EUROPEAN TELECOMMUNICATION STANDARD

FINAL DRAFT
pr **ETS 300 746**

December 1996

Source: ETSI TC-TM

Reference: DE/TM-03042

ICS: 33.020

Key words: SDH, network, protection, interworking, protocol, transmission

Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); Network protection schemes; Automatic Protection Switch (APS) protocols and operation

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Blank page

Foreword

This final draft European Telecommunication Standard (ETS) has been produced by Transmission and Multiplexing (TM) Technical Committee of the European Telecommunications Standards Institute (ETSI), in order to provide network operators and equipment manufacturers the requirement for and the specification of Synchronous Digital Hierarchy (SDH) network Automatic Protection Switching (APS) protocols, based on rings and other schemes and is now submitted for the Voting phase of the ETSI standards approval procedure.

This ETS is one of a family of related European Technical Reports (ETRs) and ETSs covering the various aspects of SDH protection:

Draft ETR 273: "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH) network protection schemes; Types and characteristics";

Draft ETR 274: "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH) protection interworking; rings and other schemes";

ETS 300 746: "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); Network protection schemes; Automatic Protection Switch (APS) protocols and operation".

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Blank page

1 Scope

This European Telecommunication Standard (ETS) specifies the Automatic Protection Switching (APS) requirements, switching initiation criteria, and the APS protocols of Synchronous Digital Hierarchy (SDH) multiplex section shared protection ring, multiplex section dedicated protection ring, multiplex section linear protection, and path trail and Sub-Network Connection (SNC) protection schemes. The APS protocols are specified in terms of their multiplex section or path overhead requirement, the signalling messages and their operations under various failure conditions.

For the network objectives, architectures, functional modelling and operations of the various SDH protection schemes, see annex C. Also, for the protection interworking and interconnection scenarios for SDH network protection schemes, see annex C.

2 Normative references

This ETS incorporates by dated or undated references, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references subsequent amendments to, or revisions of, any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 417: "Transmission and Multiplexing (TM); Generic functional requirements for Synchronous Digital Hierarchy (SDH) equipment".

[2] ITU-T Recommendation G.803: "Architectures of transport networks based on the synchronous digital hierarchy (SDH)".

[3] ITU-T Recommendation G.708: "Network node interface for the synchronous digital hierarchy".

[4] ITU-T Recommendation G.709: "Synchronous multiplexing structure".

[5] ITU-T Recommendation G.783: "Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks".

[6] ITU-T Recommendation G.841: "Types and characteristics of SDH network protection architectures".

3 Abbreviations

For the purposes of this ETS, the following abbreviations apply:

ADM	Add Drop Multiplex
AIS	Alarm Indication Signal
APS	Automatic Protection Switching
AU	Administrative Unit
AU-AIS	Administrative Unit - Alarm Indication Signal
AUG	Administrative Unit Group
AU-n	Administrative Unit (level) n
BER	Bit Error Ratio
BIP-n	Bit Interleaved Parity (of order) n
Br	Bridged
CPE	Customer Premises Equipment
DCC	Data Communication Channel
DXC	Digital Cross-Connect
EXER	EXERcise
EXER-R	EXERcise - Ring
FEBE	Far End Block Error
FERF	Far End Receive Failure

FS	Forced Switch
FS-P	Forced Switch of the Protection channel to working
FS-R	Forced Switch of working to protection - Ring
FS-W	Forced Switch of a Working channel to protection
HO VC	Higher Order Virtual Container
HO	Higher Order
HOPA	Higher Order Path Adaptation
HOPT	Higher Order Path Termination
HPC	Higher order Path Connection
HP-DEG	Higher order Path-DEGraded
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 VC	Lower Order Virtual Container
LO	Lower Order
LOF	Loss Of Frame
LOPA	Lower Order Path Adaptation
LOPT	Lower Order Path Termination
LOS	Loss Of Signal
LP	Lockout of Protection
LPC	Lower order Path Connection
LP-DEG	Lower order Path-DEGraded
LP-SSF	Lower order Path-Server Signal Fail
LP-TIM	Lower order Path-Trace Identifier Mismatch
LP-UNEQ	Lower order Path UNEQuipped
MS	Multiplex Section
MS-DPRing	Multiplex Section - Dedicated Protection Ring
MS-P	Manual Switch of the Protection channel to working
MS-R	Manual Switch of working to protection - Ring
MS-SPRing	Multiplex Section - Shared Protection Ring
MS-W	Manual Switch of a Working channel to protection
NE	Network Element
NNI	Network Node Interface
NR	No Request
OAM&P	Operations, Administration Maintenance & Provisioning
OS	Operations System
PC	Private Circuit
POH	Path OverHead
RC	Remote Concentrator
RDI	Remote Defect Indicator
RR	Reverse Request
RR-R	Reverse Request - Ring
RS	Regenerator Section
SA	Section Adaptation
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SD-R	Signal Degrade - Ring
SF	Signal Fail
SF-R	Signal Fail - Ring
SNC	Sub-Network Connection
SNC/I	Sub-Network Connection protection with Inherent monitoring
SNC/N	Sub-Network Connection protection with Non-intrusive monitoring
SOH	Section OverHead
SSF	Server Signal Fail
ST	Section Termination
STM	Synchronous Transport Module
STM-N	Synchronous Transport Module (level) N
Sw	Switched
TMN	Telecommunications Management Network
TSI	Time Slot Interchange
TU	Tributary Unit
TUG	Tributary Unit Group

TU-n	Tributary Unit (level) n
VC	Virtual Container
VC-n	Virtual Container (level) n
WTR	Wait To Restore

4 Definitions and classifications

For the purposes of this ETS, the following abbreviations apply:

4.1 General definitions

Administrative Unit (AU): See ITU-T Recommendation G.708 [3].

Administrative Unit Group (AUG): See ITU-T Recommendation G.708 [3].

Automatic Protection Switching (APS): See ITU-T Recommendation G.783 [5].

Bit Interleaved Parity (BIP): See ITU-T Recommendation G.708 [3].

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

dedicated protection: See ITU-T Recommendation G.803 [2].

dual ended operation: See ITU-T Recommendation G.803 [2].

head-end: The node that executes a bridge.

Loss Of Frame (LOF): See ITU-T Recommendation G.783 [5].

Loss Of Signal (LOS): See ITU-T Recommendation G.783 [5].

Lower Order Virtual Container (LO VC) access: The termination of a higher order VC for the purpose of adding, dropping, or cross-connecting any individual LO VC or VC group.

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

Multiplex Section (MS): See ITU-T Recommendation G.803 [2].

Multiplex Section AIS (MS-AIS): See ITU-T Recommendation G.783 [5].

Multiplex Section FERF (MS-FERF): See ITU-T Recommendation G.709 [4].

Network Node Interface (NNI): See ITU-T Recommendation G.708 [3].

pass-through: The action of transmitting the information that is being received from one multiplex section terminating port of a node which is connected to the ring to the other multiplex section terminating port of the same node.

path: See ITU-T Recommendation G.803 [2].

path AIS: See ITU-T Recommendation G.783 [5].

Path Overhead (POH): See ITU-T Recommendation G.708 [3].

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

Regenerator Section (RS): See ITU-T Recommendation G.803 [2].

restoration: See ITU-T Recommendation G.803 [2].

secondary traffic: Traffic that is carried over the protection trail when it is not used for the protection of working traffic. This is sometimes called extra traffic. Secondary traffic is not protected and is pre-empted when the protection trail is required to protect the working traffic.

Section Overhead (SOH): See ITU-T Recommendation G.708 [3].

shared protection: See ITU-T Recommendation G.803 [2].

single ended operation: See ITU-T Recommendation G.803 [2].

single point failure: Failure located at a single physical point in a sub-network. The failure may affect one or more fibres. A single point failure may be detected by any number of Network Elements (NEs).

Sub-Network Connection (SNC): See ITU-T Recommendation G.803 [2].

sub-network connection protection: See ITU-T Recommendation G.803 [2].

switch: The action of selecting traffic from the protection trail rather than the working trail.

tail-end: The node that requests the bridge.

Time Slot Interchange (TSI): The capability of changing the timeslot position of through-connected traffic (i.e. traffic that is not added or dropped from the node).

trail: See ITU-T Recommendation G.803 [2].

trail protection: See ITU-T Recommendation G.803 [2].

Tributary Unit (TU): See ITU-T Recommendation G.708 [3].

Tributary Unit Group (TUG): See ITU-T Recommendation G.708 [3].

Virtual Container (VC): See ITU-T Recommendation G.708 [3].

Wait To Restore (WTR): The condition in which a working trail meets the restoral threshold after an SD or SF condition. The transport of working traffic is ready to be reverted to the working trail from the protection trail.

working traffic: Traffic that is normally carried in a working trail, except in the event of a protection switch.

working trail: The trail over which working traffic is transported when there is no switch events.

4.2 Ring definitions

add traffic: Traffic that is inserted into a working trail at a ring node.

drop traffic: Traffic that is extracted from a working trail at a ring node.

long path: The path segment away from the span for which a ring request is initiated. Typically, there are other intermediate nodes along this path segment.

ring: A ring is constructed within a layer consisting of a set of nodes, each of which is connected to its immediate neighbour (adjacent) nodes by a trail/link connection, forming a closed loop. The capacity offered by the ring between any pair of adjacent nodes is the same.

ring request: The request sent over the long path away from the span for which the request is initiated, i.e. a long path request.

ring switching: Protection mechanism in a ring, which in the event of a switch the working traffic is carried over the protection trail away from the failure.

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

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

squelching: The process of inserting path AIS in order to prevent misconnection.

4.3 Protection classifications

Classification of SDH protection schemes is based on the ITU-T Recommendation G.803 [2] layering concept of a transport network model, see also annex C.

5 Multiplex section trail protection protocols

5.1 Multiplex section trail linear protection

5.1.1 APS requirements

An APS protocol is required to co-ordinate the bridge and switch operations between the nodes. The requirements for the protocol are listed below:

Switch time. For MS trail linear protection the switching time shall be less than 50 ms;

Secondary traffic. For 1:n MS trail linear protection, access to the protection trails may be provided as an option to accommodate secondary, low priority traffic;

Switching types. MS trail linear protection shall support both single ended and dual ended switching;

Operation Modes. The mode of operation shall be both revertive and non-revertive;

Manual control. External commands shall be provided for manual control of protection switching by the operations systems or the craftpersons.

5.1.2 Switch initiation criteria

The requests to perform protection switching can be initiated either externally or automatically.

Externally initiated commands are entered by way of the Operations System (OS) or the craftperson interface. Subclause 5.1.2.1 describes these externally initiated commands available at the OS, craftsperson, or both interfaces.

APS requests can also be initiated based on multiplex section and equipment performance criteria. Subclause 5.1.2.2 provides the automatically initiated command criteria.

5.1.2.1 Externally initiated commands

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

5.1.2.1.1 Commands not signalled on the APS channel

The descriptions of the externally initiated commands are provided below:

clear: This command clears the externally initiated command at the node to which the command was addressed. For 1:n and 1+1 revertive architecture, the NE-to-NE signalling following removal of the externally initiated commands is performed using the NR code;

The following command is useful if one span has excessive switching to protection. Another use for this command includes blocking protection access for some channels that have only traffic that does not need protection or before it become active during installation. The command is not time critical (i.e. not needed

to be completed in tens of milliseconds). Thus, it can be transmitted over the Data Communication Channel (DCC).

lockout of a working channel: This command prevents the working channel from switching to the protection channel by disabling the node's capability to request a protection switch of any kind. If any working traffic is already on protection, it is switched back to the regular working channel regardless of its condition. For 1:n and 1+1 revertive architecture, if no other requests are active, the NR code is transmitted. The lockout of a working channel should be done at both ends of the line termination to avoid unnecessary alarms. If the channel is locked out only at one end and the NE at the other end of the line initiates a switch request, after waiting a pre-set time the NE that initiated the request will assume that the response is not coming because of a failure situation and will send an alarm. This should be avoided by locking out both sides.

NOTE: This external command is not currently present in the MS linear protection protocol described in the ITU-T Recommendation G.783 [5].

5.1.2.1.2 Commands using the APS bytes

The following commands are carried over the APS bytes:

Lockout of Protection (LP): This command prevents any working channel (and the extra traffic, if possible) from access the protection channel by issuing a Lockout of Protection Request. If any working traffic is already on protection, it is switched back to the regular working channel regardless of its condition. Only channel number 0 is allowed with a Lockout of Protection request;

Forced Switch of a Working channel to protection (FS-W): This command performs the switch from the addressed working channel to the protection channel, unless a higher or equal priority switch command is active or the protection channel is in a SF condition;

Forced Switch of the Protection channel to working (FS-P): because 1+1 system can be non-revertive, forced switch of a working channel to protection command is not adequate if the traffic is already on the protection channel. Thus a command to switch the traffic back to the working channel is added: forced switch of the protection channel to working command performs the switch from the protection channel to the (regular) working channel, unless a higher or equal priority switch command is active. Since forced switch has higher priority than SF, this command will be carried out regardless of the condition of the working channel. This command is used only in 1+1 architecture;

Manual Switch of a Working channel to protection (MS-W): This command performs the switch from the addressed working channel to the protection channel, unless a higher or equal priority switch command is active or the protection channel is in a SF condition. MS-W has a lower priority than Forced Switch (FS) as shown in table 1;

Manual Switch of the Protection channel to working (MS-P): because 1+1 system can be non-revertive, manual switch of a working channel to protection command is not adequate if the traffic is already on the protection channel. Thus a command to switch the traffic back to the working channel is added: manual switch of the protection channel to working command performs the switch from the protection channel to the (regular) working channel, unless a higher or equal priority switch command is active. Since manual switch has lower priority than SF, this command will be carried out only if the working channel is not in SD or SF condition. This command is used only in 1+1 architecture;

EXERcise (EXER): This command exercises protection switching for the addressed channel without completing the actual bridge and switch, unless the protection channel is in use. The command is issued and the responses are checked, but no working traffic is affected. The aim of exercise is to test the APS channel and K1, K2 bytes processing in the APS controller.

5.1.2.2 Automatic initiated requests

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 requests automatically: Signal Failure (SF), Signal Degrade (SD), Reverse

Request (RR) and Wait to Restore (WTR). The requests are transmitted from NE to NE (not from OS to NE).

The SF request is used to protect working traffic affected by a hard-failure, while the SD request is used to protect against a soft failure. The node that receives the request, performs the activity according to the priority level, and sends the bridged indication.

The WTR 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 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 requests.

DNR and NR requests are used when there is no need for protection, after the clearing of an external command or of WTR condition. In particular, the DNR command is issued in 1+1 non-revertive system when it is used together with 1:n system

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

Signal Fail (SF): The SF condition is defined in ETS 300 417 [1]; this command is used to request protection switching for signal failures;

Signal Degrade (SD): The SD condition is defined in ETS 300 417 [1]; this command is used to request protection switching for signal degradation;

Reverse Request (RR): This command is transmitted to the tail-end NE as an acknowledgement for receiving the request. It assumes the priority of the request to which it is responding;

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 request. It is used for revertive system only;

Do Not Revert (DNR): This command is issued when there are no commands initiated from the OS , craftperson, or either of the NEs. It is used only in 1+1 non-revertive system compatible with 1:n system. If the line-terminating NE receives the RR code in response to the DNR code, it shall keep transmitting the DNR code until pre-empted;

No Request (NR): The NR code is transmitted when there is no need to use the protection channel. Extra traffic can be put on the protection channel when there is no request from either of the line-terminating NEs.

5.1.3 Protection switch protocol

Byte K1 and bit 1-5 of byte K2, shall be used for protection switching. See subclause 5.1.4 for details on the operational usage of these bytes.

Byte K1 and bit 1-5 of byte K2 shall be transmitted within the multiplex section overhead of the STM-N that is carrying the protection sections. Although they can 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. Note that bits 6-8 of byte K2 are used on all STM-N line signals to signal MS-RDI and MS-AIS.

A detected failure of the received K1 or K2 is considered as equivalent to a SF condition on the protection section.

5.1.3.1 K1 Byte

These bits shall be assigned as shown in table 1 K1 bits 1-4 carry request codes, listed in descending order of priority in table 1 K1 bits 5-8 carry the requesting channel ID for the request code indicated in K1 bits 1-4.

Table 1: Byte K1 functions

Request code (Bits 1-4)				Requesting channel identification (Bits 5-8)			
bit 1	**bit 2**	**bit 3**	**bit 4**	**bit 5**	**bit 6**	**bit 7**	**bit 8**
1111 Lockout of Protection (note 1)				Requesting channel ID is set to the channel's ID for which the request is issued:			
1110 Forced Switch							
1101 Signal fail - High Priority Channel (note 2)				0 Null Channel (note 6)			
1100 Signal fail - Low Priority Channel (note 2)				1-14 Working Channels (note 7)			
1011 Signal Degrade - High Priority Channel (note 2)				15 Extra Traffic Channel (note 8)			
1010 Signal Degrade - Low Priority Channel (note 2)							
1001 Not used (note 3)							
1000 Manual Switch							
0111 Not used (note 3)							
0110 Wait-To-Restore							
0101 Not used (note 3)							
0100 Exercise							
0011 Not used (note 3)							
0010 Reverse Request (note 4)							
0001 Do Not Revert (note 5)							
0000 No Request							

NOTE 1: Only channel number 0 is allowed with a Lockout of Protection request.
NOTE 2: For Signal Fail and Signal Degrade only, bit 4 indicates the priority assigned to the channel requesting switch action: 1 indicates high priority channel and 0 indicates low priority channel. For protection channel only code 1 is allowed. For 1+1 system only code 1 is allowed.
NOTE 3: Some network operators may use these codes for network specific purposes. The receiver shall be able of ignoring these codes.
NOTE 4: Reverse Request assumes the priority of request to which it is responding.
NOTE 5: Do Not Revert is used in 1+1 non-revertive system compatible with 1:n system only.
NOTE 6: Allowed associated priority channel: 1.
NOTE 7: Allowed associated priority channel: 0 or 1. For 1+1 system only channel number 1 is allowed with priority 1.
NOTE 8: Allowed only in 1:n system.

5.1.3.2 Bit 1-5 of K2 byte

Bit 1-5 of byte K2 shall be assigned as shown in table 2.

Table 2: Bit 1-5 of byte K2 functions

Channel identification (Bits 1-4)				Protection architecture (bit 5)
bit 1	**bit 2**	**bit 3**	**bit 4**	**bit 5**
null channel (0) if the received K1 byte indicates either null channel or the number of a locked out working channel				0 = 1+1 architecture
number of channel which is bridged (1-15), in all other cases				1 = 1:n architecture

5.1.4 Protection switch operation

This subclause is structured as follows:

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

These rules apply conceptually to a single MS linear protection APS controller operating at a node. It is choosing switching and signalling actions based on all incoming K-byte signalling, detected failures, 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 1 illustrates the conceptual operation of an MS linear protection APS controller.

5.1.4.1 Node APS state

There are two classes of node APS states: the idle state and the switching state.

5.1.4.1.1 Idle state

This state is allowed only for 1:n architecture and for 1+1 revertive architecture.

A node is in the idle state when it is not generating or detecting requests.

Rule I #1 - IDLE STATE SOURCED K BYTES: Any node in the idle state shall source the K-bytes as given in table 3.

Table 3: Byte K1 and K2 values sourced in the idle state

K1 [1-4]	=	0000 (No Request code) or 0001 (Do Not Revert code - see note)
K1 [5-8]	=	0000 protection channel ID
K2 [1-4]	=	0000 protection channel ID
K2 [5]	=	0/1 (1+1 or 1:n code)
NOTE:	Only for 1+1 non-revertive systems compatible with 1:n systems.	

5.1.4.1.2 Switching state

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

Rule S #1 - SWITCHING STATE SOURCED K-BYTES: Any node in the switching state shall source K-bytes as shown in table 4:

Table 4: Byte K1 and K2 values sourced by a node in the switching state

K1 [1-4]	=	REQUEST code
K1 [5-8]	=	requesting channel ID
K2 [1-4]	=	null channel (0) if the received K1 byte indicates either null channel or the number of a locked out working channel. Number of channel which is bridged (1-15), in all other cases
K2 [5]	=	0/1 (1+1 or 1:n code)

5.1.4.2 Node APS state transition rules

For further study.

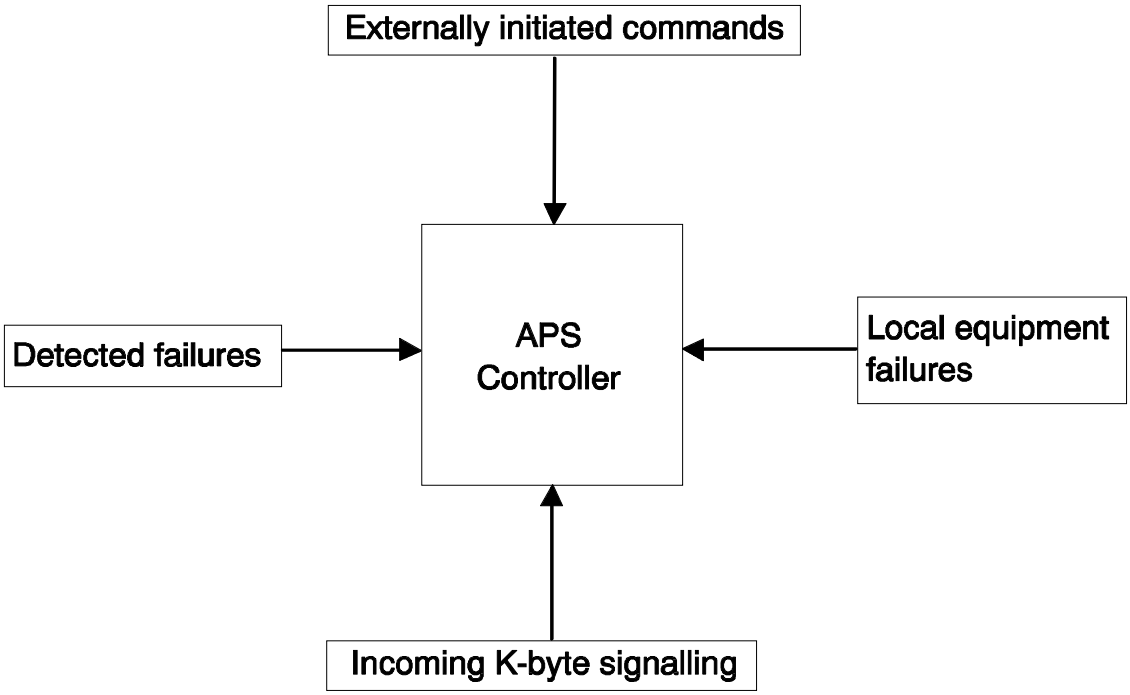


Figure 1: Conceptual MS linear protection APS controller

5.2 2-fibre multiplex section trail shared protection ring

5.2.1 APS requirements

NOTE: For the APS related objectives in SDH network protection schemes, see ETR 273, subclause 6.2 (details in annex C).

5.2.2 Switch initiation criteria

The requests to perform protection switching can be initiated either externally or automatically. Externally initiated commands are entered by way of the Operations System (OS) or the craftsperson interface. Subclause 5.2.2.1 describes these externally initiated commands available at the OS, craftsperson, or

both interfaces. APS requests can also be initiated based on multiplex section and equipment performance criteria. Subclause 5.2.2.2 provides the automatically initiated command criteria.

5.2.2.1 Externally initiated commands

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

5.2.2.1.1 Commands not signalled on the APS channel

The descriptions of the externally initiated commands are provided below:

clear: This command clears the externally initiated command and 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 command is useful if one span has excessive switching to protection. Another use for this command includes blocking protection access for some spans that have only traffic that does not need protection. The command is not time critical (i.e. not needed to be completed in tens of milliseconds). Thus, it can be transmitted over the DCC;

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

5.2.2.1.2 Commands using the APS bytes

The following commands are carried over the APS bytes:

Forced Switch of working to protection - Ring (FS-R): This command performs the ring switch from working channels to the protection channels for the span between the node at which the command is initiated and the adjacent node to which the command is destined. As this request has the highest priority, this command will be executed regardless of the state of the protection channels;

Manual Switch of working to protection - Ring (MS-R): This command performs the ring switch from the working channels to the protection channels for the span between the node at which the command is initiated and the adjacent node to which the command is destined. This occurs if the protection channels are not in an SD condition and are not satisfying an equal or higher priority bridge request (including failure of the protection channels);

EXERcise - Ring (EXER-R): This command exercises ring protection switching for the span between the node at which the command is initiated and the adjacent node to which the command is destined, without completing the actual bridge and switch. The command is issued and the responses are checked, but no working traffic is affected. The aim of exercise is to test the APS channel and K1, K2 bytes processing in the APS controller. If the protection channel should be passed through for an exercise-ring request is left for further study.

5.2.2.2 Automatically initiated commands

APS requests are also initiated based on multiplex section and equipment performance criteria detected by the NE. All the working and protection channels are monitored regardless of the failure or degradation conditions (i.e., after a switch has been completed, all appropriate performance monitoring is continued). The NE initiates the following bridge requests automatically: Signal Failure (SF), Signal Degrade (SD), Reverse Request (RR), and Wait to Restore (WTR). The bridge requests are transmitted from NE to NE (not from OS to NE).

The SF bridge request is used to protect working traffic affected by a hard-failure, while the SD bridge request is used to protect against a soft failure. The bridge requests are transmitted on both the short and long paths. Each intermediate node verifies the destination node ID of the long path bridge request and relays the bridge request. The destination node receives the bridge request, performs the activity according to the priority level, and sends the bridged indication.

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

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

Signal Fail - Ring (SF-R): The SF condition is defined in ETS 300 417 [1]; it is protected using the ring switch. Hence, this command is used to request ring switching for signal failures;

Signal Degrade - Ring (SD-R): The SD condition is defined in ETS 300 417 [1]; any degraded multiplex section is protected using the ring switch. Hence, this command is used to request ring switching for signal degradations;

Reverse Request - Ring (RR-R): This command is transmitted to the tail-end NE on the short path as an acknowledgement 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.

5.2.3 Protection switch protocol

Two APS bytes, K1 and K2, shall be used for protection switching. See subclause 5.2.4 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.

5.2.3.1 K1 byte

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

Table 5: Byte K1 functions

Bridge request code (Bits 1-4)				Destination node identification (Bits 5-8)			
bit 1	**bit 2**	**bit 3**	**bit 4**	**bit 5**	**bit 6**	**bit 7**	**bit 8**
1111 Reserved for 4 fibre APS protocol 1110 Reserved for 4 fibre APS protocol 1101 Forced Switch (Ring) FS-R 1100 Reserved for 4 fibre APS protocol 1011 Signal Fail (Ring) SF-R 1010 Reserved for 4 fibre APS protocol 1001 Reserved for 4 fibre APS protocol 1000 Signal Degrade (Ring) SD-R 0111 Reserved for 4 fibre APS protocol 0110 Manual Switch (Ring) MS-R 0101 Wait-To-Restore WTR 0100 Reserved for 4 fibre APS protocol 0011 Exerciser (Ring) EXER-R 0010 Reserved for 4 fibre APS protocol 0001 Reverse Request (Ring) RR-R 0000 No Request NR				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 the default APS bytes).			
NOTE: Reverse request assumes the priority of the bridge request to which it is responding.							

5.2.3.2 K2 byte

Byte K2 shall be assigned as shown in table 6.

Table 6: Byte K2 functions

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

5.2.4 Protection algorithm operation

This subclause is structured as follows:

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

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

Figure 2 illustrates the conceptual operation of an MS shared protection ring APS controller.

The following set of general rules apply:

Rule G #1 - BRIDGE REQUEST VALIDATION:

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 or short path code, note that the MS-RDI and MS-AIS signals terminate at multiplex section terminating elements as specified in ETS 300 417 [1].

5.2.4.1 Ring node APS state

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

5.2.4.1.1 Idle state

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

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

Table 7: Byte K1 and K2 values sourced in the idle state

K1 [1-4]	=	0000 (No Request code)
K1 [5-8]	=	destination NODE ID
K2 [1-4]	=	source NODE ID
K2 [5]	=	0 (short path code)
K2 [6-8]	=	000 (idle code)

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

Rule I #2 - IDLE STATE RECEIVED K-BYTES: Any node in the idle state shall terminate K1 and K2 in both directions.

5.2.4.1.2 Switching state

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

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

Rule S #1a: Any node in the switching state shall source K-bytes as shown in table 8:

Table 8: Byte K1 and K2 values sourced by a node in the switching state

K1 [1-4]	=	BRIDGE REQUEST code
K1 [5-8]	=	destination NODE ID
K2 [1-4]	=	source NODE ID
K2 [5]	=	0/1 (short/long path code)
K2 [6-8]	=	STATUS code

Rule S #1b: Any node in the switching state shall source a bridge request code on the short path and a bridge request code on the long path. Both bridge requests have the same priority (or one of them is a Reverse Request), and protect the same span. The exceptions is the isolated node case See figure 3 for the isolated node signalling cases.

Rule S #1c: Whenever a node in the switching state terminates a new short path K-byte bridge request from an adjacent node, of equal or higher priority than the bridge request it is currently executing, over the same span, it shall source a bridge request of the same priority on the corresponding long path. Whenever a node receives ring bridge requests on both short paths from its adjacent nodes, indicating that both signals it is sending are failed (SF), the long path bridge request shall take precedence over the short path Reverse Requests. This rule takes precedence over Rule S #1b in case of multiple bridge requests at the same node (see figure 3 part a).

Rule S #1d: Whenever a node detects an incoming failure on the working and on the protection channels, it shall always source over the short path a short path ring bridge request , even in the case of multiple failures, as long as the ring bridge request is not pre-empted by a higher priority bridge request. (See figure 3 part 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 3 part c).

Rule S #2 - SWITCHING STATE RECEIVED K-BYTES: Any node in the switching state shall terminate K1 and K2 in both directions.

Rule S #3 - UNIDIRECTIONAL BRIDGE REQUEST ACKNOWLEDGEMENT: As soon as it receives a bridge request or bridge request , 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 co-exist:

- FS-R with FS-R;
- SF-R with SF-R;
- FS-R with SF-R;

In these cases, the ring splits into multiple subrings.

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 bridge request on the long path, it shall drop its bridge and switch, and shall signal and act on its highest priority input. Note that Reverse Requests and other allowed co-existing ring bridge requests with a short path code are considered valid ring bridge requests.

5.2.4.1.3 Pass-through state

A node is in the full pass-through state when it transmits on one side, all the K1 and K2 bytes and the protection channels, which it receives on the other side. The full pass-through is bi-directional. Time slot interchange of traffic passing through a node is not supported by the current version of the protocol and is left for further study.

Rule P #1 - FULL PASS-THROUGH STATE SOURCED AND RECEIVED K-BYTES: When a node is in full pass-through, it transmits on one side, all the K1 and K2 bytes which it receives from the other side.

Rule P #2 - REMAINING IN THE FULL PASS-THROUGH STATE DURING SIGNALLING TRANSITIONS: When a node that is in the fullpass-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). Further clarification of this rule is for further study.

5.2.4.2 Ring node APS state transition rules

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

Rule Basic #1 - STATE TRANSITION TRIGGERS: All state transitions are triggered by an incoming K-byte change, a WTR expiration, an externally initiated bridge request, or a locally detected failure;

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

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

Ring Map Types: Each node on a ring shall maintain a ring map describing the ring connectivity and a local cross-connect map indicating the source and destination of all added, dropped, and passed-through AU-4s;

AU-4 Squelching: AU-4 squelching shall be performed at the switching nodes by inserting AU-AIS. The switching node shall, by comparing K-byte addresses (crossing K-bytes) to the information contained in the ring map, identify which nodes are missing. From this information and the cross-connection map, it shall identify which AU-4s are added and dropped at these nodes and shall squelch them bi-directionally. Refer to Annex A for details on squelching mechanism.

NOTE: Time Slot Interchange (TSI) is not supported by the current version of the protocol. The squelching requirements for TSI are for further study.

The requirements to support LO VC access are for further study;

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 5, unless the bridge requests are allowed to coexist.

5.2.4.2.1 Transitions between the idle and full pass-through state

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

Rule I-P #1a: The transition from the idle state to the full pass-through state 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 pass-through, according to Rule I-P #1b;

Rule I-P #1b: For any ring bridge request, the intermediate nodes on the long path shall go into full pass-through;

Rule I-P #2 - TRANSITION FROM THE PASS-THROUGH STATE TO THE IDLE STATE: A node shall revert from full pass-through state to the idle state when it detects No Request codes in K1 bits 1-4 and Idle codes in K2 bits 6-8, from both directions. Both directions revert simultaneously from the full pass-through state to the idle state.

5.2.4.2.2 Transitions between the idle and switching states

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

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

- a valid 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;
- 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 SD-R and MS-R bridge requests 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 EXER, the node shall signal as for any other bridge request, but shall not execute the bridge or switch;

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

Rule I-S #2 - TRANSITION FROM THE SWITCHING STATE TO THE IDLE STATE: A node shall revert from the switching state to the idle state when it detects NR codes in byte K1 bits 1-4 and idle codes in byte K2 bits 6-8 from both directions. The transition from the switching state to the idle state shall be a three-step transition:

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

Step 2: Upon reception of the No Request code, and of the indication that the switch has been dropped, the head-end node shall drop its bridge and its switch, and source the Idle code in both directions. The indication that the switch has been dropped is received on the short path for span bridge requests, and on the long path for ring bridge requests;

Step 3: Once the tail-end detects incoming idle codes, it shall also drop its bridge and switch and source the Idle code in both directions.

Note that there are cases in which no bridge or switch is to be dropped (e.g. for EXER, or switches that could not 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, therefore cannot properly execute protection switching;

NOTE: The default APS code at this moment is defined as follows: the transmitted K1 and K2 bytes have the source node ID equal to the destination node ID.

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

Rule I-S #5 - A node receiving long path ring bridge requests destined to itself from both of its neighbours shall take no action based on these bridge requests;

Rule I-S #6 - A node receiving the APS bytes which it is sourcing in both directions shall transition to the idle state;

Rule I-S #7 - When a node receives a Reverse Request code over the span which it is protecting, and when that same node is sending a Reverse Request code, it shall drop its bridge and switch as described in Rule I-S #2, except for bridge 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.

5.2.4.2.3 Transitions between switching states

This subclause provides the set of rules necessary to co-ordinate the transition between switching states.

The following transition rules apply:

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

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

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

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

Rule S-S#2 (ITU-T Recommendation G.841 [6] -> S-S#2f) SWITCH PREEMPTION: when a NE that is currently executing a ring switch receives a ring bridge request (due to a locally detected failure, an externally initiated command or a ring bridge request destined to it) of greater priority for an adjacent span that the ring switch it is executing, it shall:

- drop the ring bridge and switch immediately;

- execute the higher priority ring bridge request (as detailed in rule I-S#1);

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

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

Rule S-S #3 (ITU-T Recommendation G.841 [6] ->S-S #5) - A node receiving long path ring bridge requests destined to itself from both of its neighbours shall drop its bridge and switch.

5.2.4.2.4 Transitions between switching and full pass-through state

Rule S-P#1a (ITU-T Recommendation G.841 [6] ->S-P#1e): When a node that is currently executing a ring switch receives a long path ring bridge request for a non adjacent span of greater priority than the ring switch it is executing, it shall drop its bridge and switch immediately, then enter full pass-through;

Rule S-P#1b (ITU-T Recommendation G.841 [6] ->S-P#1f): When a node that is currently executing a ring switch has as its highest priority input long path ring bridge requests not destined to itself from both directions, it shall drop its bridge and switch immediately, then enter full pass-through;

Rule S-P #2 (ITU-T Recommendation G.841 [6] ->S-P #2a) - FULL PASS-THROUGH TO SWITCHING TRANSITIONS: 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 co-existing bridge request destined to that NE;

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

- determine if there is any need for squelching and squelch accordingly;
- execute the ring bridge and switch.

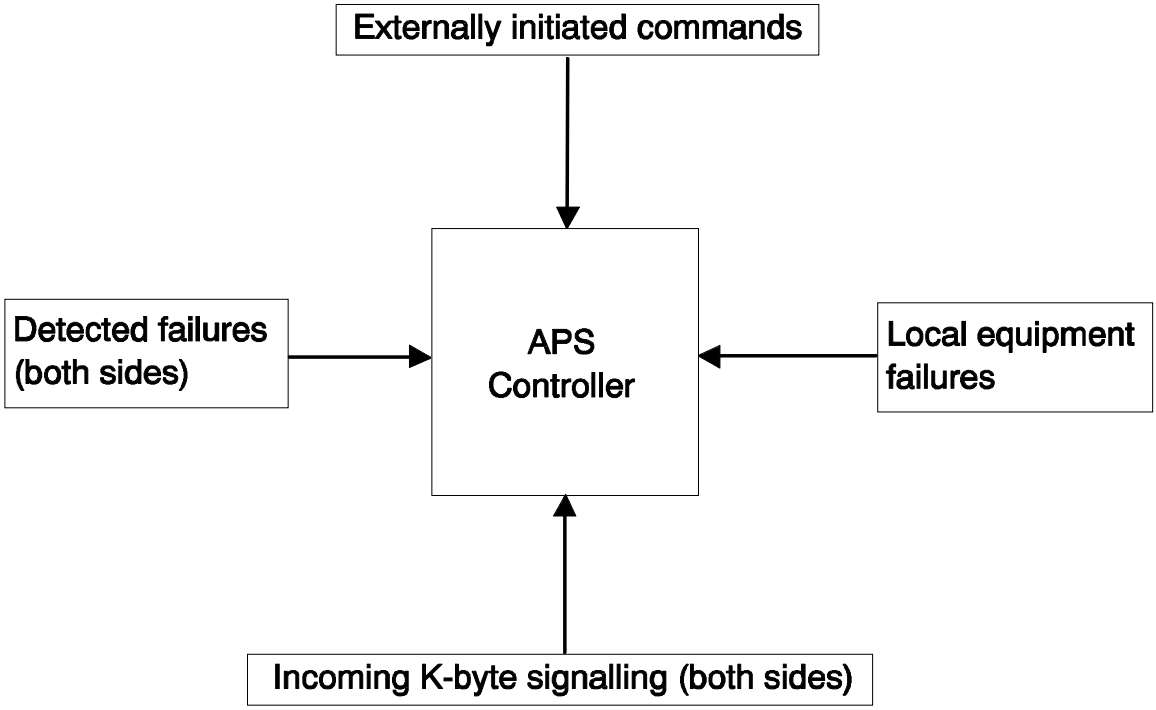
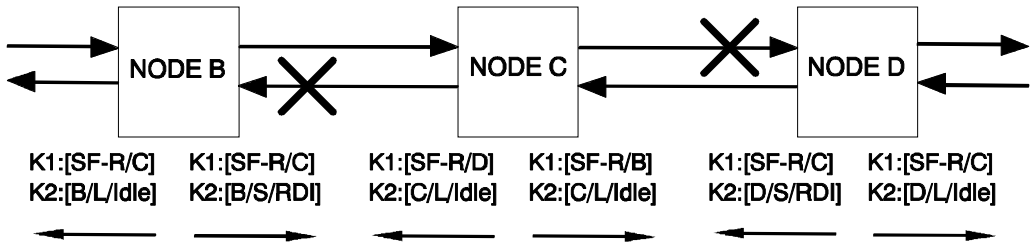
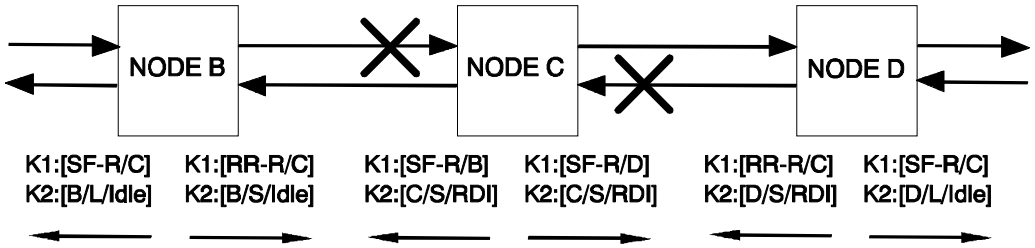


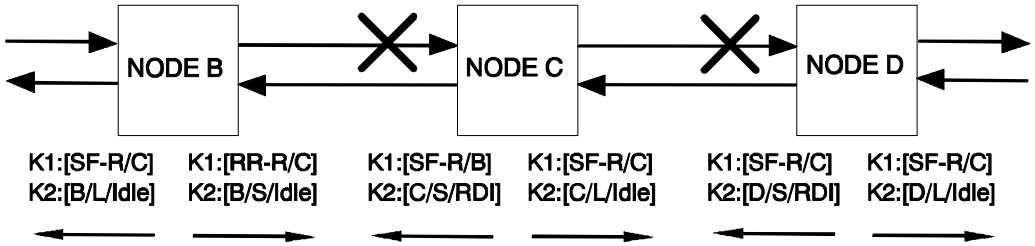
Figure 2: Conceptual MS shared protection ring APS controller



a) Node C is told of cuts



b) Node C detects cuts



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

Figure 3: Isolated node signalling (signalling states prior to nodes B and D establishing a ring bridge and switch)

5.3 4-fibre multiplex section trail shared protection ring

The 4-fibre ring is for further study.

5.4 2-fibre multiplex section trail dedicated protection ring

The APS protocol described in this subclause is applicable only to 1+1 architecture.

An APS protocol for 1:1 architecture with secondary traffic is for further study. It is proposed to base this protocol on the APS protocol for multiplex section trail shared protection rings.

NOTE: It is very unlikely that the MS-DPRing will be used in more than a very limited number of applications.

5.4.1 APS requirements

5.4.1.1 Requirements for the protocol

The protocol is used to synchronize switching at both ends of a failed span in case of unidirectional failure and to transport external commands:

- **Dual end switching:** In case of section failure, both ends have to loop-back their traffic together. The protocol has to ensure the synchronization of the switching;

- **External commands:** The protocol has to transport external commands;

- **Misconnections:** This protection scheme is dedicated; this means that two different resources never share the same protection resource. Therefore, misconnections are not possible and the protocol does not have to avoid misconnections;

- **Passing through:** When the traffic is looped back, it has to go round the failure through the other nodes of the ring. As long as there is no low priority traffic, protection resource can permanently be in pass through in all the nodes and the protocol does not have to initiate passing through.

5.4.1.2 Use of linear MS trail protocol

The MS Dedicated ring protocol is compatible with the existing protocol for 1+1 dual ended revertive linear MS trail protection.

This means that an MS dedicated protection ring can be made using equipment provided with 1+1 dual ended linear MS trail protection.

Nevertheless, a specific rewriting of the protocol is proposed here in order to take into account the different type of reconfiguration (loop-back instead of switch) and the fact that there is not a distinction between working and protection fibres.

5.4.2 Switch initiation criteria

The request to perform protection switching can be initiated either externally or automatically.

5.4.2.1 Externally initiated commands

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

5.4.2.1.1 Commands not signalled on the APS channel

The descriptions of the externally initiated commands are provided below:

clear: This command clears the externally initiated command and 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.

5.4.2.1.2 Commands using the APS bytes

The following commands are carried over the APS bytes:

Lockout of Protection (LP): This command prevents the ring switch. Even if the command is signalled on the ASP channel, it shall be sent externally to both the nodes of the span;

Forced Switch of Working to protection (FS-W): This command performs the ring switch from working channels to the protection channels for the span between the node at which the command is initiated and the adjacent node to which the command is destined;

Manual Switch of Working to protection (MS-W): This command performs the ring switch from the working channels to the protection channels for the span between the node at which the command is initiated and the adjacent node to which the command is destined;

EXERcise (EXER): This command exercises protection switching for the span between the node at which the command is initiated and the adjacent node to which the command is destined, without completing the actual switch. The command is issued and the responses are checked, but no working traffic is affected. The aim of exercise is to test the APS channel and K1, K2 bytes processing in the APS controller.

The lockout of working channel external command is a network objective (see annex C). This command is not supported by this APS protocol.

5.4.2.2 Automatically initiated commands

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

Signal Fail (SF): The SF condition is defined in ETS 300 417 [1]; it is protected using the ring switch. Hence, this command is used to request switching for signal failures;

Signal Degrade (SD): The SD condition is defined in ETS 300 417 [1]; any degraded multiplex section is protected using the ring switch. Hence, this command is used to request switching for signal degradations;

Reverse Request (RR): This command is transmitted to the tail-end NE as an acknowledgement;

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 for the same span.

5.4.3 Protection switch protocol

The APS protocol for 2 fibre Multiplex Section Trail Dedicated Ring is derived from the protocol for Multiplex Section Trail Linear Protection described in subclause 5.1.

5.4.3.1 K1 byte generation rules

K1 indicates a request for a ring switch.

The K1 generation rules are the same contained in subclause 5.1 for the 1+1 MS linear dual ended revertive protocol, with the following exception: the lockout of protection external command is not applicable.

The request are listed in table 9 in priority order. For each request, the code used in bits 1 to 5 of byte K1 is indicated.

The priority shown in the table is the same valid for the MS linear protection APS protocol. In this case, switching in different spans are completely independent and requests for different spans can coexist on the ring, resulting in a ring segmentation, regardless of their priority.

In addition, due to the independence of requests on different span, the following requests: forced switch, signal fail, signal degrade and manual switch have the same effect.

Table 9: Priority of requests

Bits 1234	Condition, state or request	Priority	Acronym
1111	Lockout of protection	Highest	LP
1110	Forced switch		FS-W, FS-P
1101	Signal fail - high priority		SF
1100	Signal fail - low priority		
1011	Signal degrade - high priority		SD
1010	Signal degrade - low priority		
1001	Unused		
1000	Manual switch		MS-W, MS-P
0111	Unused		
0110	Wait-to-restore		WTR
0101	Unused		
0100	Exercise		EXER
0011	Unused		
0010	Reverse Request		RR
0001	Unused		
0000	No request	Lowest	NR
NOTE: Bits 5 to 8 of K1 shall be set to 0001.			

5.4.3.2 K2 byte generation rules

As defined in subclause 5.1.3.2.

5.4.4 Protection algorithm operation

The protection is achieved by looping back one direction to the other. Thus, a direction of a VC is protected by the other direction of the same VC. The operator have the choice, VC per VC to make the working traffic on one fibre or the other. In the case of an isolated ring, it can be more convenient to put all the working traffic on one fibre and all the protected resources on the other. Nevertheless, when rings are interconnected, the possibility to put on the same fibre both working and protection gives an extra level of flexibility.

The bridge is permanently carried out.

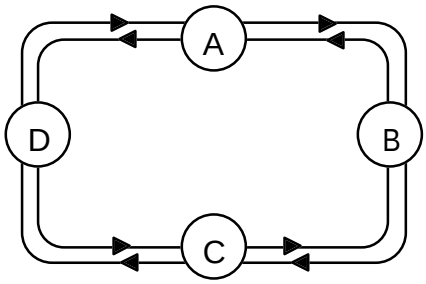
Table 10 shows a set of rules for the generation of the requests and the corresponding actions.

Table 10: Protocol rules

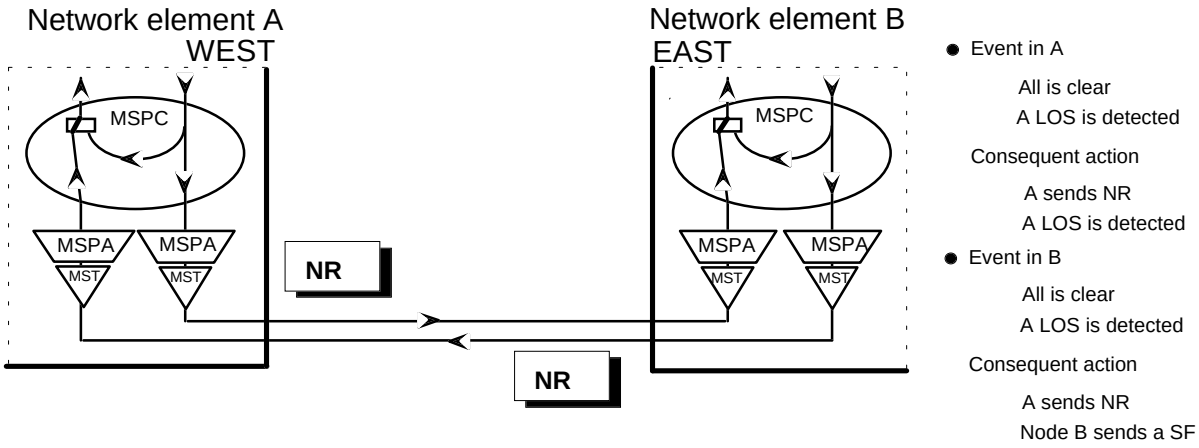
Rule	Event	Action on switch	Signalling in K1
1	A local SF or a SD is detected	Loop-back is performed	SF or SD is sent
2	A remote SF or SD is received	Loop-back is performed	RR is sent
3	A NR is received	Loop-back is released	NR is sent
4	A RR is received	WTR starts	WTR is sent
5	WTR expires	Loop-back is released	NR is sent
6	Clear	Clears all switch commands	
7	Lockout of protection	Prevents loop-back	
8	Forced switch	Forces loop-back	
9	Manual switch	Forces loop-back	
10	Exercise	Loop-back not actually completed	

Below are some examples of ring reconfiguration in the case of failure. They are valid both for a signal degrade or a signal fail.

5.4.4.1 Ring without failure

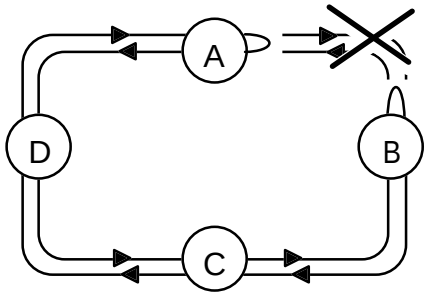


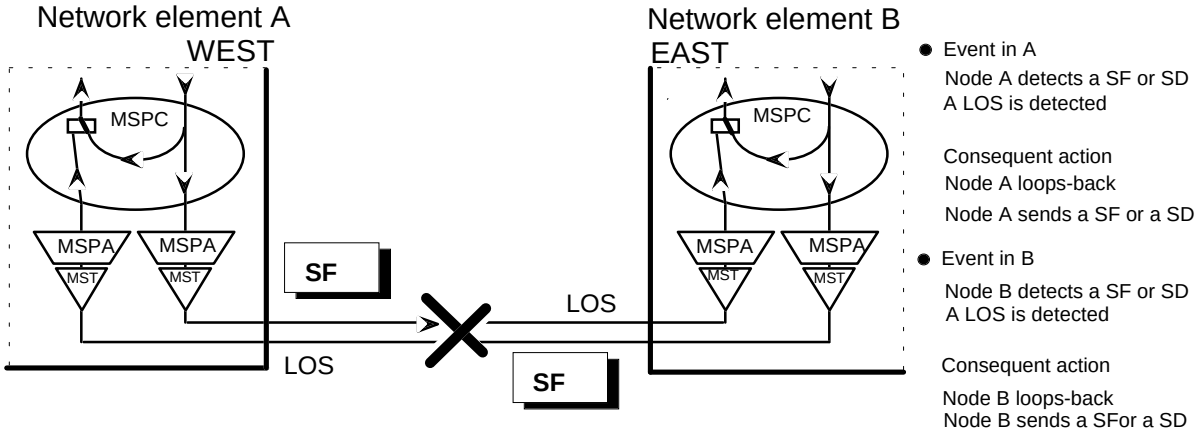
On all these schemes, the two ends of a section are represented with the protection function. The K1 message issued by the ends of the section are given in the rectangles by the fibres.



5.4.4.2 Bi-directional failure

In this case, both ends detect the failure and perform loop-back.

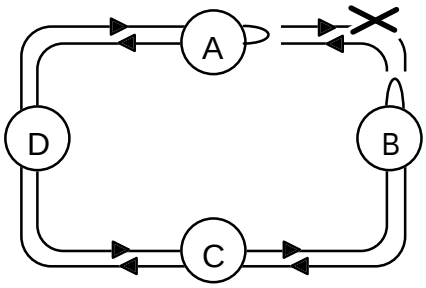


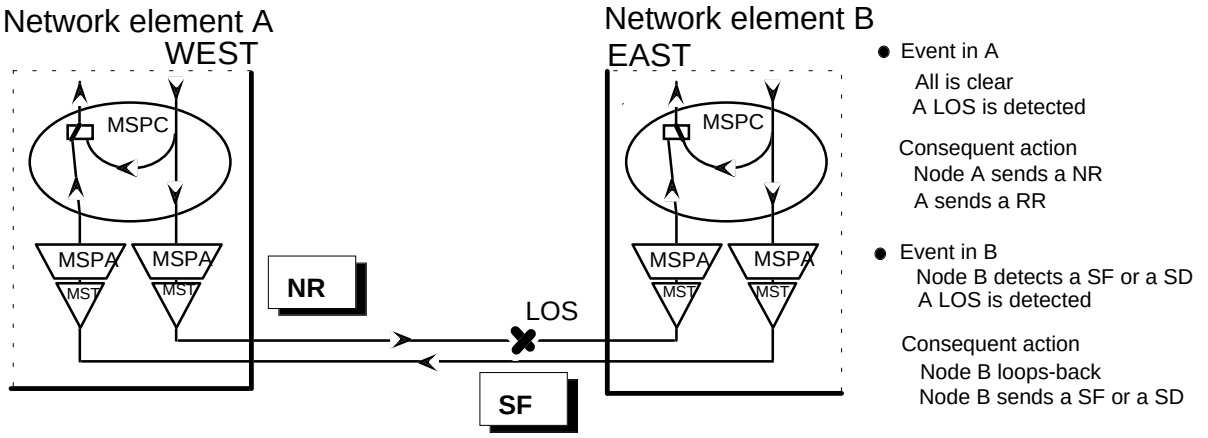


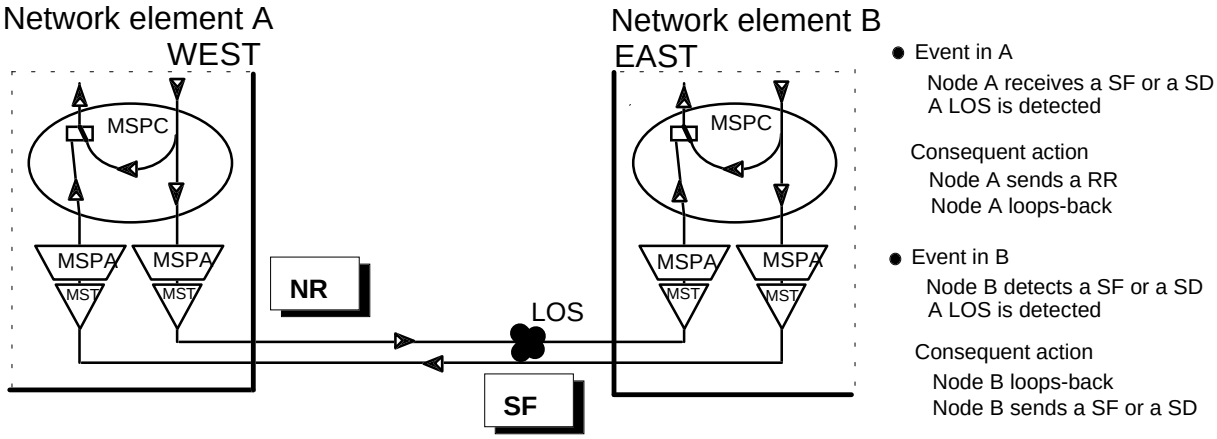
Network healing is now completed.

5.4.4.3 Unidirectional failure

In this case, only one end of the section detects the failure. It performs loop-back and sends a message to the other end so that it also loops-back.



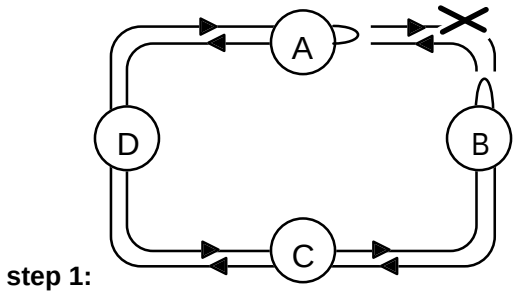




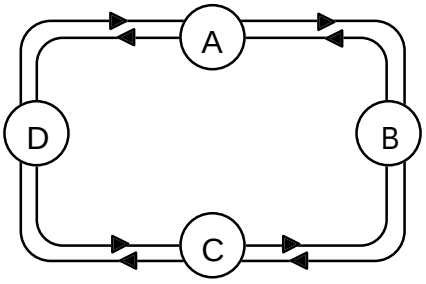
Network healing is now completed.

5.4.4.4 The failure is repaired

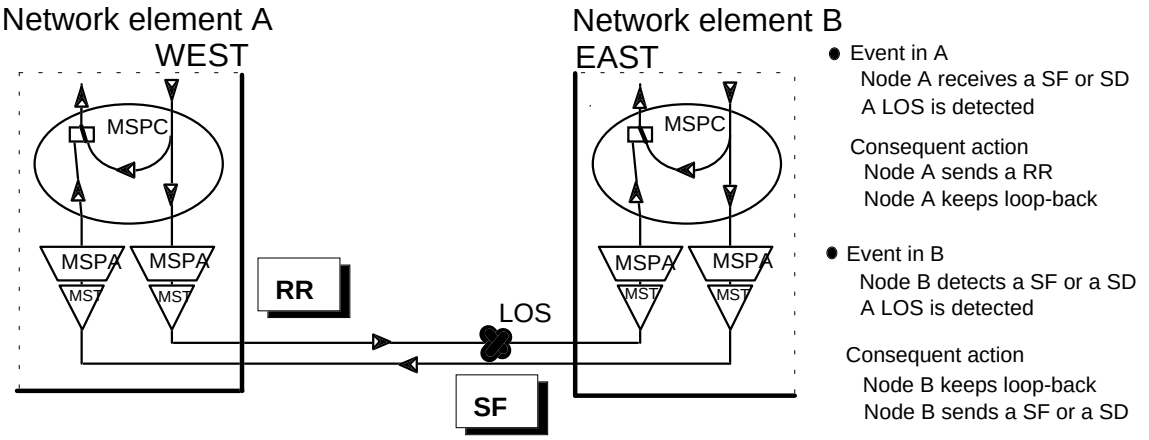
The two cases (one fibre and two fibres) will be considered. On a first step the fibre from AB to A is re-paired and then the other one.



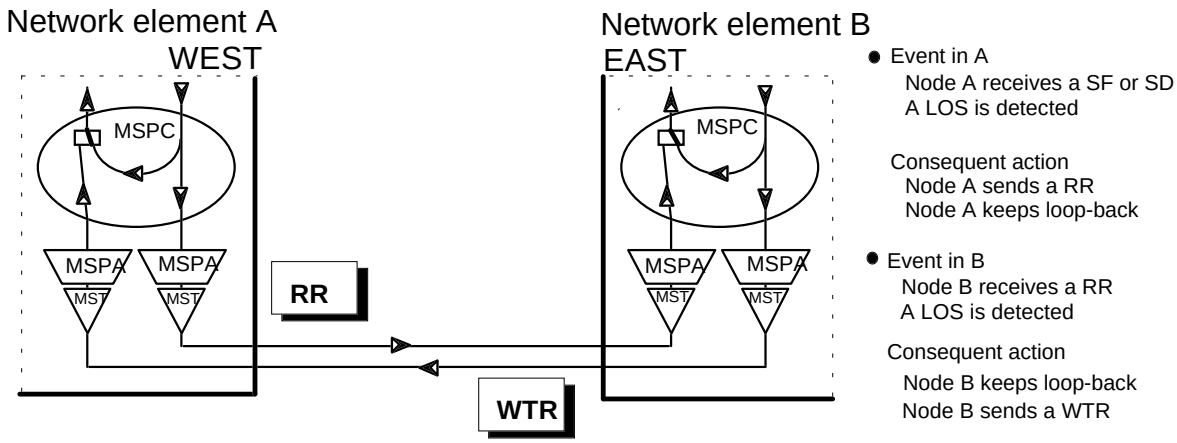
step 1:



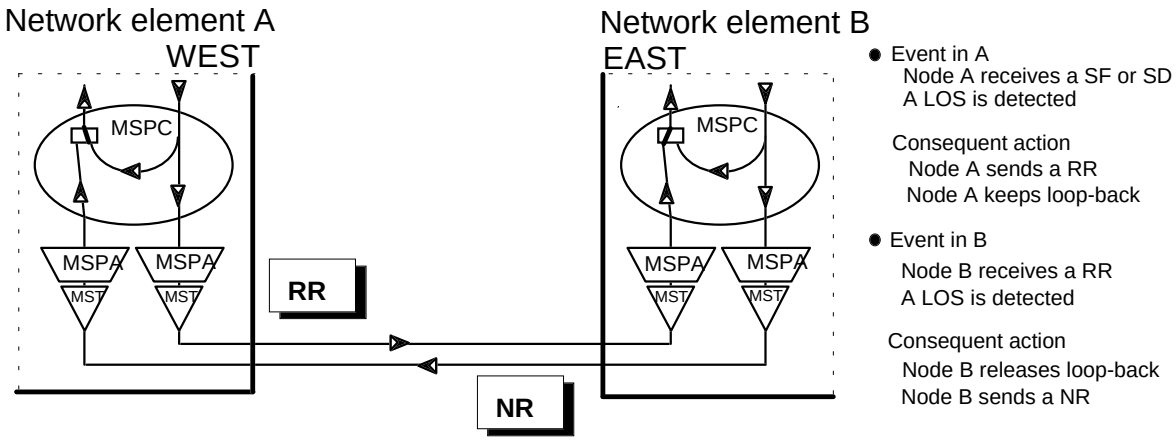
step 2:

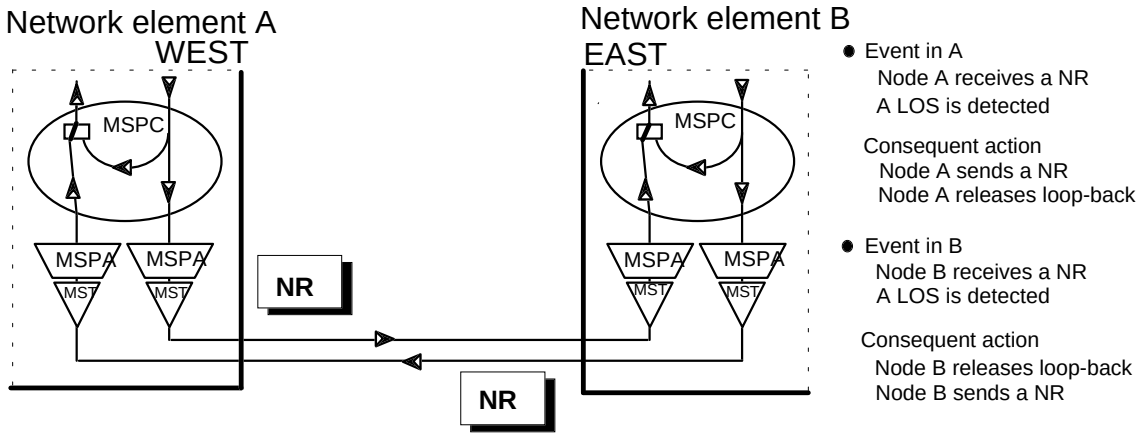


The second fibre is repaired. The Wait-to-Restore is activated.



Wait-to-Restore expires. The network is in normal mode.





6 Path protection protocols

6.1 LO/HO trail protection

6.1.1 APS Requirements

NOTE: For the APS related objectives in SDH network protection scheme, see ETR 273, clause 7 (details in annex C).

6.1.2 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.

6.1.2.1 1+1 single-ended protection

A request can be:

1) an automatically initiated command (SF or SD) associated with a VC trail;
2) a state (Wait-To-Restore, No Request) of the VC trail protection process; or
3) an externally initiated command (Clear, Lockout, Forced Switch, Manual Switch).

For 1+1 single-ended protection architecture, all requests are local. The priority of local requests is given in table 11.

Table 11: 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 single-ended switching is being performed and no APS protocol is supported over the protection channel, Signal Fail on the protection channel does not interfere with the ability to perform a forced switch to protection.	
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.	

6.1.2.1.1 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: Clears all switch commands listed below:

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 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 from the protection VC trail to the working VC trail (unless an equal or higher priority switch request is in effect);

NOTE 1: 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 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 from the protection VC trail to the working VC trail (unless an equal or higher priority switch request is in effect);

NOTE 2: 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.

6.1.2.1.2 Automatically initiated commands

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

6.1.2.1.2.1 Higher order automatically initiated commands

For HO VCs, the Signal Fail automatically initiated command is defined as the presence of one or more of the following defect conditions detected in the higher order path termination function (described in ETS 300 417 [1]):

- higher order path server signal fail (HP-SSF) defect. HP-SSF arises from such server layer defects as AU loss of pointer (AU-LOP) or AU-AIS;

- higher order path unequipped (HP-UNEQ) defect;

- higher order path trace identifier mismatch (HP-TIM) defect (if this condition is enabled by the network provider to be used);

The HP-TIM contributions to the SF condition is optional, and its definition is for further study.

For HO VCs, the Signal Degrade automatically initiated command is defined as the presence of the following defect condition detected in the higher order path termination function (described in ETS 300 417 [1]):

- higher order path degraded (HP-DEG) defect.

6.1.2.1.2.2 Lower order automatically initiated commands

For LO VCs, the Signal Fail automatically initiated command is defined as the presence of one or more of the following defect conditions detected in the lower order path termination function (described in ETS 300 417 [1]):

- lower order path server signal fail (LP-SSF) defect. LP-SSF arises from such server layer defects as TU loss of pointer (TU-LOP) or TU-AIS;

- lower order path unequipped (LP-UNEQ) defect;

- lower order path trace identifier mismatch (LP-TIM) defect (if this condition is enabled by the network provider to be used);

The LP-TIM contribution to the SF automatically initiated command is optional, and its definition is for further study.

For LO VCs, the Signal Degrade automatically initiated command is defined as the presence of the following defect condition detected in the lower order path termination function (described in ETS 300 417 [1]):

- lower order path degraded (LP-DEG) defect.

6.1.2.2 1+1 dual-ended protection

For further study.

6.1.2.3 1:1 protection

For further study.

6.1.3 Protection switching protocol

6.1.3.1 1+1 single-ended protection

In this architecture, there is no APS channel required.

6.1.3.2 1+1 dual-ended protection

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

6.1.3.3 1:1 protection

This is for further study.

6.1.4 Protection algorithm operation

6.1.4.1 1+1 single-ended protection

6.1.4.1.1 Control of the bridge

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

6.1.4.1.2 Control of the selector

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

If an hold-off time has been provisioned, after the hold off expiration the NE should check if the switching criteria is still valid and in that case it should execute the switch. The hold off time should be provisionable from 0 to 10 sec. in step of 100 ms.

6.1.4.1.2.1 Revertive mode

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

To prevent frequent operation of the selector due to an intermittent fault, a failed trail shall become fault-free. After the failed trail meets this criterion, (and no other externally initiated commands are present) a fixed period of time shall elapse before it is used again as the working channel. This period is called Wait-To-Restore (the range for this time is for further study). After this state, switching does not occur. An SF or SD condition shall override the WTR. After the WTR period is completed, a No Request state is entered. Switching then occurs from the protection channel to the working channel.

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

6.1.4.1.2.2 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.

6.1.4.2 1+1 dual-ended protection

This is for further study.

6.1.4.3 1:1 protection

This is for further study.

6.2 LO/HO SNC protection

6.2.1 APS requirements

NOTE: For the APS related objectives in SDH network protection scheme, see ETR 273, clause 8 (details in annex C).

6.2.2 Switch initiation criteria

6.2.2.1 1+1 single-ended protection

A request can be:

1) an automatically initiated command (SF or SD) associated with a VC sub-network 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 1+1 architecture, all requests are local. The priority of local requests is given in table 12.

Table 12: 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 single-ended switching is being performed and no APS protocol is supported over the protection channel, Signal Fail on the protection channel does not interfere with the ability to perform a forced switch to protection.	
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.	

6.2.2.1.1 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: Clears all switch commands listed below:

Lockout of Protection (LP): Prevents the selector from switching to the protection VC sub-network connection, by issuing a Lockout of Protection request;

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

NOTE 1: 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 sub-network connection, this command will be carried out regardless of the condition of the working VC sub-network connection.

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

NOTE 2: 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 sub-network connection, this command will be carried out only if the working VC sub-network connection is not in the Signal Fail or Signal Degrade automatically initiated command.

6.2.2.1.2 Automatically initiated commands

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

6.2.2.1.2.1 Higher order automatically initiated commands

For HO VCs, the Signal Fail automatically initiated command is defined as the presence of one or more of the following defect conditions detected in the higher order path overhead monitoring function (described in ETS 300 417 [1]):

For SNC/N and SNC/I:

- higher order path server signal fail (HP-SSF) defect. HP-SSF arises from such server layer defects as AU loss of pointer (AU-LOP) or AU-AIS;

For SNC/N only:

- higher order path unequipped (HP-UNEQ) defect;

- higher order path trace identifier mismatch (HP-TIM) defect (if this condition is enabled by the network provider to be used);

The HP-TIM contribution to the SF condition is optional, and its definition is for further study.

For HO VCs, using SNC/N, the Signal Degrade automatically initiated command is defined as the presence of the following defect condition detected in the higher order path overhead monitoring function (described in ETS 300 417 [1]):

- higher order path degraded (HP-DEG) defect.

6.2.2.1.2.2 Lower order automatically initiated commands

For LO VCs, the Signal Fail automatically initiated command is defined as the presence of one or more of the following defect conditions detected in the lower order path overhead monitoring function (described in ETS 300 417 [1]):

For SNC/N and SNC/I:

- lower order path server signal fail (LP-SSF) defect. LP-SSF arises from such server layer defects as TU loss of pointer (TU-LOP) or TU-AIS;

For SNC/N only:

- lower order path unequipped (LP-UNEQ) defect;

- lower order path trace identifier mismatch (LP-TIM) defect (if this condition is enabled by the network provider to be used).

The LP-TIM contribution to the SF automatically initiated command is optional, and its definition is for further study.

For LO VCs using SNC/N, the Signal Degrade automatically initiated command is defined as the presence of the following defect condition detected in the lower order path overhead monitoring function (described in ETS 300 417 [1]):

- lower order path degraded (LP-DEG) defect.

6.2.2.2 Other architectures

For further study.

6.2.3 Protection switching protocol

6.2.3.1 1+1 single-ended protection

In this architecture, there is no APS channel required.

6.2.3.2 Other architectures

For further study.

6.2.4 Protection algorithm operation

6.2.4.1 1+1 single-ended protection algorithm

6.2.4.1.1 Control of the bridge

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

6.2.4.1.2 Control of the selector

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

If an hold-off time has been provisioned, after the hold off expiration the NE should check if the switching criteria is still valid and in that case it should execute the switch. The hold off time should be provisionable from 0 to 10 sec. in step of 100 ms.

6.2.4.1.2.1 Revertive mode

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

To prevent frequent operation of the selector due to an intermittent fault, a failed trail shall become fault-free. After the failed trail meets this criterion, (and no other externally initiated commands are present) a

fixed period of time shall elapse before it is used again as the working channel. This period is called Wait-To-Restore (the range for this time is for further study). After this state, switching does not occur. An SF or SD condition shall override the WTR. After the WTR period is completed, a No Request state is entered. Switching then occurs from the protection channel to the working channel.

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

6.2.4.1.2.2 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.

6.2.4.2 Other architectures

For further study.

Annex A (normative): Squelching mechanism in MS-Shared Protection Rings

This annex provides a description of the squelching mechanism in MS-Shared Protection Rings. The modification needed for the squelching mechanism in case of dual node interworking between MS-SPRings is also addressed.

A.1 Squelching of HO traffic

A.1.1 Case of single ring

Figure A.1 shows an MS-SPRing with two paths, one between node B and node D and the other between node D and node F, sharing the same time slot (AU-4#1). In case either a nodal failure of node D or a multiple failure resulting in the isolation of node D occurs, the switching nodes C and E perform a ring switch and there could be a misconnection for the traffic between B and F. To avoids this misconnection the squelching of the traffic is required: the switching nodes C and E insert AU-AIS on the traffic that is transmitted over the AU-4#N/2+1 and on the traffic that is received over the AU#N/2+1, due to the bridge and switch action. This squelching mechanism is shown in figure A.2 in case of nodal failure.

In the most general case where, due to multiple failures, the ring is segmented the switching nodes should squelch all the AU-4s carrying traffic which has the two terminations in different segments of the ring and therefore can be potentially misconnected.

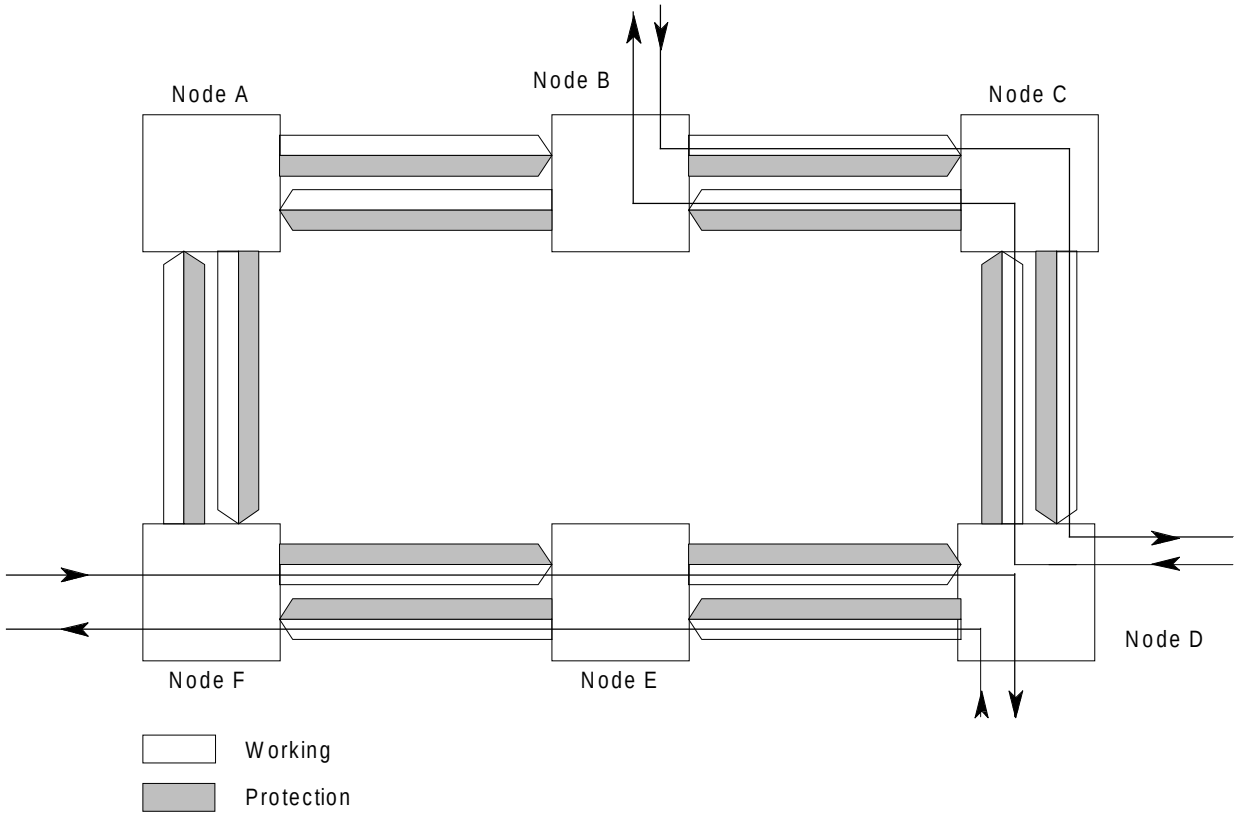


Figure A.1

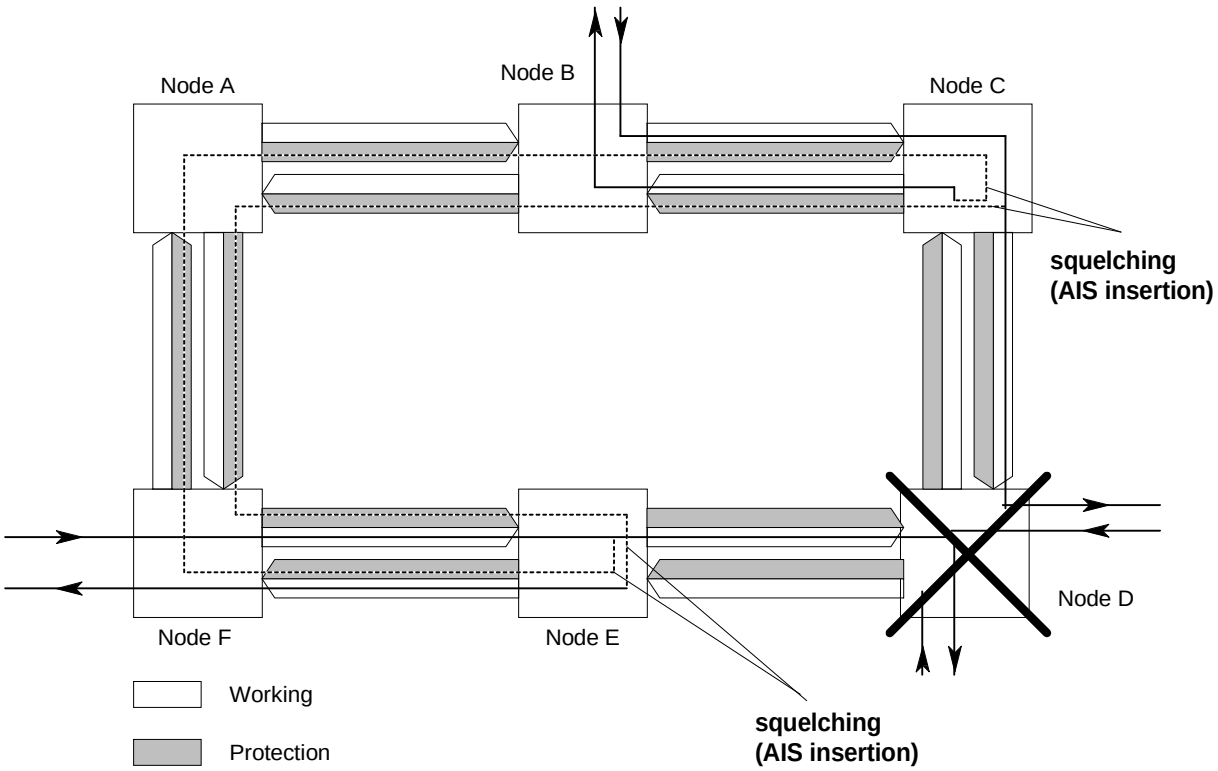


Figure A.2

A.1.2 Case of dual node ring interworking

Figure A.3 shows two MS-SPRings interconnected in two nodes. Two paths sharing the same time slot (AU-4#1) are highlighted the first one belongs to ring 1 and the second one transits from ring 1 to ring 2, using the dual node interworking between the two rings.

In case either a nodal failure of the secondary interconnection node or a multiple failure resulting in the isolation of that node occur, the local traffic of ring 1 and the interworking traffic are mis-connected. To avoid this misconnection, the switching nodes perform a squelching of the traffic as in the case of single ring described before. Figure A.4 shows the situation of a nodal failure in the secondary interconnection node of ring 1.

When the failure occurs in the primary interconnection node, a secondary connection between Node A and the secondary interconnection node need to be performed in order to maintain the transit of the interworking traffic between ring 1 and ring 2, therefore the switching nodes are required not to squelch this traffic. This case is shown in figure A.5.

The above considerations apply also in the case of dual node ring interworking between an MS-SPRing and a different kind of protected ring.

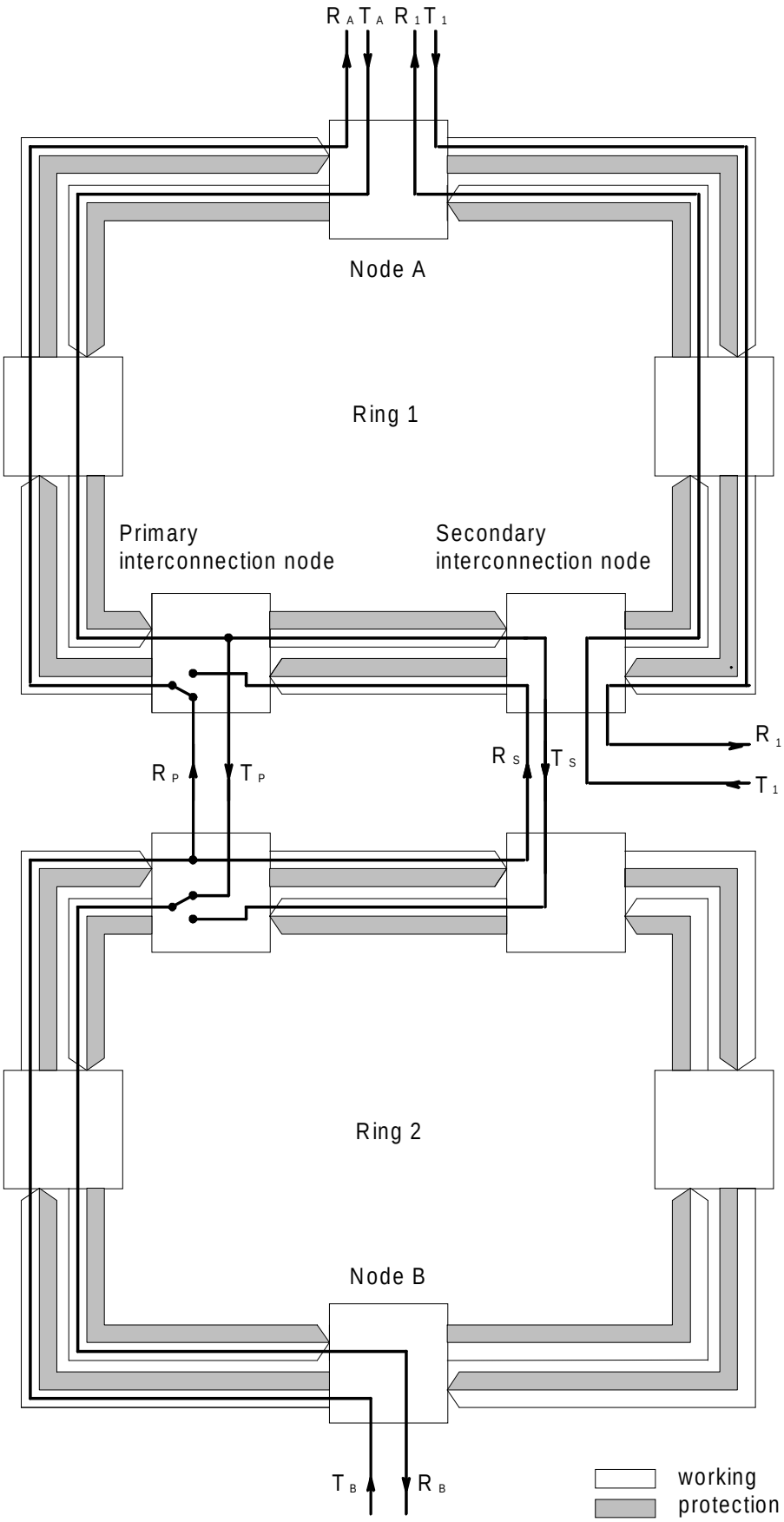

R A T A R 1 T 1
Node A
Ring 1
Primary
interconnection node
Secondary
interconnection node
R P
T P
R S
T S
R 1
T 1
Ring 2
Node B
T B
R B
working
protection

Figure A.3

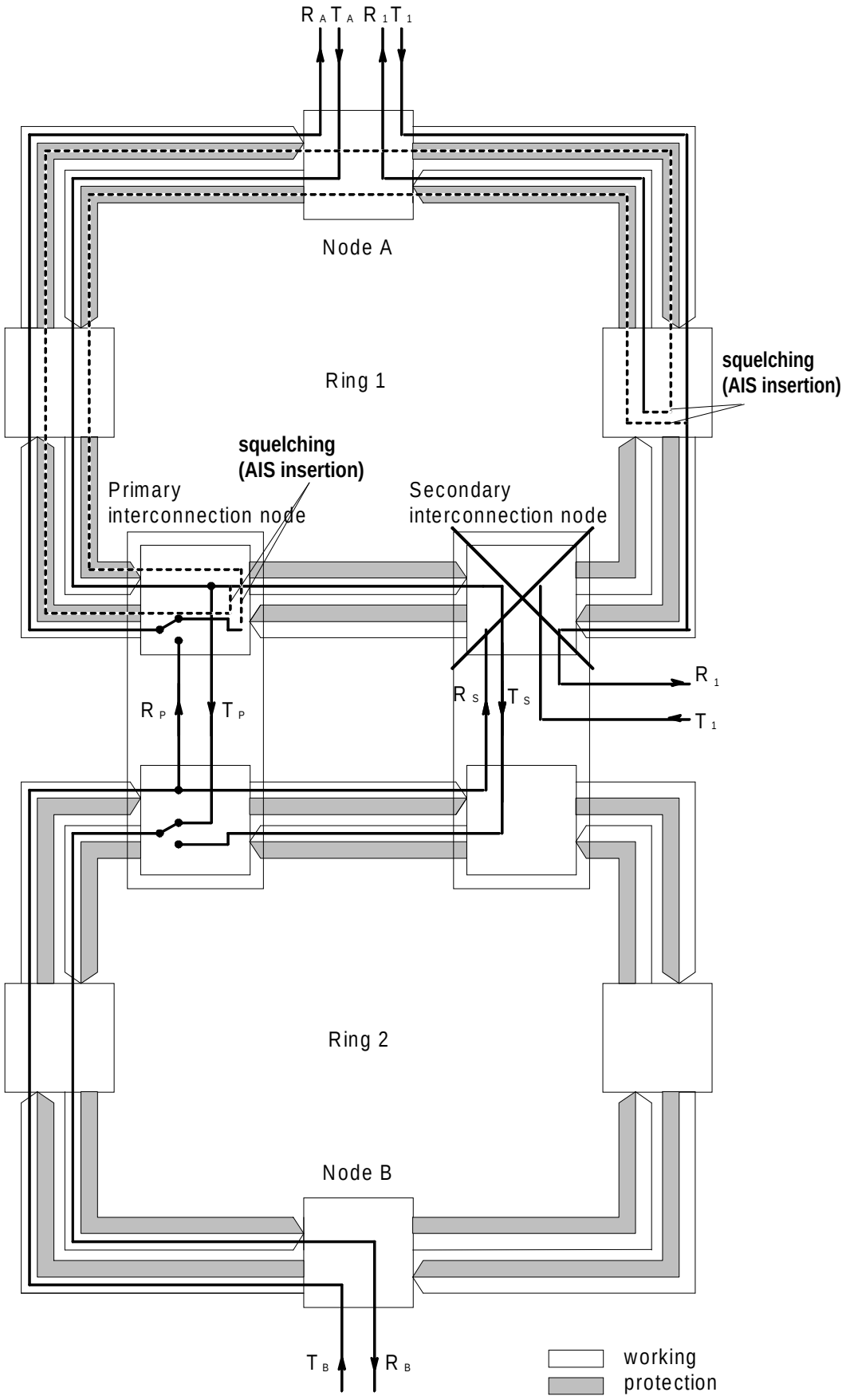

R A T A R 1 T 1
Node A
Ring 1
squelching
(AIS insertion)
squelching
(AIS insertion)
Primary
interconnection node
Secondary
interconnection node
R P
T P
R S
T S
R 1
T 1
Ring 2
Node B
T B
R B
working
protection

Figure A.4

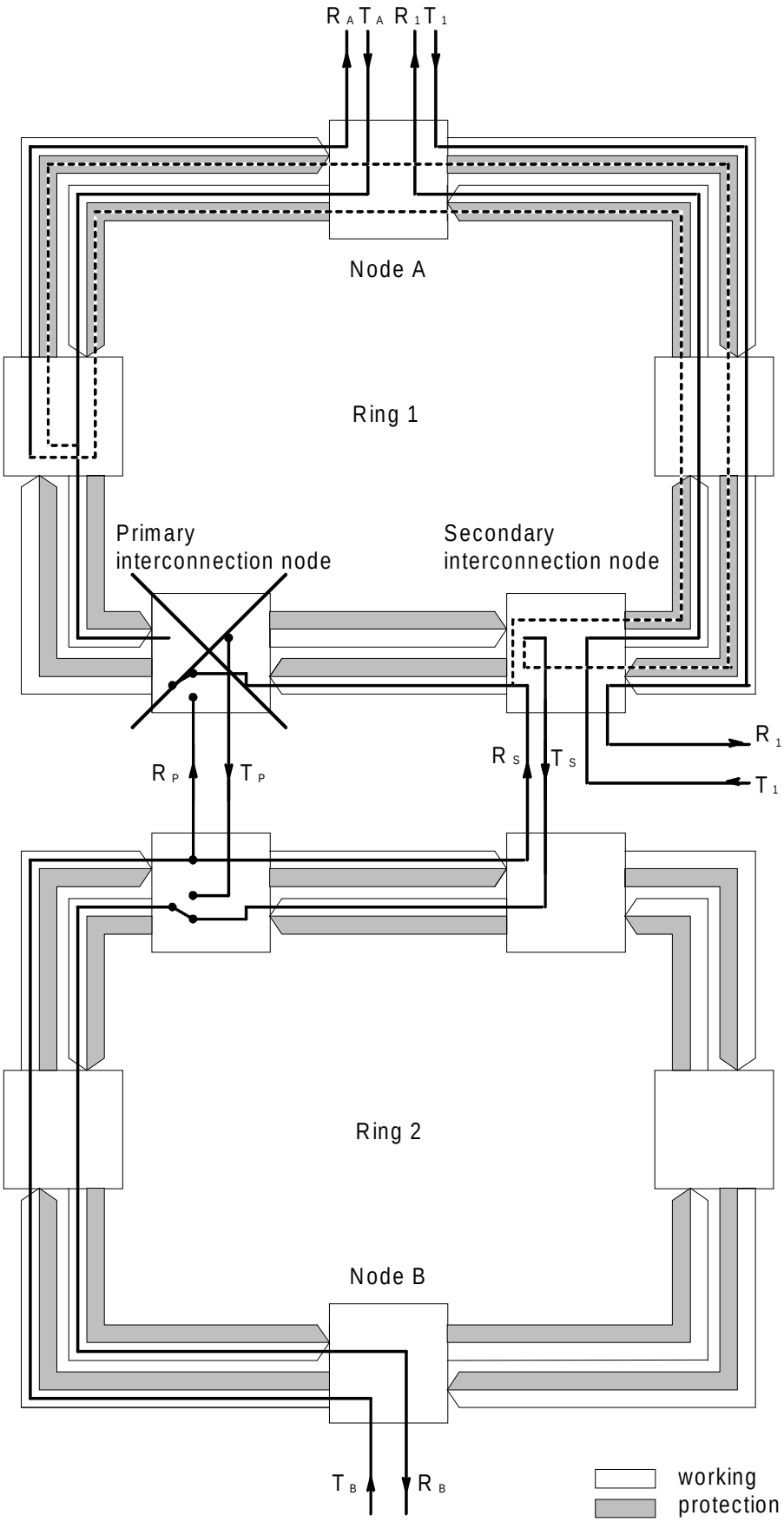

R A T A R 1 T 1
Node A
Ring 1
Primary
interconnection node
Secondary
interconnection node
R P
T P
R S
T S
R 1
T 1
Ring 2
Node B
T B
R B
working
protection

Figure A.5

Annex B (informative): Examples of protection switching in an MS shared protection ring

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

B.1 Unidirectional signal fail (ring)

This example covers the case of a unidirectional SF condition.

See figure B.1a.

The initial state of the ring is the idle state.

At time T1, Node F detects an SF condition on its working and protection channels. It becomes a switching node (Rule I-S #1a) 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, enters switching state and transmits an SF ring bridge request on the long path, and a Reverse Request on the short path (Rules I-S #1a, and S #3). 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 acknowledgement 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.

See figure B.1b.

At time T2, 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 #2a). 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 #2b).

See figure B.1c.

At time T3, 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.

B.1.1 Derivation of switching delay

The switching delay for the unidirectional signal fail in the worst case can be evaluated for a 16 nodes ring with a maximum length of 1 200 km.

Let Dp be the processing delay in a pass-through node, J×Dp the processing delay in a switching node, 0,375 ms the time it takes to validate a new message (three frames) and assuming that transmission delay over a fibre system be 5 μs/km the contributions to the delay are:

Time it takes to node F to generate first request:	J×Dp
Time it takes to the intermediate nodes to move to pass-through:	14×(Dp+0,375)
Time it takes to node E to process the request:	J×Dp+0,375
Time it takes to node E to generate the acknowledgement request:	J×Dp
Time it takes to the intermediate nodes to pass-through the message from E (see note):	14×Dp
Time it takes to node F to process the request from node E:	J×Dp+0,375

The transmission delay over the fibre is (long path): $\frac{15}{16}(1\,200\text{x}0{,}005)$

Then the total switching delay Sd is:

$$Sd = (4\text{x}J\text{x}Dp) + (28\text{x}Dp) + (16\text{x}0{,}375) + 2\text{x}\frac{15}{16}\text{x}(1\,200\text{x}0{,}005)$$

NOTE: A node in pass-through state is supposed not to check the incoming K-bytes for three frames before relaying them on the outgoing signal.

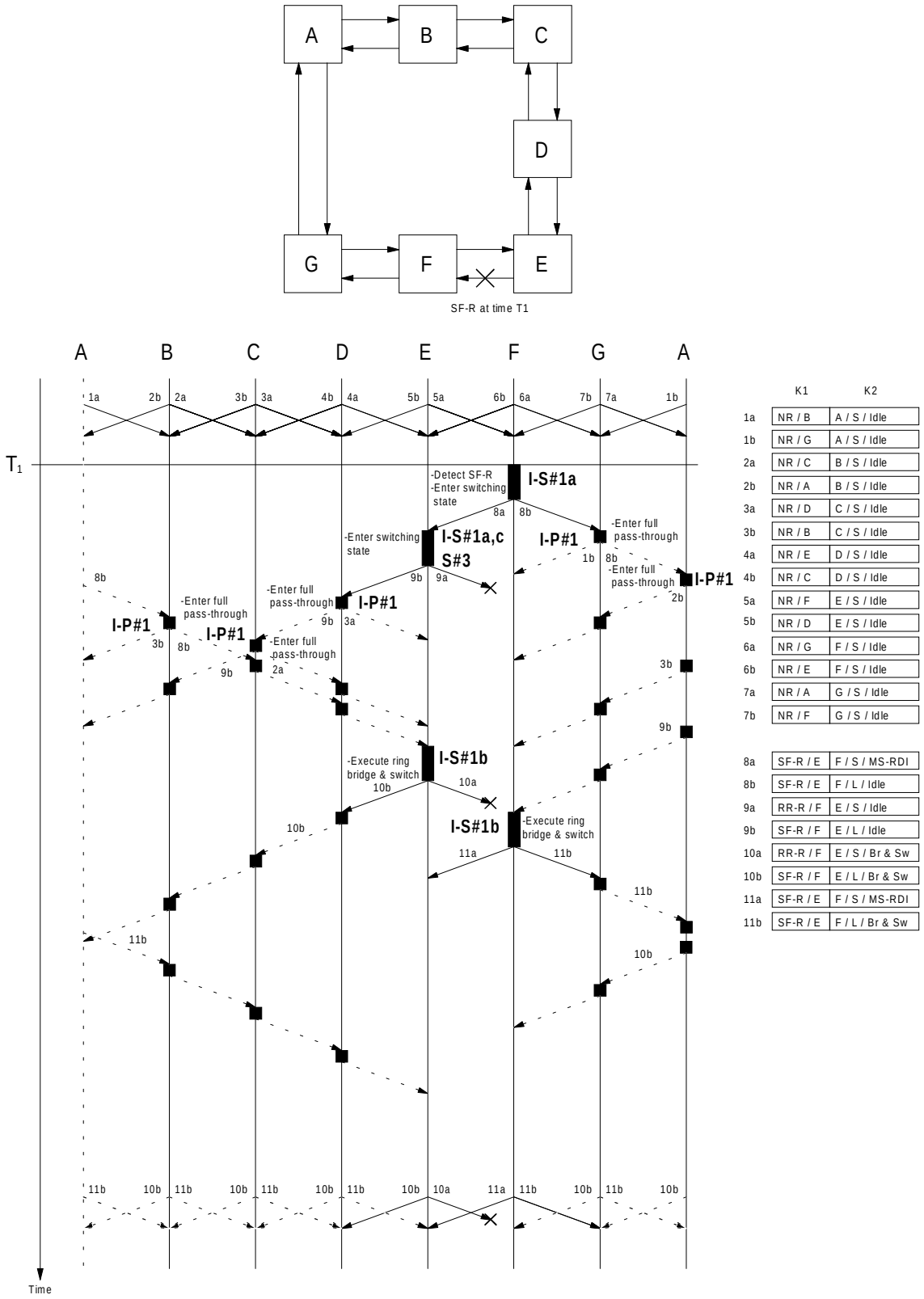


Figure B.1a: Example of unidirectional SF-R

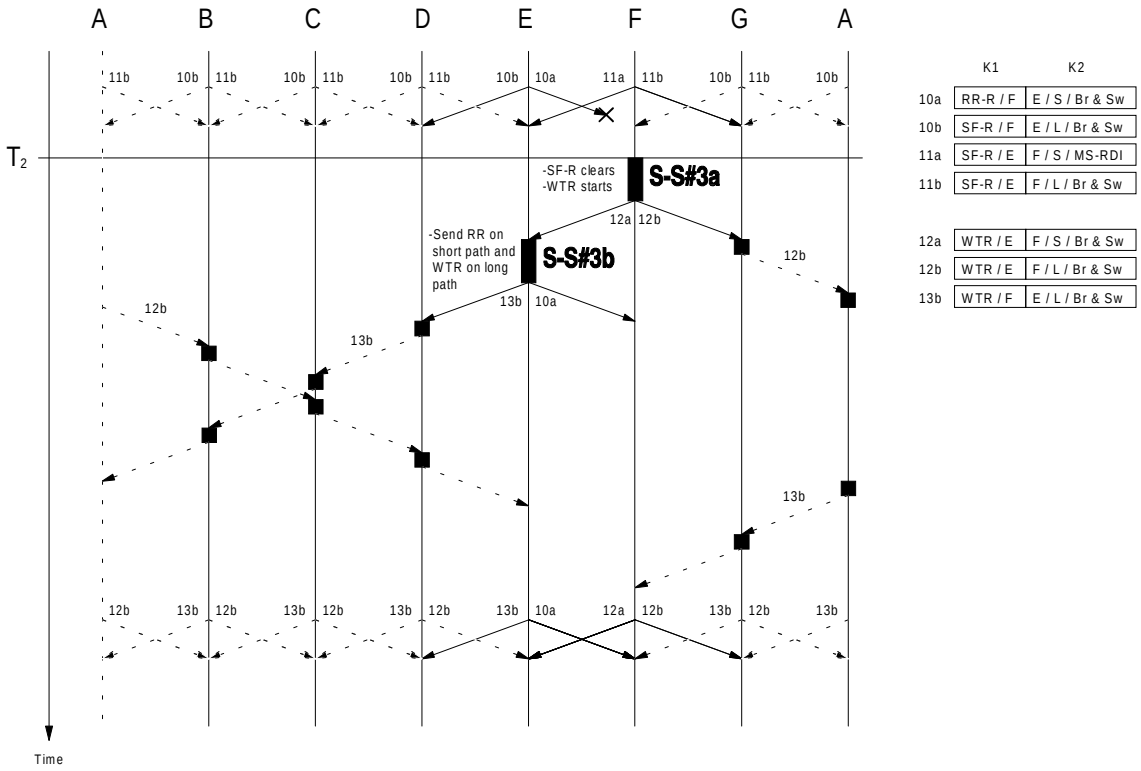


Figure B.1b: Example of unidirectional SF-R (continued)

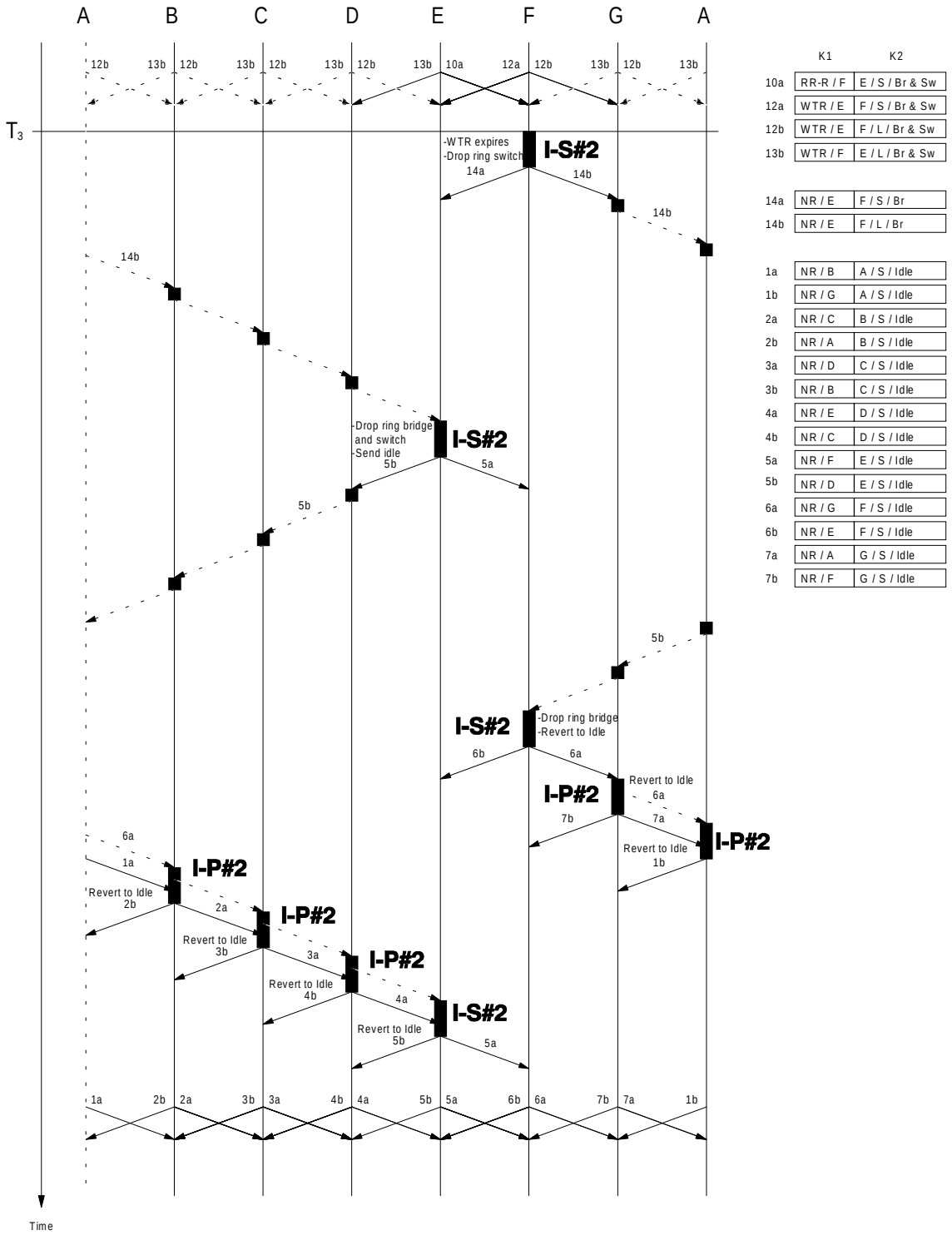


Figure B.1c: Example of unidirectional SF-R (concluded)

B.2 Bi-directional signal fail (ring)

This example covers the case of a bi-directional SF condition.

See figure B.2a.

The initial state of the ring is the idle state.

At time T1, Nodes E and F detect an SF condition on their working and protection channels. They become switching nodes (Rule I-S #1a) 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.

See figure B.2b.

At time T2 when the SF-R condition clears, the K-byte values that nodes E and F receive indicate to both E and F that they are Head Ends of a unidirectional SF condition on the span, which pre-empts WTR. For this condition, the SF-R priority should 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.

See figure B.3c.

At time T3, the WTR interval expires. 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.

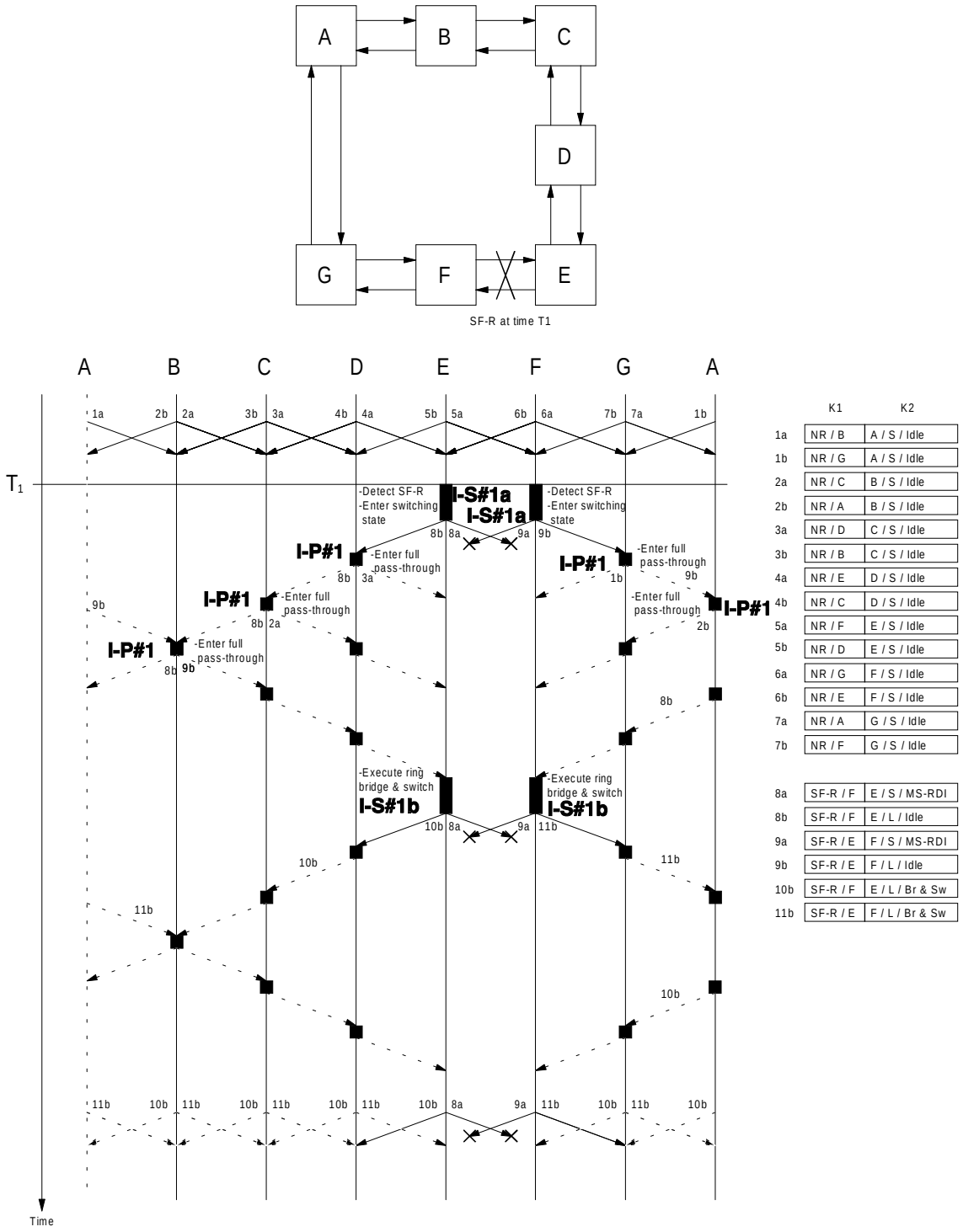


Figure B.2a: Example of bi-directional SF-R (continued)

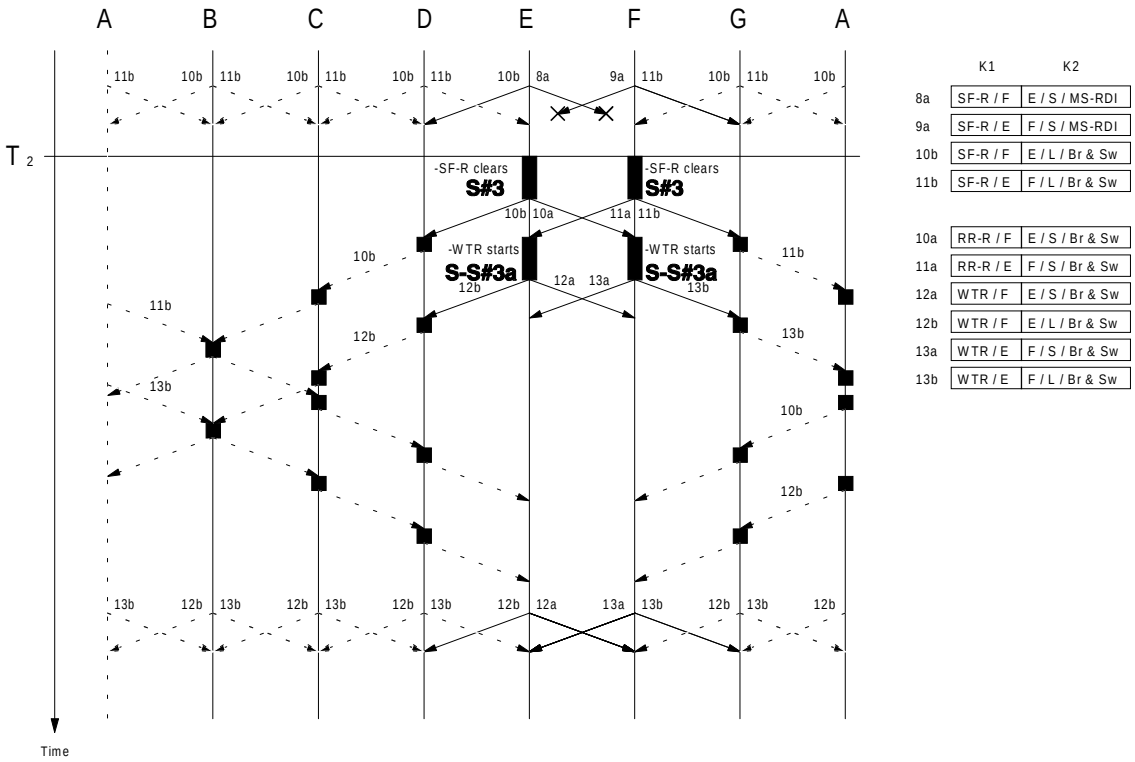


Figure B.2b: Example of bi-directional SF-R (continued)

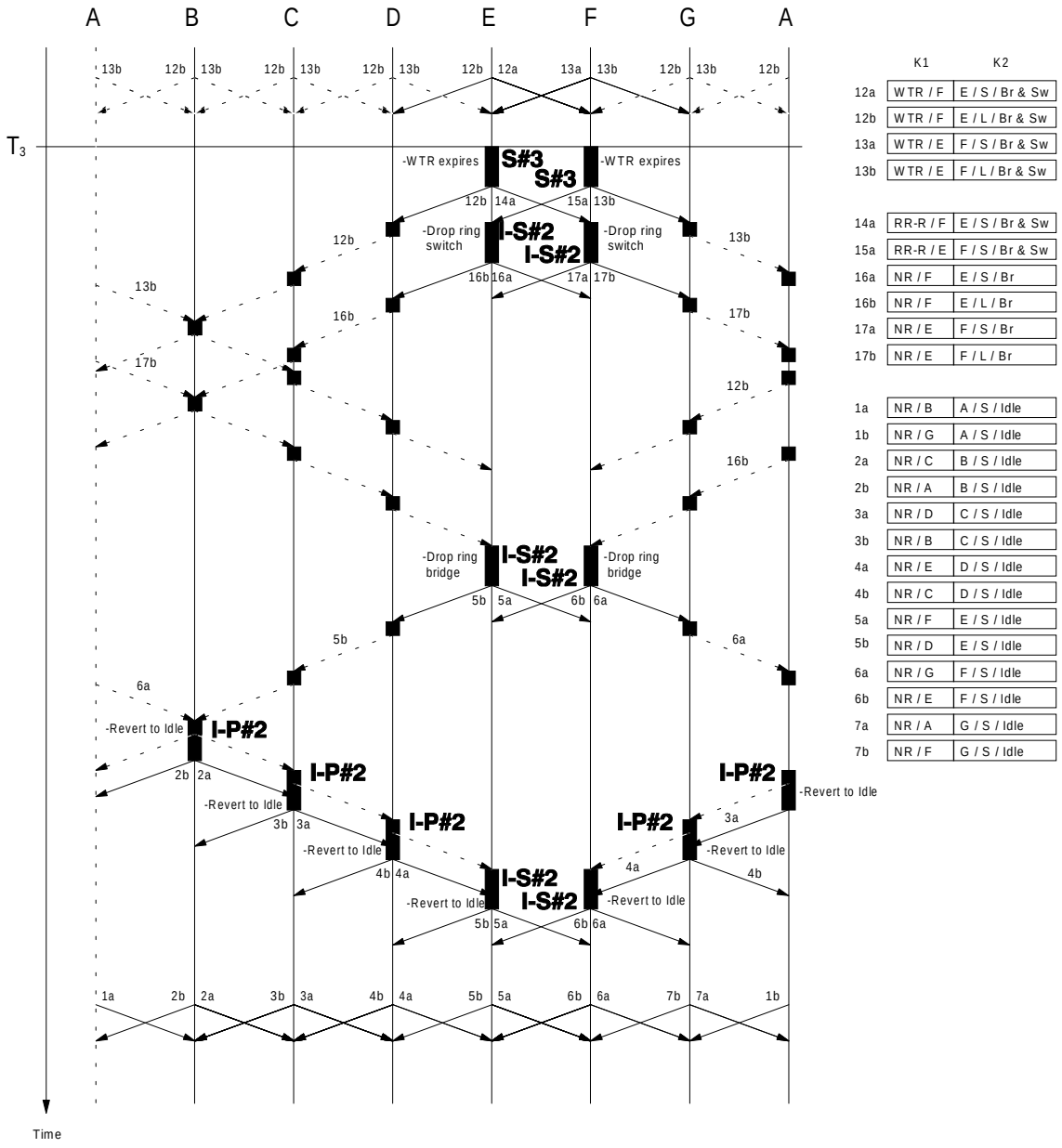


Figure B.2c: Example of bi-directional SF-R (concluded)

B.3 Unidirectional signal degrade (ring)

In this example, a ring switch is executed and cleared for a ring SD condition.

See figure B.3.

The initial state of the ring is the idle state.

At time T1, node F detects a ring SD condition. It becomes a switching node (Rule I-S #1a) 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 acknowledgement 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 acknowledgement from Node F, completes the switch.

Signalling reaches steady-state.

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

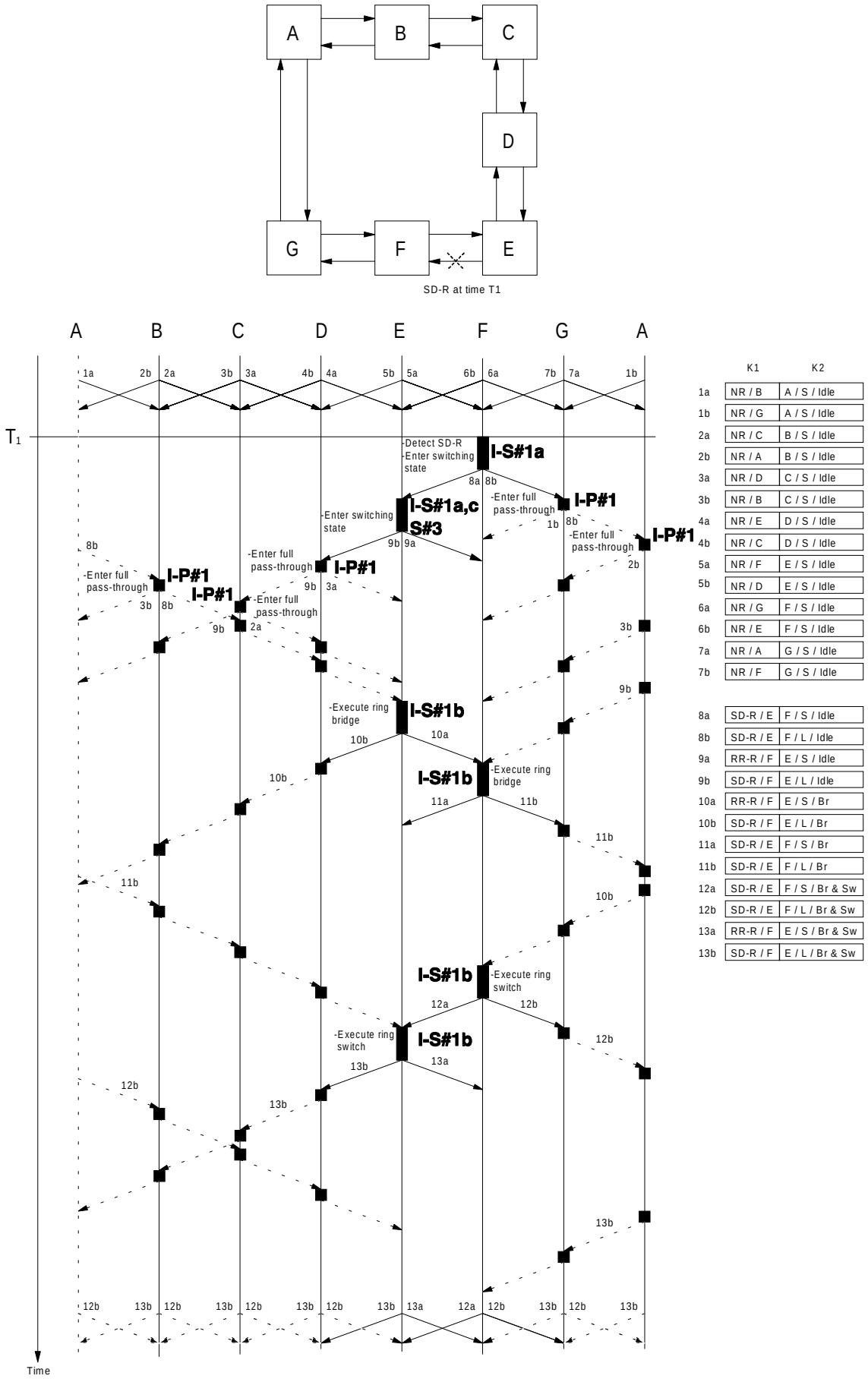


Figure B.3: Example of unidirectional SD-R

B.4 Detection and clearing of a unidirectional SF-R in presence of another unidirectional SF-R on a non-adjacent span

See figure B.4.

This example covers the case of a unidirectional signal fail - ring coexisting with another unidirectional signal fail - ring that had previously existed on a non-adjacent span.

The initial state of the ring is the idle state. At time T1, Node F detects an SF condition on its working and protection channels. The signalling proceeds in a manner as shown in figure B.1a (at time T1 in the figure). The signalling reaches steady state.

At time T2, Node C detects an SF condition on its working and protection channels. Node C becomes a switching node (Rule S-P #2, 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 #2, point 3). Node B also squelches traffic if necessary, executes a ring bridge and switch, and sources ring bridge requests in both directions (Rule 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.

At time T3, 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 #1a). This permits the short path ring Reverse Request signal from Node B to reach Node E. Node E still considers this to be a valid ring bridge request, so Node E retains its ring bridge and switch (Rule S #5 note). Node B, upon receiving both ring bridge requests that are not destined to it, drops its bridge and switch and enters full pass-through (Rule S-P #1b). Signalling reaches steady state.

At time T4 (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 B.1b and B.1c.

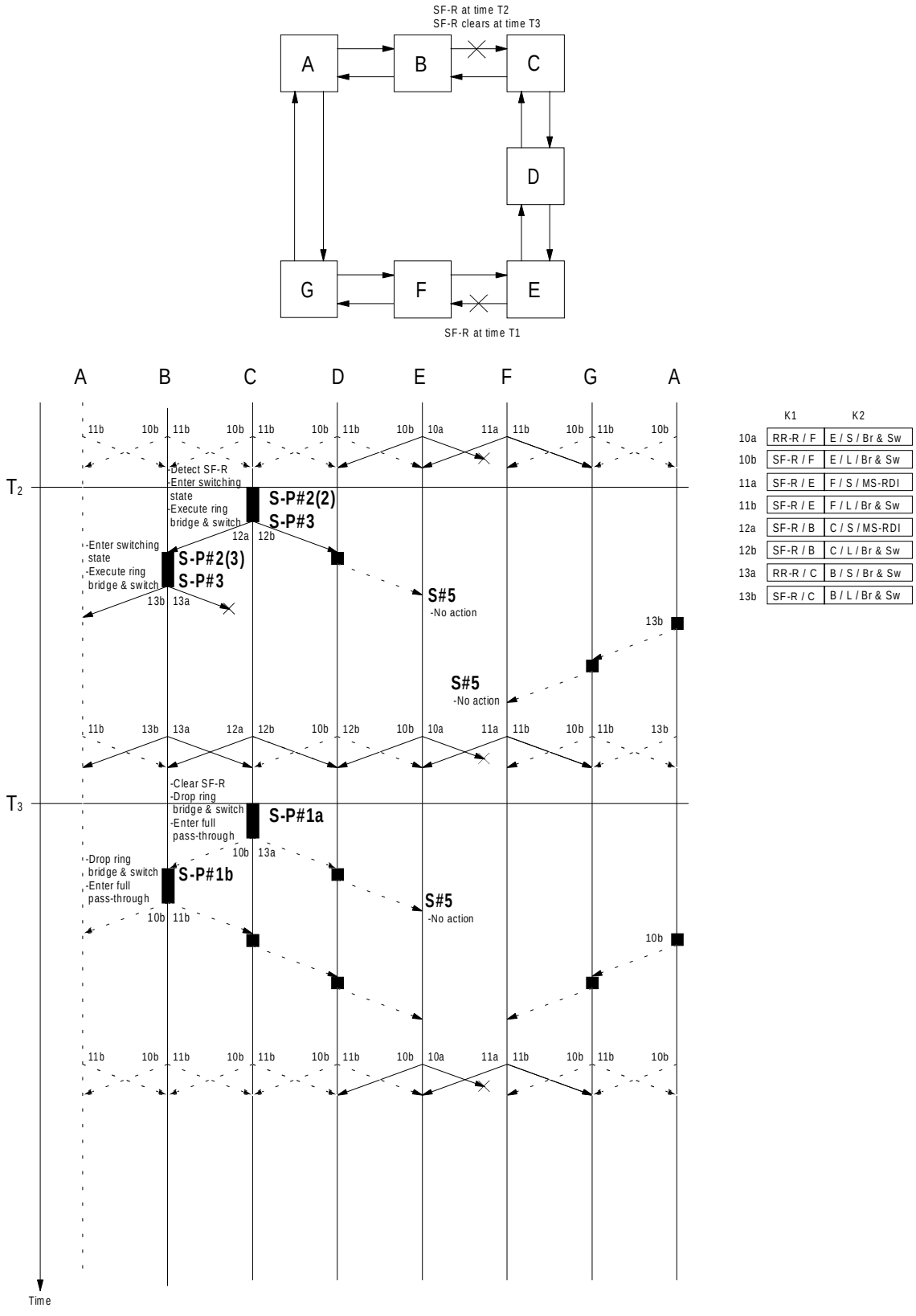


Figure B.4: Example of detection and clearing of a unidirectional SF-R in presence of another unidirectional SF-R on non adjacent span

B.5 Unidirectional SF-R pre-empting a unidirectional SD-R on a non-adjacent span

See figure B.5.

This example covers the case of a unidirectional signal fail - ring pre-empting a unidirectional signal degrade - ring that had previously existed on a non-adjacent span.

The initial state of the ring is the idle state. At time T1, Node F detects an SD-R condition on its working and protection channels. The signalling proceeds in a manner as shown in figure B.3 (at time T1). The signalling reaches steady state.

At time T2, Node C detects an SF-R condition on its working and protection channels. Node C becomes a switching node (Rule S-P #2, point 2), squelches traffic if necessary and sources ring bridge requests in both directions (S #1). Node B, upon seeing the bridge request from Node C, becomes a switching node (Rule S-P #2, point 3). Node B also squelches traffic if necessary and sources ring bridge requests in both directions (S#3). When the SF-R request from node C reaches node E, node E drops ring bridge and switch and enter full pass through (Rule S-P#1a). When the SF-R request from node C reaches node F, node F drops ring bridge and switch and enter full pass through (Rule S-P#1b). Finally, node B and C execute bridge and switch as in figure B.1a. The signalling reaches steady state.

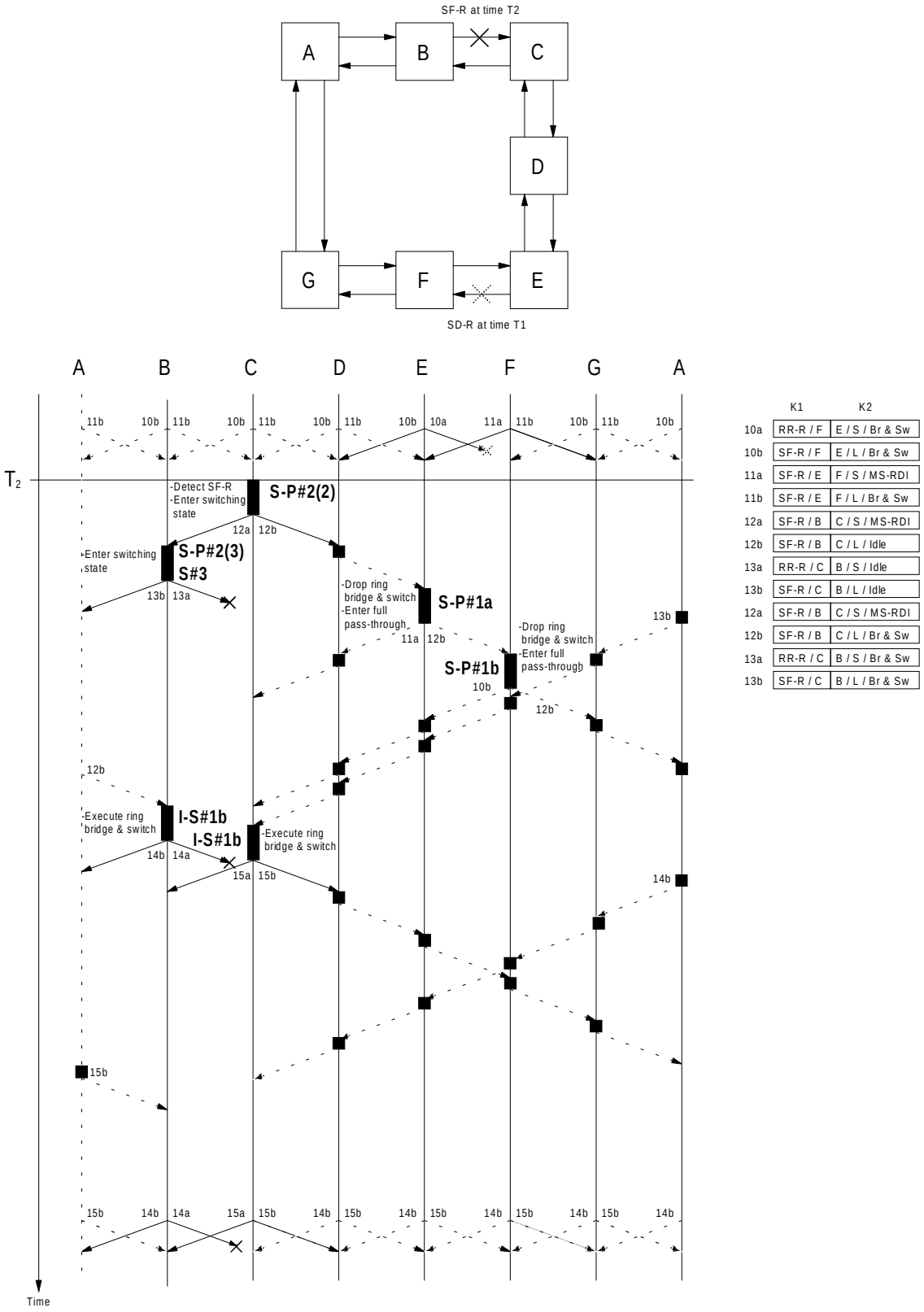


Figure B.5: Example of a unidirectional SF-R pre-empting a unidirectional SD-R on a non adjacent span

B.6 Unidirectional SD-R pre-empting a unidirectional MS-R on an adjacent span

See figure B.6.

This example covers the case of a unidirectional signal degrade - ring pre-empting a unidirectional manual switch - ring that had previously existed on an adjacent span.

The initial state of the ring is the idle state. At time T1, Node F receives a MS-R external command, to be executed with E. The signalling proceeds in a manner as shown in figure B.3 (at time T1 in the figure), with the exception that the present request is a MS-R The signalling reaches steady state.

At time T2, Node E detects an SD-R condition on its working and protection channels, coming from node D: it drop the ring bridge and switch and sources ring bridge requests in both directions (S-S #2). Node D, upon seeing the bridge request from Node C, becomes a switching node (Rule S-P #2, point 3) and sources ring bridge requests in both directions (S#3). When the SD-R request from node D reaches node F, node F drops ring bridge and switch and enter full pass through (Rule S-P#1b). Finally, node E and D execute bridge and switch as in figure B.3. The signalling reaches steady state.

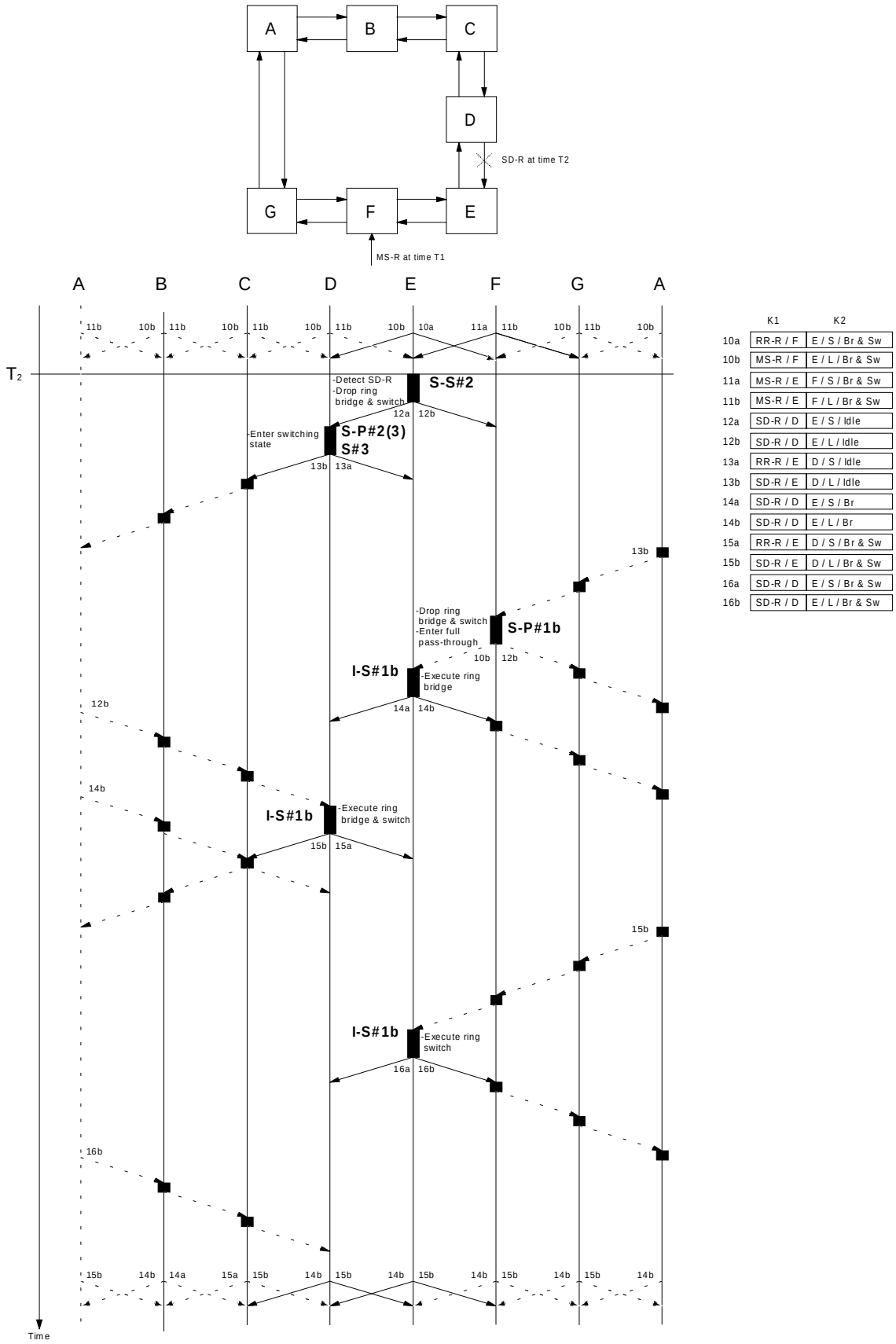


Figure B.6: Example of a unidirectional SD-R pre-empting a unidirectional MS-R on an adjacent span

Annex C (informative): Bibliography

The following documents were also used in the preparation of this ETS:

- ETR 085: "Transmission and Multiplexing (TM); Generic functional architecture of transport network".

- ETR 114: "Transmission and Multiplexing (TM); Functional architecture of Synchronous Digital Hierarchy (SDH) Transport networks".

- ETR 152: "Transmission and Multiplexing (TM); High bitrate Digital Subscriber Line (HDSL) transmission systems on metallic local lines; HDSL core specification and applications for 2 048 kbit/s based access digital sections including HDSL dual-duplex Carrierless Amplitude Phase Modulation (CAP) based system".

- Draft ETR 273: "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH) network protection schemes; Types and characteristics".

- Draft ETR 274: "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH) protection interworking; rings and other schemes".

- ETS 300 147 (1995): "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH) Multiplexing structure".

History

Document history			
April 1996	Public Enquiry	PE 105:	1996-04-08 to 1996-08-30
December 1996	Vote	V 116:	1996-12-09 to 1997-01-31