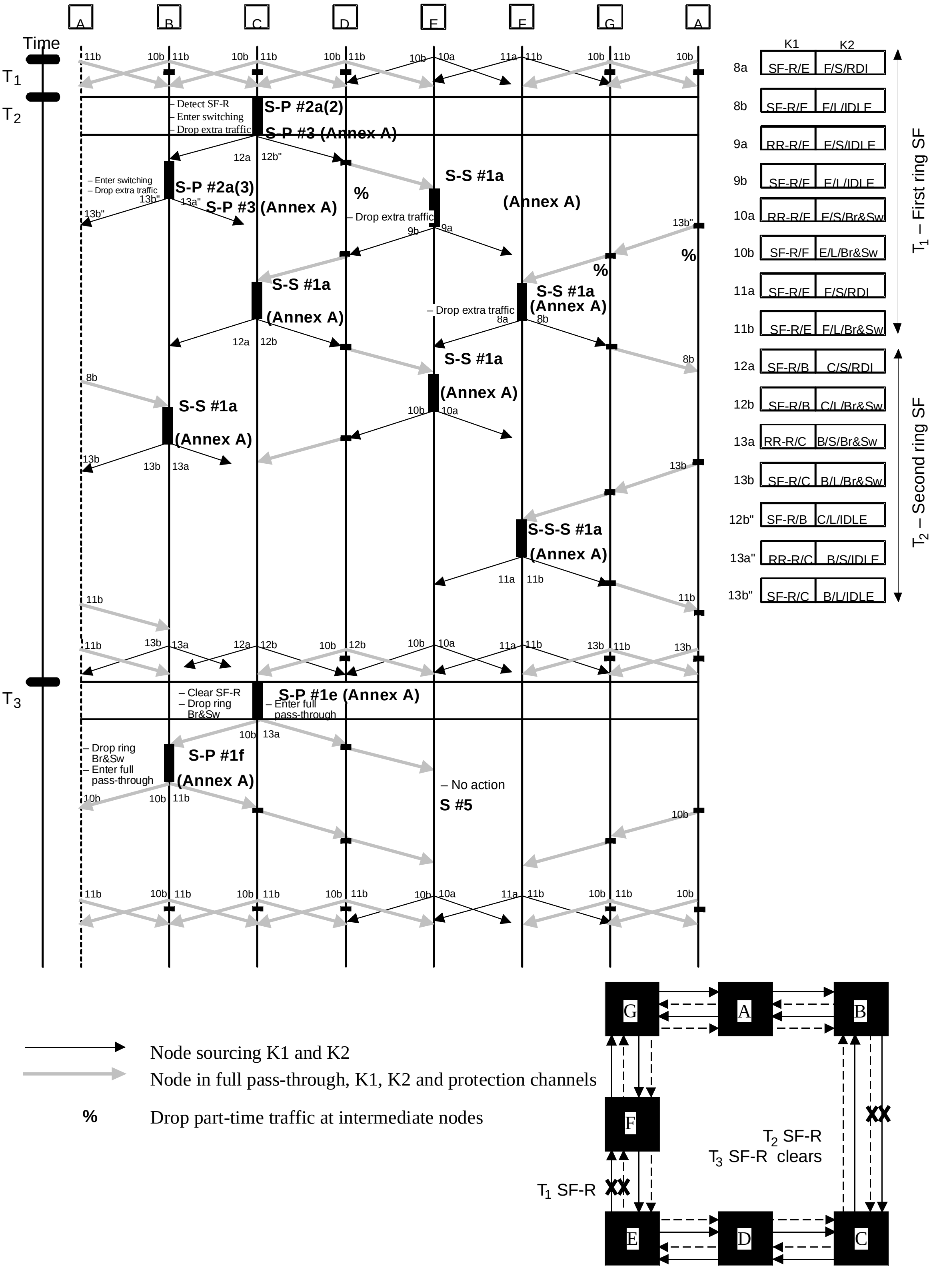
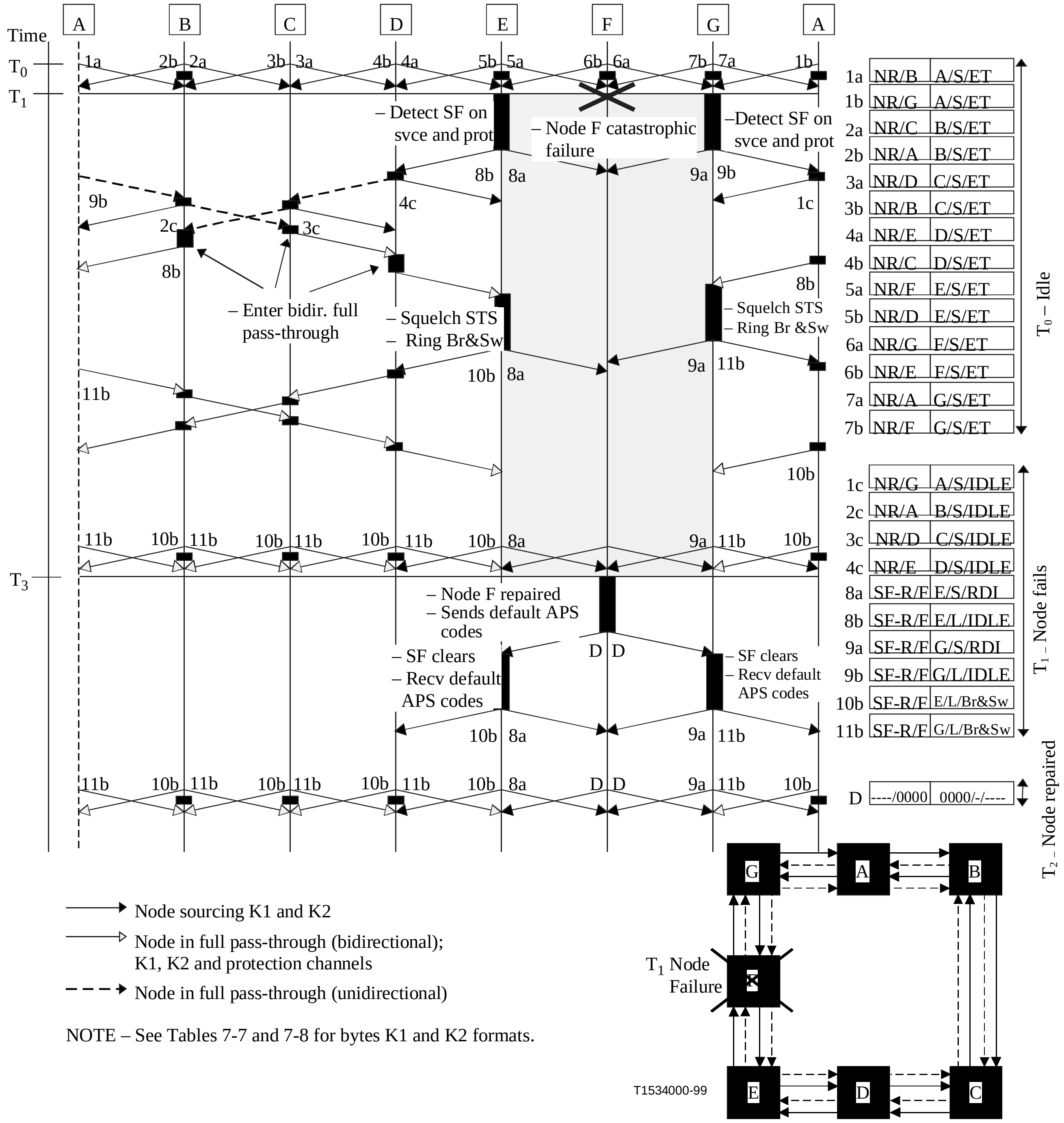


Figure I.9/G.841 – Four-fibre MS shared protection ring – Unidirectional SF-R plus unidirectional SF-R on non-adjacent spans



	K1	K2
8a	SF-R/E	F/S/RDI
8b	SF-R/F	E/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)



1a	NR/B	A/S/ET
1b	NR/G	A/S/ET
2a	NR/C	B/S/ET
2b	NR/A	B/S/ET
3a	NR/D	C/S/ET
3b	NR/B	C/S/ET
4a	NR/E	D/S/ET
4b	NR/C	D/S/ET
5a	NR/F	E/S/ET
5b	NR/D	E/S/ET
6a	NR/G	F/S/ET
6b	NR/E	F/S/ET
7a	NR/A	G/S/ET
7b	NR/F	G/S/ET
1c	NR/G	A/S/IDLE
2c	NR/A	B/S/IDLE
3c	NR/D	C/S/IDLE
4c	NR/E	D/S/IDLE
8a	SF-R/F	E/S/RDI
8b	SF-R/F	E/L/IDLE
9a	SF-R/F	G/S/RDI
9b	SF-R/F	G/L/IDLE
10b	SF-R/F	E/L/Br&Sw
11b	SF-R/F	G/L/Br&Sw
D	----/0000	0000/-/----

Node sourcing K1 and K2

Node in full pass-through (bidirectional); K1, K2 and protection channels

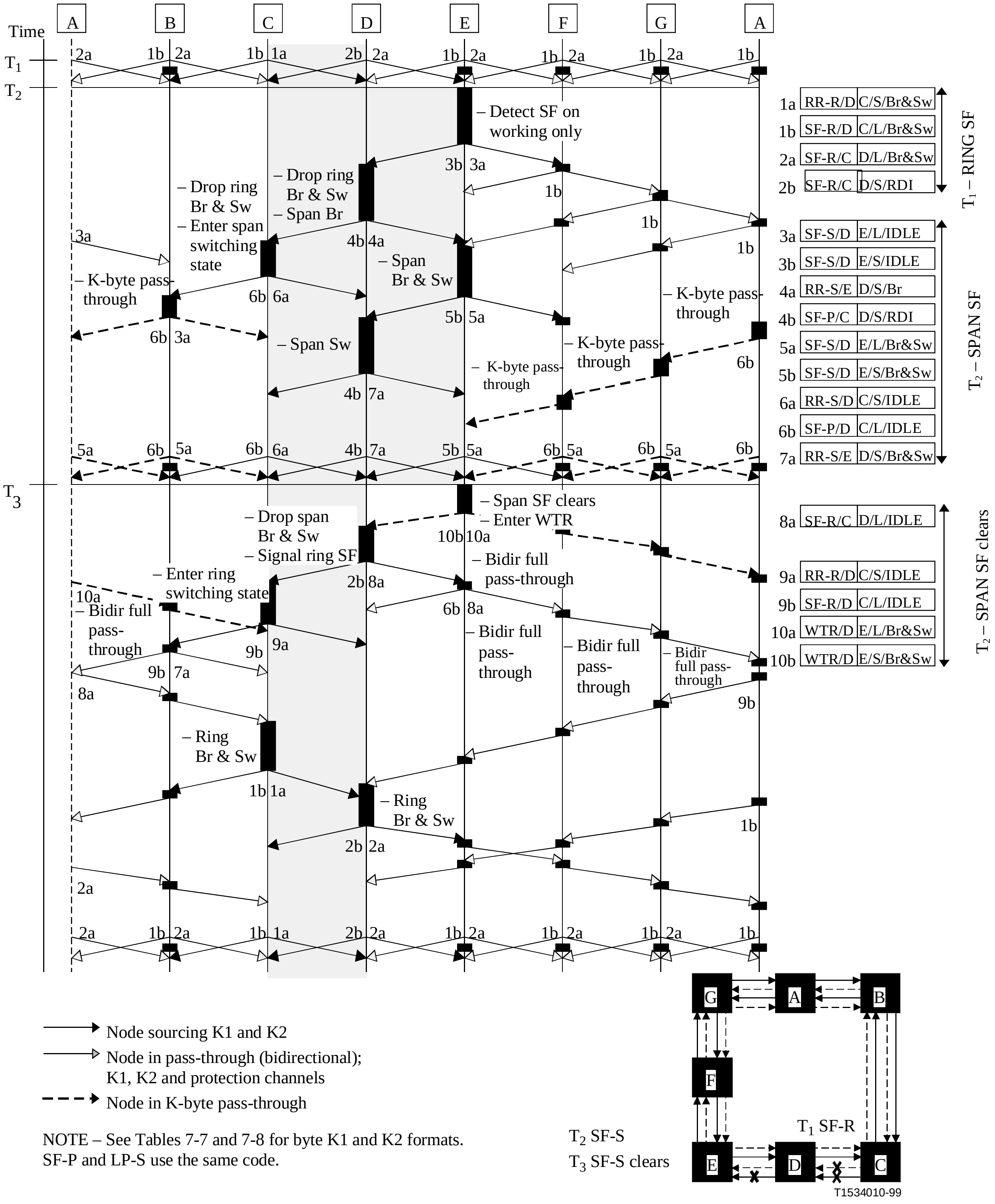
Node in full pass-through (unidirectional)

NOTE – See Tables 7-7 and 7-8 for bytes K1 and K2 formats.

Signalling from nodes E and G does not change until they receive non-default APS codes

Default APS codes are defined as having K1 ID value = K2 ID value with the remaining bits = don't care

Figure I.11/G.841 – Four-fibre MS shared protection ring – Node failure on a ring with extra traffic



NOTE – See Tables 7-7 and 7-8 for byte K1 and K2 formats. SF-P and LP-S use the same code.

Figure I.12/G.841 – Four-fibre MS shared protection ring – Unidirectional SF-S pre-empting a unidirectional SF-R on adjacent spans – SF-S and SF-R detected on adjacent nodes

APPENDIX II

Generalized squelching logic

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

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

II.1 Squelching for unidirectional (and bidirectional) circuits

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

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

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

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

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

II.2.1 Multiply dropped unidirectional circuits

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

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

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

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

II.2.2 Multiply sourced unidirectional circuits

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

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

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

II.2.3 Application to ring interworking

For the ring interworking described in Recommendation G.842, the bidirectional interworking circuit is a multiply dropped circuit with two drops (drop and continue), and is a multiply sourced circuit with two sources in the other direction. The squelching for ring interworking is precisely the combination of the squelching for multiply dropped and multiply sourced circuits given above. More generally, the squelching rules discussed here extend to unidirectional circuits with combinations of multiple drops, multiple sources, or multiple broadcasts.

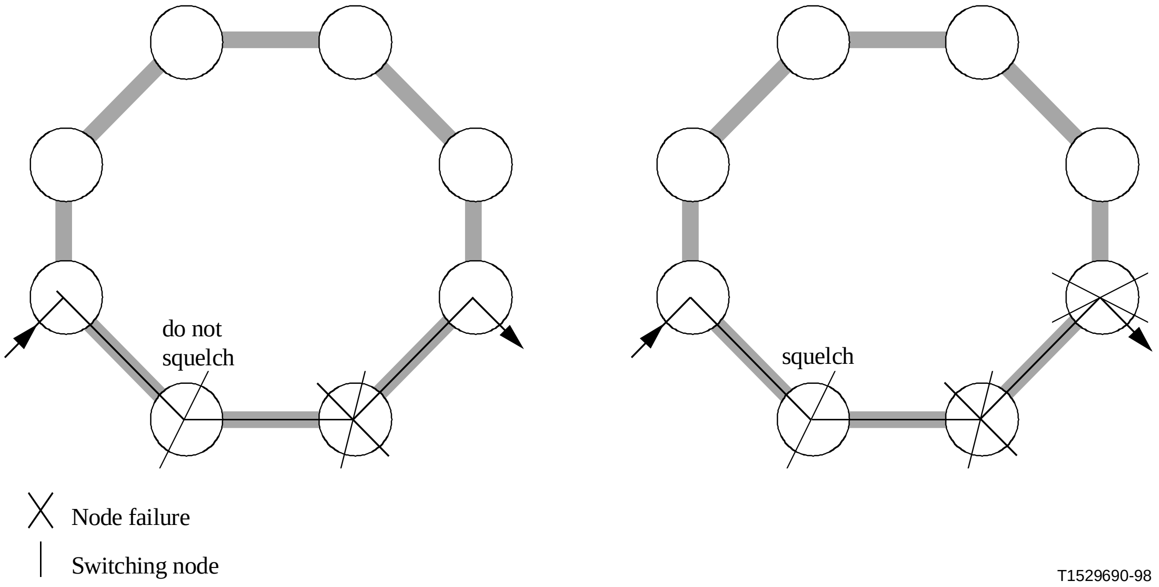


Figure II.1/G.841 – Unidirectional circuit squelching example where the failure is in the direction of the unidirectional circuit

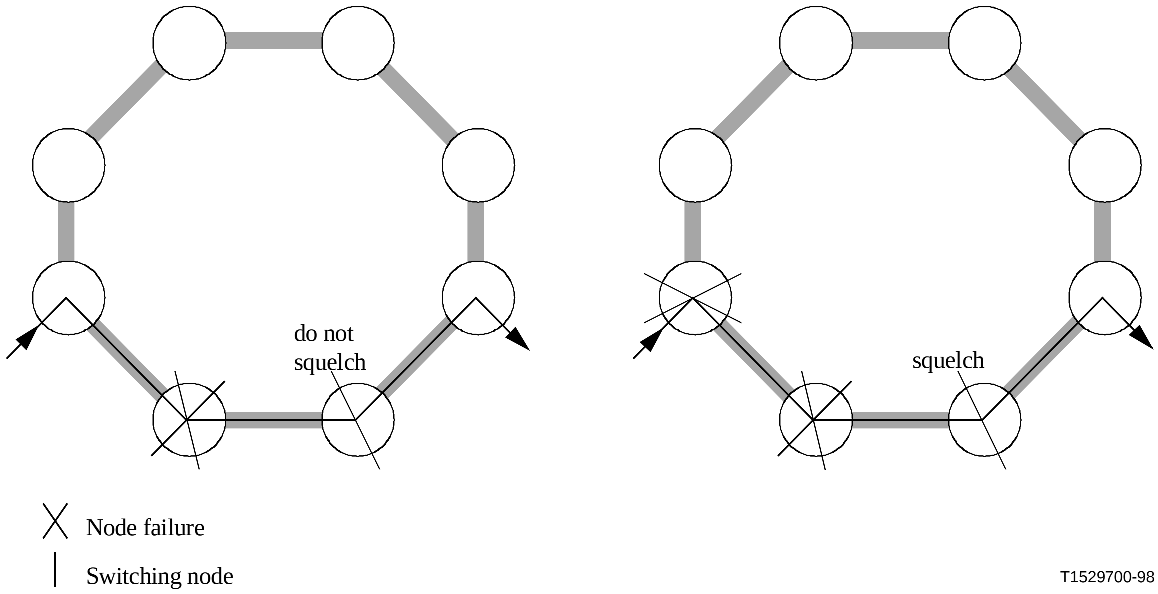


Figure II.2/G.841 – Unidirectional circuit squelching example where the failure is in the opposite direction from the unidirectional circuit

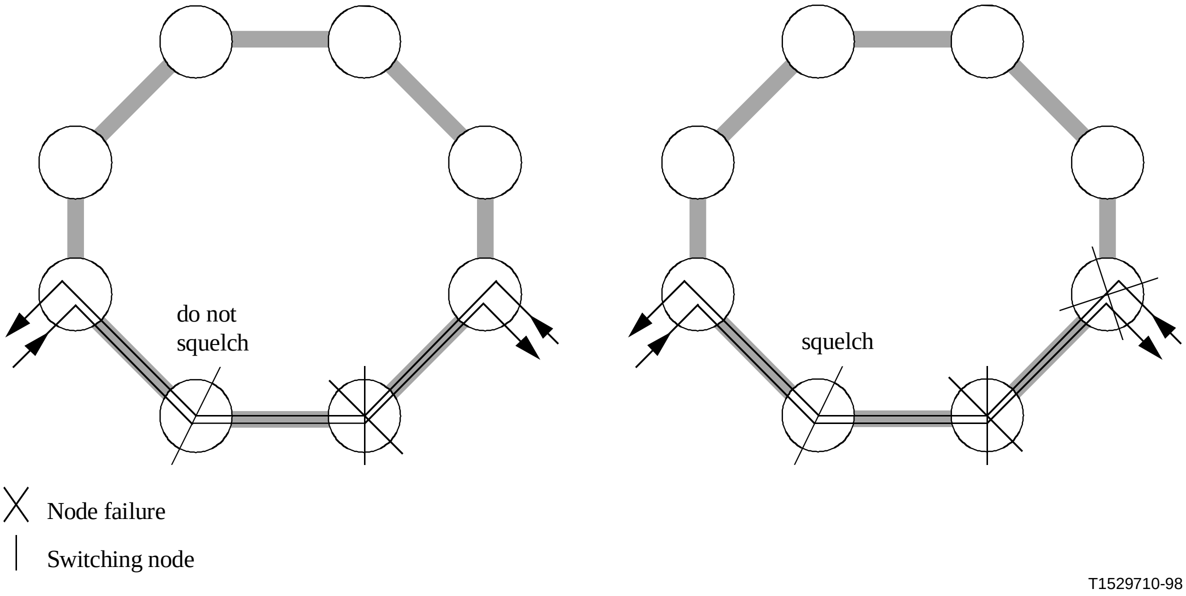


Figure II.3/G.841 – Bidirectional circuit squelching example

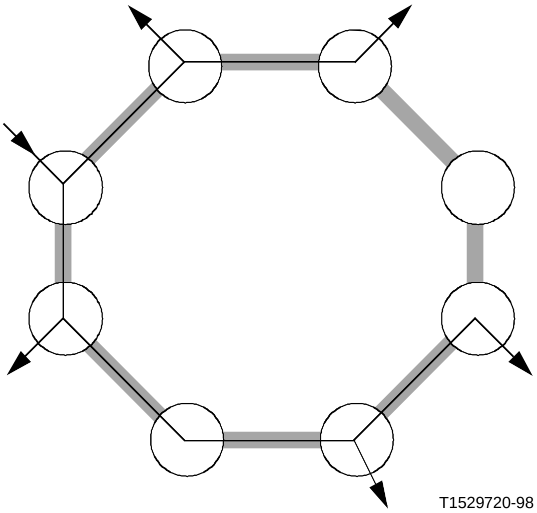


Figure II.4/G.841 – Multiply dropped unidirectional circuit example

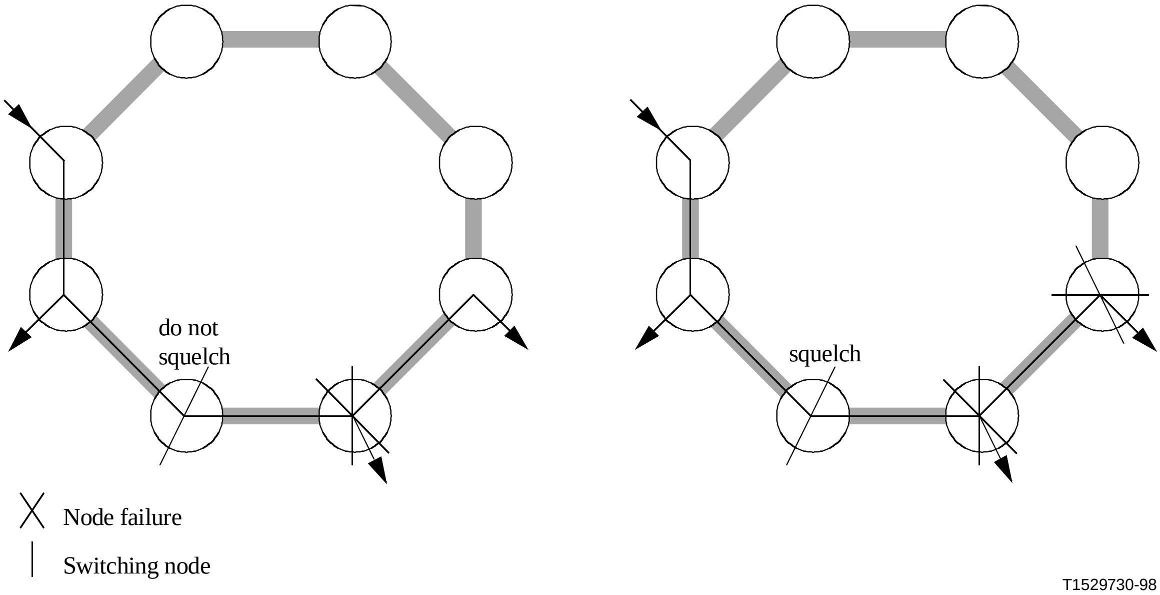


Figure II.5/G.841 – Multiply dropped unidirectional circuit squelching example where the failure is in the direction of the unidirectional circuit

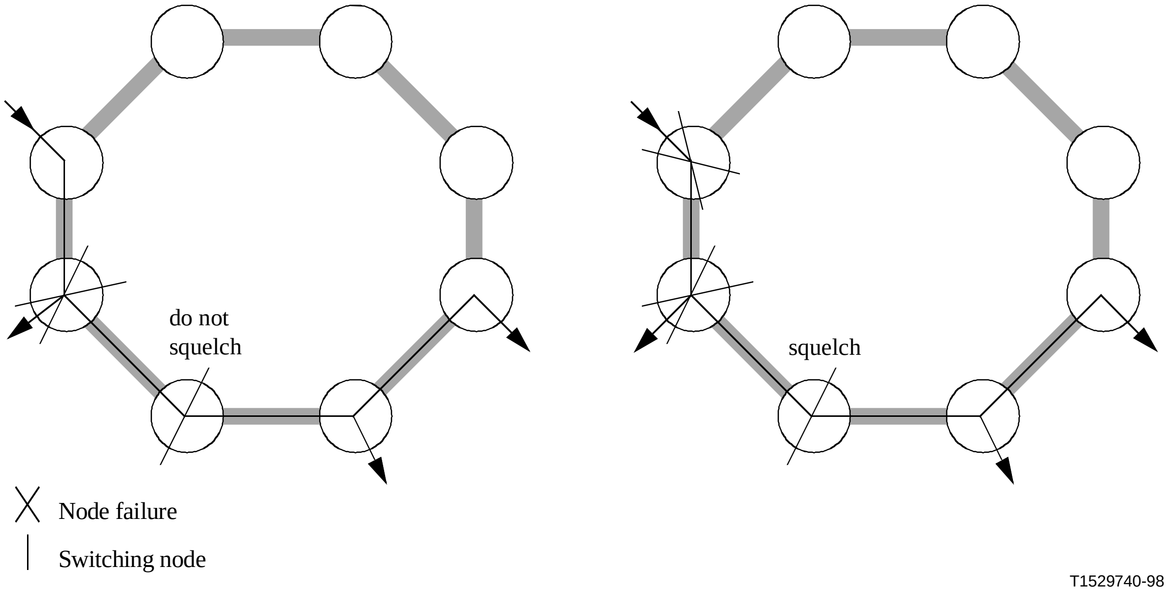


Figure II.6/G.841 – Multiply dropped unidirectional circuit squelching example where the failure is in the opposite direction from the unidirectional circuit

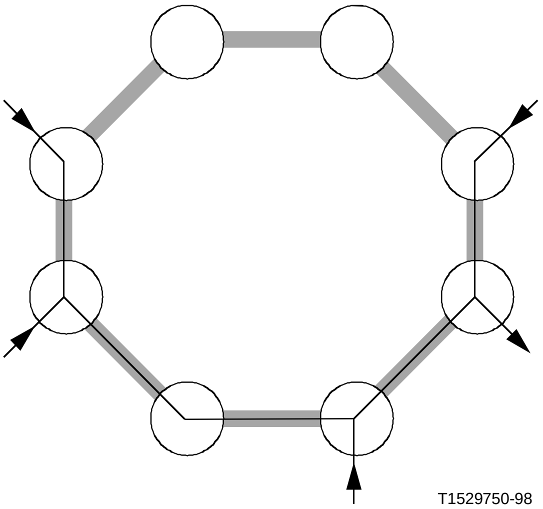


Figure II.7/G.841 – Multiply sourced unidirectional circuit example

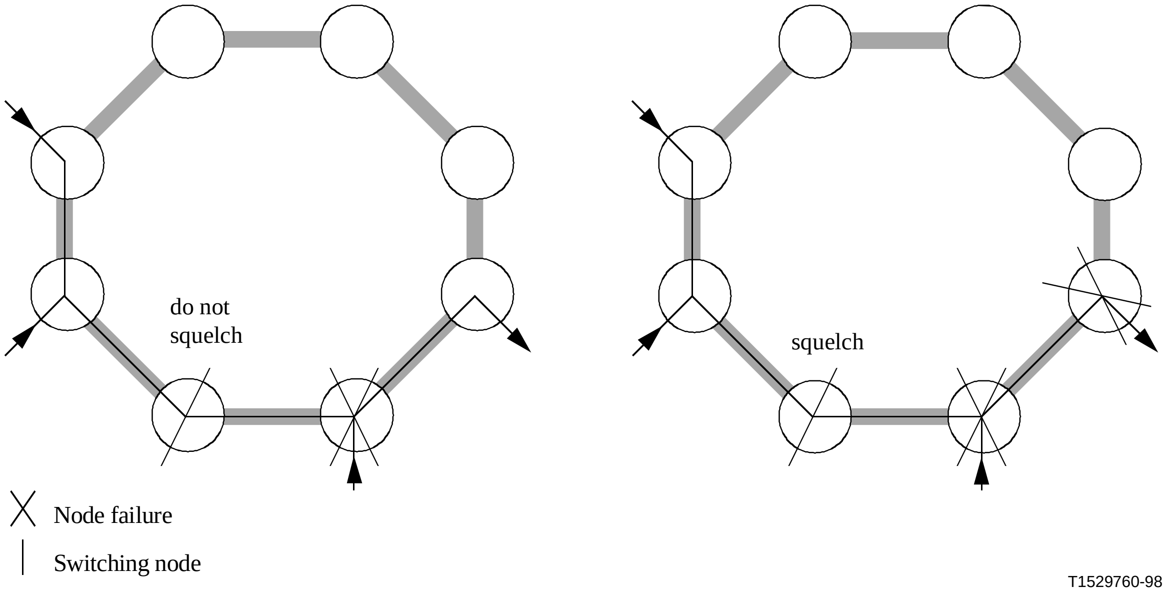


Figure II.8/G.841 – Multiply sourced unidirectional circuit squelching example where the failure is in the direction of the unidirectional circuit

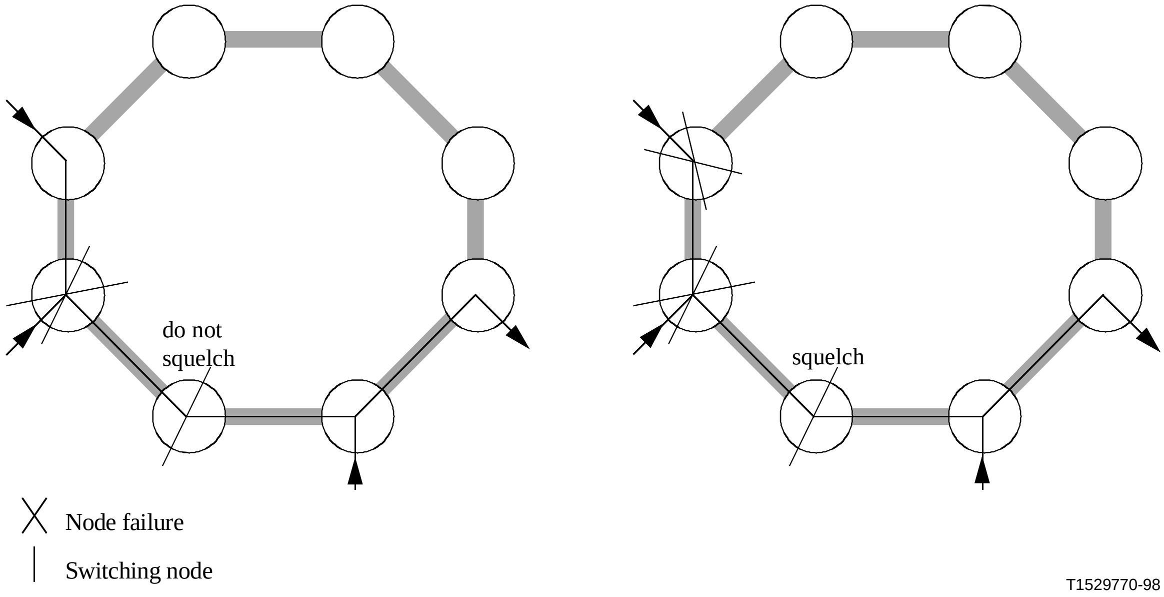


Figure II.9/G.841 – Multiply sourced unidirectional circuit squelching example where the failure is in the opposite direction from the unidirectional circuit

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure
Series Z	Programming languages