TS 101 010 V1.1.1 (1997-11)

Technical Specification

Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); Network protection schemes; Interworking: rings and other schemes

European Telecommunications Standards Institute

Reference
DTS/TM-03041 (9co00icr.PDF)

Keywords
SDH, rings, protection, interworking, APS, protocols

ETSI Secretariat

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

X.400
c= fr; a=atlas; p=etsi; s=secretariat

Internet
secretariat@etsi.fr
http://www.etsi.fr

Contents

Intellectual Property Rights 5
Foreword 5
1 Scope 6
2 Normative references 6
3 Abbreviations 6
4 Definitions and classifications 7
4.1 General definitions 7
4.2 Ring Definitions 9
4.3 Classification of network recovery schemes 9
4.4 Protection partitioning and layering 9
4.4.1 Introduction 9
4.4.1.1 Protection partitioning concept 10
4.4.1.2 Protection layering concept 10
4.4.2 Definition of protection layer 10
4.4.3 Protection interworking architectures 10
4.4.3.1 Intra-layer network protection architecture 11
4.4.3.2 Inter-layer network protection architecture 13
5 Protection interworking objectives 15
5.1 Traffic availability 15
5.2 Protection independence 16
5.3 Fault coverage 16
5.3.1 Defects related to signal loss 17
5.3.2 Defects related to signal degradation 17
5.3.3 Defects related to misprovisioning 17
5.4 Interconnecting subnetworks protected at different layers 17
5.5 Capability to interconnect networks using different protection schemes 18
5.6 Minimisation of traffic interruption 18
5.7 Operation modes 18
5.8 Capacity utilisation 18
6 Subnetwork interconnection architectures 22
6.1 Single node interconnecting architecture 22
6.2 Dual node interconnecting architectures 22
6.2.1 Mechanisms to implement dual node interconnecting architectures 22
6.2.1.1 Virtual ring interconnecting architecture 23
6.2.1.2 Drop and continue interconnecting 23
6.3 Application of interworking architectures on real network topologies 24
7 Interworking between similar protection schemes 26
7.1 MS SPRING 26
7.1.1 Two MS shared protection rings connected by one node 26
7.1.2 Two MS shared protection rings connected by two nodes 28
7.2 LO/HO trail protection 31
7.2.1 VC trail protected subnetworks interconnected by one node 31
7.2.2 Two VC trail protected subnetworks interconnected by two nodes 34
7.3 LO/HO subnetwork connection protection 37
7.3.1 SNC protected subnetworks interconnected by one node 37
7.3.2 Two SNC-P Subnetworks Interconnected by Two Nodes 41
8 Interworking between different protection schemes 47
8.1 Dual node interworking between MS-SPRING and SNC-P subnetworks 47
8.2 Single Node Interworking between MS-SPRING and SNC-P 49

9 Comparison of protection interconnection schemes 51

10 Network applications 52
10.1 Interconnecting ring subnetworks with 4/3/1 Digital Cross-Connects 52
10.2 Stacked ring configuration 53
10.3 Interworking of protection between networks belonging to different operators 54

11 Conclusions and recommendations 56

Annex A 58
A.1 Introduction 58
A.1.1 Protection independence 58
A.1.2 Routing 59
A.2 MS-SPRING to SNCP dual node drop and continue subnetwork interconnection 60
A.2.1 Normal conditions 60
A.2.2 Failure in MS SPRing Primary interconnection node I1 61
A.2.3 Failure in MS SPRing Primary interconnection node I1. Node failure in SNCP subnetwork 62
A.2.4 Failure in MS SPRing Primary interconnection node I1. Cable cut in SNCP subnetwork 63
A.2.5 Failure in one interconnection link 64
A.3 MS-SPRING to MS-SPRING dual node drop and continue subnetwork interconnection 65
A.3.1 Normal conditions 65
A.3.2 Failure in MS SPRing 1 Primary interconnection node I1 66
A.3.3 Failure in MS SPRing 1 Primary interconnection node I1. Node failure in MS SPRing 2 67
A.3.4 Failure in MS SPRing 1 Primary interconnection node I1. Cable cut in MS SPRing 2 68
A.3.5 Failure in one interconnection link 69
A.4 SNCP to SNCP dual node drop and continue subnetwork interconnection 70
A.4.1 Normal conditions 70
A.4.2 Failure in SNCP subnetwork 1 interconnection node I1 71
A.4.3 Failure in SNCP subnetwork 1 interconnection node I1. Node failure in SNCP subnetwork 2 72
A.4.4 Failure in SNCP subnetwork 1 interconnection node I1. Cable cut in SNCP subnetwork 2 73
A.4.5 Failure in one interconnection link. 74

Annex B (informative): Bibliography 75

History 76

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETR 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr).

Pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETR 314 (or the updates on http://www.etsi.fr/ipr) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Transmission and Multiplexing (TM) in order to give guidance to network operators and equipment manufacturers on the Synchronous Digital Hierarchy (SDH) network protection interworking, based on rings and other schemes.

The present document is one of a family of related TSs and European Telecommunications Standards (ETSs) covering the various aspects of SDH protection:

TS 101 009: "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); Network protection schemes; Types and characteristics".

TS 101 010: "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); Network protection schemes; 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".

1 Scope

The present document describes the criteria, principles, objectives, requirements and architectures of protection interworking between multiplex section shared protected rings, multiplex section linear protection, and Higher Order/lower Order (HO/LO) Virtual Container (VC) trail and subnetwork connection protection schemes. The SDH protection interworking scenarios between the same and different protection schemes are described.

The network objectives, architectures, functional modelling and operations of the various SDH protection schemes are described in TS 101 009 [1]. The protection switching initiation criteria and the Automatic Protection Switching (APS) protocols of the various SDH protection schemes are specified in ETS 300 746 [2].

2 Normative references

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] TS 101 009 V1.1.1: "Transmission and Multiplexing (TM);Synchronous Digital Hierarchy (SDH); Network protection schemes; Types and characteristics".

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

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

[4] ITU-T Recommendation G.707: "Network Node Interface for the Synchronous Digital Hierarchy (SDH)".

[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".

[7] ITU-T Recommendation G.842: "Interworking of SDH Network Protection Architectures".

3 Abbreviations

For the purposes of the present document, the following definitions apply:

ADM	Add Drop Multiplex
AIS	Alarm Indication Signal
APS	Automatic Protection Switching
AU	Administrative Unit
AUG	Administrative Unit Group
AU-n	Administrative Unit (level) n

BER	Bit Error Ratio
DXC	Digital cross-Connect
HO	Higher Order
LO	Lower Order
LOF	Loss Of Frame
LOS	Loss Of Signal
MS	Multiplex Section
MS-SPRING	Multiplex Section Shared Protection RINGs
NA	Not Applicable
NC-P / I	Network Connection Protection / Inherent monitoring
NC-P / N	Network Connection Protection / Non-intrusive monitoring
NE	Network Element
POH	Path OverHead
RDI	Remote Defect Indication
RS	Regenerator Section
SD	Signal Degrade
SDH	Synchronous Digital Hierarchy
SF	Signal Fail
SNC	Sub-Network Connection
SNC-P	Sub-Network Connection-Protection
SNC-P / I	Sub-Network Connection Protection / Inherent monitoring
SNC-P / N	Sub-Network Connection Protection / Non-intrusive monitoring
STM	Synchronous Transport Module
STM-N	Synchronous Transport Module (level) N
TIM	Trace Identifier Mismatch
TTI	Trail Trace Identifier
TU	Tributary Unit
TUG	Tributary Unit Group
UNEQ	UNEQuipped indication
VC	Virtual Container
VC-n	Virtual Container (level) n
WTR	Wait To Restore

4 Definitions and classifications

4.1 General definitions

For the purposes of the present document, the following definitions apply:

Administrative Unit (AU): See ITU-T Recommendation G.707 [4].

Administrative Unit Group (AUG): See ITU-T Recommendation G.707 [4].

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

Bi-directional operation: Synonym for dual ended operation.

Bit Interleaved Parity (BIP): See ITU-T Recommendation G.707 [4].

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

dedicated protection: See ITU-T Recommendation G.803 [3].

disjointed routes: These are routes which use different fibre ducts and through different nodes to avoid single points of failure.

drop and continue: A function within a ring node where traffic is both extracted from the working channels on the ring (drop), and transmitted onwards on the ring (continue).

dual ended operation: See TS 101 009 V1.1.1 [1].

NOTE: The dual ended operation is synonymous of bi-directional switching, the same can be said about single ended operation and unidirectional switching.

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

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

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

Multiplex Section (MS): See ITU-T Recommendation G.803 [3].

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

Multiplex Section RDI (MS-RDI): See ITU-T Recommendation G.707 [4].

Network Connection Protection (NC-P): Network connection protection is the largest subnetwork connection protection that can be established between two trail terminating equipment.

Path Overhead (POH): See ITU-T Recommendation G.707 [4].

primary interconnection node: It is an interconnection node in a dual node interconnection MS-SPRING architecture using drop and continue containing the switch and drop and continue function.

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 [3].

restoration: See ITU-T Recommendation G.803 [3].

secondary interconnection node: It is an interconnection node in a dual node interconnection MS-SPRING architecture using drop and continue containing only aggregate to tributary connection functions.

secondary traffic See extra traffic.

Section Overhead (SOH): See ITU-T Recommendation G.707 [4].

shared protection: See ITU-T Recommendation G.803 [3].

single ended operation: See TS 101 009/V1.1.1 [1].

single point failure: Failure [ai1][ai2] located at a single physical point in a ring: The failure may affect one or more fibres. A single point failure may be detected by any number of nodes.

sub-network connection: See ITU-T Recommendation G.803 [3].

sub-network connection protection: See ITU-T Recommendation G.803 [3].

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

tail-end: The node that requests the bridge.

trail: See ITU-T Recommendation G.803 [3].

trail protection: See ITU-T Recommendation G.803 [3].

Tributary Unit (TU): See ITU-T Recommendation G.707 [4].

Tributary Unit Group (TUG): See ITU-T Recommendation G.707 [4].

Uni-directional operation: Synonym for single ended operation.

Virtual Container (VC): See ITU-T Recommendation G.707 [4].

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

For the purposes of the present document, the following definitions apply:

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.

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 between any pair of nodes of the ring is the same.

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

4.3 Classification of network recovery schemes

This subclause describes the architectural features of the main strategies which may be used to enhance the availability of a transport network. This enhancement is achieved by the replacement of failed or degraded transport entities. The replacement is normally initiated by the detection of a defect, performance degradation or an external management request.

Protection: This makes use of pre-assigned capacity between the nodes. The simplest architecture has one dedicated protection entity for each working entity (1+1). The most complex architecture has m protection entities shared amongst n working entities (m:n).

Restoration: This makes use of any capacity available between nodes. In general the algorithms used for restoration will involve re-routing. When restoration is used some percentage of the transport network capacity will be reserved for re-routing working traffic.

4.4 Protection partitioning and layering

4.4.1 Introduction

A telecommunication network could be implemented using many protection schemes simultaneously to achieve the traffic availability and speed of restoration objectives required for each kind of service supported.

A network having to satisfy such a variety of traffic survivability requirements could be modelled using the layering and partitioning principles.

Hence, the protected transport network can be decomposed into a number of independent transport network layers with a client/server association between adjacent layers. Thus the concepts of partitioning and layering are orthogonal as shown in figure 3.5 of ITU-T Recommendation G.803 [3].

4.4.1.1 Protection partitioning concept

The partitioning concept is important as a framework for defining:

a) significant administrative boundaries between network operators jointly providing end-to-end trail or network connection within a single layer with the objective of confining the protection actions to the network where the failure occurred;

b) domain boundaries within the layer network of a single operator with a view to increase the overall network resilience.

4.4.1.2 Protection layering concept

The layering concept of the transport network is based on the following assumptions:

a) each protection sublayer can be classified into similar functions;

b) it is simpler to design and operate each protection sublayer separately than it is to design and operate the entire transport network as a single entity;

c) a protection sublayer provides autonomous capabilities such as automatic protection switching, traffic restoration against malfunctions or failures, human errors and management misoperations. Each layer is able to have its own operations and maintenance capability such as protection switching and automatic failure recovery against malfunctions or failures and mis-operations due to human errors.

Unlike the transport layers, the protection sublayers tend to interact with each other, hence a protection control strategy may be required to optimise the overall protected network behaviour.

4.4.2 Definition of protection layer

Subnetwork connection protection and trail APS with diverse routing, self healing rings and service re-routing using reconfigurable DXCs are few examples of survivable architectures for the telecommunication network. Each one of these architectures can be modelled as a protection layer as they fit in the definition of the protection layering concept.

The following mechanisms could be modelled as protection layers:

a) the replacement of a protected trail with a protecting trail if the former fails or its performance falls below the required level;

b) the replacement of a protected subnetwork connection with a protecting subnetwork connection if the former fails or its performance falls below the required level;

c) the replacement of a protected trail with a protecting trail if the former fails or its performance falls below the required level by means of a re-routing algorithm.

4.4.3 Protection interworking architectures

The basic inter-working architectures and sub-architectures are:

Intra-layer:

- single;
- chained;
- nested.

Inter-layer:

- nested;
- chained;
- hybrid.

4.4.3.1 Intra-layer network protection architecture

Definition

The intra-layer network protection architecture protects traffic by using one or more protection mechanisms. These are all resident in the same layer of the layered protected network.

From the above definition, three types of sub-architectures are identified:

Single intra-layer network protection architecture.

The single intra-layer network architecture protects traffic by using an end to end protection mechanism. Figures 1a and 1b illustrate the definition, where the flow indicates the service protected and the boxes represent the protection mechanisms in terms of pure architectures.

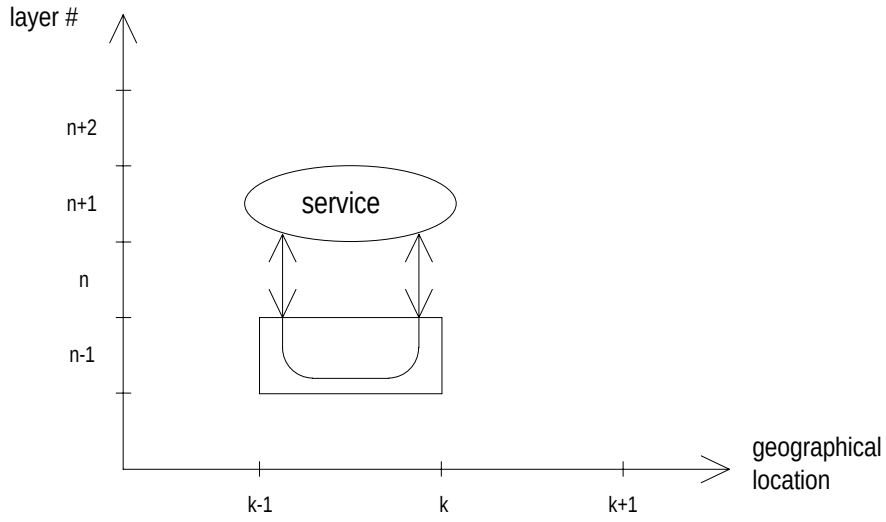

Figure 1a: Single intra-layer network protection architecture

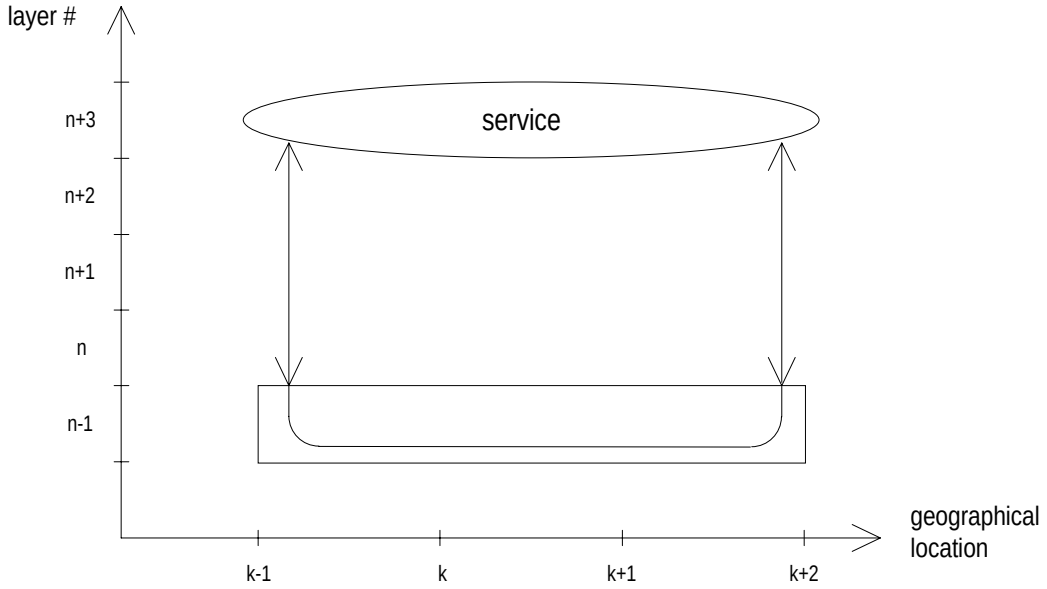

Figure 1b: Single intra-layer network protection architecture

Examples of the single intra-layer network protection architecture could be:

- MS-SPRINGs with ADMs;
- 1+1 MS protected systems;
- SNC-P rings;
- mesh of 4/4 DXCs with restoration;
- mesh of 4/3/1 DXCs.

Chained intra-layer network protection architecture.

The chained intra-layer network architecture protects traffic by using more than one independently protected sub-networks. Figures 2a and 2b illustrate a possible implementation of the definition.

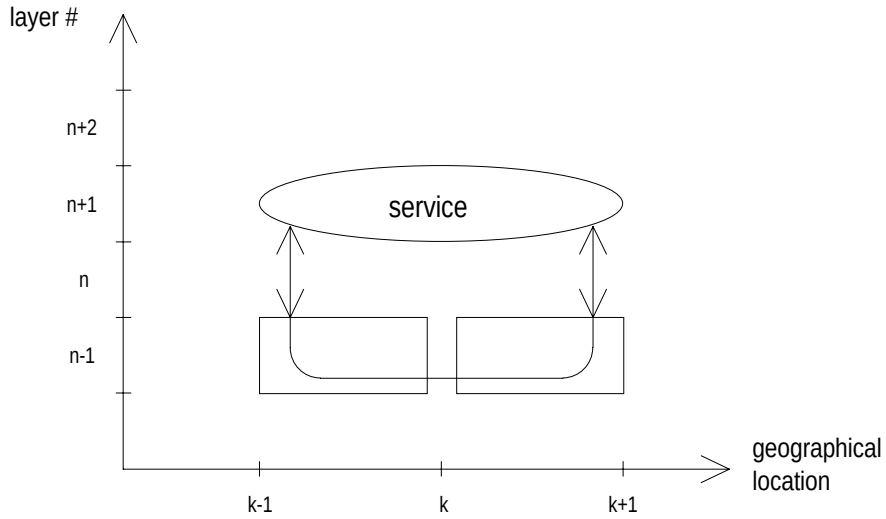

Figure 2a: Chained intra-layer network protection architecture

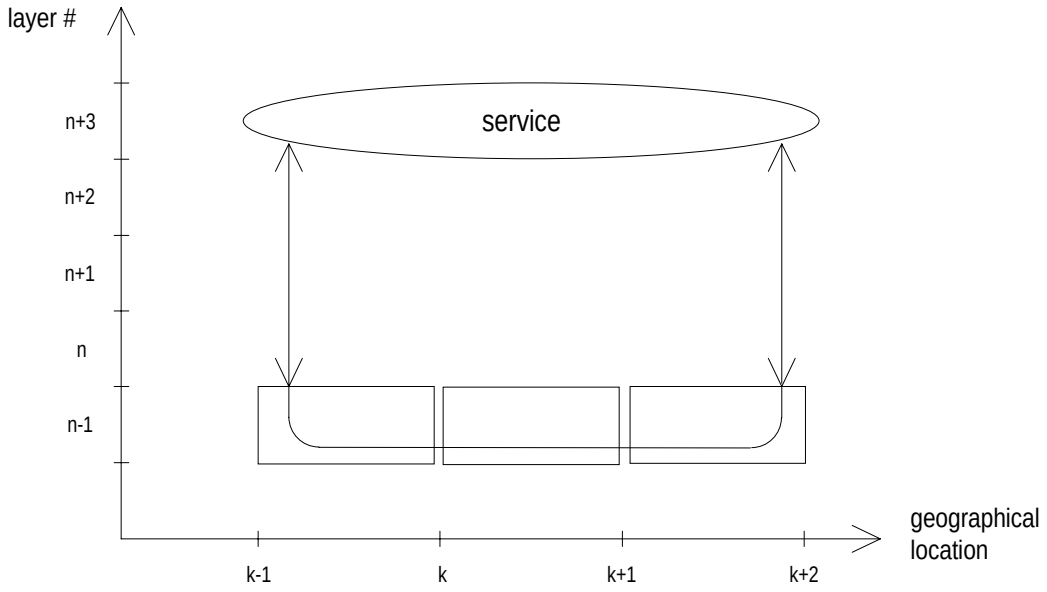

Figure 2b: Chained intra-layer network protection architecture

Examples of the chained intra-layer network protection architecture could be:

- interconnected LO-VC SNC-P rings;
- interconnected HO-VC SNC-P rings;
- MS-SPRINGs with ADMs interconnected using 1+1 MS protected systems;
- 1+1 MS protected chained systems;
- chained 1+1 protected systems.

Nested intra-layer network protection architecture.

The nested inter-layer network architecture protects traffic by nesting more than one protection mechanism in one layer. This means that the service is concurrently protected by all the available protection mechanisms. Figure 3 illustrates a possible implementation of the definition.

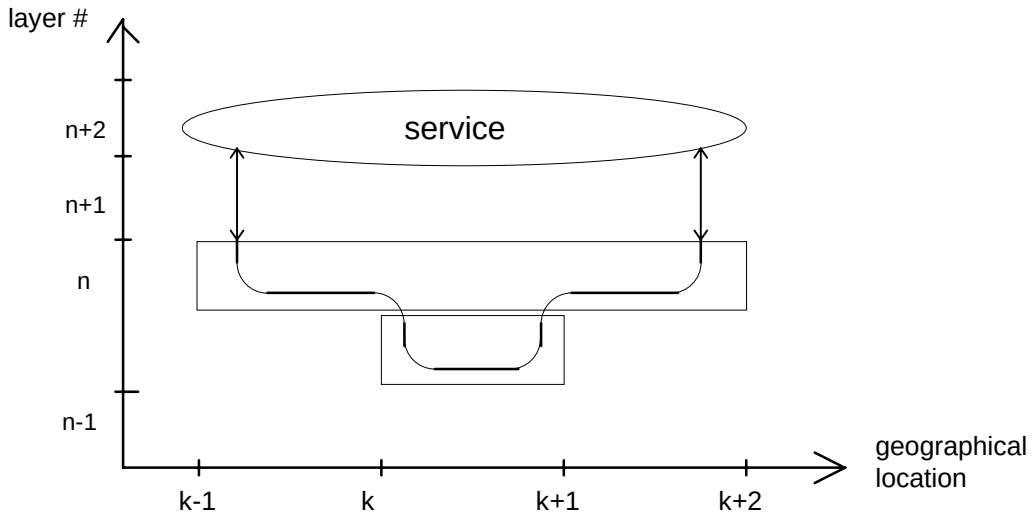

Figure 3: Nested intra-layer network protection architecture

Examples of the nested intra-layer network protection architecture could be:

- mesh of 4/4 DXCs with restoration and SNC-P protection.

4.4.3.2 Inter-layer network protection architecture

Definition

In an inter-layer network protection architecture, the traffic is protected by more than one protection mechanisms. These are located in more than one layer of the layered protected network. From the above definition, three types of sub-architectures are identified.

Nested inter-layer network protection architecture.

The nested inter-layer network architecture protects traffic by nesting more than one protection mechanism each one at different layers. This means that the service is concurrently protected by all the available protection mechanisms. Figure 4 illustrates a possible implementation of the definition.

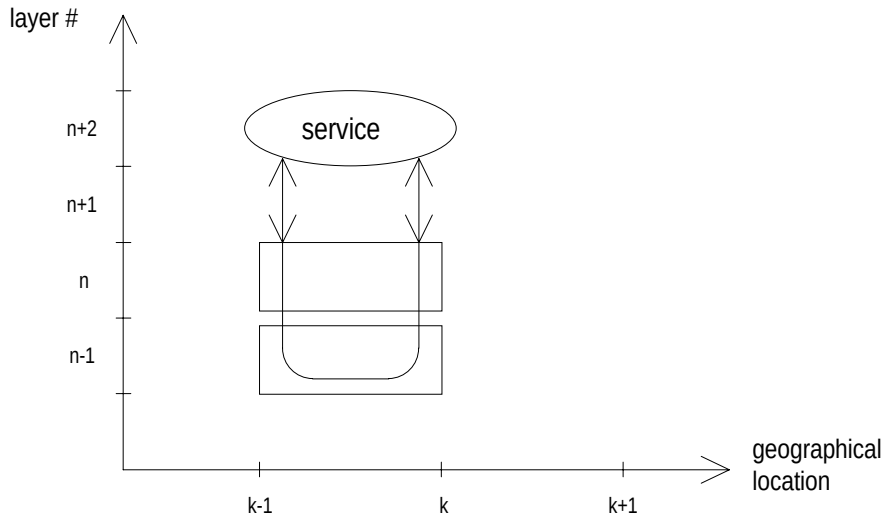

Figure 4: Nested inter-layer network protection architecture

Examples of the nested inter-layer network protection architecture could be:

- MS-SPRINGs and HO/LO VC trail protection;
- 1+1 MS protected Systems and HO/LO NC-P/N protection;
- chained 1+1 MS protected Systems and HO/LO NC-P/N protection.

Chained inter-layer network protection architecture.

The chained inter-layer network architecture protects traffic using more than one independently protected sub-networks in different layers. Figure 5 illustrate a possible implementation of the definition.

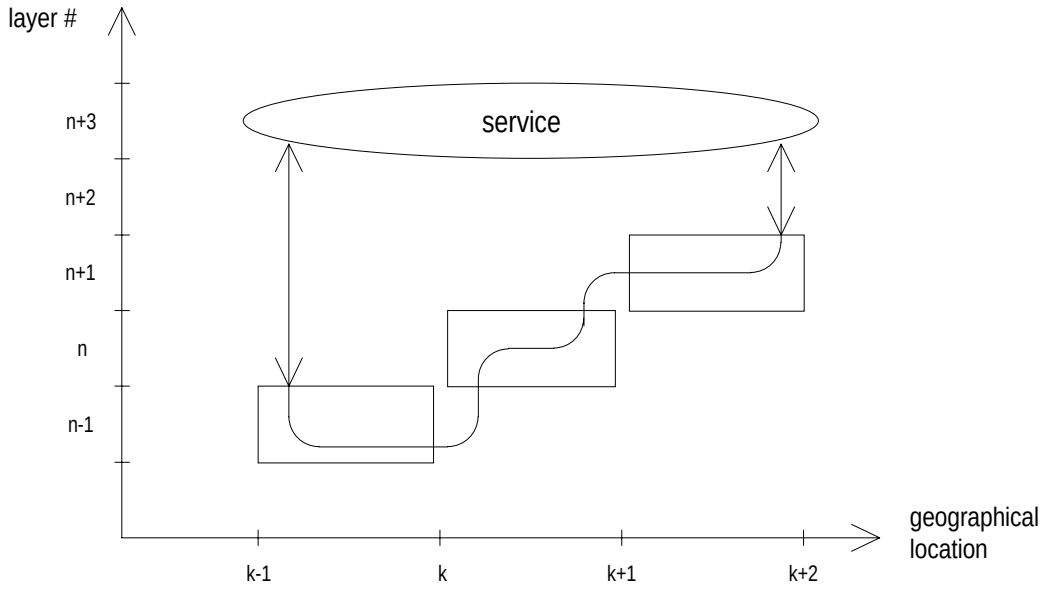

Figure 5: Chained inter-layer network protection architecture

Examples of the chained inter-layer network protection architecture could be:

- interconnected MS-SPRINGs using drop and continue.

Hybrid inter-layer network protection architecture.

The hybrid inter-layer network architecture is a mixture of the nested inter-layer, chained inter-layer and chained intra-layer architectures. This architecture protects traffic by using more than one protected sub-networks in one or more layers concurrently with an end to end protection mechanism. Figure 6 illustrate a possible implementation of the definition.

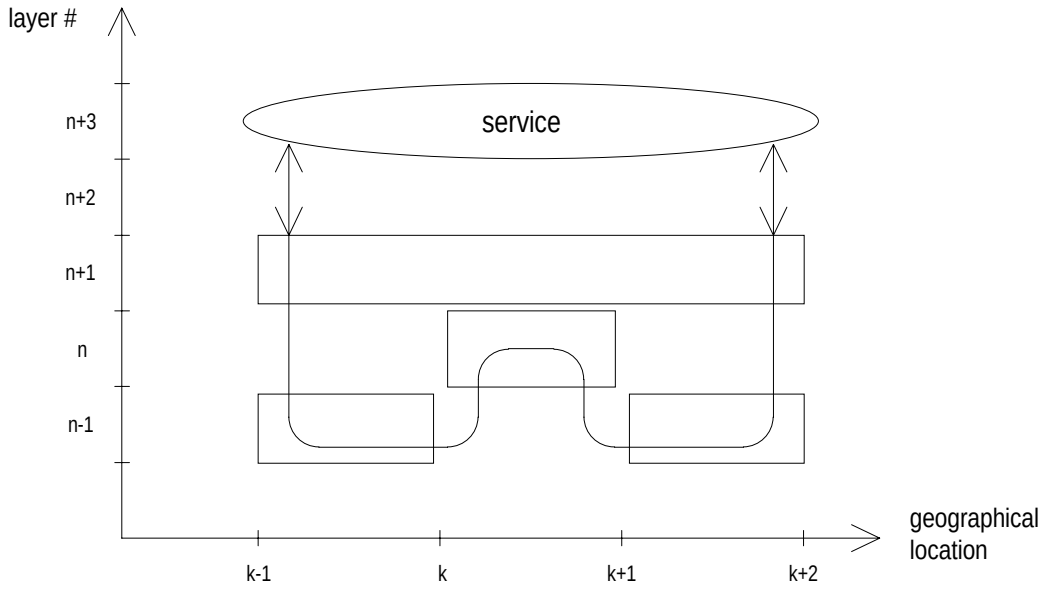

Figure 6: Hybrid inter-layer network protection architecture

Examples of the hybrid inter-layer network protection architecture could be:

- mesh of 4/4 DXCs with restoration connected with 1+1 protected line systems;
- NC-N protection over interconnected MS-SPRINGs using drop and continue.

5 Protection interworking objectives

The following objectives apply to networks where various SDH protection schemes interwork.

5.1 Traffic availability

In general availability is a measure of the degree to which an item is in an operable state when called upon to perform.

The traffic availability in the protection inter-working realm addresses the availability of traffic in interconnected sub-networks which could be supporting the same or different protection mechanisms. Three levels of availability can be defined:

Level 1: The method used to interconnect subnetworks allows inter sub-network traffic to be subject to a lesser level of robustness when compared with traffic that stays on a single sub-network (intra sub-network traffic). This implies that in the event of a single failure the protection inter-working scheme may not be able to restore all the inter sub-network traffic whereas all intra sub-network traffic is restored.

Level 2: The method used to interconnect subnetworks ensures that inter sub-network traffic is subject to the same level of robustness when compared with traffic that stays on a single sub-network (intra sub-network traffic). This implies that in the event of a single failure the protection inter-working scheme can restore all inter and intra sub-network traffic.

Level 3: In addition to level 2 properties the method of interconnecting sub-networks is able to survive a scenario in which two or more sub-networks are each experiencing a single independent failure at the same time without affecting the robustness of either inter or intra sub-network traffic.

5.2 Protection independence

The objective of protection independence is to prevent failures in one subnetwork influencing switching operations in all the interconnected subnetworks that carry the end to end trail or network connection.

The effect of protection independence is desirable in cases of multi-operator interworking. From an administrative and maintenance point of view, protection independence avoid confusing maintenance crews as the switching actions take place only in the administered domain where the failure actually occurred.

Dual node interconnection architectures have been designed to increase the network survivability and optionally provide protection independence for the interconnected subnetworks.

In dual node interconnected architectures based on drop and continue, the following mechanisms need to be used together to improve the degree of protection independence:

- placing of the selectors to some predefined default positions;
- hold-off time;
- revertive mode of operation.

Ignoring for the time being any differences in delays on the working and spare subnetwork connections, by positioning the selectors as illustrated in the specific cases addressed in clauses 7 and 8, a failure in a subnetwork causes a switch action only in the selectors belonging to the domain where the failure occurred. This is because they are the only ones to receive traffic on one side and a server signal fail on the other side. All the other selectors in other interconnected subnetworks should receive server signal fail signals on both their inputs, preventing any switching action.

As the positioning of the selectors is so important, the use of revertive mode of operation is crucial to keep their normal positioning independently of the failure history of the network.

Considering now the differences in transmission delays between working and spare subnetwork connections, to avoid undesirable switching actions across the subnetworks, it is required to set the hold off time in the switches. This allows for persistence checking, thus protecting after the switches' inputs are stable.

Single node interconnecting architectures would require only the provisioning of hold off time to improve the degree of protection independence.

In general, the implementation of protection independence in subnetworks may introduce some trade-offs with other objectives listed in this subclause.

The implementation of protection independence may have an impact on the switching time due to the inclusion of the hold off time attribute in the selectors.

Specifically for drop and continue architectures, protection independence may have an impact on the traffic quality of service, as the revertive mode of operation causes two traffic hits per failure in the network.

5.3 Fault coverage

The fault coverage objective is for a protection scheme to protect against several types of faults in the network.

Traffic outages can be classified into three groups:

- those causing signal loss, such as fibre cuts;
- those causing signal degradation, such as radio link fading and optical interface degradation;
- those causing misconnections and misprovision due to software failures, management mis-operations, procedural errors.

NOTE: The fault coverage objective is generally applicable to protection, i.e. it is not restricted to protection interworking only.

The faults translate into the defect listed in the following subclauses.

5.3.1 Defects related to signal loss

MS-AIS

LOS

LOF

AU/TU AIS

AU/TU LOP

Hence, protection mechanisms that use the above listed defects as protection switching criteria are eligible to increase traffic availability of the network against the most common types of network failures. MS trail protection and SNC-P/ I are examples of such protection mechanisms.

5.3.2 Defects related to signal degradation

MS - SD

S4 / S3 / S12 SD

Protection mechanisms that use the above listed defects as protection switching criteria are suitable to increase the traffic performance against network link degradation. MS trail protection and SNC-P/N are examples of such protection mechanisms.

5.3.3 Defects related to misprovisioning

RS / S4 / S3 / S12 TIM

S4 / S3 / S12 UNEQ

For these types of traffic failures, only protection schemes with extended VC monitoring capabilities are capable of offering improvements in traffic availability.

Examples of these types of protection mechanisms are VC trail protection and SNC-P / N . MS trail protection takes into account only RS TIM.

5.4 Interconnecting subnetworks protected at different layers

It should be possible to interconnect subnetworks protected at different layers.

When interconnecting HO-VC and LO-VC protected subnetworks the following comments apply:

For dual node interconnected rings with drop and continue, the drop and continue selectors in the HO-VC layer rings should be able to switch choosing the trail without defects. Digital cross-connects may be placed in the ring interconnecting nodes, DXCs enable traffic interconnected between LO-VC layer and HO-VC layer subnetworks to be groomed. The DXCs, connecting HO-VC switching NEs and LO-VC switching NEs, may source HO-VCs in the HO-VC layer ring carrying the same LO-VC content with different HO-VC TTIs. Hence any switching at the HO-VC interconnecting nodes will cause HO-VC TIM, suppressing all its LO-VCs content. To avoid this, it is recommended to disable the HO-VC TTI mismatch detection in the HO-VC drop and continue interconnecting nodes and in those nodes where the HO-VC is terminated. The LO-VC contained in these HO-VCs will be left with TIM detection enabled. HO-VC TIM detection will be left enabled for HO-VC not carrying LO-VCs. This will insure complete trail connectivity supervision at both the LO-VC and HO-VC layers.

In the case of single node interconnection, both LO and HO TTI may be enabled and no special TTI considerations apply.

5.5 Capability to interconnect networks using different protection schemes

The capability to interconnect subnetworks using different protection schemes refers to the ability to have protection inter-working between subnetworks using different protection schemes. The objective is to have subnetworks protected using different protection mechanisms interwork with each other without the need for any inter - network automatic protection signalling.

5.6 Minimisation of traffic interruption

The objective is to minimise traffic interruption.

There are several contributors to the traffic interruption time which are, the failure detection time, the switching time, the hold off time and the effect of sequential switching in certain failure scenarios like node failure in the interconnecting drop and continue architecture.

In the latter case, there is an extension of the traffic interruption as both subnetworks involved switch one after the other.

Hold off time is used to improve the degree of protection independence, to avoid ripple effect caused by the interworking of protections schemes or by different transmission delays.

The protection schemes can also have an impact on the switching time. Switching at the MS layer shall be completed in 50 ms, see ETS 300 746 [2], whereas switching at the VC layer may take longer time when many VCs are involved.

5.7 Operation modes

The objective is to allow each of the interconnected subnetworks to be operated in any operation mode. The modes of operation could be:

a) revertive or non revertive;

b) single ended or dual ended switching.

Sometimes, the protection mechanisms impose their natural mode of operation, for example, on one hand MS-SPRING is only dual ended and revertive, on the other hand SNC-P is single ended and may be revertive or non revertive.

Regarding the interconnecting architectures themselves, for example drop and continue, is inherently single ended.

If protection independence is required for the drop and continue architecture, revertive mode of operation may be required in the selectors.

5.8 Capacity utilisation

The capacity utilisation objective is to minimise the overall occupied bandwidth associated to a given interworking scheme for a given level of traffic survivability. The use of drop and continue interworking and the particular combination of subnetwork protection schemes will affect the traffic capacity utilisation achieved.

The occupied bandwidth is made up from two components - the traffic between drop and continue nodes in the same subnetwork (e.g. between nodes I1 and I2 in figure 13a) and the traffic transiting the subnetwork between the ingress and the egress drop and continue node pairs (e.g. between nodes I1 and I2 in figure 13a).

In all schemes the drop and continue architecture normally results in the continue signal occupying bandwidth between the drop and continue nodes (and on any intervening links if these nodes are not adjacent). This capacity will not be available for other intra subnetwork traffic.

With MS-SPRINGs an alternative implementation of drop and continue is possible in which the continue traffic is carried within the VC-4s normally reserved for protection, this is called "continue on protection". This avoids occupying working bandwidth between drop and continue but has different traffic availability properties. In this case a failure in one ring would preclude protection in the drop and continue connection. Details of this are left for further study.

In most instances the capacity utilised by the transiting traffic is unaffected by the combination of protection schemes.

The exception to this being where MS-SPRINGs interwork with SNC-P without drop and continue functionality, see figure 7a.This shows the use of two independent trails transiting the MS-SPRINGs.

The alternative solution using drop and continue in the SNC-P subnetwork (see figure 7b) avoids the unnecessary duplication of transiting trails.

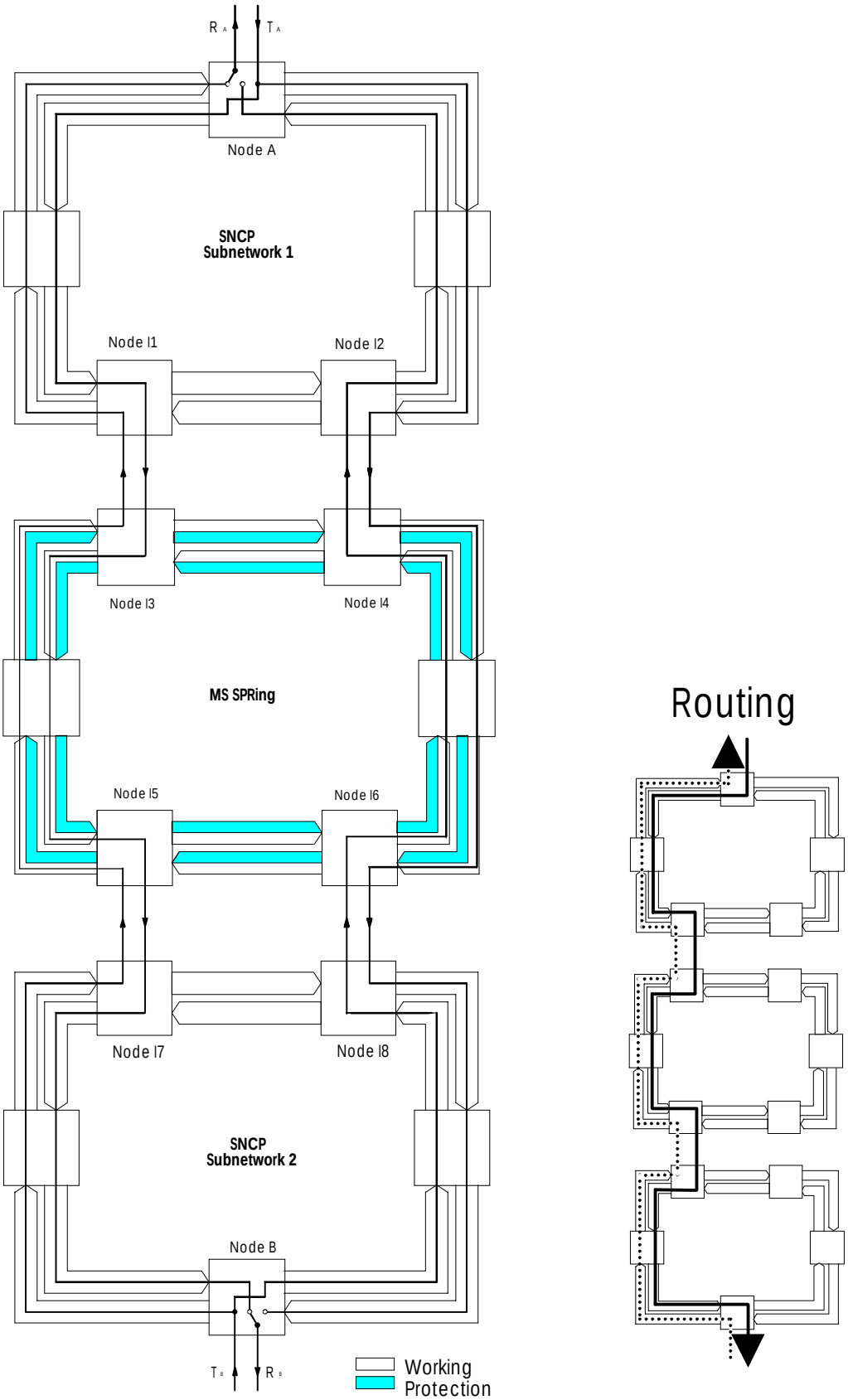

Figure 7a: SNCP-MSSPRing-SNCP dual node interconnection

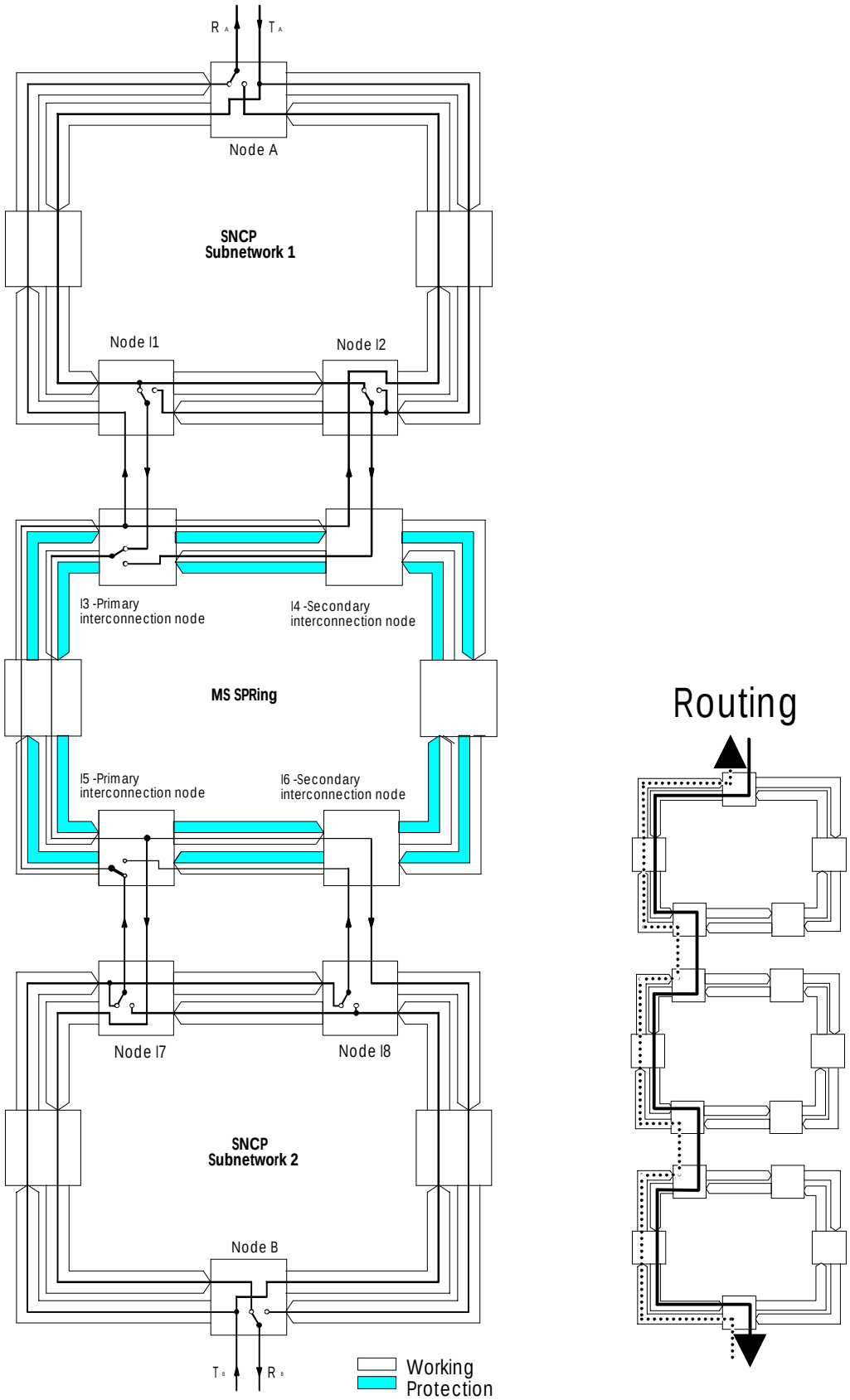

Figure 7b: SNCP-MSSPRing-SNCP dual node drop and continue interconnection

6 Subnetwork interconnection architectures

A major need to connect subnetworks together is based on the requirement to establish a network connection amongst subnetworks to satisfy a demand that has trail termination points on different subnetworks.

The subnetwork interconnection architectures described in the following clauses do to some degree satisfy the protection interworking objectives defined in clause 5.

Two main network interconnecting architectures are identified:

- single node;
- dual node.

6.1 Single node interconnecting architecture

It is an interworking arrangement between two subnetworks where a single node in each subnetwork is interconnected. A trail or subnetwork connection in this arrangement can survive a single failure in either subnetwork but it will not survive a failure in the interconnecting nodes. Figures 8a and 8b illustrate single node interconnecting architectures by sharing a span and by sharing the node.

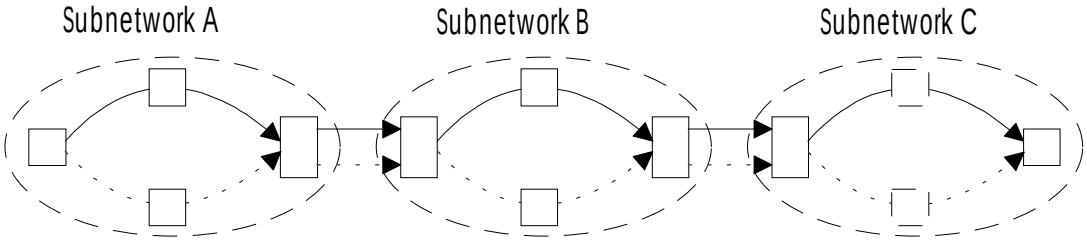

Figure 8a: Single node interconnecting architecture by sharing the span

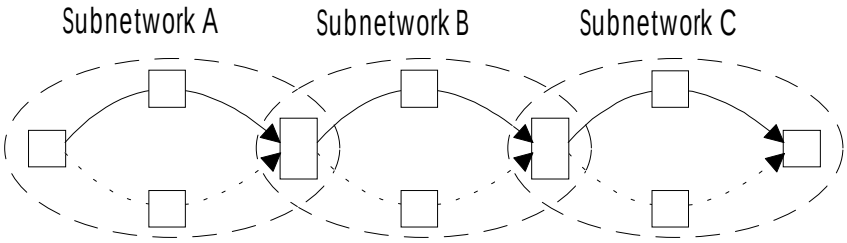

Figure 8b: Single node interconnecting architecture by sharing the node

6.2 Dual node interconnecting architectures

Dual node interconnecting architectures provide network connection by using node diversity. This means that the protected and protecting trails or subnetwork connections may be routed across different nodes when going from one network to another. Subnetwork interconnecting nodes could be co-located in the same office connected by intra-office links or they could be in different central offices interconnected through inter-office links.

6.2.1 Mechanisms to implement dual node interconnecting architectures

There are two dual node interconnecting architectures that fulfil, to some degree, the protection interworking objectives. These are:

- virtual ring architecture;
- drop and continue architecture.

6.2.1.1 Virtual ring interconnecting architecture

The virtual ring architecture is the simplest implementation of a dual node interconnecting architecture. It is a point to point SDH structure that is formed by a protected and a protecting trail or subnetwork connection as shown in figure 9a. The protected and protecting trails or subnetwork connections are physically different. Routing can be uniform or diverse. The location of the SNC-P selectors dictate where the ends of the logical ring are.

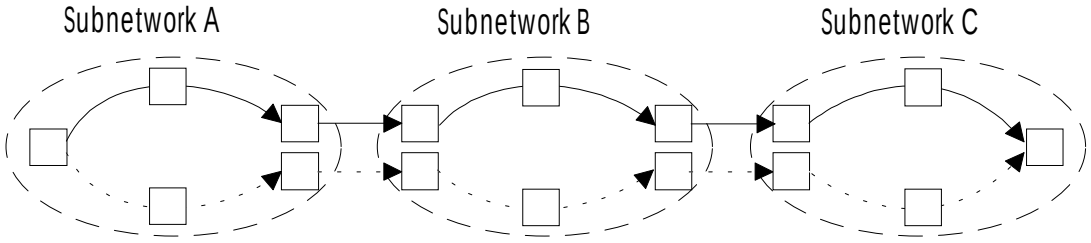

Figure 9a: Virtual Ring dual node interconnecting architecture

The virtual ring interconnecting architecture can be realised with various topologies. These topologies are the following:

- overlapping subnetworks;
- dual parenting.

Overlapping subnetworks is a topology where only two nodes are used between the two interconnected subnetworks.

Dual parenting is a network architecture where a trail terminating node is connected to a subnetwork by using two disjoint routes.

The figures 9b and 9c illustrate the above mentioned topologies respectively.

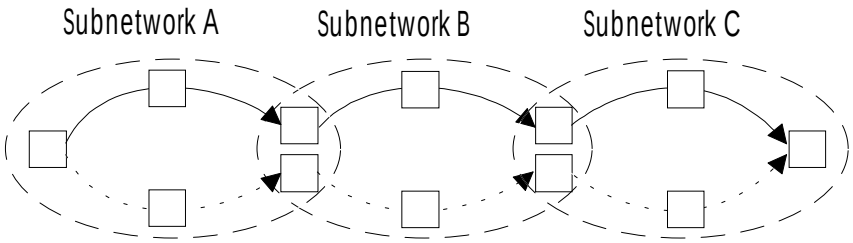

Figure 9b: Overlapping subnetwork dual node interconnecting architecture

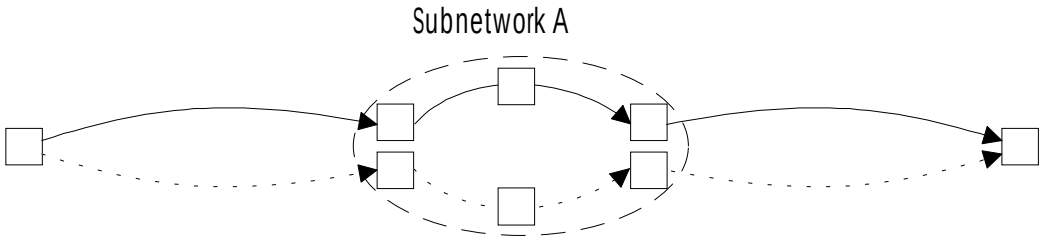

Figure 9c: Dual parenting interconnecting architecture

6.2.1.2 Drop and continue interconnecting

The drop and continue architecture is implemented through a 1+1 SNC-P single ended connection between the nodes that are involved in the dual node architecture.

This architecture can be used to interconnect the following types of subnetworks:

- SNC-P to SNC-P subnetwork;
- MS-SPRING to MS-SPRING;
- MS-SPRING to SNC-P.

Figures 10a, 10b and 10c describe respectively SNC-P to SNC-P, MS-SPRING to MS-SPRING and MS-SPRING to SNC-P interworking showing only one traffic direction.

Detailed description of the above interconnecting possibilities are given in clauses 7 and 8.

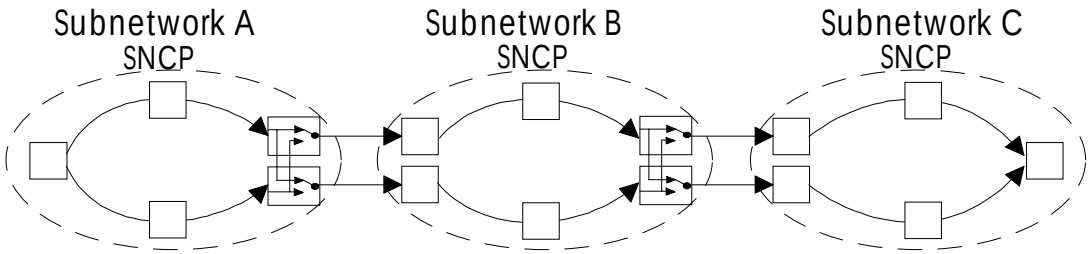

Figure 10a: SNC-P to SNC-P drop and continue interworking

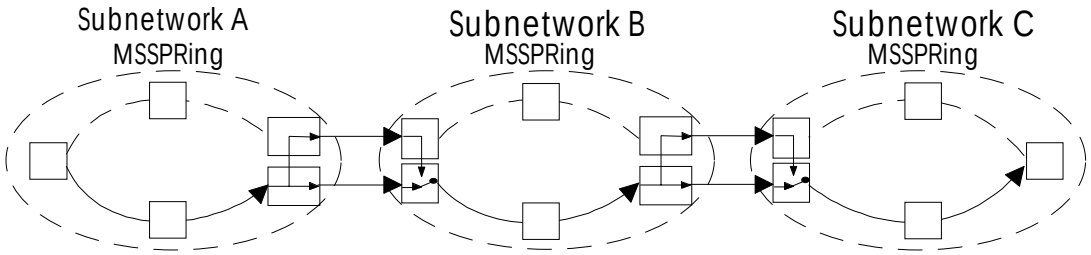

Figure 10b: MS-SPRING to MS-SPRING drop and continue interworking

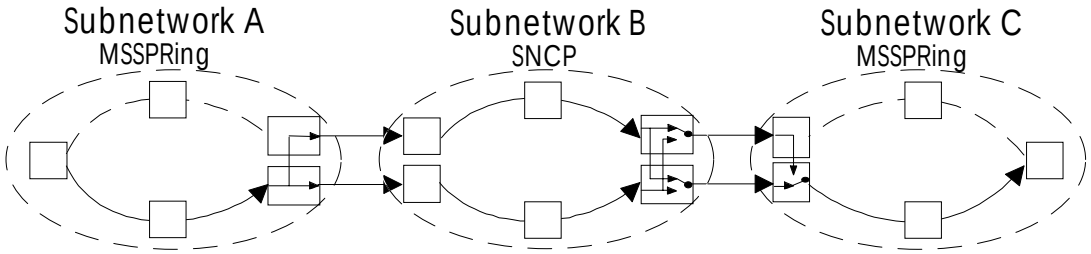

Figure 10c: MS-SPRING to SNC-P drop and continue interworking

6.3 Application of interworking architectures on real network topologies

The previous clauses illustrated the logical connections of subnetworks using one or two node interconnecting architectures. When the logical structure is applied in to a real network topology, the following applies:

a) the interconnecting network may be larger than just a simple fibre connection. It may be a complex subnetwork, for example a ring or a DXC;

b) the interconnecting nodes in a dual node architecture need not be adjacent.

It is, however, necessary for the interconnecting HO or LO signals to pass unchanged through the interconnecting subnetwork and the nodes between the non-adjacent interconnecting nodes. This is because the drop and continue is an SNC-P 1+1 protection scheme.

Both topics are illustrated in figures 11a and 11b, they show dual node interconnection of SNC-P and MS-SPRING, respectively.

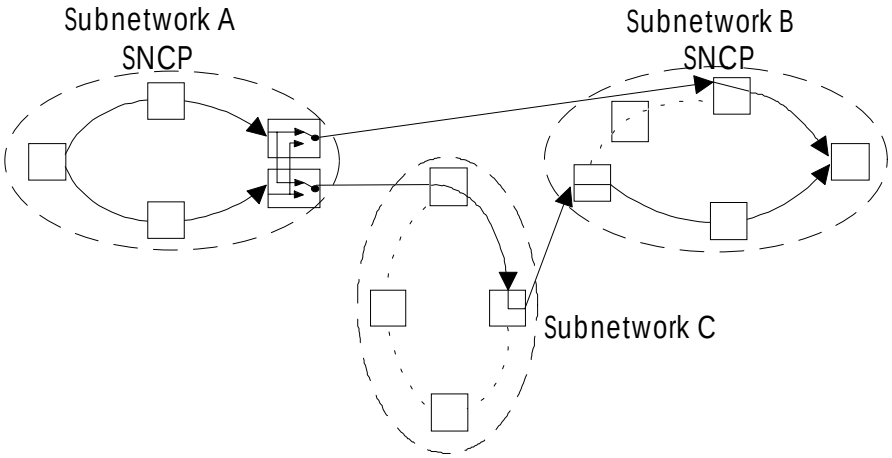

Figure 11a: SNCP-SNCP dual node drop and continue Interconnecting with transit nodes

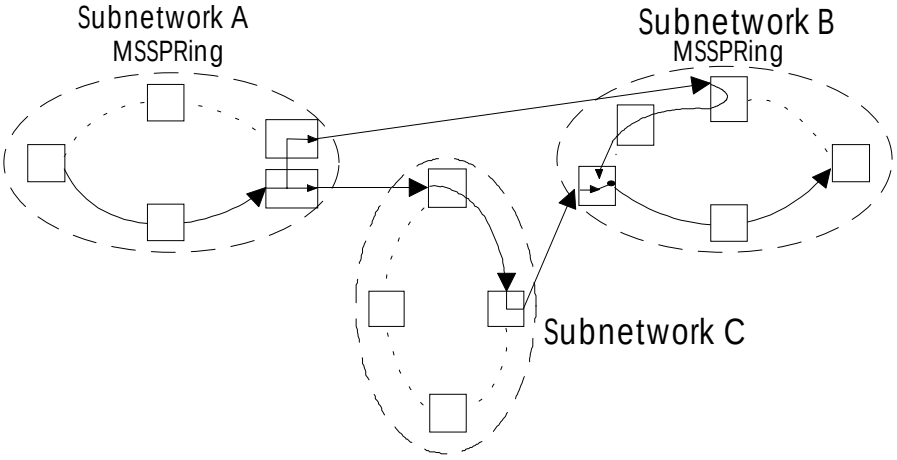

Figure 11b: MSSPRing-MS-SPRing dual node drop and continue interconnecting with transit nodes

7 Interworking between similar protection schemes

7.1 MS SPRING

7.1.1 Two MS shared protection rings connected by one node

Figure 12 shows the architecture of single node interworking for a single VC-4 between MS-SPRINGs. This interworking scheme can be classified as a chained intra-layer protection interworking. This interworking scheme has no impact on the squelching mechanism in each MS-SPRING. Table 1 shows the conformance of this interconnection scheme with the objectives given in clause 5.

Table 1: Interworking conformance of MS-SPRINGs interconnected by one node

Protection interworking objectives	Conformance
Traffic availability	Level 1
Protection independence	Yes
Fault coverage	Conforms to subclause 5.3.1
Subnetworks protected at different layer	No LO-VC
Different protection schemes	NA
Traffic interruption	See subclause 5.6
Operation modes	Dual ended / revertive
Capacity utilisation	See subclause 5.8

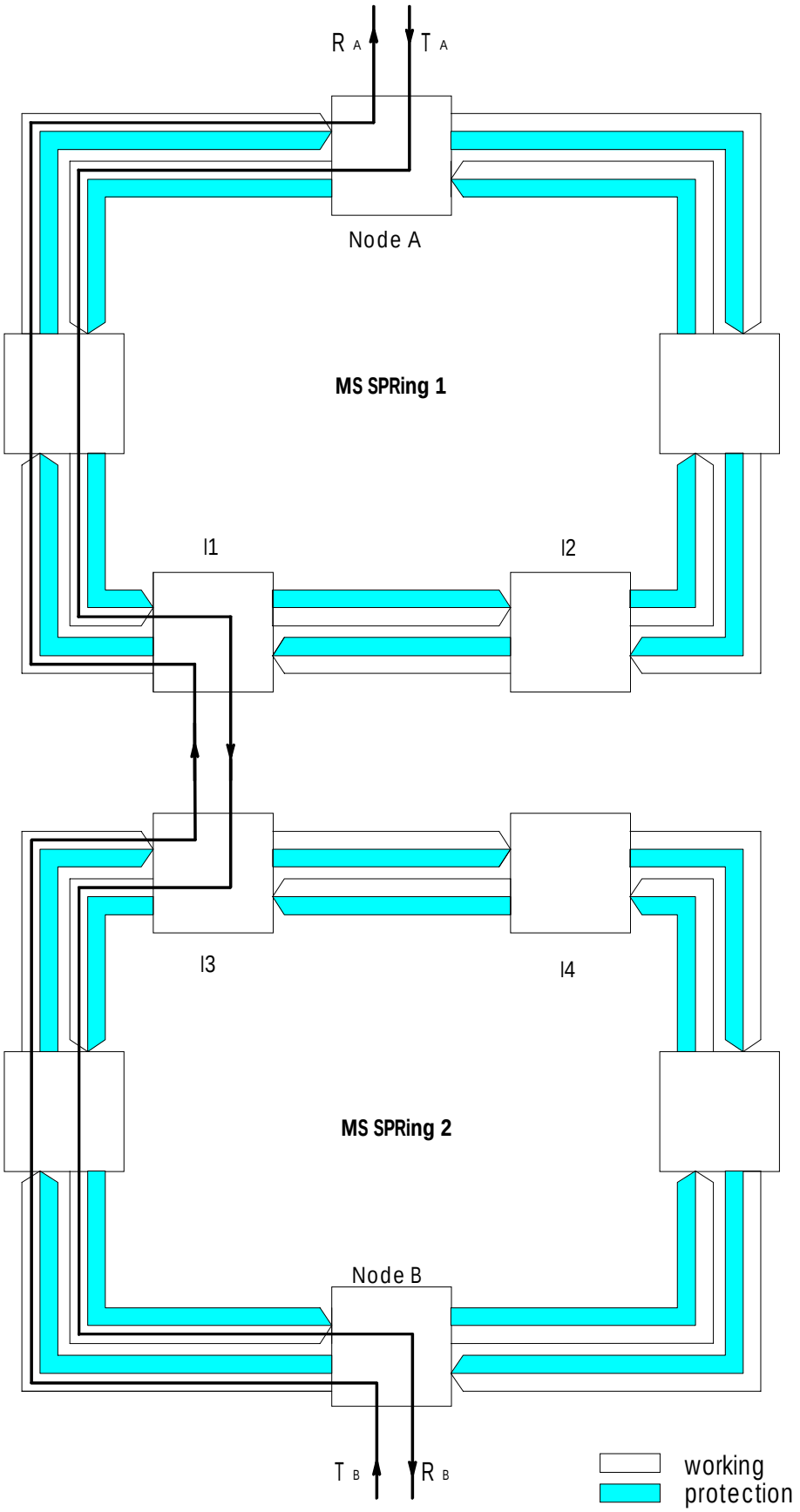

Figure 12: MS SPRING virtual ring single node interconnection

7.1.2 Two MS shared protection rings connected by two nodes

Figures 13a and 13b show the architecture of dual node interworking for a single VC-4 between MS-SPRINGs. This interworking scheme can be classified as a chained inter-layer protection interworking. The role of primary and secondary interconnecting nodes can be assigned on a per VC-4 basis.

For each direction of transmission, the signal is sent from the source node to the primary interconnection node, around the side of the ring not crossing the secondary interconnection node. When the signal reaches the primary interconnection node, it is dropped at that node and continued onto the secondary interconnection node, using the drop and continue feature. Then the signal is sent from primary and the secondary interconnection node to the second ring. The secondary interconnection node of the second ring transmits the signal to the primary interconnection node of the same ring. Thus, the primary interconnection node of the second ring can select from two signals coming from the two nodes of the first ring and transmits one of them towards the signal termination node, around the side not crossing the secondary interconnection node.

In both cases illustrated in figures 13a and 13b, the switches positions are set in such a way that the working signal uses the drop signal to allow protection independence.

The squelching mechanism of the two interconnected MS-SPRINGs has to take into account the drop and continue function in the primary interconnection node. In case of a complete failure of that node, it should allow the direct connection between the source node and the secondary interconnection node. Table 2 shows the conformance of this interconnection scheme with the objectives given in clause 5.

Table 2: Interworking conformance of MS-SPRINGs interconnected by two nodes

Protection interworking objectives	Conformance
Traffic availability	Level 3
Protection independence	Yes
Fault coverage	Conforms to subclause 5.3.1
Subnetworks protected at different layer	No LO-VC
Different protection schemes	NA
Traffic interruption	See subclause 5.6
Operation modes	Dual ended / revertive
Capacity utilisation	See subclause 5.8

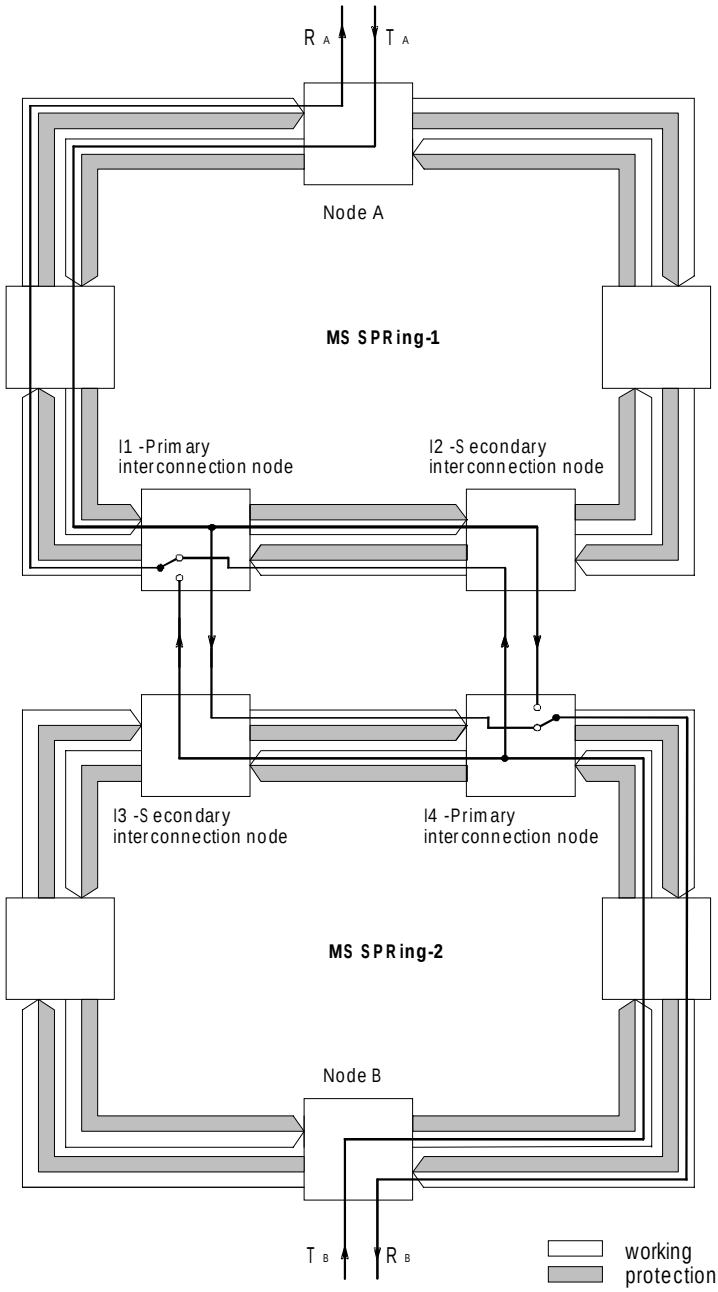

Figure 13a: MS-SPRINGs interconnected by drop and continue (case a)

To improve the degree of protection independence the following apply:

- Node A to Node B-direction: use the drop for working channels, in order to reduce the chance that the selector in I4 switches due to a failure in the upper network;
- Node B to Node A-direction: same principle. This leads to Go and Return working traffic being on different routes in the interconnection architecture;
- this preferred routing leads to the need for revertive operation, if one still wants to restore the preferred routing after particular failure clearance;
- applying a hold-off time can prevent undesirable switching in I4 due to a failure between node A and I1 in the upper MS SPRing and a delay difference in the interconnection architecture. Similar approach for the selector in I1.

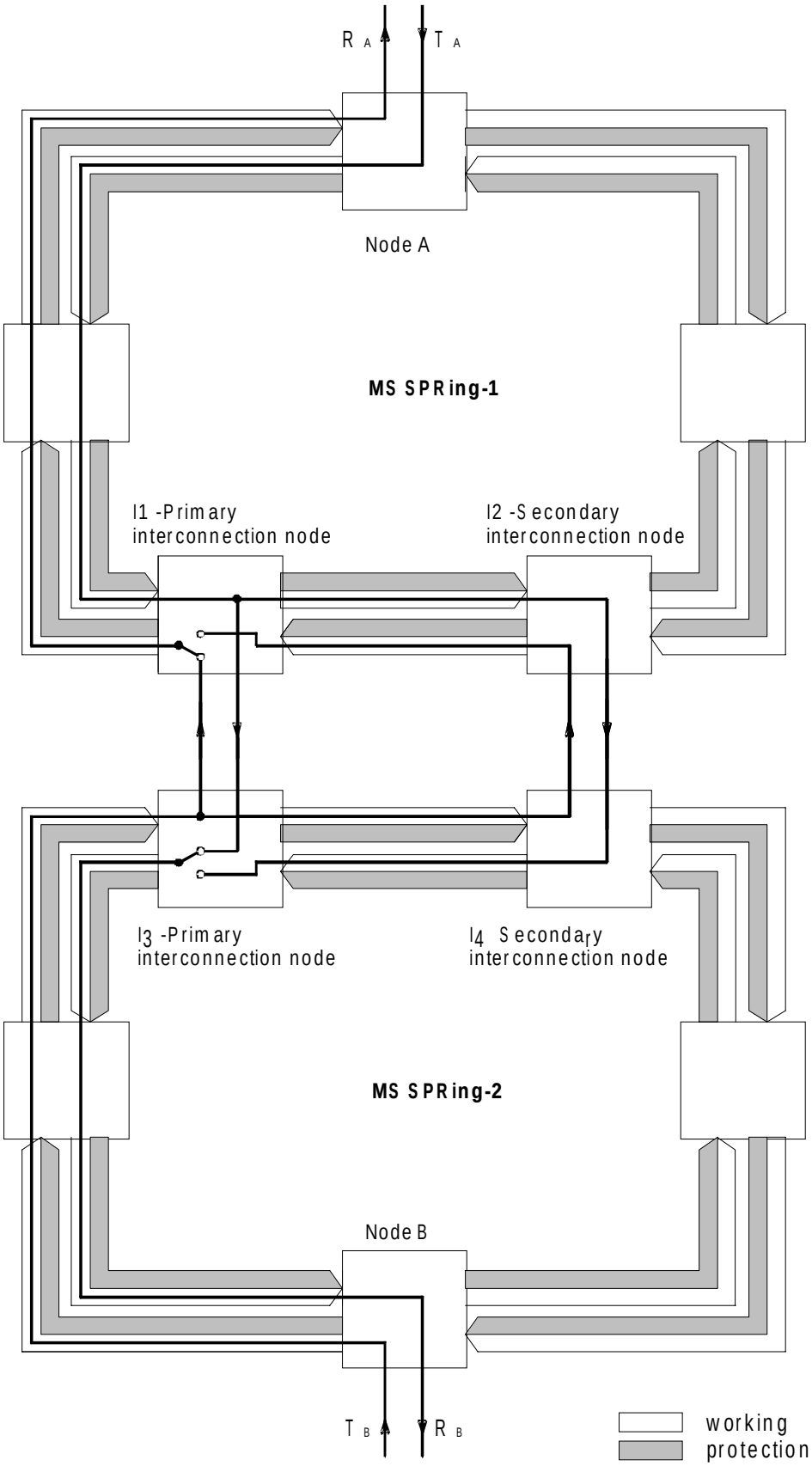

Figure 13b: MS-SPRINGs interconnected by Drop and Continue (case b)

Case b is very similar to case a, with one difference: Go and Return working traffic can be on the same route.

7.2 LO/HO trail protection

7.2.1 VC trail protected subnetworks interconnected by one node

A trail running from one subnetwork to another is split at the source, both protecting and protected trails pass through the single interconnecting node, and are then terminated in another subnetwork, where the trail terminating node chooses the best performing trail. This description is valid for both directions of the trail.

Figure 14a and 14b illustrate the interconnection scheme.

Table 3 shows the conformance of this interconnection scheme with the objectives given in clause 5.

Table 3: Interworking conformance of VC trail protected subnetworks interconnected by one node

Protection interworking objectives	Conformance
Traffic availability	Level 1
Protection independence	No
Fault coverage	Conforms to subclauses 5.3.2 and 5.3.3
Subnetworks protected at different layer	No
Different protection schemes	NA
Traffic interruption	See subclause 5.6
Operation modes	Dual ended / Single ended Revertive / Non-Revertive
Capacity utilisation	See subclause 5.8

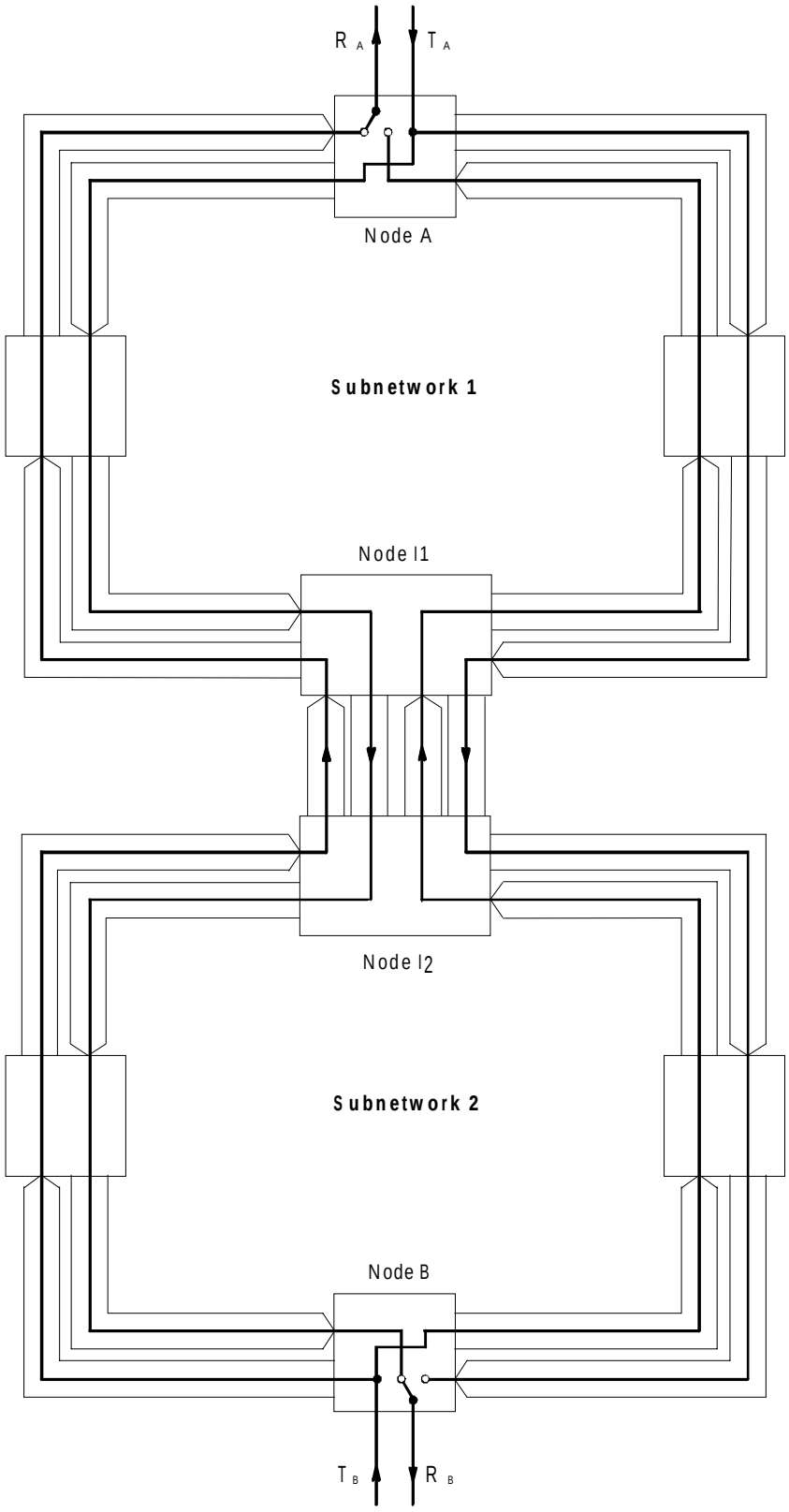

Figure 14a: VC Trail protection virtual ring single node interconnection

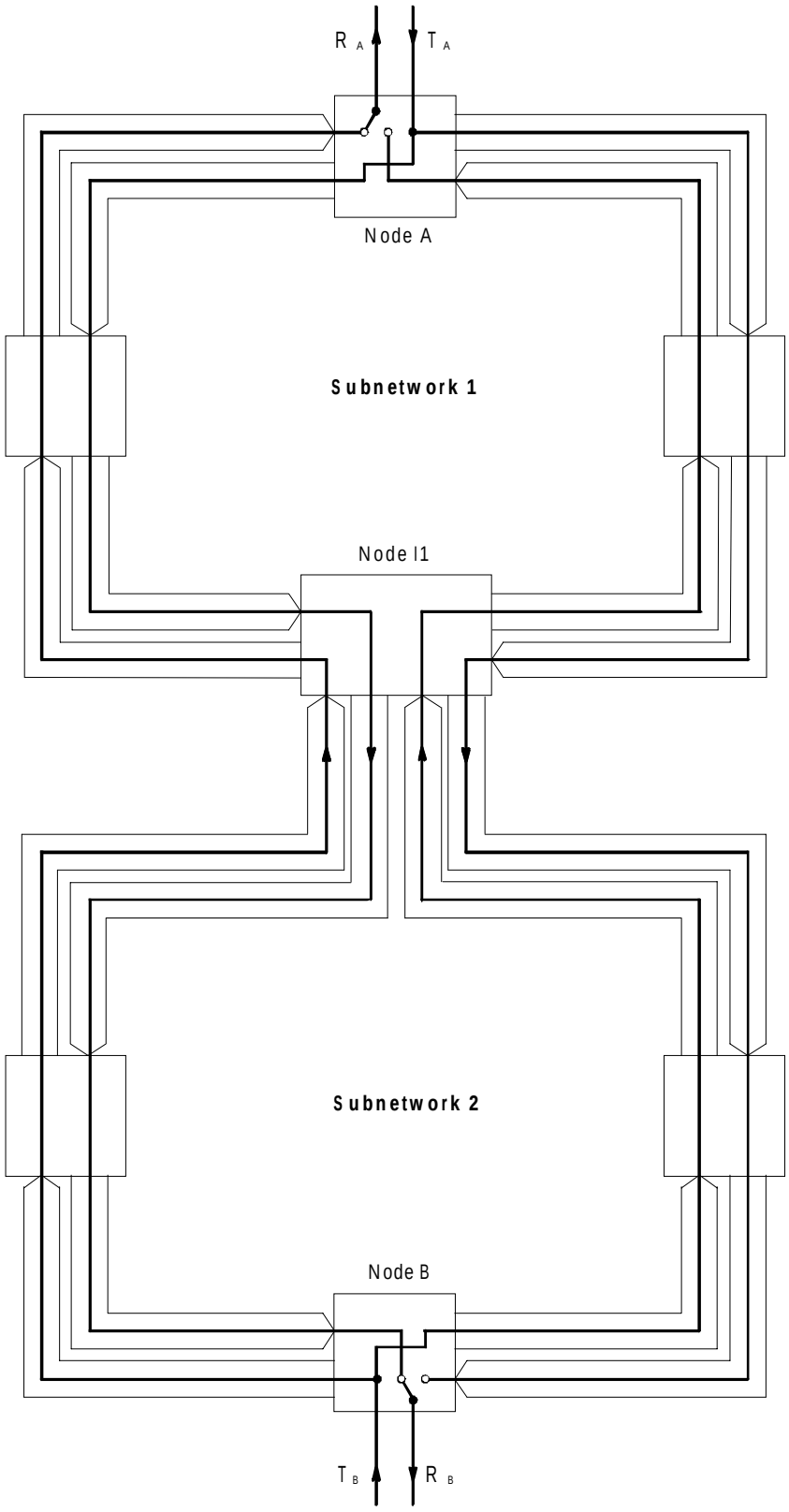

Figure 14b: VC Trail protection overlapping subnetwork single node interconnection

7.2.2 Two VC trail protected subnetworks interconnected by two nodes

There is one dual node interconnecting architecture to interconnect VC trail protected subnetworks. This is the virtual ring architecture.

Virtual ring is a point to point topological structure that is formed by a protected trail and a protecting trail as shown in figure 15a. The protected and protecting trails are routed on different fibre spans and equipment to insure disjoint routes. Routing can be either uniform or diverse. The location of the VC trail selectors dictates where the ends of the virtual ring are.

Table 4 shows the conformance of this interconnection scheme with the objectives given in clause 5.

Table 4: Interworking conformance of VC trail protected subnetworks interconnected by two nodes

Protection interworking objectives	Conformance
Traffic availability	Level 2
Protection independence	No
Fault coverage	Conforms to subclauses 5.3.2 and 5.3.3
Subnetworks protected at different layer	No
Different protection schemes	NA
Traffic interruption	See subclause 5.6
Operation modes	Dual ended / Single ended Revertive / Non Revertive
Capacity utilisation	See subclause 5.8

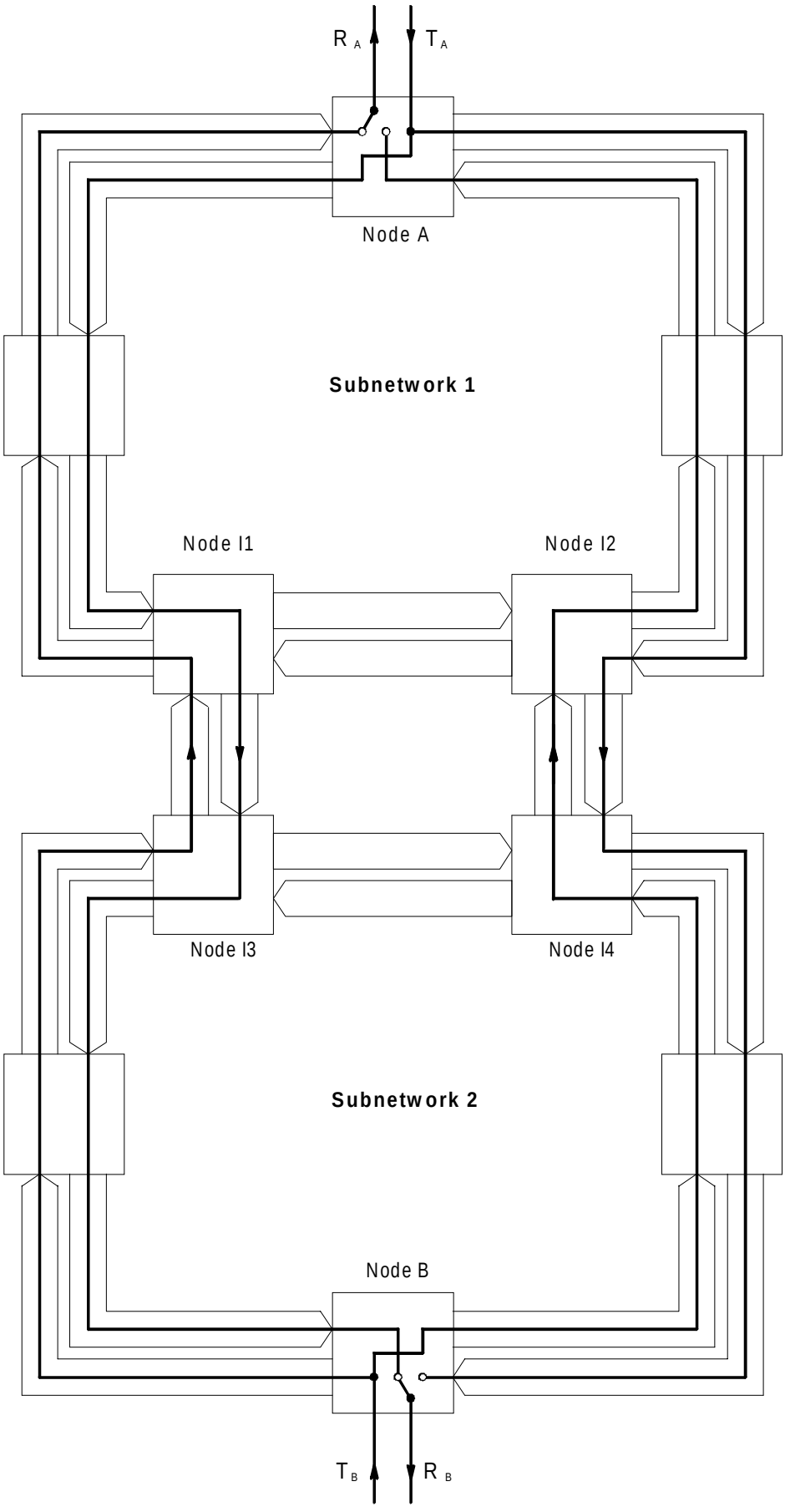

Figure 15a: VC trail protection virtual ring architecture

The virtual ring interconnecting architecture can be realised with topologies requiring fewer nodes. The figures 15b and 15c illustrate two examples of virtual ring architecture.

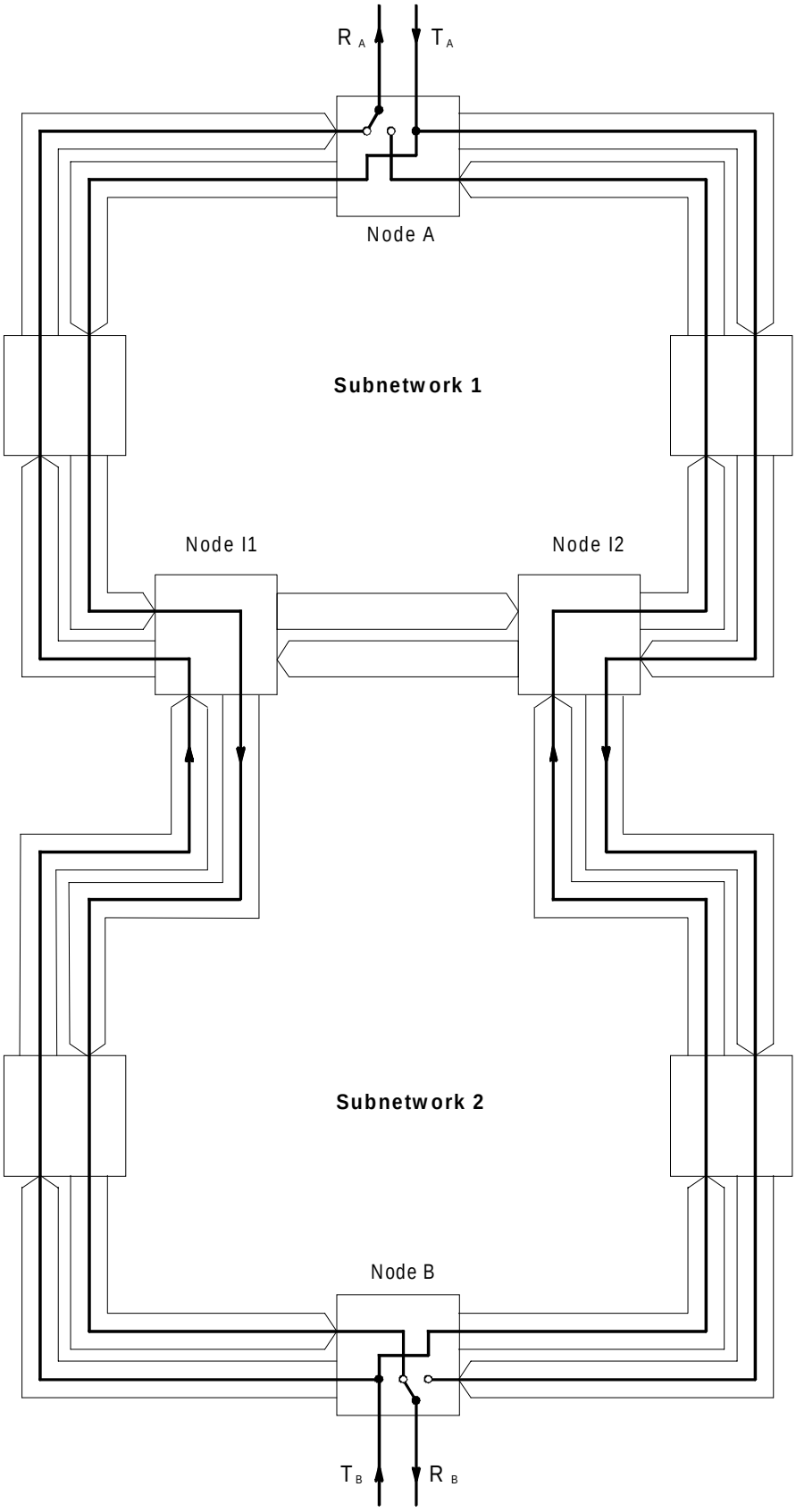

Figure 15b: VC Trail protection on overlapping subnetworks

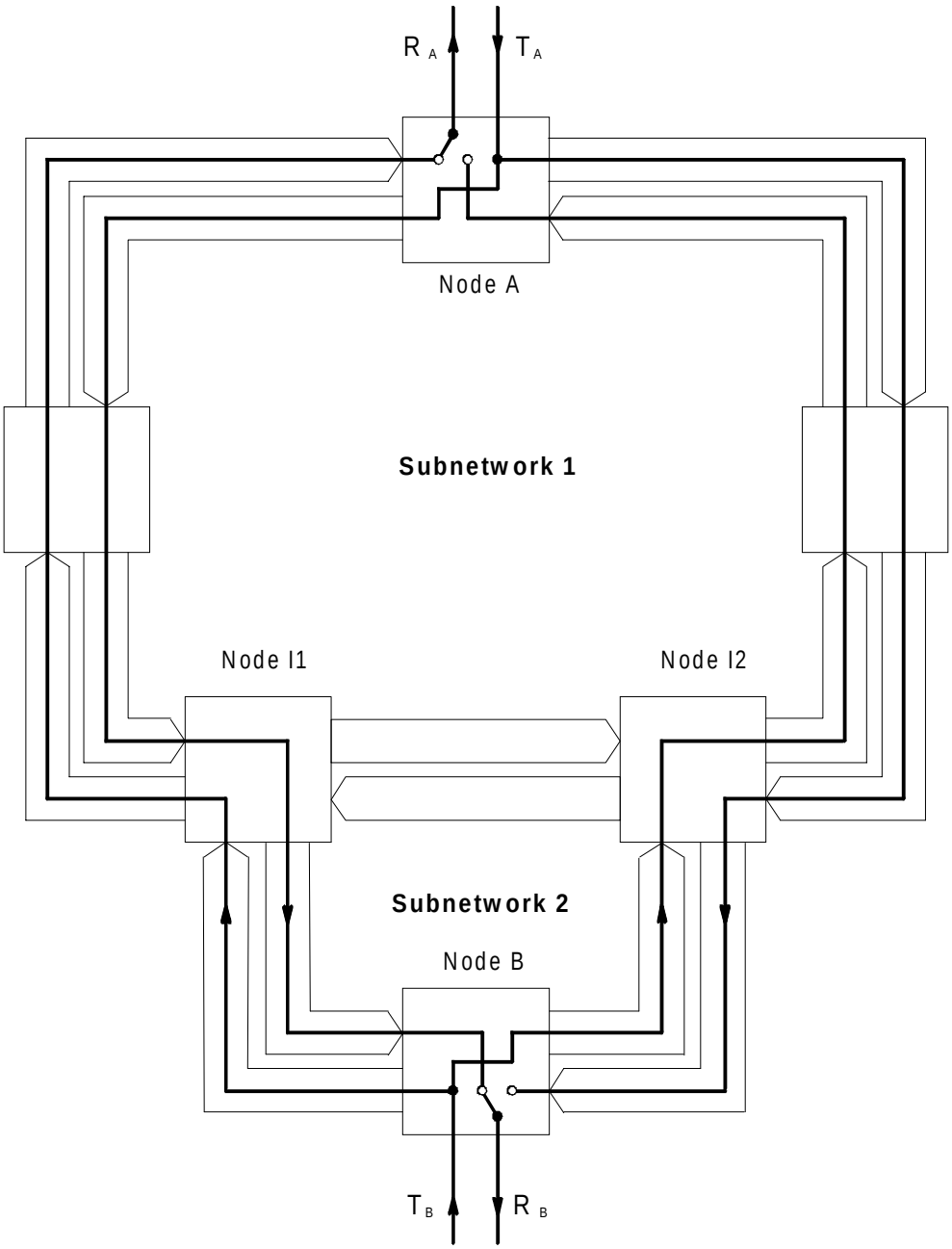

Figure 15c: VC trail protection over dual parented access nodes

It is important to clarify that neither single ended nor dual ended VC trail protection subnetworks can be interconnected by using the drop and continue architecture.

Dual ended VC trail protection and drop and continue are incompatible protection mechanisms. This is due to the appearance of trace identifier mismatch problems in the trail termination points when the switches in the interconnecting nodes operate as a consequence of a subnetwork failure.

7.3 LO/HO subnetwork connection protection

7.3.1 SNC protected subnetworks interconnected by one node

A subnetwork connection traversing a number of subnetworks can be protected autonomously at each subnetwork using subnetwork connection protection mechanisms. The nodes used to interconnect the subnetworks will support switching and bridging capabilities to achieve subnetwork connection protection as shown in figures 16a and 16b.

Table 5 shows the conformance of this interconnection scheme with the objectives given in clause 5.

Table 5: Interworking conformance of SNC-P protected subnetworks interconnected by one node

Protection interworking objectives	Conformance
Traffic availability	Level 1
Protection independence	Yes
Fault coverage	Conforms to subclauses 5.3.2 and 5.3.3
Subnetworks protected at different layer	Yes
Different protection schemes	NA
Traffic interruption	See subclause 5.6
Operation modes	Single ended Revertive / Non-Revertive
Capacity utilisation	See subclause 5.8

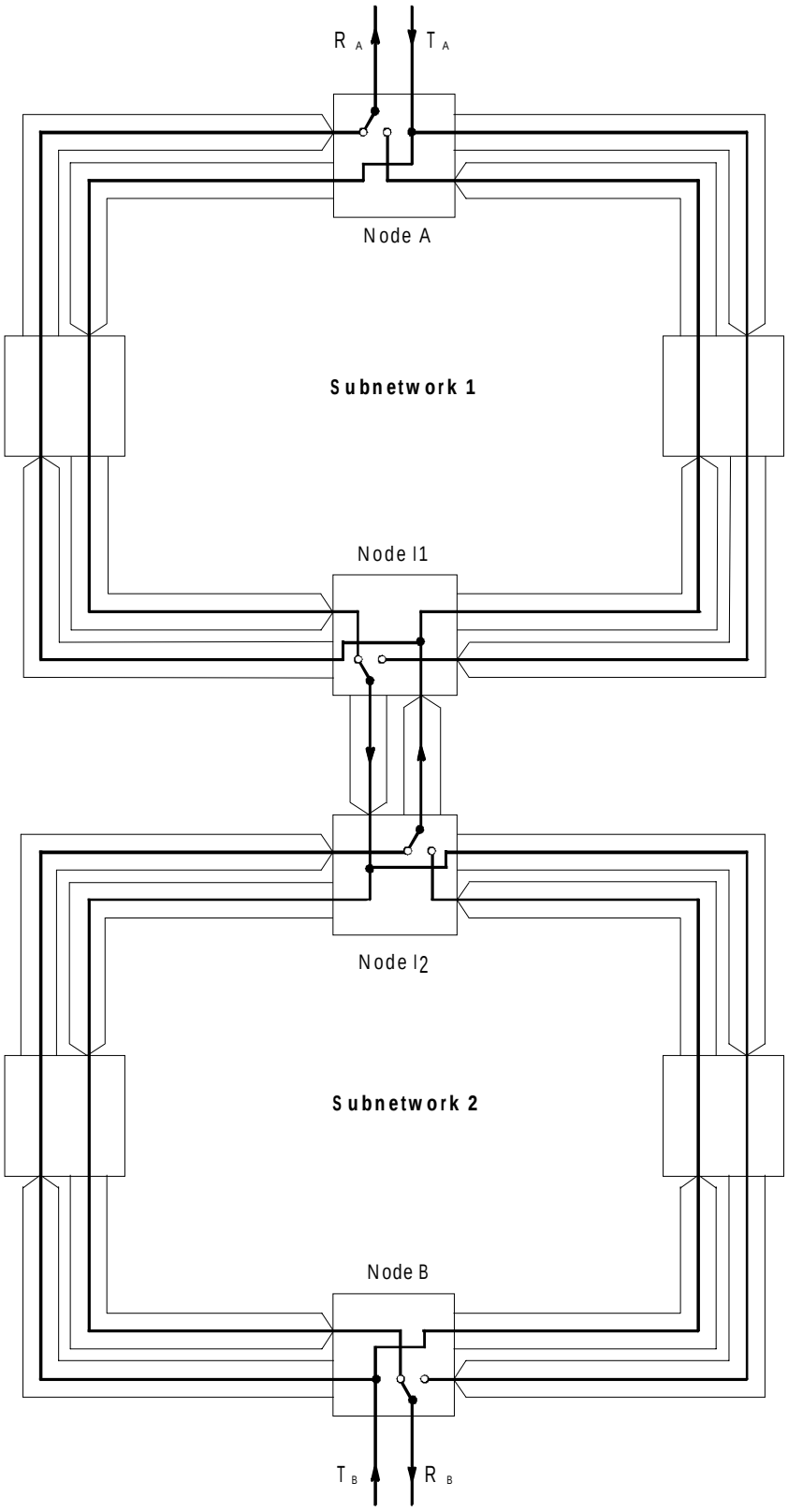

Figure 16a: SNC-P virtual ring single node interconnection

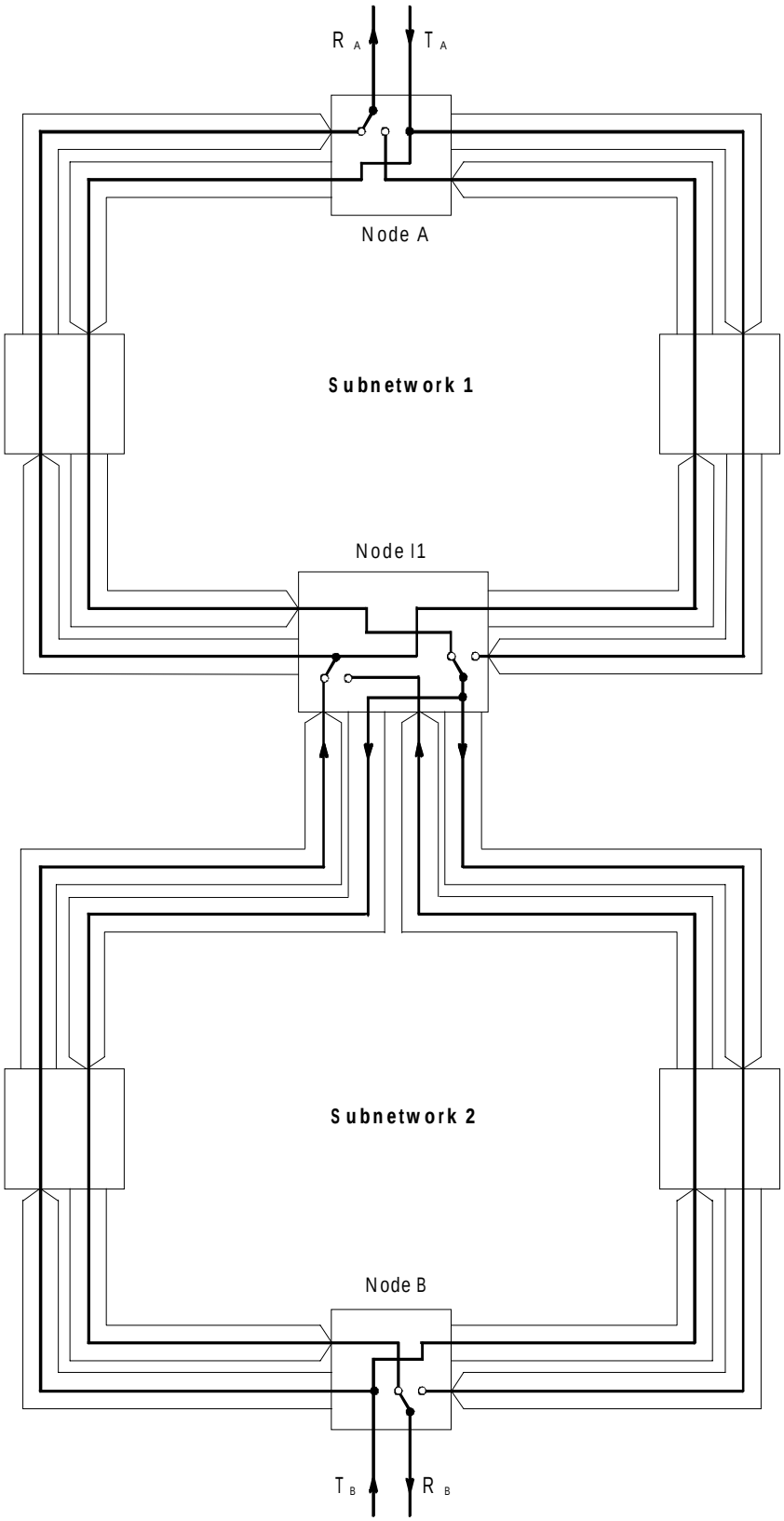

Figure 16b: SNC-P overlapping subnetwork single node interconnection

7.3.2 Two SNC-P Subnetworks Interconnected by Two Nodes

There are two dual node interconnecting architectures to interconnect subnetwork connection protected subnetworks. These are:

- virtual rings architecture;
- drop and continue architecture.

A virtual ring is a point to point topological structure that is formed by a protected subnetwork connection and a protecting subnetwork connection as shown in figure 17a. The protected and protecting subnetwork connections are routed on different fibre spans and equipment to insure disjoint routes. Routing can be either uniform or diverse. The location of the SNC-P selectors dictate the location of the ends of the virtual ring.

Table 6 shows the conformance of this interconnection scheme with the objectives given in clause 5.

Table 6: Interworking conformance of SNC-P protected subnetworks interconnected by two nodes with virtual ring

Protection interworking objectives	Conformance
Traffic availability	Level 2
Protection independence	No
Fault coverage	Conforms to subclauses 5.3.2 and 5.3.3
Subnetworks protected at different layer	Yes
Different protection schemes	NA
Traffic interruption	See subclause 5.6
Operation modes	Single ended Revertive / Non-Revertive
Capacity utilisation	See subclause 5.8

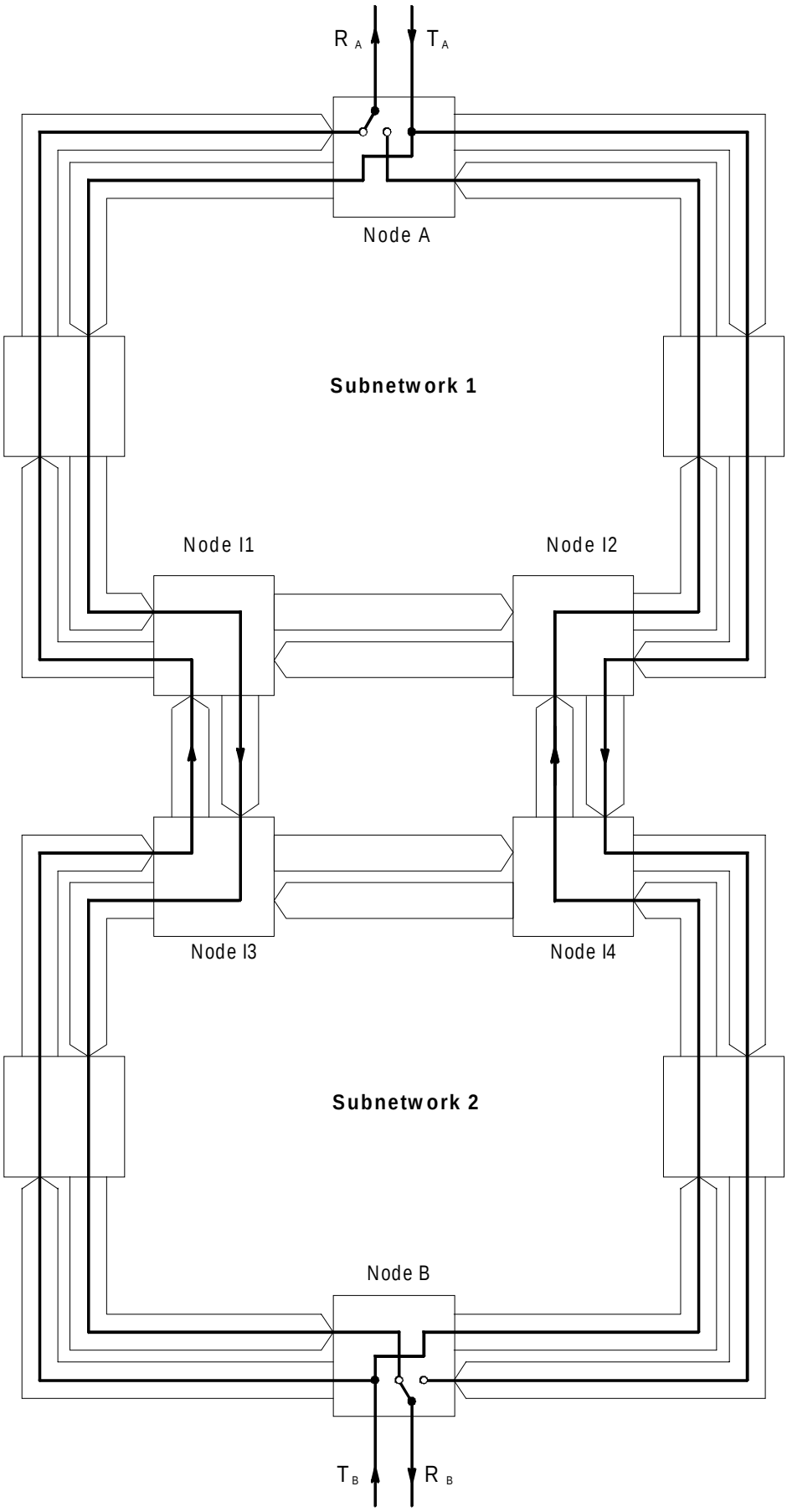

Figure 17a: SNC-P virtual ring architecture

The virtual ring interconnecting architecture can be realised with topologies requiring fewer nodes. The figures 17b and 17c illustrates the above mentioned topologies respectively.

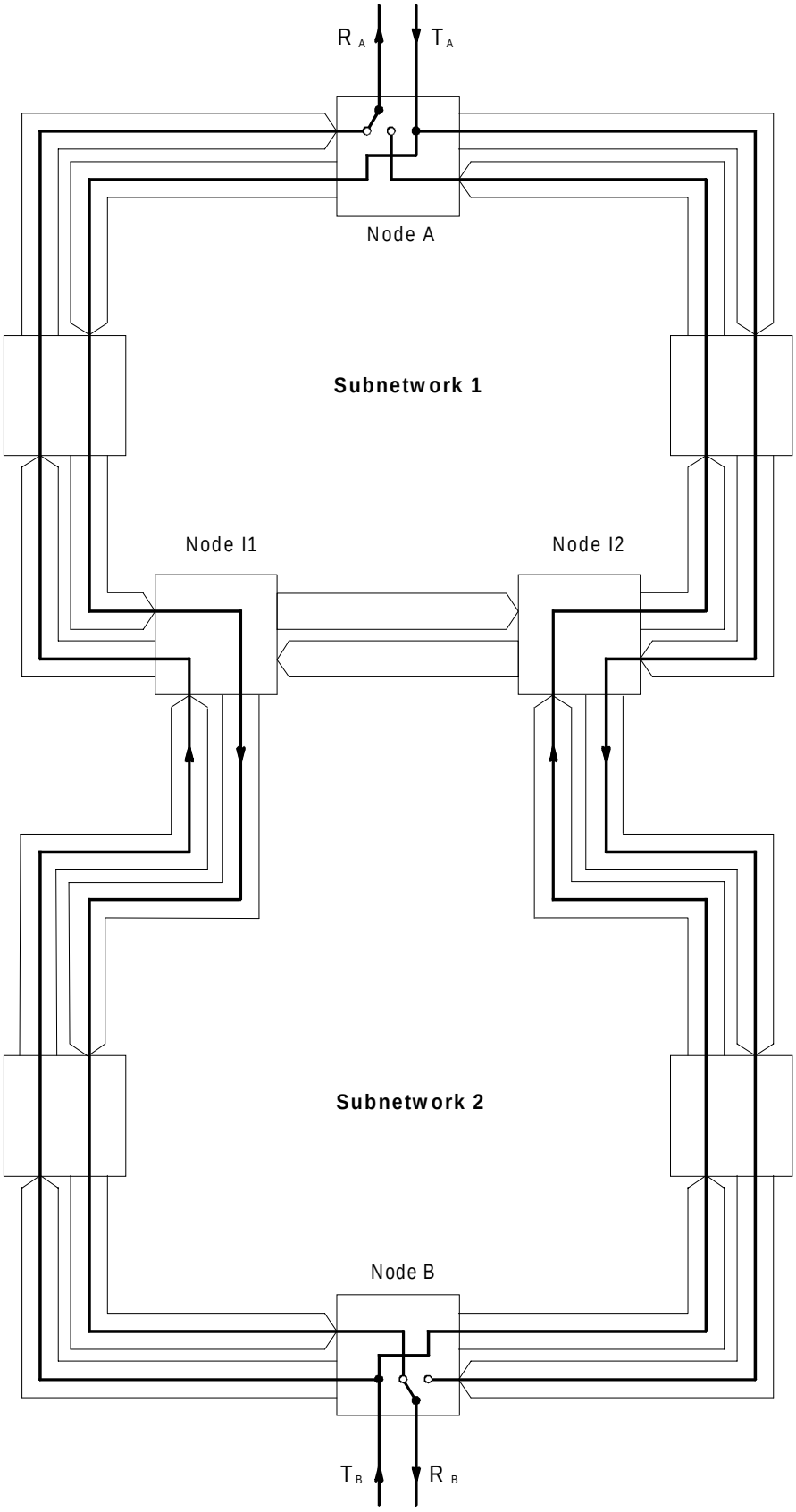

Figure 17b: SNC-P on overlapping rings

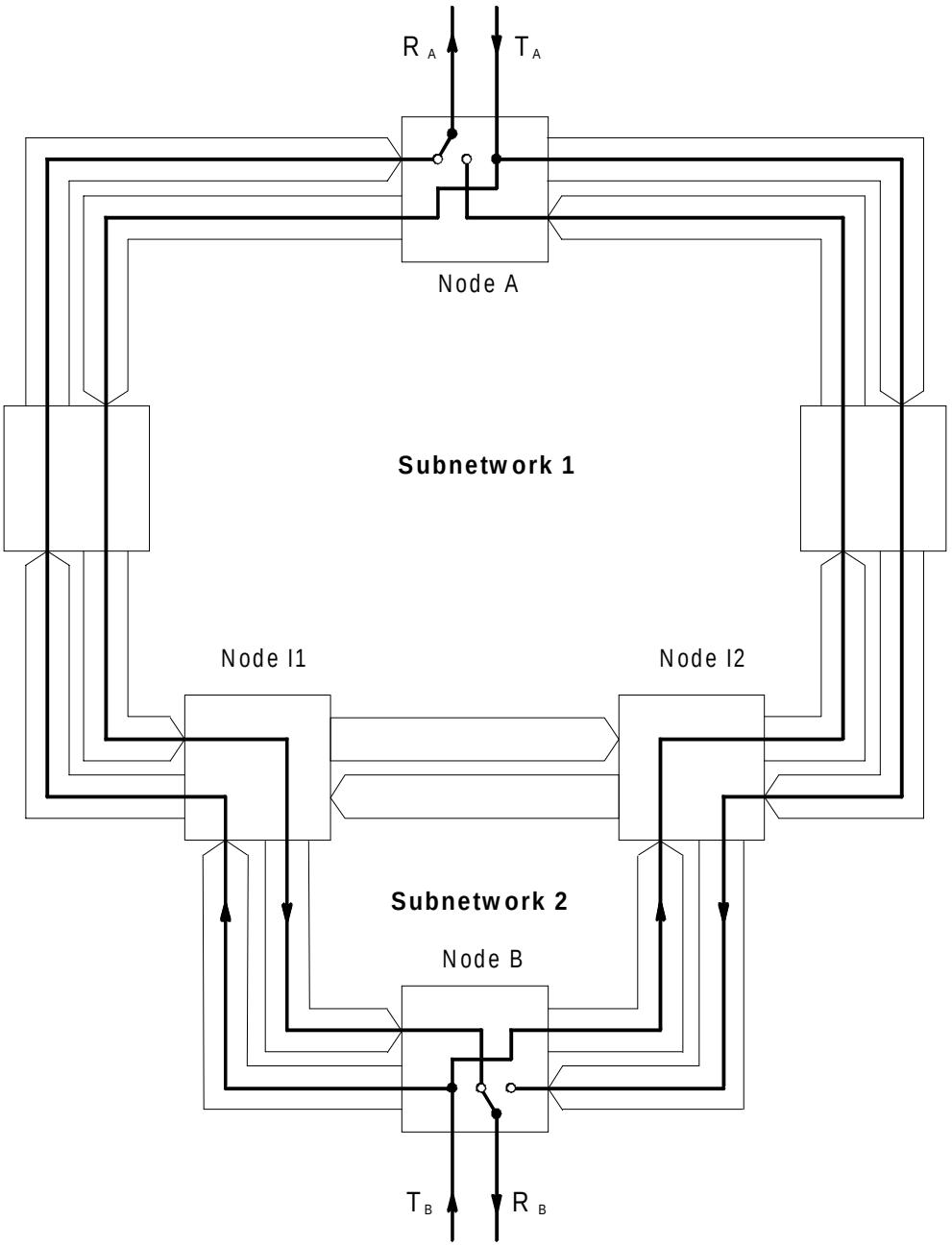

Figure 17c: SNC-P on dual parented access nodes

Figure 17d shows the architecture of dual node interworking between SNC-P protected subnetworks using the drop and continue architecture. This interworking scheme can be classified as a chained intra-layer protection interworking.

For each direction of transmission, the signal is sent from the source node through two diverse subnetwork connections. When each of the two signals reaches an interconnection node, it is dropped at that node and continued onto the other interconnection node, using the drop and continue feature.

Thus, each interconnection node can select from two signals coming from different protecting and protected sub-network connections. The output of the selector in each interconnection node is then sent to the second subnetwork.

Each of the interconnection nodes in the second subnetwork takes its respective signal coming from the first subnetwork and transmits it towards the signal termination node, away from the other interconnection node. Finally, the sink node makes the selection between the two signals from the two directions around the second subnetwork.

Due to the symmetry of this scheme, the primary and secondary interconnection node are completely equivalent.

If protection independence is required, the three following conditions need to be implemented:

a) provision the switches in the nodes with the hold off time required to cope with fibre / equipment delay differences in the working and protected connections in each subnetwork;

b) provision of the switches in the nodes with revertive mode of operation;

c) placing of the switches in the nodes in the default position as shown in figure 17d.

Table 7 shows the conformance of this interconnection scheme with the objectives given in clause 5.

Table 7: Interworking conformance of SNC-P protected subnetworks interconnected by two nodes with drop and continue

Protection interworking objectives	Conformance
Traffic availability	Level 3
Protection independence	Yes
Fault coverage	Conforms to subclauses 5.3.2 and 5.3.3
Subnetworks protected at different layer	Yes
Different protection schemes	NA
Traffic interruption	See subclause 5.6
Operation modes	Single ended Revertive / Non-Revertive
Capacity utilisation	See subclause 5.8

Regarding the example in figure 17d, to improve the degree of protection independence the following apply:

- node A to Node B-direction: use the drop for working channels, in order to reduce the chance that the selector in node B switches due to a failure in the upper network;

- node B to Node A-direction: same principle. Go and Return working traffic can be on the same route in the interconnection architecture;

- this preferred routing leads to the need for revertive operation, if one still wants to restore the preferred routing after particular failure clearance;

- applying a hold-off time can prevent undesirable switching in B due to a failure in the upper SNCP subnetwork and a delay difference in the interconnection architecture. Similar approach for the selector in A.

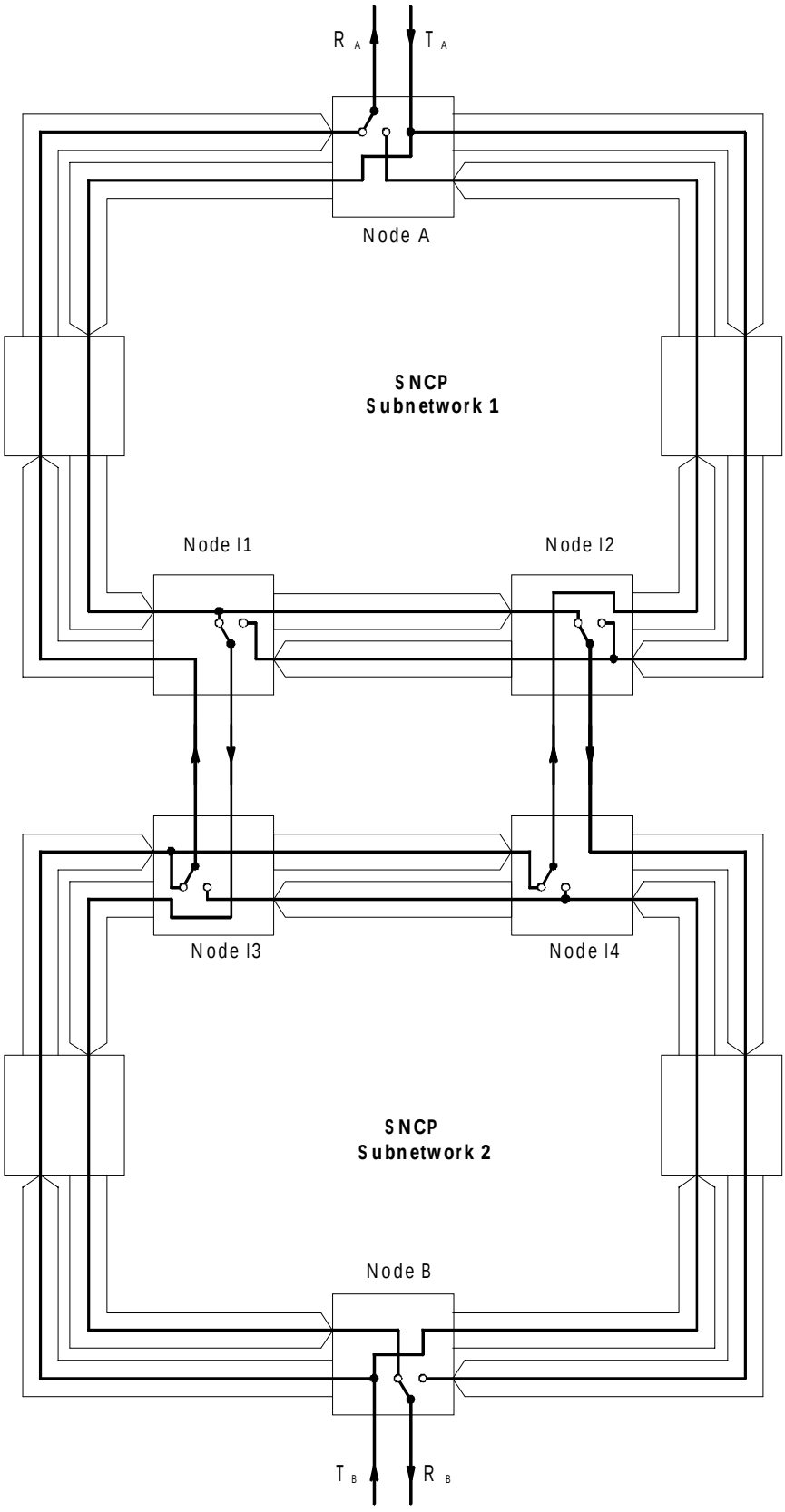

Figure 17d: Default position of selectors to improve protection independence

8 Interworking between different protection schemes

8.1 Dual node interworking between MS-SPRING and SNC-P subnetworks

Figure 18 shows the architecture of dual node interworking between an MS-SPRING subnetwork and a SNC-P subnetwork. This interworking scheme can be classified as a chained inter-layer protection interworking.

For MS-SPRING to SNC-P direction of transmission, the signal is transmitted from the source node to the primary interconnection node, around the side of the ring not crossing the secondary interconnection node. When the signal reaches the primary interconnection node, it is dropped at that node and continued onto the secondary interconnection node using the drop and continue feature. Then the signal is sent at the secondary node to the SNC-P subnetwork. Each of the interconnection nodes in SNC-P subnetwork takes its respective signal from the MS-SPRING subnetwork and transmits it towards the signal termination node away from the other interconnection node. Finally, the sink node makes the selection between the two signals from the two directions around the SNC-P subnetwork.

If protection independence is required, the three following conditions need to be implemented:

a) provision the switches in the nodes with the hold off time required to cope with fibre / equipment delay differences in the working and protected connections in each subnetwork;

b) provision of the switches in the nodes with revertive mode of operation;

c) placing of the switches in the nodes in the default position as shown in figure 18.

Table 8 shows the conformance of this interconnection scheme with the objectives given in clause 5.

Table 8

Protection interworking objectives	Conformance
Traffic availability	Level 3
Protection independence	Yes
Fault coverage	MS-SPRING conforms with 5.3.1 SNC-P conforms to subclauses 5.3.2 and 5.3.3
Subnetworks protected at different layers	Yes
Different protection schemes	Yes
Traffic interruption	See subclause 5.6
Operation modes	MS-SPRING: Dual ended / Revertive SNC-P: Single ended Revertive / Non-revertive
Capacity utilisation	See subclause 5.8

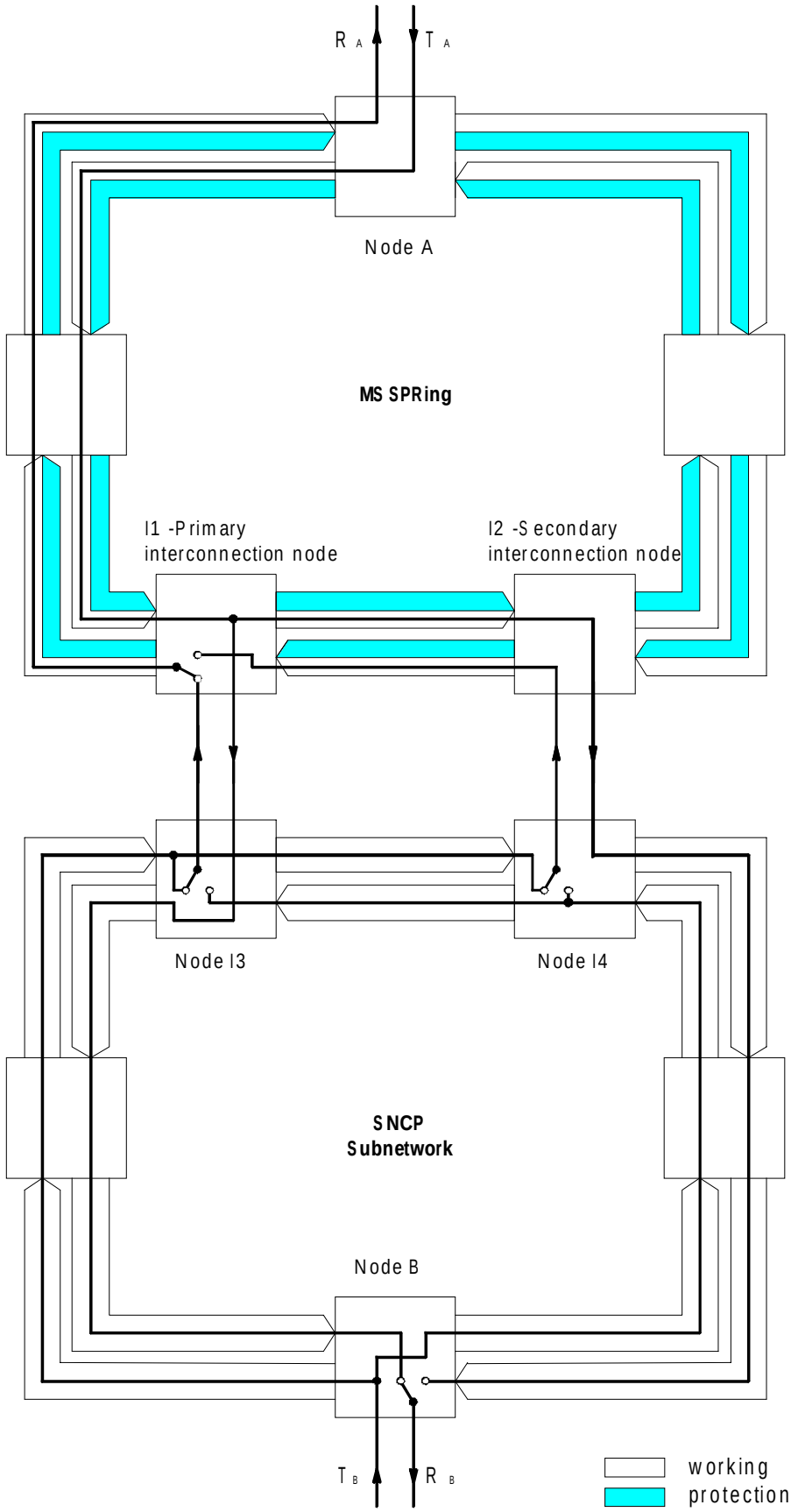

Figure 18: SNC-P and MS-SPRING interconnection using drop and continue

To improve the degree of protection independence the following apply:

- node A to Node B-direction: use the drop for working channels, in order to reduce the chance that the selector in node B switches due to a failure in the upper network;
- node B to Node A-direction: the selectors in I3 and I4 are put on the same side for independence. Go and Return working traffic can be on the same route in the interconnection architecture;
- this preferred routing leads to the need for revertive operation, if one still wants to restore the preferred routing after particular failure clearance.

Applying a hold-off time can prevent undesirable switching in B due to a failure in the upper MS SPRing and a delay difference in the interconnection architecture. In the other direction a hold-off time in node I1 can avoid switching in case of a failure between node B and I3. The failure will be later noticed at the not selected side of the selector in I1, due to transmission delay difference.

8.2 Single Node Interworking between MS-SPRING and SNC-P

Figure 19 illustrates the single node interconnection between MS-SPRING and SNC-P subnetworks. This interworking can be classified as chained inter-layer or chained intra-layer, depending on the layer at which subnetwork connections are protected in the SNC-P subnetwork. Table 9 lists the conformance of this scheme to the protection interworking objectives found in clause 5.

Table 9: Interworking conformance of Single Node MS-SPRING and SNC-P interconnection

Protection interworking objectives	Conformance
Traffic availability	Level 1
Protection independence	Yes
Fault coverage	Conforms with subclause 5.3.1
Subnetworks protected at different layers	Yes
Different protection schemes	Yes
Traffic interruption	See subclause 5.6
Operation modes	- Dual ended / Revertive for MS-SPRING - Single ended Revertive / Non-Revertive for SNC-P
Capacity utilisation	See subclause 5.8

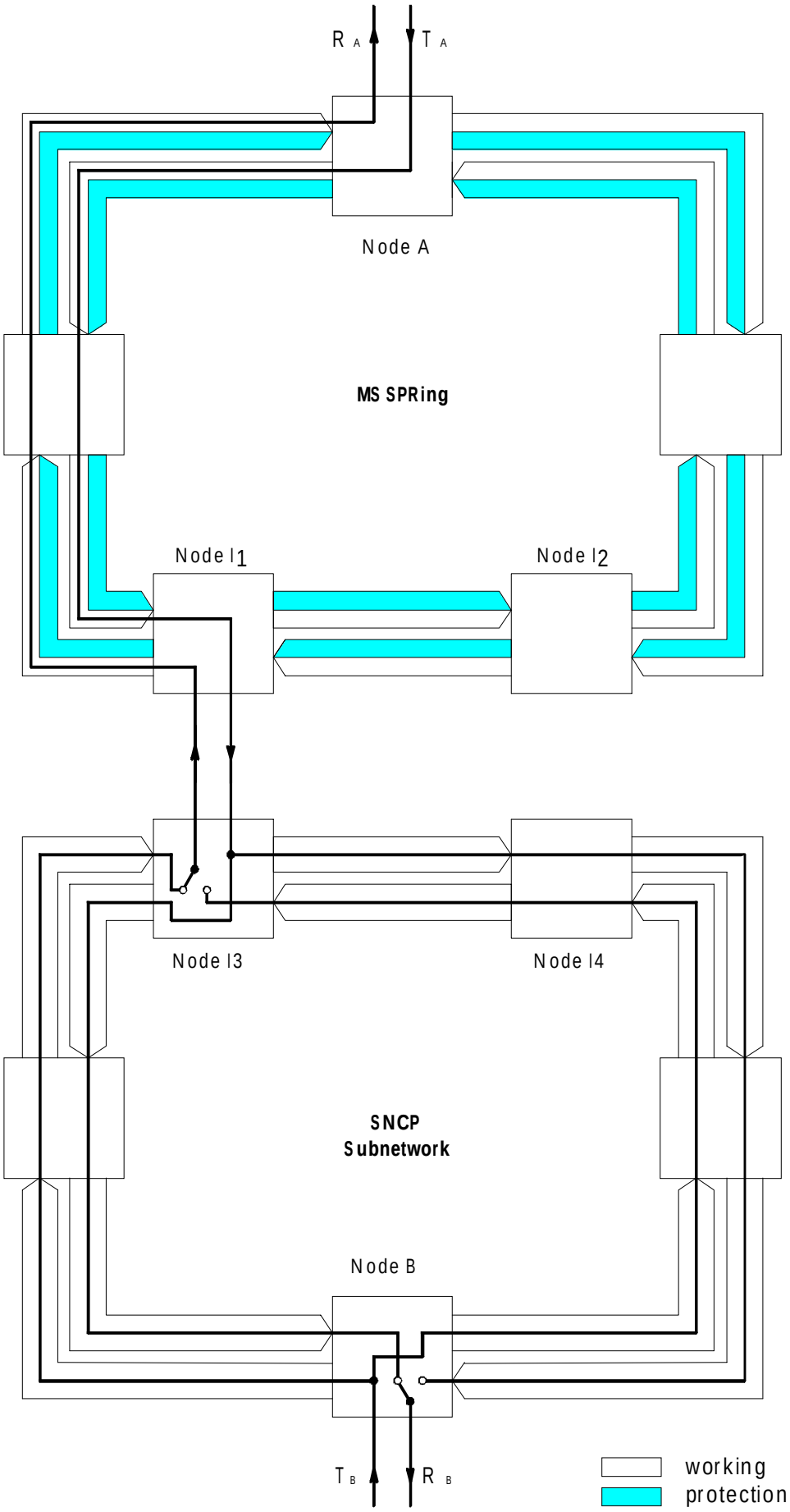

Figure 19: MS-SPRING and SNC-P interconnected by one node

9 Comparison of protection interconnection schemes

Basically there are four types of protection schemes:

- linear MS protection;
- MS SPRING protection;
- linear trail or subnetwork connection protection per subnetwork, SNC-P;
- linear trail or network connection (end-to-end) protection, i.e. NC or Trail Protection.

Interworking between the different types of protection schemes shall be possible. It is foreseen that there are cases in which reliable, i.e. dual node, interconnection between network operator domains and/or subnetworks with different types of protection schemes is required. By applying dual node interconnection no single point of failure will exist. In the remainder of this clause dual node interworking is assumed.

Bandwidth efficiency in the Core Network.

Applying end-to-end network connection protection for a part of the traffic in combination with MS SPRING in the regional or core part of the network will automatically lead to double protection in the part of the network which has ring protection in the MS layer (see figure 20).

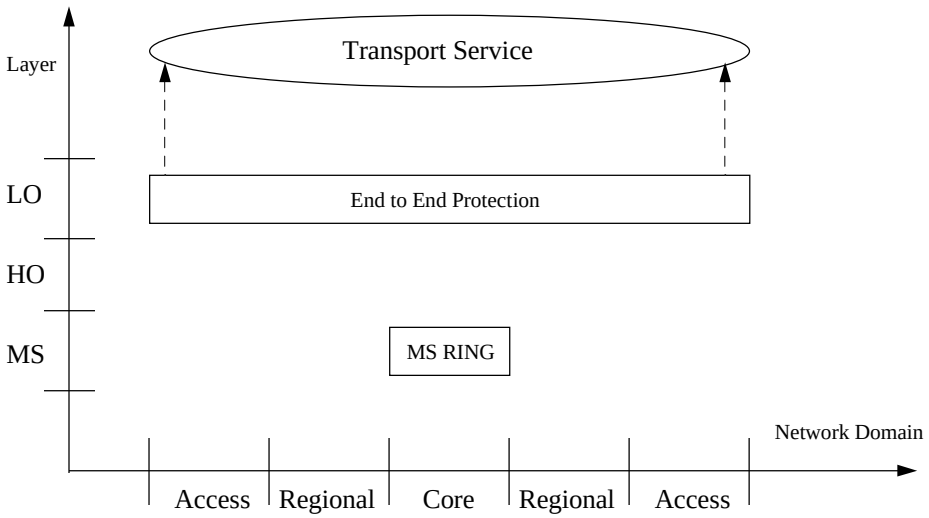

Figure 20: Combining end to end protection with MS-SPRING

Selective SNC-P protection, e.g. in the access or regional part of the network, in combination with MS ring protection, e.g. MS SPRING in the core network, makes it possible to be more efficient in the MS ring protected part, in comparison with selective end-to-end network connection protection. It is desirable to avoid the doubling of required capacity in the MS ring protected part (see figure 21).

The MS-SPRING uses one route per traffic direction. Protection is accomplished by looping around the ring. SNC-P is based on having, in each direction, two diverse routes and a selector. The dual node architecture with drop and continue function and SNC protection selector can be used to make these two schemes interwork. Note that in all cases of interconnection of a subnetwork , with linear protection for that subnetwork (SNC-P), with a ring (MS-SPRING) protected subnetwork some form of drop and continue function and SNC selector is needed. By applying the drop and continue function and SNC protection selector the doubling of required protection capacity in the core network will be avoided.

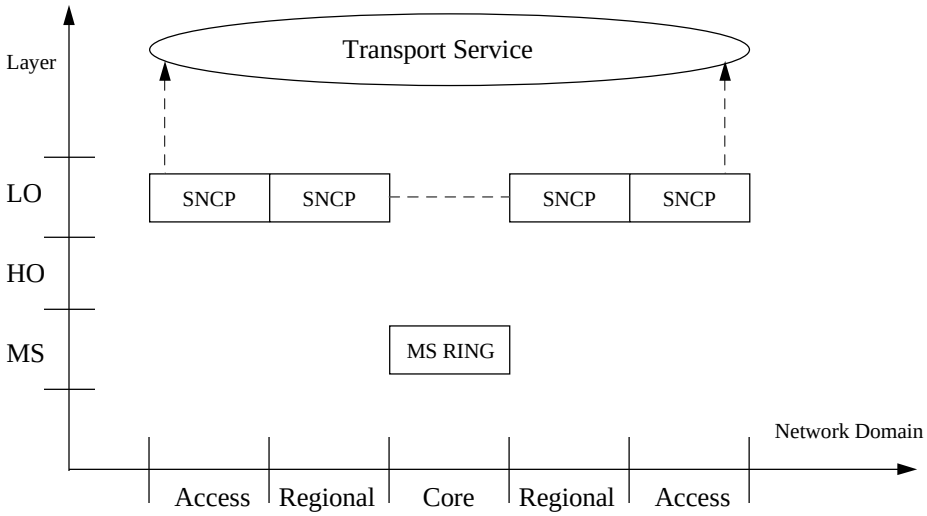

Figure 21: Combining SNC-P and MS-SPRING with Drop and Continue

10 Network applications

10.1 Interconnecting ring subnetworks with 4/3/1 Digital Cross-Connects

As in any network made of interconnected subnetworks, inter subnetwork traffic issues have important implications on the overall network architecture.

The network application described in this suclause addresses dual node interconnected subnetworks using drop and continue to achieve high availability of traffic. Furthermore, the subnetworks are considered to be protected and administered at different layers. As an example, a number of access subnetworks administered at LO-VC are interconnected to a metropolitan subnetwork administered and protected at HO-VC. The interconnecting nodes include 4/3/1 DXCs to provide a number of functions, some of these are:

- to interconnect the rings and provide local access;
- to provide network traffic flexibility and grooming;
- to facilitate end to end circuit set up from a centralised operating system.

The metropolitan subnetwork is protected by using MS-SPRING and the access subnetworks are protected by using SNC-P. Although the drop and continue is implemented differently in either type of protected subnetworks, they are compatible with each other.

Figure 22 shows the network application where 4/3/1s DXCs are used in the interconnecting nodes. These cross-connects interconnect traffic in an entire office, not just traffic within one subnetwork. As the majority of the traffic is switched 2 Mbit/s , the network shall be administered at the LO-VC layer. As traffic moves through the subnetworks, some is dropped at intermediate nodes and the rest is sent on to distant subnetworks and nodes. Therefore traffic that is connected between subnetworks, is composed of traffic to be dropped from that ring and traffic to be forwarded on to another ring. In this example three rings are interconnected at nodes A and B, these are the sites showing the need for cross-connects to achieve flexible traffic connectivity. Although cables could be run from each system to each other, there is a lot of inflexibility in hardwiring tributaries. Hardwiring limits the capacity between any two subnetworks since

there are a limited number of tributaries available. A cross-connect on the other hand can have the entire tributary capacity from each system cabled to it and provide non-blocking interconnection between each subnetwork.

From an economical standpoint, it is desirable to have subnetworks administered at the highest layer possible, generally VC-4, but traffic to be dropped is generally VC-12 based. Therefore if some VC-12 administration is required in a subnetwork, it would be better to have VC-12s on only one VC-4, rather than on all of them. The 4/3/1 DXC can groom all VC-12s that are dropped in a node, into a VC-4, which is then the only VC-4 that requires VC-12 processing.

As in any other example of HO-VC / LO-VC interworking, some precautions are needed when configuring the HO-VC and LO-VC trail trace identifiers.

It is recommended to disable the HO-VC TTI mismatch detection in the HO-VC drop and continue interconnecting nodes and in those nodes where the HO-VC is terminated. The LO-VC contained in these HO-VCs will be left with TIM detection enabled. HO-VC TIM detection will be left enabled for HO-VC not carrying LO-VCs. This will insure complete trail connectivity supervision at both the LO-VC and HO-VC layers.

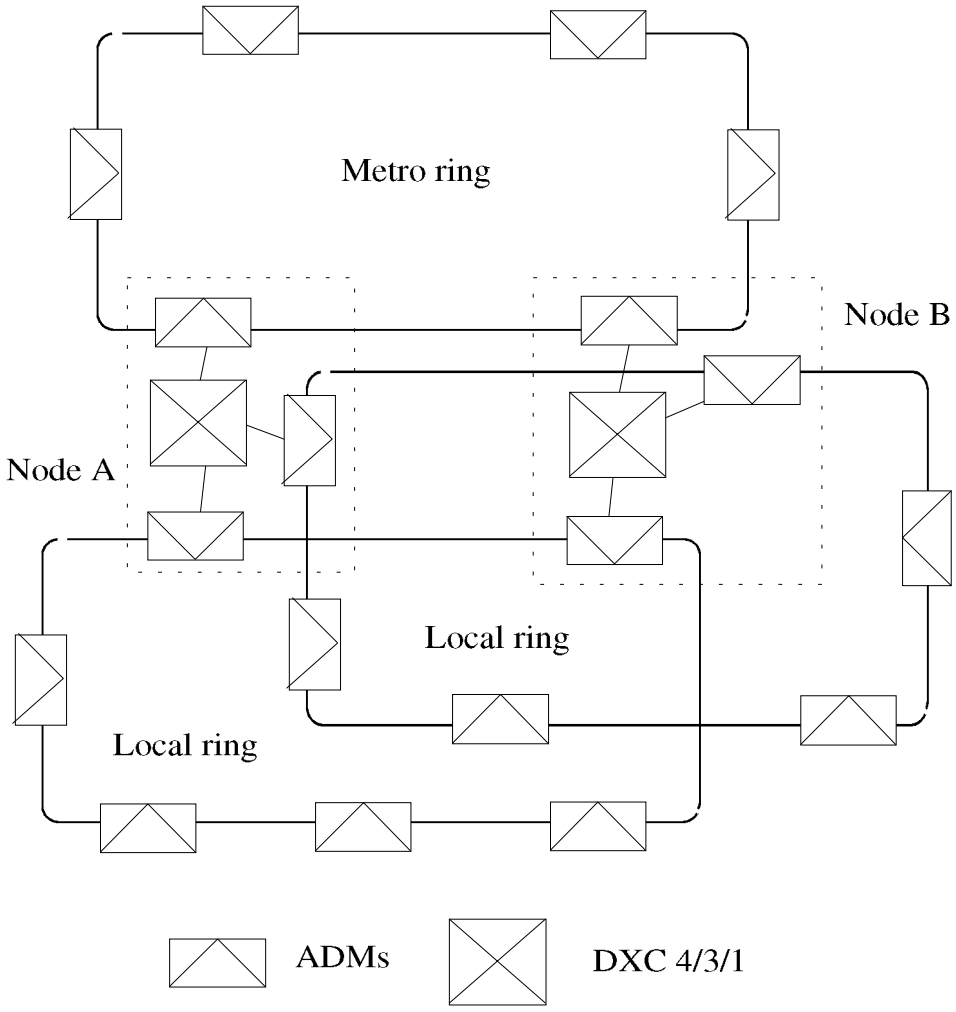

Figure 22

10.2 Stacked ring configuration

Figure 23 shows an example of a stacked ring configuration. There are two STM-16 MS-SPRINGs which interwork through two interconnected hub nodes (Nodes 1 and 2).

The nodes in each ring serve the same geographical region.

The interworking arrangement allows interconnectivity between nodes in different rings building up to a 32 node subnetwork.

This configuration is an example of chained inter-layer protection. Notice that the rings nodes and traffic load have to be arranged to minimise interring traffic. The additional traffic between node 1 and node 2 may alter the capabilities of the single ring to route intra-ring traffic.

Note that if drop and continue is used, the maximum interring bandwidth is equal to 8 VC-4s for STM-16 MS-SPRINGs minus the amount of VC-4s used already for intra-ring traffic between nodes 1 and 2.

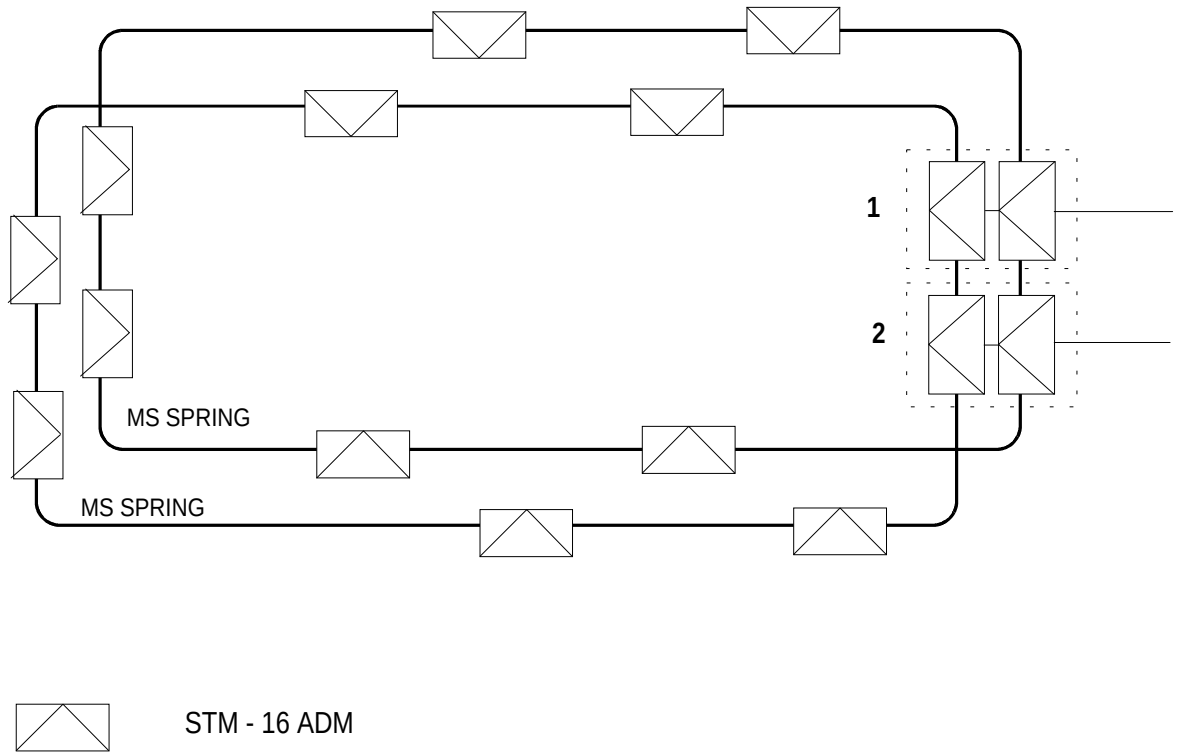

Figure 23: Two MS SPRings in stacked ring configuration

10.3 Interworking of protection between networks belonging to different operators

When network operators want to interconnect their networks the performance of connections spanning the networks may be enhanced by interworking between the protection mechanisms in each network.

For this application any combination of protection mechanisms may be used.

The protection mechanism in each network may be different or two or more networks may have the same protection mechanism. Assuming the operators want to protect to the edge of their network, the basic architecture will be chained.

The architecture may be inter-layer or intra-layer.

Figure 24 shows the general situation for the interconnection of two operators' networks. A hybrid architecture may also exist, for example where there is also trail protection spanning both operators' networks.

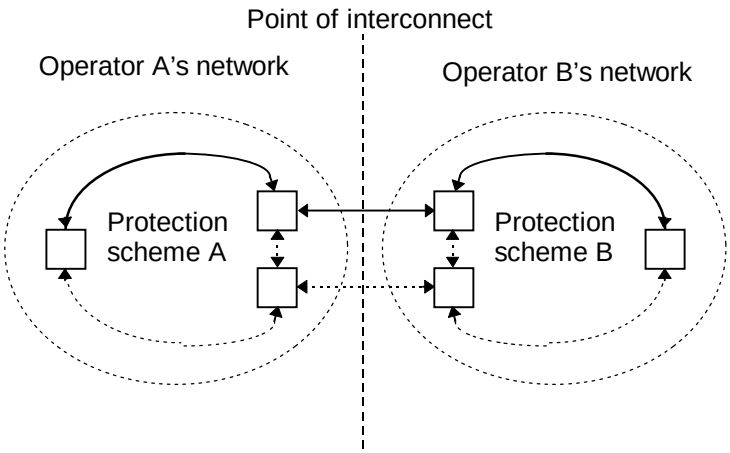

Figure 24: Interworking of protection between networks belonging to different operators: chained architecture

Figure 25 shows a specific example of a situation with a multi-operator where both operators use MS-SPRINGs and a protected LO VC (trail or network connection) spans both networks.

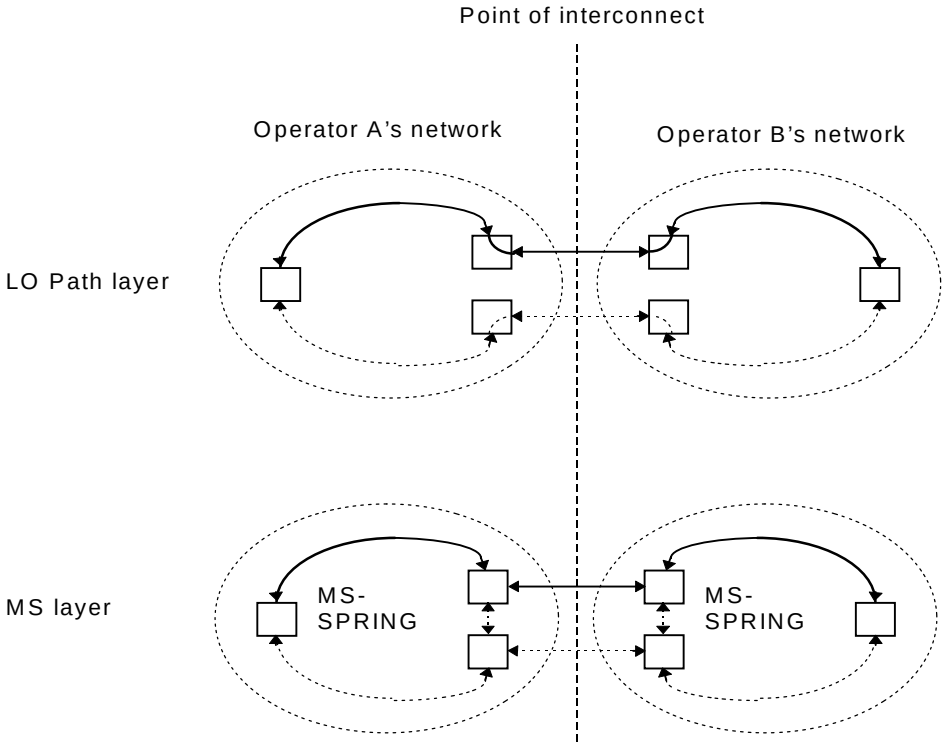

Figure 25: An example of interworking of protection between networks belonging to different operators

11 Conclusions and recommendations

Network survivability is an important factor in the design and evaluation of SDH transport networks as more traffic is carried by the same infrastructure and more telecom services customers will be served by ever bigger central offices.

Also customers now expect a higher level of reliability. In the present document, some methods on how to extend the traffic availability performance from single subnetworks to multiple interconnected subnetworks are given.

One important conclusion is that by partitioning networks in a number of independently protected subnetworks, the overall traffic availability increases as the network can tolerate simultaneous network faults and maintenance operations in different subnetworks. This can be achieved by single node interconnecting mechanisms or dual node interconnecting mechanisms. The dual node interconnecting architecture has the advantage that it avoids a single point of failure in the network. If in addition the drop and continue is used, the network can withstand simultaneous failures in both subnetworks.

The drop and continue architecture is incompatible with VC trail protection due to the appearance of trace identifier mismatch problems in the trail termination points when the switches in the interconnecting nodes operate as a consequence of a network failure.

A key objective is to improve the degree of protection independence so that a failure in one subnetwork does not lead to switching events in other subnetworks.

This is considered to be important by operators because it could be confusing for the centralised operations and maintenance system in one subnetwork domain to interpret protection switching event reports from NEs in its subnetwork where no real fault has occurred. Either single node or dual node interconnection with drop and continue can isolate switching effects to the subnetwork where the failure occurred and hence provide protection independence. For the interconnection of subnetworks in which one or both use SNC-P, then the following mechanisms are needed to give protection independence:

- provision the switches in the nodes with the hold off time required to cope with delay differences in the working and protected subnetwork connections in each subnetwork;
- provision of the switches in the nodes with revertive mode of operation;
- using pre-defined default positions in the selectors.

Recommendations:

The final recommendations that emerge from the present document are summarised below:

1) MS SPRing - MS SPRing interworking:
   - suitable for core networks based on MS SPRings;
   - use drop and continue architecture.
2) SNC-P - SNC-P interworking:
   - suitable for core networks which have been designed to use SNC-P, or access networks;
   - the preferred interconnection architecture depends on the level of availability required and the size and topology of the network.
3) VC Trail protection:
   - dual node interconnection to provide a virtual ring;
   - applicable for dual parenting of customer sites.
4) End to end protection, e.g. for leased line services which require ultra-high availability:
   - use end to end HO/LO Network Connection Protection or HO/LO VC trail protection in addition to other subnetwork schemes deployed in the intervening network.

5) MS SPRing or SNC-P in conjunction with HO VC restoration at the lower network layers:

- provides protection against multiple failures;
- to provide capacity management / traffic routing capability. Cross connect capability required at the interconnection nodes.

Summary of interworking schemes:

Table 10: Interworking between subnetworks using the same protection scheme

Protection schemes	Interconnection architecture	Level of traffic availability	Modes of operation supported
Two MS SPRings	Single node	Level 1	Dual Ended Revertive
Two MS SPRings	Dual node - virtual ring	NA	NA
Two MS SPRings	Dual node - drop and continue	Level 3	Dual Ended Revertive
Two VC Trail subnetworks	Single node	Level 1	Dual Ended/Single Ended Revertive/non revertive
Two VC Trail subnetworks	Dual node - virtual ring	Level 2	Dual Ended/Single Ended Revertive/non revertive
Two VC Trail subnetworks	Dual node - drop and continue	NA	NA
Two SNC-P subnetworks	Single node	Level 1	Single Ended Revertive/non revertive
Two SNC-P subnetworks	Dual node - virtual ring	Level 2	Single Ended Revertive/non revertive
Two SNC-P subnetworks	Dual node - drop and continue	Level 3	Single Ended Revertive/non revertive

Table 11: Interworking between subnetworks using different protection schemes

MS SPRing - SNC-P	Single node	Level 1	**MS SPRing:** Dual Ended, Revertive **SNC-P:** Single Ended, Revertive/non revertive
MS SPRing - SNC-P	Dual node - virtual ring	NA	NA
MS SPRing - SNC-P	Dual node - drop and continue	Level 3	**MS SPRing:** Dual Ended, Revertive **SNC-P:** Single Ended, Revertive/non revertive

NA = Not Applicable

Annex A

A.1 Introduction

A.1.1 Protection independence

This annex contains four failure conditions for each of the possible dual node drop and continue interconnection schemes between SNCP and MS-SPRINGs (see figure A.1).

In this examples it is assumed that in failure conditions, protection switching schemes have a certain priority when interconnected. First the we take in consideration the ring automatic protection schemes like MS SPRing and then the drop and continue SNC switches present in the interconnection and end nodes.

It is assumed that in order to get protection independence in dual node interconnection hold off time, SNC selectors position and revertive mode of operation are used.

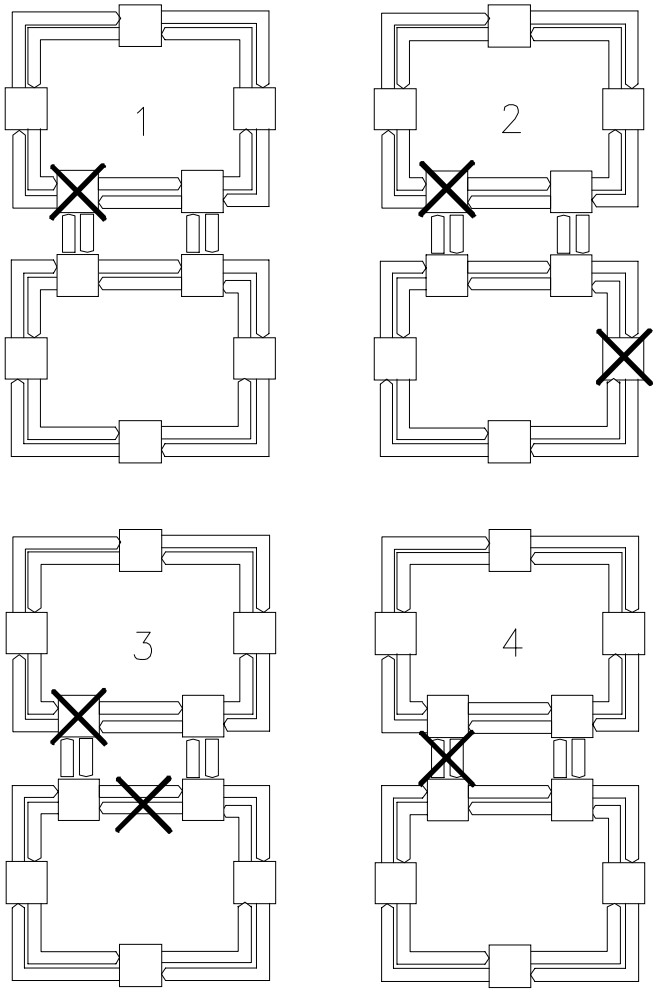

Figure A.1: Failure conditions

A.1.2 Routing

In the examples of this annex, communication is established using uniform routing in rings, interconnection links and subnetworks. In figure A.2 the routing in normal conditions is shown.

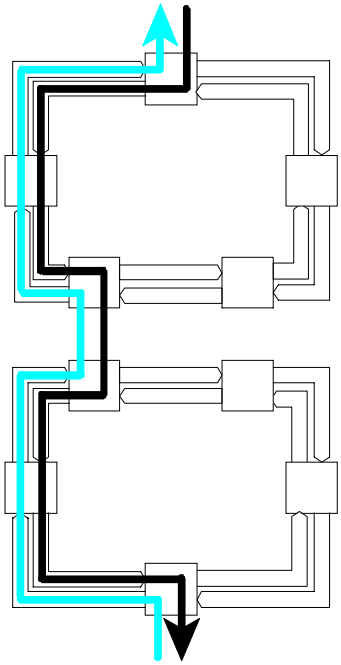

Figure A.2: Routing

A.2 MS-SPRING to SNCP dual node drop and continue subnetwork interconnection

A.2.1 Normal conditions

Figure A.3 shows a subnetwork interconnection scheme between a MS -SPRING and a SNCP.

Both subnetworks are dual node interconnected by two links and SNC drop and continue switches are needed in the interconnection nodes The communication is uniformly routed.

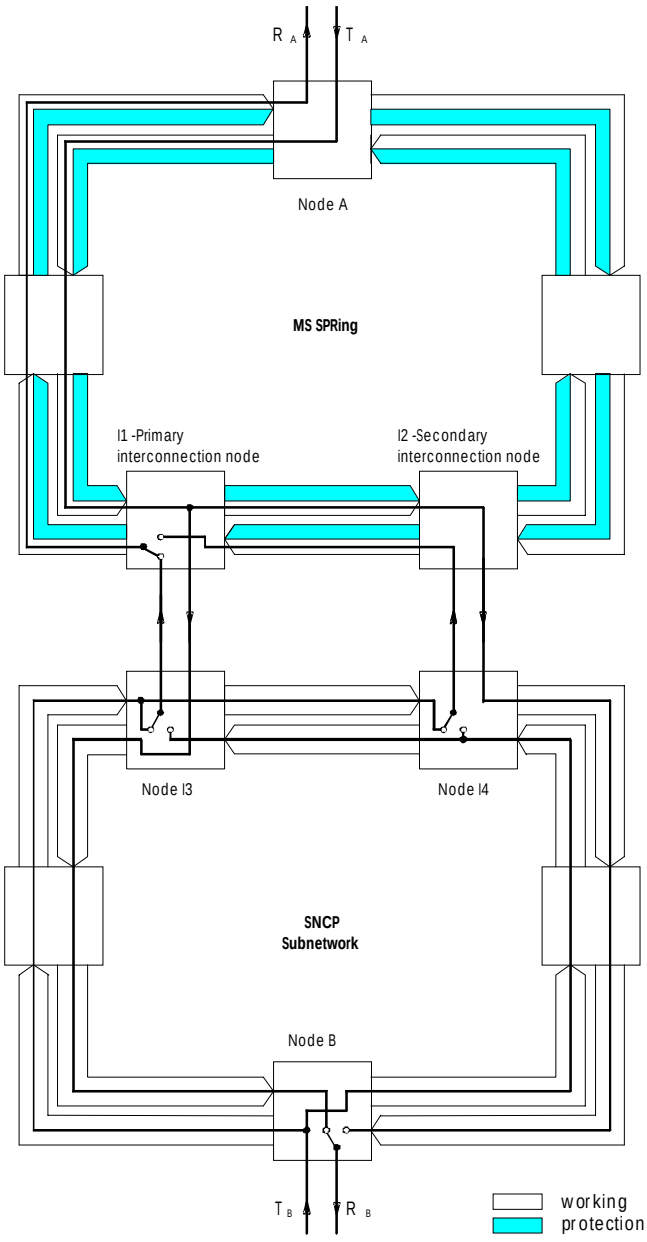

Figure A.3

A.2.2 Failure in MS SPRing Primary interconnection node I1

In figure A.4 the MS SPRing recovers with bridge and switching actions performed in the adjacent nodes to the failure. The SNC switch present in the end node B switches and maintains Node A to node B communication through the interconnection node I4.

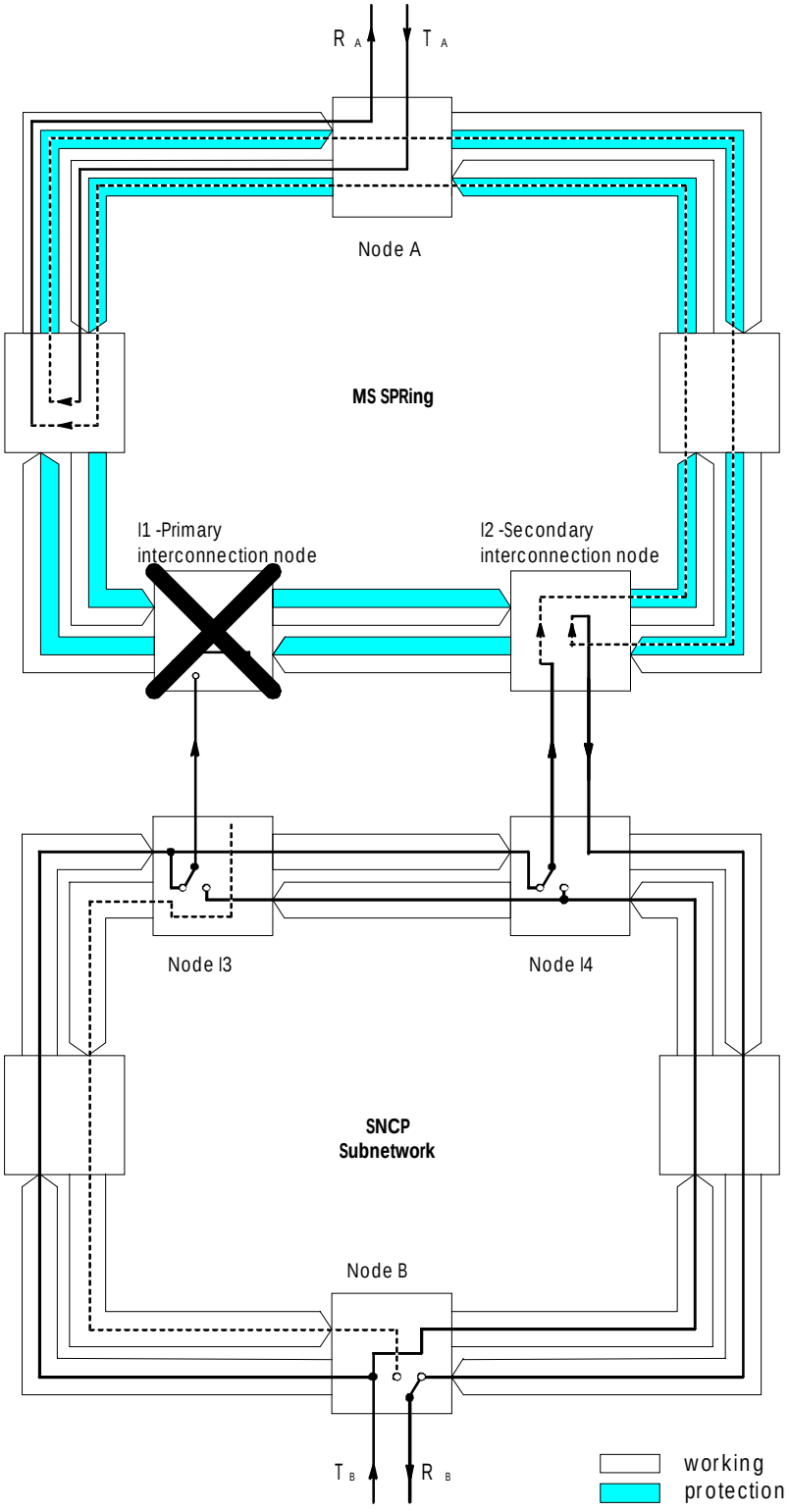

Figure A.4

A.2.3 Failure in MS SPRing Primary interconnection node I1. Node failure in SNCP subnetwork

In figure A.5 the MS SPRing recovers with bridge and switching actions performed in the adjacent nodes to the failure. However with this kind of multiple failure in SNCP interconnections using drop and continue, **communication from node A to node B is lost.**

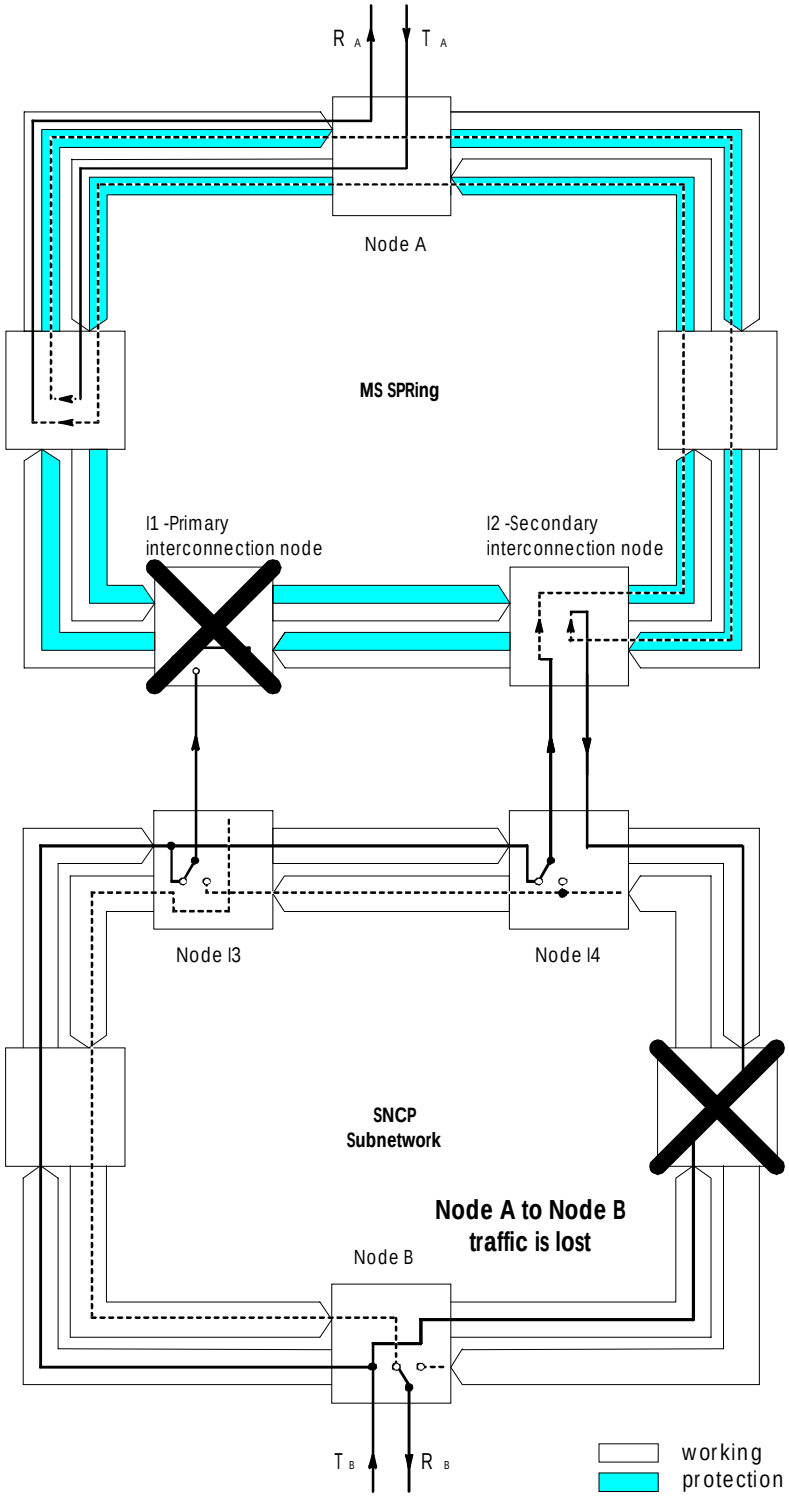

Figure A.5

A.2.4 Failure in MS SPRing Primary interconnection node I1. Cable cut in SNCP subnetwork

In figure A.6 the MS SPRing recovers with bridge and switching actions performed in the adjacent nodes to the failure. In the SNCP subnetwork both SNC switches present in node I4 and end node B switch.

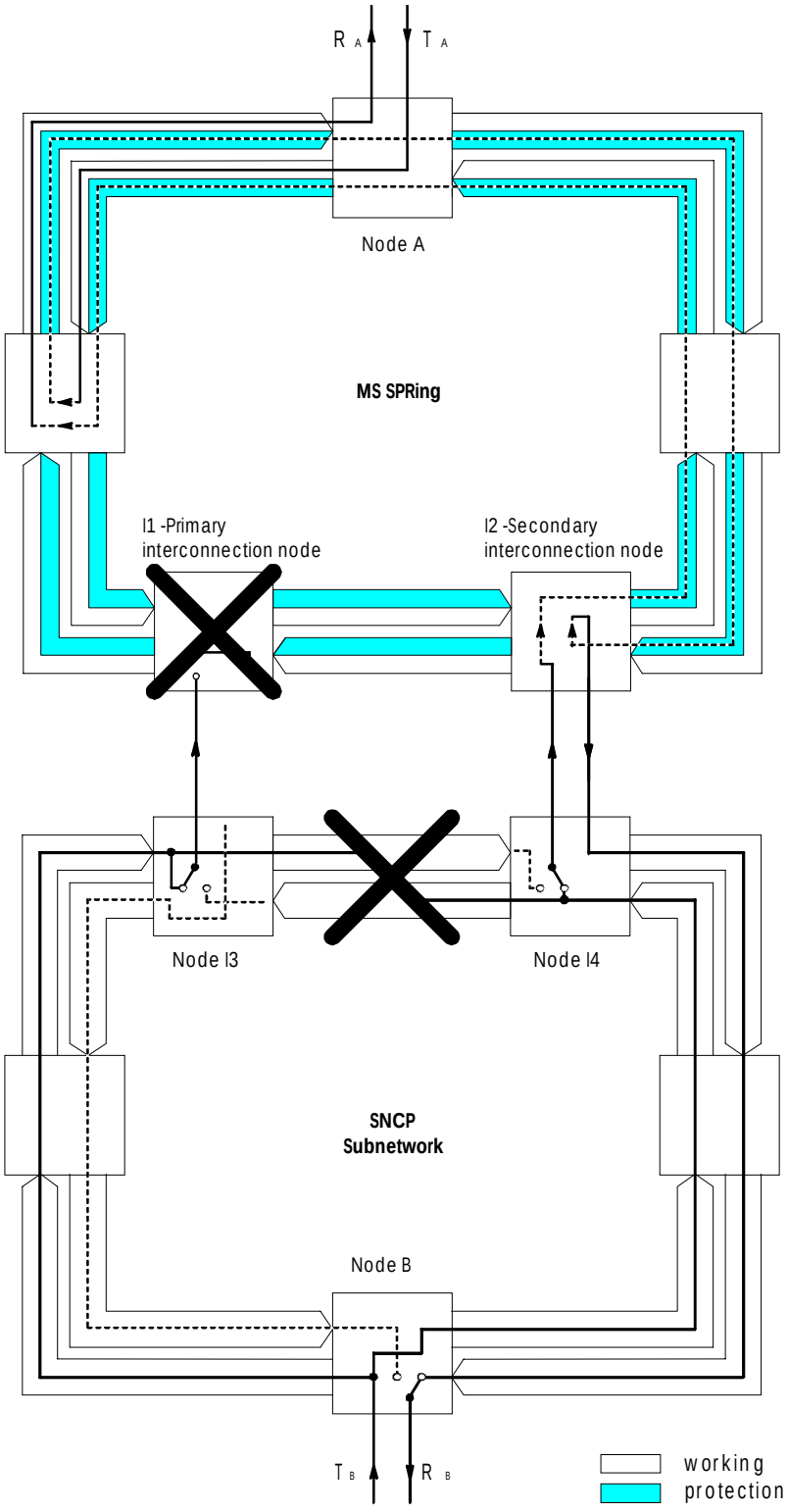

Figure A.6

A.2.5 Failure in one interconnection link

In figure A.7 the SNC switch present in primary interconnection node I1 switches in order to maintain the communication from node B to node A by the other interconnection link. The SNC switch present in the end node B switches and maintains Node A to node B communication trough the interconnection node I4.

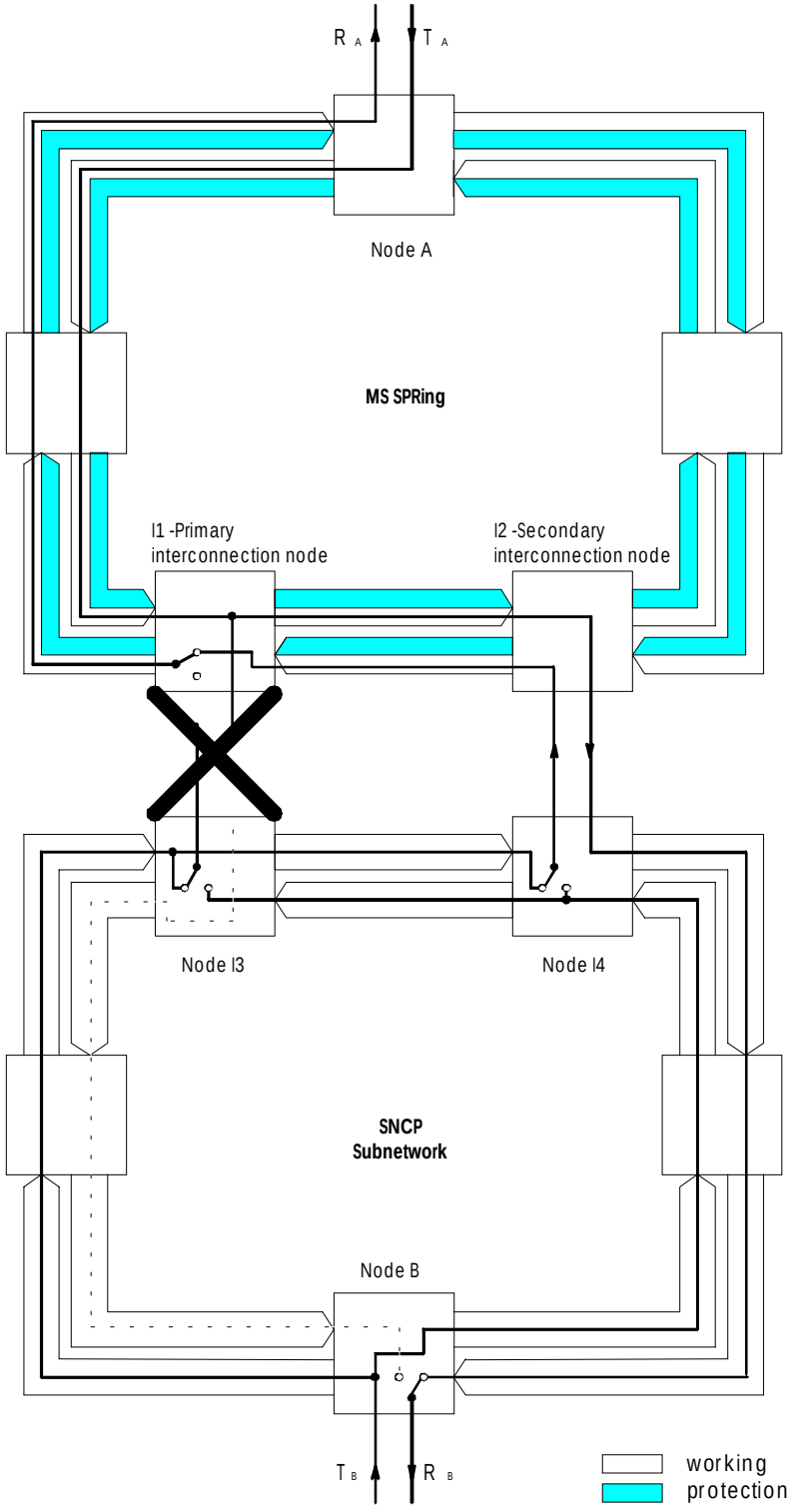

Figure A.7

A.3 MS-SPRING to MS-SPRING dual node drop and continue subnetwork interconnection

A.3.1 Normal conditions

Figure A.8 shows a subnetwork interconnection scheme between two MS SPRINGs.

Both rings are dual node interconnected by two links and SNC drop and continue switches are needed in the interconnection nodes The communication is uniformly routed.

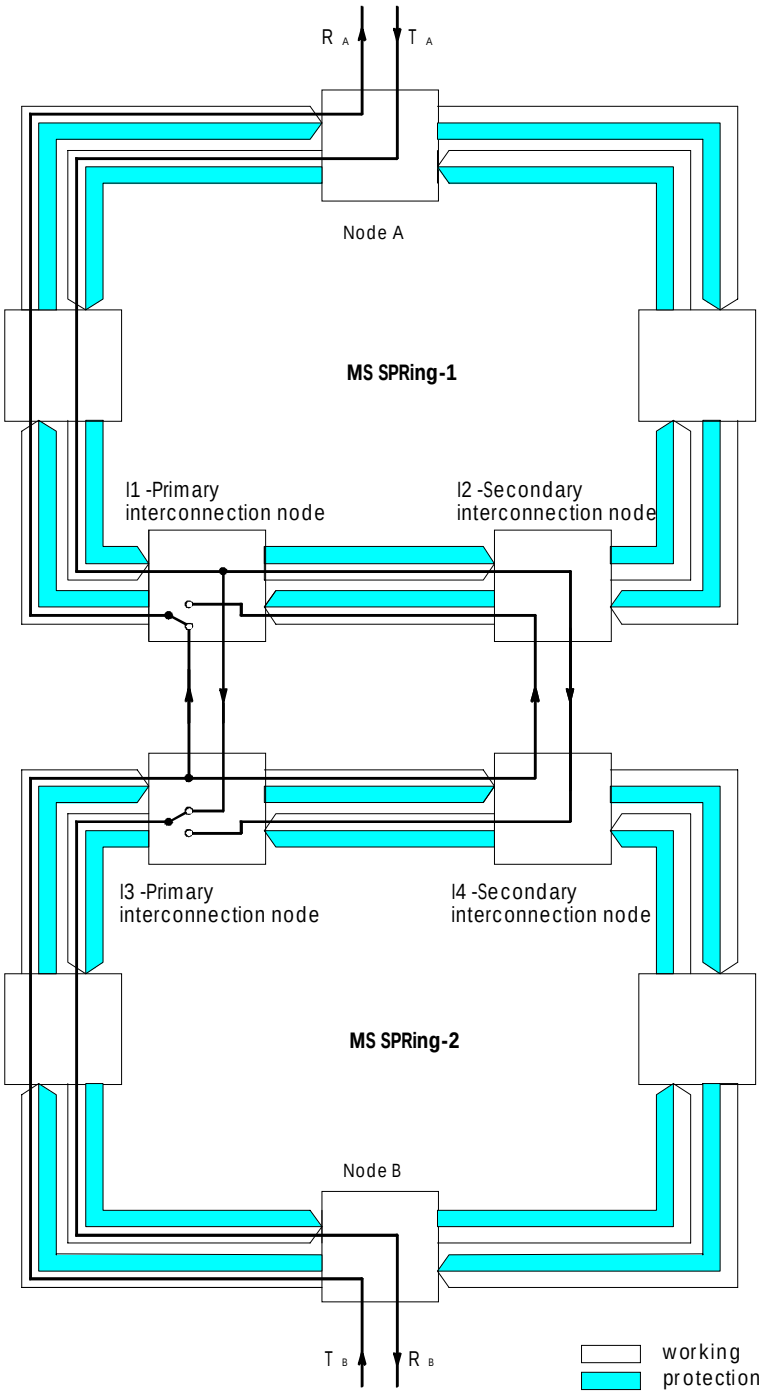

Figure A.8

A.3.2 Failure in MS SPRing 1 Primary interconnection node I1

In figure A.9 the MS SPRing 1 recovers with bridge and switching actions performed in the adjacent nodes to the failure.

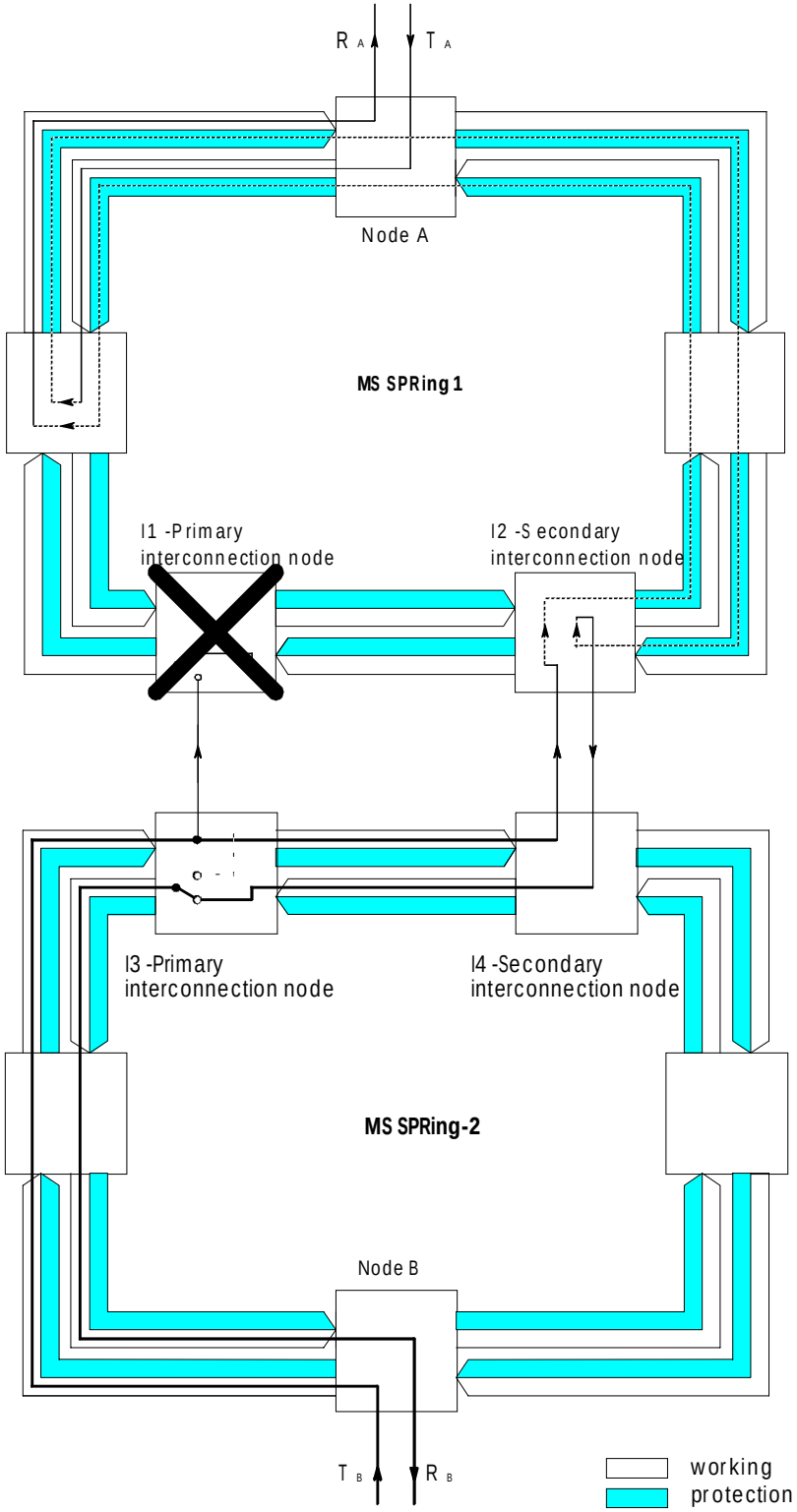

Figure A.9

A.3.3 Failure in MS SPRing 1 Primary interconnection node I1. Node failure in MS SPRing 2

In figure A.10 the MS SPRing 1 recovers with bridge and switching actions performed in the adjacent nodes to the failure. In MS-SPRINGs 2 the failure does not affect the shown path.

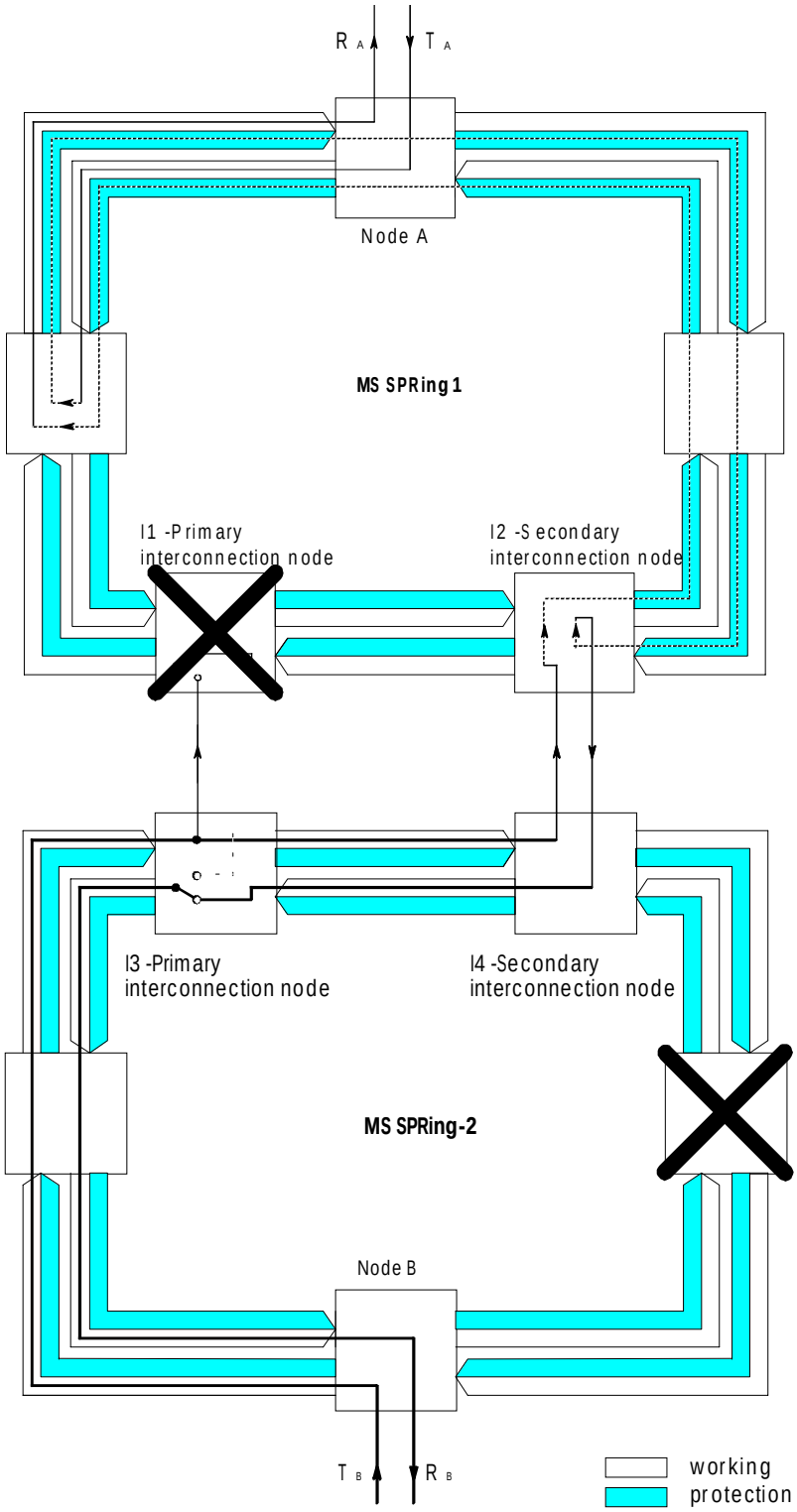

Figure 10

A.3.4 Failure in MS SPRing 1 Primary interconnection node I1. Cable cut in MS SPRing 2

In figure A.11 both MS SPRings recover with bridge and switching actions performed in the adjacent nodes to the failure.

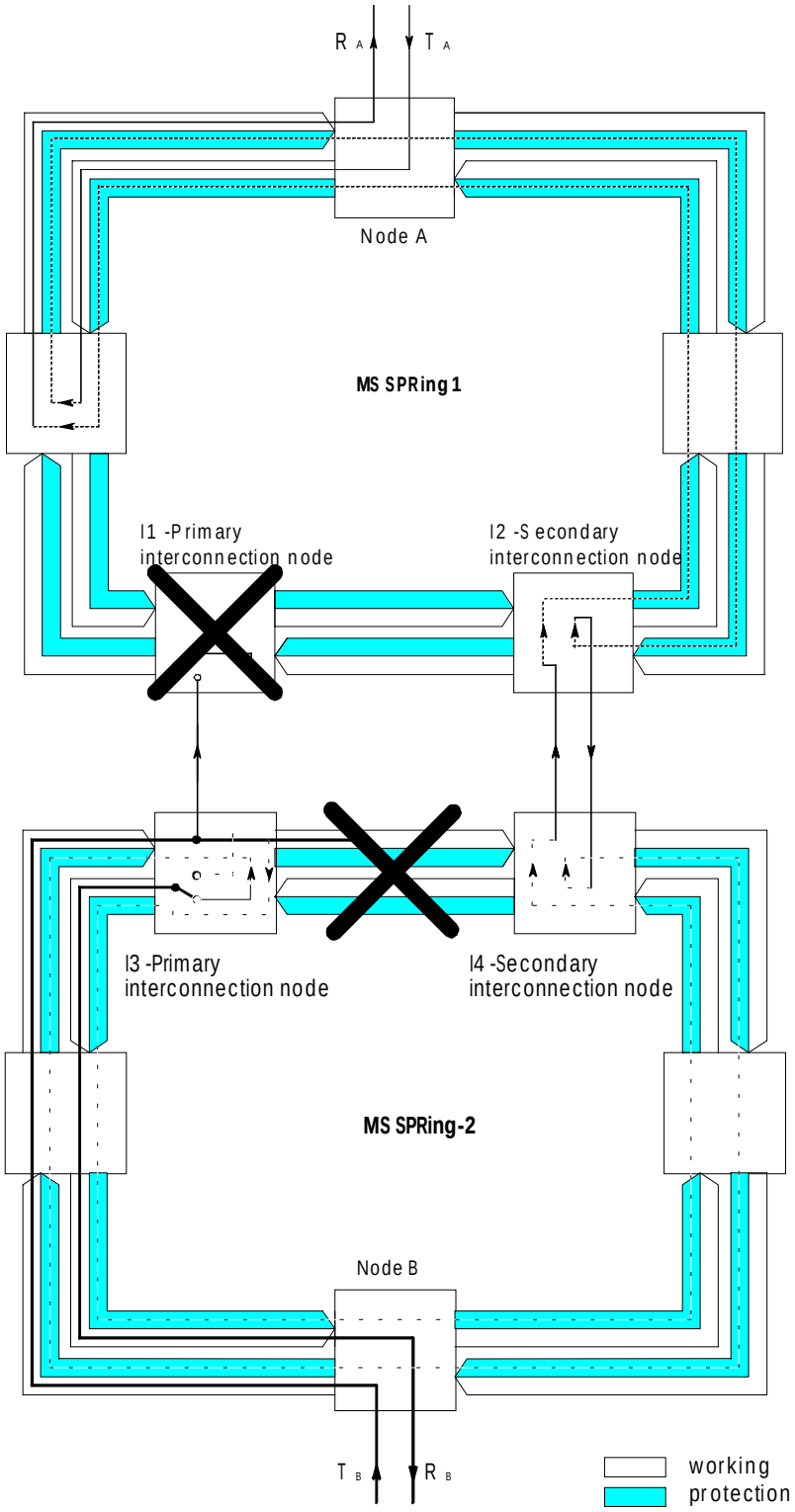

Figure A.11

A.3.5 Failure in one interconnection link

In figure A.12 the SNC switches present in both I1 and I3 interconnection nodes switch in order to maintain the communication by the other interconnection link.

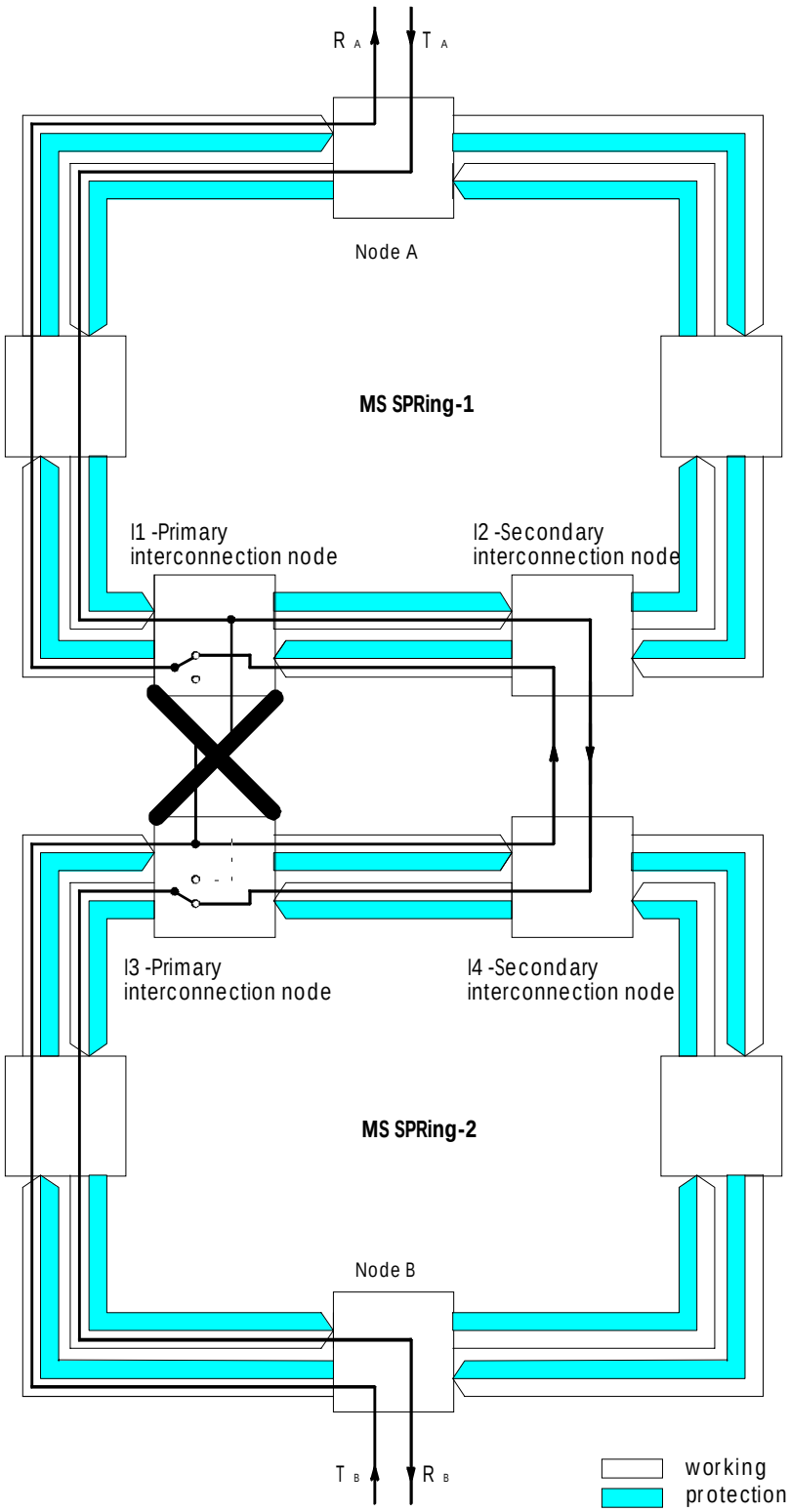

Figure A.12

A.4 SNCP to SNCP dual node drop and continue subnetwork interconnection

A.4.1 Normal conditions

Figure A.13 shows a subnetwork interconnection scheme between two SNCPs.

Both SNCPs are dual node interconnected by two links and SNC drop and continue switches are needed in the interconnection nodes The communication is uniformly routed.

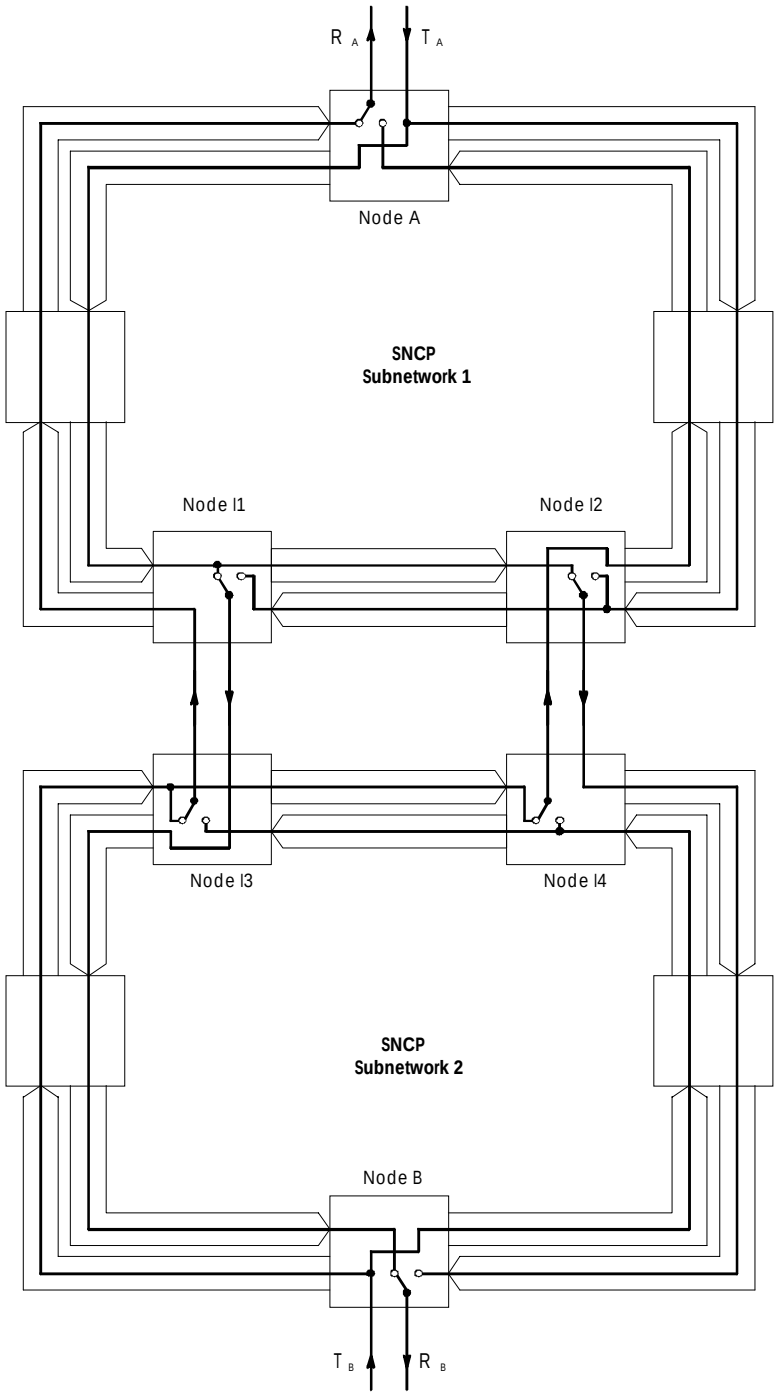

Figure A.13

A.4.2 Failure in SNCP subnetwork 1 interconnection node I1

In figure A.14 the SNC switches present in interconnection node I2 and in the end node B switch in order to maintain the communication from node A to node B. End node A switches in order to maintain the communication from node B to node A.

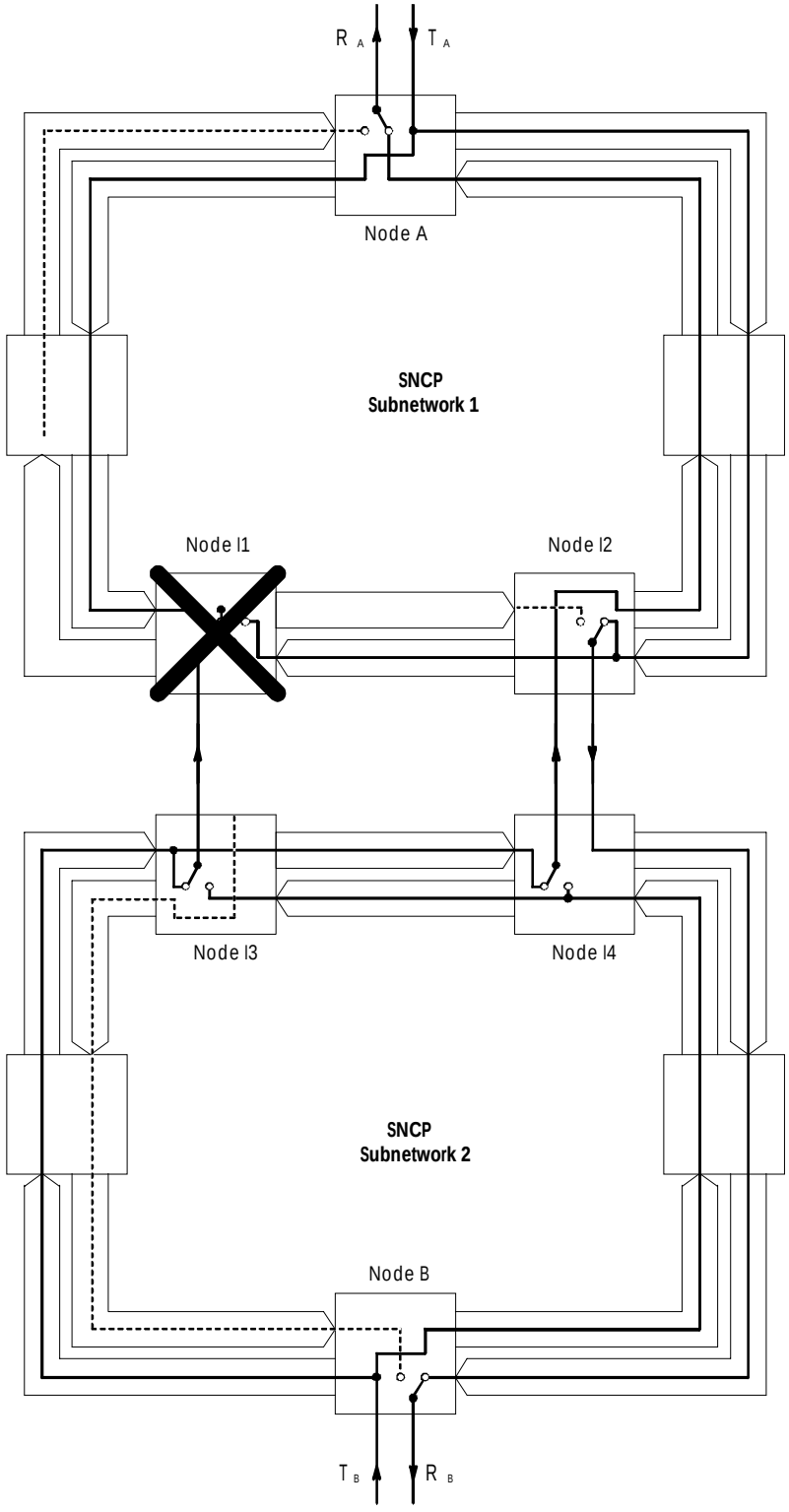

Figure A.14

A.4.3 Failure in SNCP subnetwork 1 interconnection node I1. Node failure in SNCP subnetwork 2

In figure A.15, the end node A switches in order to maintain the communication from node B to node A.

The SNC present in interconnection node I2 switches in order to maintain the communication from node A to node B. However with this kind of multiple failure in SNCP interconnection using drop and continue, **communication from node A to node B is lost.**

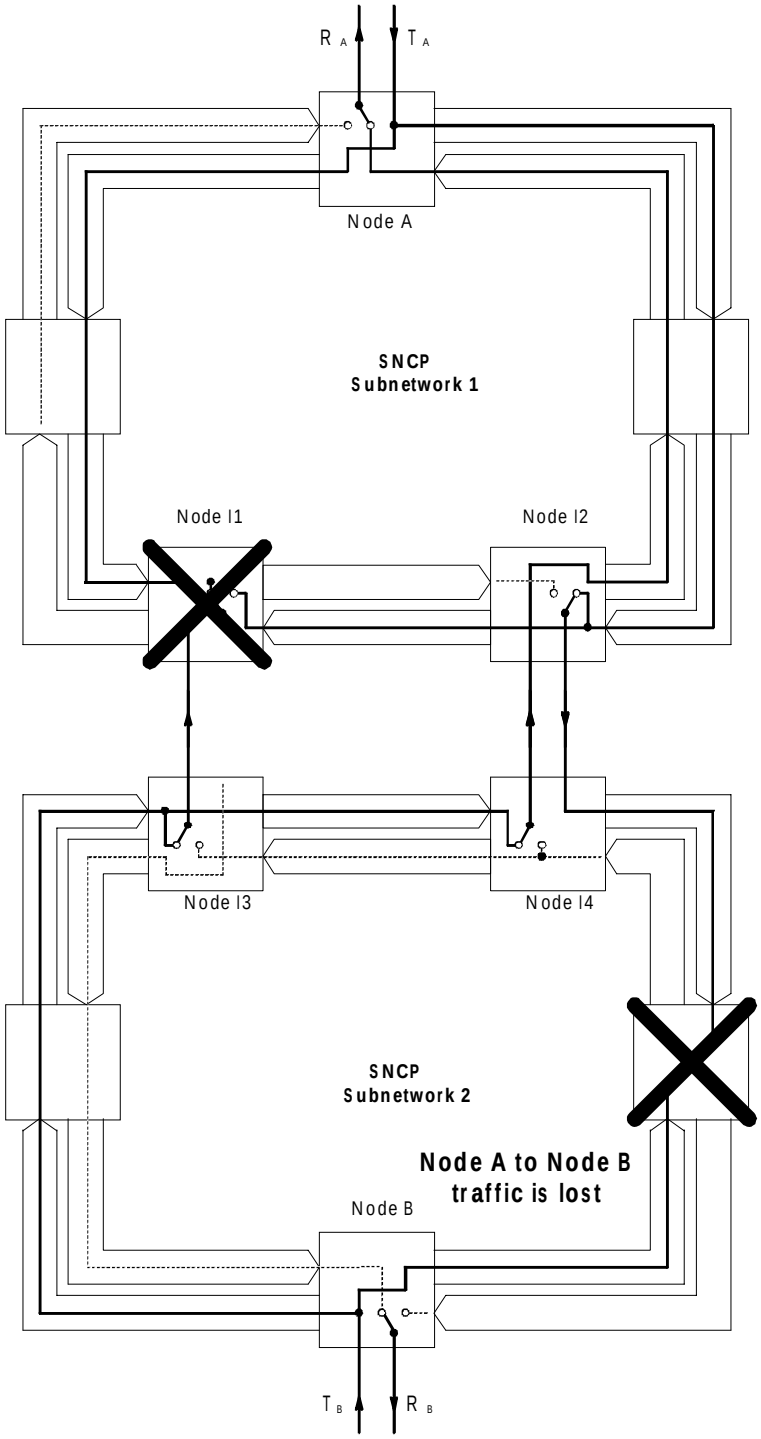

Figure A.15

A.4.4 Failure in SNCP subnetwork 1 interconnection node I1. Cable cut in SNCP subnetwork 2

In figure A.16, the end node A and interconnection node I4 switch in order to maintain the communication from node B to node A.

End node B and interconnection node I2 switch in order to maintain the communication from node A to node B.

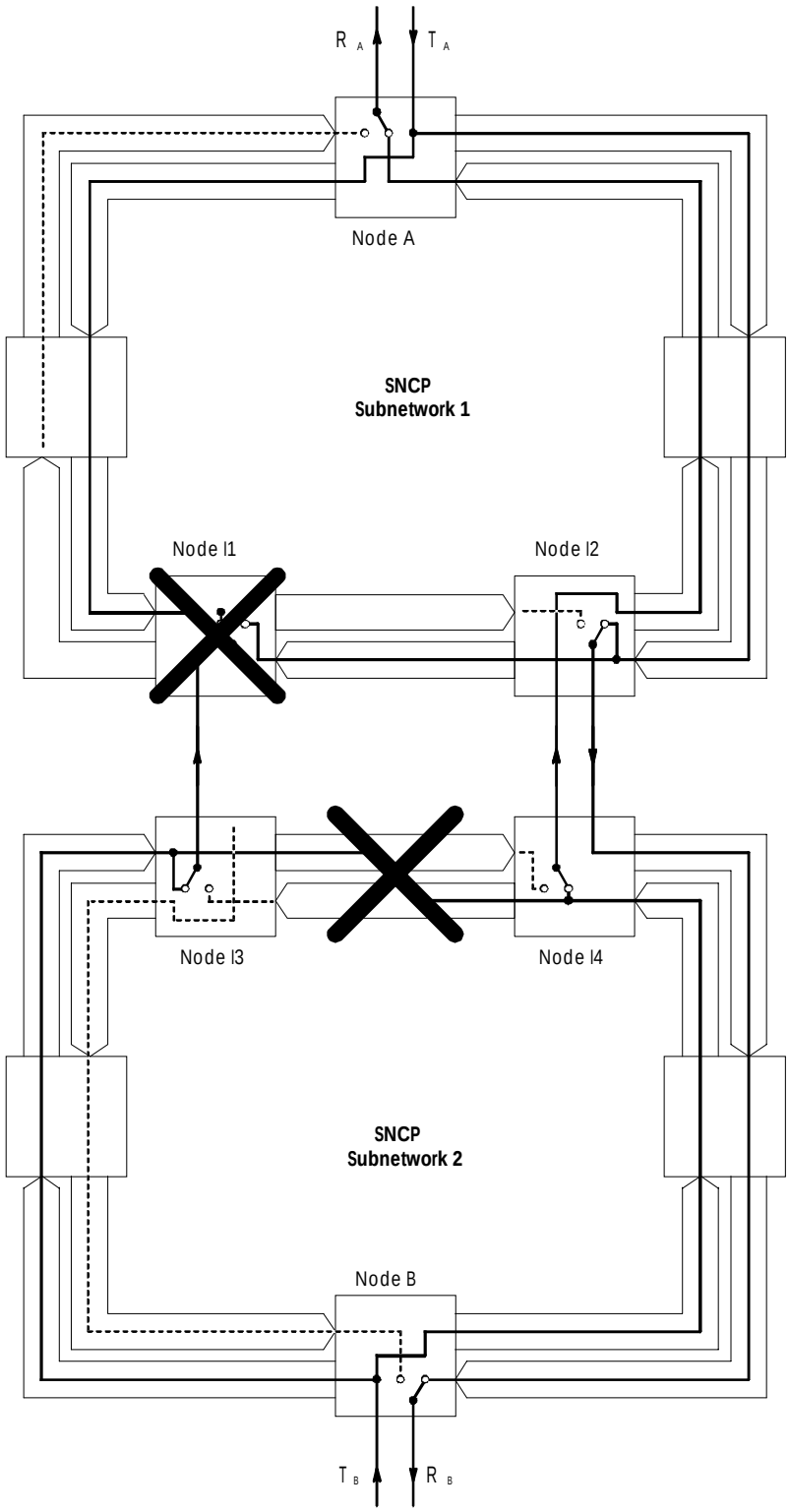

Figure A.16

A.4.5 Failure in one interconnection link.

In figure A.17, the end node A switches in order to maintain the communication from node B to node A.

End node B switches in order to maintain the communication from node A to node B.

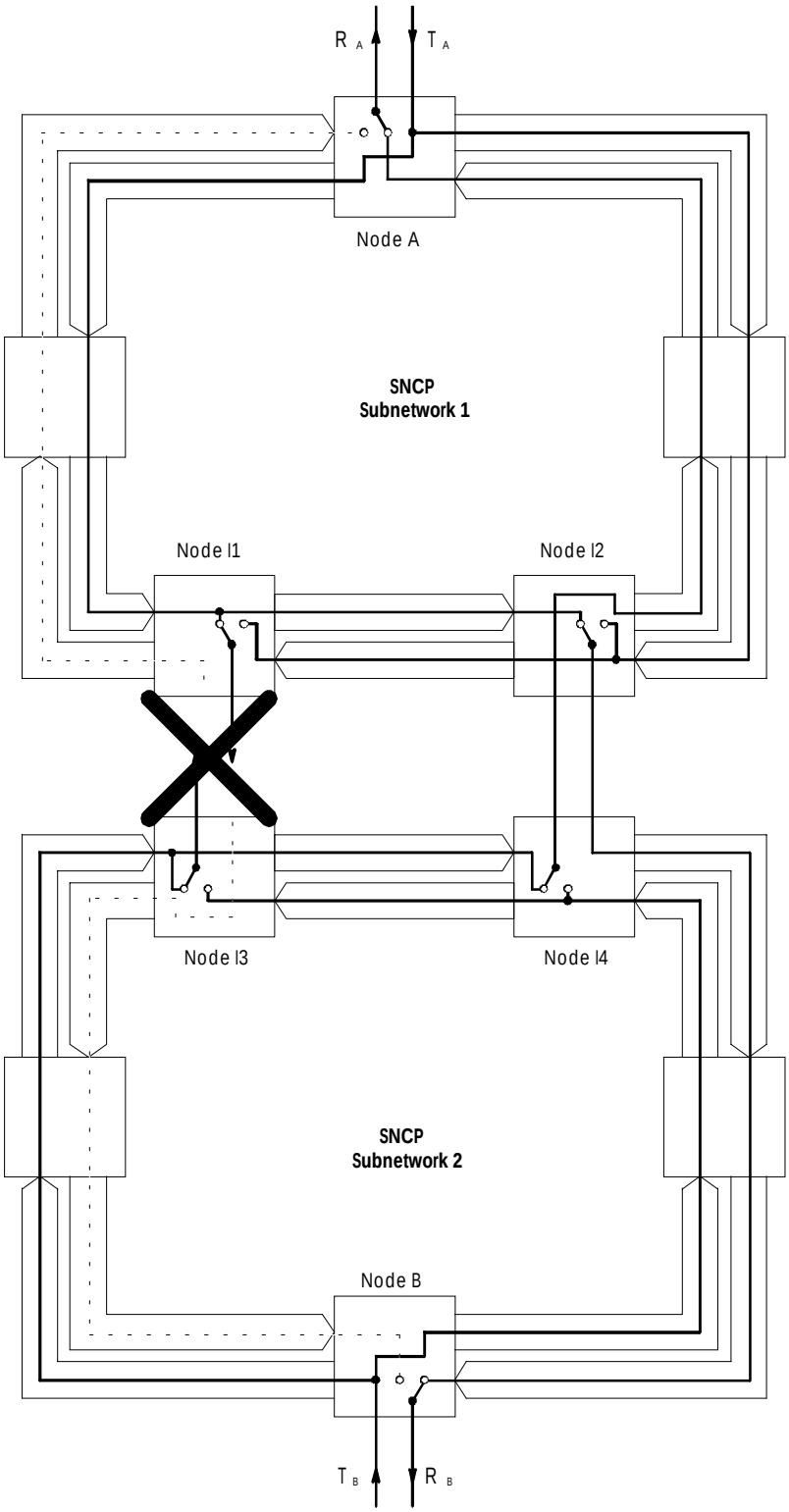

Figure A.17

Annex B (informative): Bibliography

- ETR 114: "Transmission and Multiplexing (TM); Functional architecture of Synchronous Digital Hierarchy (SDH) Transport networks".
- ETR 085: "Transmission and Multiplexing (TM); Generic functional architecture of transport network".
- ETS 300 462: "Transmission and Multiplexing (TM); Generic requirements for synchronization networks".
- ETS 300 147 (1997): "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH); Multiplexing structure".
- ETS 300 417-1-1: "Transmission and Multiplexing (TM); Generic functional requirements for Synchronous Digital Hierarchy (SDH) equipment; Part 1-1: Generic processes and performance".

History

Document history		
V1.1.1	November 1997	Publication

ISBN 2-7437-1819-6
Dépôt légal : Novembre 1997